****

[](http://www.alukah.net/)

**مراحل**

**القرصنة الإلكترونية**

**أحمد محمد عبد الرؤوف المنيفي**

**وكيل نيابة جبلة/ اليمن**

**البريد الإلكتروني**

**ahmedalmoniefy@yahoo.com**

## شكر وتقدير

أشكر زوجتي التي صبرت معي وتحملت الظروف الصعبة في فترة تجهيز هذا الكتاب.

أشكر القائمين على [**شبكة الألوكة**](http://www.alukah.net) الذين أتاحوا لي نشر أبحاثي على موقع الشبكة وإخراجها إلى النور بعد أن كانت حبيسة الأدراج، وأسأل الله تعالى أن يجزيهم الخير من فضله في الدنيا والآخرة، وأن يجعلهم رافدا من روافد العلم والخير.

أشكر الحاج علي محمد حمزة على سخاءه معي وعلى كل المساعدة التي قدمها لي أثناء فترة إعداد هذا الكتاب.

أشكر أهلي وأقاربي الذين دعموني وشجعوني على إعداد الأبحاث التي نشرتها على شبكة الألوكة وفي مقدمتهم الدكتور فيصل الخراساني الذي قدم لي الدعم والمساندة، والأخ فؤاد علي حمزة الذي عاش معي هذه الفكرة حتى تحولت إلى حقيقة واقعة، والأخ جمال حمزة على مواقفه تجاهي.

## مقدمة

يهدف هذا الكتاب الى كشف المنهجية التي يتبعها القراصنة والمجرمون المعلوماتيون في الدخول الى الحاسب الآلي، ومن ثم ارتكاب الجرائم المختلفة فيه، وتتكون هذه المنهجية من مراحل متعاقبة تمثل في مجملها السلوك الإجرامي في هذا النوع الحديث والخطير من الجرائم، وقد تناول الكتاب هذه المراحل تفصيلا وكشف أسرارها، وشرح الطرق والأدوات المستخدمة فيها، حتى أن الكتاب يجعل القارئ يسير مع المجرم خطوة بخطوة، ويطلعه على أدواته وأساليبه وفنون الاختراق المختلفة التي يتبعها عند قيامه بالاختراق.

والكتاب يجعل القارئ يفهم كيف تتم الجرائم الإلكترونية، ولكنه لا يعلمه الاحتراف، فاحتراف هذه الجرائم بعيد كل البعد عن غرض المؤلف، ولذلك فإن الكتاب يهم بالدرجة الأولى من يريد أن يفهم كيف يحدث هذا النوع الحديث من الجرائم لكي يجتهد لإيجاد حلول شرعية له، أوبدافع حب المعرفة والإطلاع.

وكنت قد تناولت مبحث موجز عن مراحل القرصنة في كتاب " السرقة الالكترونية وحكمها في الاسلام " ووعدت القارئ حينها أن أخرج كتاب أخر يتناول مراحل السرقة الالكترونية على نحو أكثر تفصيلا، ولذلك جاء هذا الكتاب المفصل وفاء بالوعد، ولكي يكون مساعدا لمن يريد البحث في مسائل القرصنة الالكترونية، ويحاول إيجاد حلول شرعية لها.

وبما أن الكتاب يتضمن الكثير من المسائل الحاسوبية التقنية الخاصة بالاختراق ومراحل السرقة الالكترونية، فقد كان من الضروري التمهيد له بجزء خاص يتناول الحاسوب وآلية عمله يساعد القارئ الغير متخصص على فهم الكتاب، وقد يلاحظ القارئ أن هذا الجزء التمهيدي طويل بعض الشيء، لكنني جمعت له فيه كل ما يحتاجه لفهم مختلف مسائل الاختراق والسرقة الالكترونية، وبحيث يمكنه الاستغناء بهذا الفصل عن الرجوع الى الكتب المتخصصة في علم الحاسوب والاتصالات، وقد كان ذلك عن تجربة شخصية، إذ أنني اضطررت من أجل فهم هذه المسائل الى البحث في عدد كبير من الكتب والمراجع الفنية المتخصصة في الحاسوب، فأحببت أن أوفر على القارئ هذا العناء. ومع ذلك فهو جزء غير إلزامي إذ يمكن للقارئ المتخصص تجاوزه والقفز الى متن الكتاب مباشرة، لكن هذا الجزء مفيد لمن ليس لديه معرفة كبيرة بهذه التقنية الحديثة، وكذلك لفهم كثير من المسائل التقنية الواردة في منهجية الإختراق.

**المنهج المتبع في اعداد الكتاب:** ان كل مباحث هذا الكتاب الفنية قد تم اعدادها بمنهج اسلامي خالص، وهو منهج علماء الأصول الذي يقوم على الربط بين بين الجزئيات والكليات، وبناء أصول كلية من جزئيات متعددة ومتفرقة، ولعل اهم ملامح تطبيق المنهج الاسلامي في هذا الكتاب يتضمن ما يلي:

1. رد الادوات والتطبيقات الخاصة بهذه الجريمة الى منهجيات عامة، كلما امكن ذلك، حيث يعمد الكتاب الى شرح المنهجية العامة المستخدمة في هذه البرامج والادوات قبل التطرق لها على انفراد.
2. أعاد الكتاب تنظيم وتأطير أنواع اختراق الحاسب الآلي وردها الى منهجية عامة للدخول، وانشأ الكتاب مبحث خاص بالدخول عبر الثغرات البرمجية، وشرح فيه تفصيلا منهجية الدخول بهذا الاسلوب، والتقنية المستخدمة فيه، وذلك من اجل رد بعض الادوات والتطبيقات التي تستخدم في الاختراق الى منهجية عامة، ترجع اليها، مثل الاداة ميتاسبلويت، وهذا المبحث غير موجود في المراجع العالمية الخاصة بالاختراق،
3. تضمن الكتاب مبحث خاص بمرحلة نسخ البيانات والمعلومات، وتم اضافة هذا المرحلة الى مراحل القرصنة الالكترونية في هذا الكتاب، وهذه المرحلة لم تتناولها المراجع العالمية والعربية كمرحلة خاصة، وقد جاءت على منوال المراحل الاخرى في الاعتماد على رد الجزئيات الى الكليات، والرد الى منهجيات عامة.

هذه هي بعض ملامح التطبيق العملي لمنهج علماء الأصول، على الجوانب الفنية والتقنية في هذا الكتاب، وقد شرحت منهج علماء الأصول في كتاب آخر صدر عبر شبكة الألوكة بعنوان " منهج الحكم على المصلحة التي لا نص فيها عند الأصوليين ".

أخيرا أحمد الله تعالى الذي وفقني لكتابة هذه الكتب، ولأن أخرج علما أحسبه نافعا للناس، فالحمدلله الذي بنعمته تتم الصالحات،

**أحمد محمد عبدالرؤوف المنيفي**

## الجزء الأول

## مقدمة عن الحاسب الالي

## المبحث الاول

## الحاسب الآلي

يعرف الحاسب الالي بانه الة وظيفتها قبول البيانات ومعالجتها لتحويلها الى معلومات[[1]](#footnote-1).

البيانات

ادخال اخراج

معالجة

معالجة (الكمبيوتر) معلومات

و البيانات التي يعالجها الحاسب الالي تعرف بانها الحقائق والمواد الخام، مثل الاعداد او الكلمات او الرموز خاصة.

وهي في صورتها الأولية كأرقام ورموز لا معنى لها، لكن اذا ما تم معالجتها وارتبطت مع بعضها بشكل منطقي مفهوم، تحولت الى معلومات مفيدة، والحاسب الالي هو الذي يقوم بعملية الربط المنطقي بين البيانات وتحويلها الى معلومات مفيدة[[2]](#footnote-2).

الحاسب الالي يقوم بمعالجة البيانات وتحويلها الى معلومات من خلال العديد من الاجراءات والوظائف، والكل وظيفة من هذه الوظائف وحدة مادية او برمجية تقوم بها. تتضمن الوظائف الرئيسية لمعالجة البيانات بواسطة الحاسب الالي ثلاث وظائف، الادخال، المعالجة، الاخراج، واما الوحدات والمعدات التي تقوم باداء هذه الوظائف فهي وحدة الادخال، ووحدة المعالجة، ووحدة الاخراج، ونتناول في الفقرات التالية الوحدات والبرامج التي تقوم بهذه الوظائف والتي يتكون منها الحاسب الالي.

**المطلب الاول**

**الوحدات المادية في الحاسب الالي**

**تمهيد:**

يتكون الحاسب الالي من اجهزة دخل، لإدخال البيانات، واجهزة معالجة، لمعالجة البيانات وتحويلها الى معلومات مفيدة، واجهزة اخراج لإخراج المعلومات الى المستفيد

الشكل التالي يوضح هذه المكونات:



توضح هذه الصورة مكونات الحاسب الالي، في مقدمة الصورة لوحة المفاتيح، وهي الجهاز الذي يقوم بادخال البيانات، فوق لوحة المفاتيح توجد شاشة العرض، وهي جهاز الاخراج الذي يتم من خلاله عرض المخرجات من بيانات ومعلومات على المستفيد، والمخرجات يتم عرضها على الشاشة مؤقتة، واذا اردنا الحصول على مخرجات دائمة، يمكن ان نقوم بارسال هذه المخرجات الى الطابعة، لاستخراج نسخة مطبوعة دائمة منها، والطابعة هي جهاز الاخراج الرئيسي الثاني بعد الشاشة، وتوجد ايضا السماعات التي تخرج الصوت من الحاسب والتي اصبح استخدامها واسعا في الوقت الحاضر.

صندوق وحدة النظام يوجد بداخله المعالج والذاكرة، وتسمى وحدة النظام بوحدة المعالجة المركزية، وهي اهم وحدة في الحاسب، لانها بمثابة العقل المفكر له، وهي التي تقوم بعملية المعالجة للبيانات، وفي الصندوق من جهة الخارج توجد فتحات لاجهزة التخزين، مثل سواقات الاقراص الضوئية، والفلاش ميموري. وبالاضافة الى وظيفة التخزين فان الاقراص الضوئية والفلاش ميموري تستخدم كأجهزة ادخال ايضا، حيث يتم في معظم الاحيان نسخ البرامج والمدخلات من الاقراص او الفلاشات الى الذاكرة.

**مكونات نظام الحاسب الآلي:**

**۱.وحدات الادخال:**

وهي الوحدات التي تستخدم في ادخال البيانات والبرامج الى جهاز الحاسب الالي، ومن امثلتها، لوحة المفاتيح، الفارة، الماسح الضوئي.

**۲.وحدات الاخراج:**

وهي التي تقوم بإظهار نتائج العمليات التي يقوم بها الحاسب الالي، ومن امثلة وحدات الاخراج ؛ شاشة الحاسب، الطابعة، السماعات[[3]](#footnote-3).

**۳.وحدة أو صندوق النظام:**

المعالج الدقيق والمكونات الاخرى الداخلية للحاسب الالي، توضع غالبا داخل صندوق مربع او مستطيل يسمى صندوق النظام، ويتضمن صندوق النظام بالاضافة الى المعالج الدقيق، لوحة الام، والاقراص الصلبة، ووحدة التغذية للحاسب الالي، ومكونات اخرى، وتتصل هذه المكونات الداخلية للحاسب باجهزه الدخل والخرج من خلال توصيل هذه الاجهزة بفتحات ومنافذ توجد في مؤخرة صندوق النظام، الوحدات الداخلية الرئيسية داخل هذا الصندوق، هي المعالج الدقيق او ما يطلق عليه وحدة المعالجة المركزية، والذاكرة.

الشكل التالي يبين صندوق وحدة النظام:



**مكونات وحدة النظام:**

**1-وحدة المعالجة المركزية cpu**

وحدة المعالجة المركزية هي العقل المفكر في الحاسب، وبمثابة الدماغ للانسان، وهي التي تتحكم وتدير جميع اجزاء ومكونات الحاسب الاخرى، كما انها تقوم باجراء المعالجات اللازمة للبيانات وتحويلها الى معلومات، وتقوم وحدة المعالجة بهذه المهام والوظائف بواسطة البرامج، لان البرامج هي التي تحدد لوحدة المعالجة المركزية خطوات واجراءات المعالجة التي تقوم بها، فالحاسب الة صماء لا يستطيع انجاز اي مهمة بدون برنامج، ومصدر الذكاء في كل حاسب الي هو البرامج وليس المعدات[[4]](#footnote-4).

يتكون المعالج من شريحة او رقاقة الكترونية، لها عدة اطراف او ارجل تتصل بواسطتها بمكونات الحاسب الاخرى، الصورة التالية تبين احد انواع المعالجات:

****

يحتوي المعالج على وحدة للحساب والمنطق، ووحدة اخرى للتحكم، وسوف نتناولها فيما يلي[[5]](#footnote-5):

أ\_وحدة الحساب والمنطق:

وهي الوحدة التي تقوم بتنفيذ جميع العمليات الحسابية، والمتطقية، التي تتطليها عملية المعالجة، وتتالف وحدة الحساب والمنطق من مجموعة من الدوائر الالكترونية، تقوم هذه الدوائر بعمليات، الجمع، والضرب، والطرح، والمقارنة، والنسخ، وتنقسم الى دوائر الكترونية حسابية، تنفذ الاعمال الحسابية، ودوائر الكترونية منطقية تنفذ الاعمال المنطقية مثل المقارنة.

ب\_وحدة التحكم:

تعتبر وحدة التحكم اساس عمل وحدة المعالجة المركزية، وهي التي تنظم العمليات التي تقوم بها وحدة الحساب والمنطق، وتنسق بين وحدات ومكونات الحاسب الاخرى لتنفيذ عمليات المعالجة.

وتقوم وحدة التحكم بذلك من خلال عدد من المكونات داخلها هي، مسجل التعليمة، عداد البرنامج، والساعة.

**الذاكرة الرئيسية: ymain memor:**

يتطلب الحاسب الالي ذاكرة لكي يقوم بمعالجة البيانات فيها، وتعد الذاكرة بمثابة مكان العمل بالنسبة للمعالج، مثلها مثل الورقة التي يجري عليها المحاسب عملياته الحسابية، والمهندس رسوماته، او الملعب الذي يجري عليه الرياضي الالعاب المختلفة، والمعالج هنا يخزن في الذاكرة البرنامج الذي يبين له خطوات العمل، والبيانات التي يجري عليها التنفيذ، ثم يقوم بتنفيذ البرنامج ومعالجة للبيانات داخلها وفقا لتعليمات البرنامج.

ولفهم طبيعة الذاكرة فانه يمكن تخيلها على شكل صفوف متراصة من صناديق البريد، والتي يكون كل صندوق فيها له عنوان خاص به عبارة عن رقم معين كما هو معروف.

وتقابل صناديق البريد هذه وحدات التخزين في الذاكرة، فشريحة الذاكرة تتكون من وحدات تخزين، كل منها لها عنوان عبارة عن رقم معين، وكل وحدة منها تشبه صندوق بريد معين، ولكن الذاكرة مع ذلك تختلف في كثير من خصائصها عن صناديق البريد:

1- في صندوق البريد يمكن لنا ان نضع رسالة فيها تعليمات او كتالوج، ثم في اليوم الثاني يمكننا ان نضع فوقها رسالة فيها بيانات عن شخص او شيء، وهكذا، وتتجمع تلك الرسائل القديمة والجديدة في الصندوق، بدون ان يؤثر اي منها على الاخرى، فلا يؤدي وضع الرسالة الثانية الى محو الاولى، وانما تظل كل رسالة كما هي، ويختلف صندوق البريد عن الذاكرة في ذلك، لانه عندما نضع بيانات في الذاكرة، فان ذلك يؤدي الى محو البيانات السابقة، وحلول البيانات الجديدة محلها.

2-ايضا فانه اذا استرجعنا الرسائل من صندوق البريد، فانه يصبح فارغا، اما في الذاكرة فان استرجاع او اخذ البيانات لا يؤثر على وجودها في الذاكرة، فالذي يحدث اننا ناخذ نسخة فقط من البيانات، بينما يظل الاصل في الذاكرة[[6]](#footnote-6).

يتم تخزين البيانات والبرامج داخل الذاكرة في وحدات التخزين، وعندما يريد المعالج ان يحصل على بيانات او تعليمات برمجية، لعملية المعالجة، فانه يصل اليها من خلال عناوين وحدات التخزين، حيث يقوم اولا بالبحث عن وحدة التخزين التي تحمل العنوان المحدد، وعندما يجد العنوان يجلب البيانات او تعليمة البرنامج من هذا العنوان[[7]](#footnote-7).

**انواع الذاكرة:**

تنقسم الذاكرة الرئيسية الى نوعين:

أ\_ذاكرة الرام RAM:

وهذه الذاكرة هي ذاكرة العمل للمعالج، والمكان الذي يتم فيه معالجة البيانات، وتنفيذ البرامج، وتتم في هذه الذاكرة عمليات الادخال للبيانات والبرامج.



ويلاحظ بالنسبة لذاكرة الرام RAM ما يلي:

۱.انها ذاكرة مؤقتة، وتفقد محتوياتها بمجرد انقطاع التيار الكهربائي، ولذلك فهي لا تستخدم للحفظ الدائم للبرامج والبيانات، واذا اردنا ان نحفظ البرامج والبيانات بصورة دائمة، فان علينا ان ننسخها الى القرص الصلب.

۲.انه يمكن القراءة منها، والكتابة عليها، اي انها ذاكرة قراءة وكتابة للمعالج، وقراءة البيانات من المعالج تتم بنسخها من الذاكرة، مع بقاء محتوياتها كما هي، واما الكتابة على الذاكرة، فانها تؤدي الى محو البيانات السابقة، ويحل محلها البيانات والكتابة الجديدة. وكذلك فانه عندما يتم الانتهاء من تنفيذ برنامج معين، ويتم نقل برنامج جديد لتنفيذه في الذاكرة، يحل البرنامج الجديد محل الاول.

ب\_ذاكرة القراءة فقط ROM:

ومن اهم خصائص هذه الذاكرة انه يمكن القراءة منها فقط، ولا يمكن الكتابة عليها، او تعديل محتوياتها، وهذه الذاكرة يكون التخزين فيها دائم، ولا تفقد محتوياتها بانقطاع التيار الكهربائي، ولذلك فهي تستخدم في تخزين البرامج التي يحتاجها الحاسب بصورة دائمة، مثل برامج الاقلاع، والبيوس، والمترجمات[[8]](#footnote-8).

## المطلب الثاني: البرمجيات

**تمهيد:**

يشبه البعض العلاقة بين المعدات المادية للحاسوب، وبين البرامج، بالعلاقة بين الروح والجسد، ولا شك ان هذا التشبيه يخالف الواقع، اذ الروح من خلق الله، وهي سر من الاسرار التي يعجز البشر عن فهمها، ومع ذلك فان هذا المثال يقرب الى الذهن فكرة الصلة بين المعدات والبرامج، وذلك ان المكونات والمعدات المادية بدون برامج، تكون الات صماء خاملة وميتة، لا يستطيع الانسان الاستفادة منها، ولكن البرامج هي التي تسخر لنا امكانات الحاسب، وقدراته الهائلة، وبدون برامج لا نستطيع التواصل مع الحاسب، ولا نستطيع الاستفادة من قدراته، فالبرامج هي وسيلة التواصل الوحيدة للانسان مع الحاسب، وهي الطريقة لتوظيف قدراته في بناء المجتمع.

تتكون برمجيات الحاسب من عدة انواع من الانظمة والبرامج، ومن هذه الانواع ما يسمى ببرامج التطبيق، وهي برامج يتم اعدادها للاستفادة من الحاسب في مجالات مختلفة، مثل المجالات التجارية، والادارية، والمالية،.. الخ، وتتميز هذه البرامج بانها تتفاعل مع المستخدم مباشرة، ويمكنه شرائها، او تحميلها، ومن ثم الاستفادة منها في المجال الذي يريده.

ولكن في طبقة اخرى تحت برامج التطبيق يوجد نوع اخر من البرامج يعمل بطريقة سرية لا يشاهدها المستخدم، ولكنه مهم جدا لانه يشكل حلقة الوصل بين المستخدم وبرامجه التطبيقية من ناحية، وبين الحاسب الالي بمكوناته ومعداته المادية من ناحية اخرى، ويطلق عليها برامج النظام، ومن اهم هذه البرامج برنامج نظام التشغيل.

ان برامج التطبيق لا تستطيع التواصل مباشرة مع الجانب المادي للحاسب، ولذلك تعمل برامج النظام، وبرامج نظام التشغيل كحلقة وصل بين برامج التطبيق، وبين المعدات او المكونات المادية للحاسب[[9]](#footnote-9)

**برنامج التطبيق**

**نظام التشغيل**

**الكيان المادي ( المعدات** )

برا

**1\_ برامج النظام[[10]](#footnote-10)**

برامج النظام مصممة لادارة العتاد والمعدات المادية للحاسب، وهي التي تتولى تشغيل الحاسب، وادارة اجزاء الحاسب ومكوناته المادية، مثل المعالج، ووحدات الادخال والاخراج.

وتنقسم برامج النظام الى نوعين، برنامج البيوس، ونظام التشغيل:

**۱.برنامج البيوس BIOS:**

يخزن برنامج البيوس في ذاكرة الروم ROM، وهي كما اشرنا ذاكرة قراءة فقط، فلا يمكن الكتابة والتعديل عليها، كما انها ذاكرة دائمة وثابتة، لا تفقد محتوياتها عند انقطاع الطاقة والكهرباء عنها.

تكتب برامج البيوس في الذاكرة اثناء تصنيعها، وتبقى فيها مدة حياة الحاسب، وهي التي تساعد الحاسب على الاقلاع، وبمجرد وصل الحاسب بالتيار الكهربائي، يقوم المعالج تلقائيا بقراءة برنامج البيوس من ذاكرة الروم، وتنفيذ تعليمات الاقلاع المكتوبة فيه، وهي تعليمات ثابتة لا تتغير، لانها تتعلق بتشغيل الحاسب، وادارة اتصالاته مع الملحقات، كما انها تظهر في شاشة الحاسب عند بداية التشغيل.

وحدة المعالجة المركزية مصممة على ان تقوم بقراءة تعليمات البيوس وتنفيذها، واول هذه التعليمات تتعلق بفحص اجزاء النظام، مثل الذاكرة، والمنافذ، واجهزة الادخال والاخراج، ثم بعد اتمام عملية الفحص، يقوم برنامج البيوس بتوجيه المعالج الى مكان العثور على نظام التشغيل، وتحميله من القرص الصلب الى الذاكرة الرئيسية، ويتم في هذه المرحلة تحميل جزء من نظام التشغيل وهو النواة، ثم يتولى نظام التشغيل بعد وصوله الى الذاكرة جلب بقية الاجزاء، وادارة مختلف مكونات الحاسب المادية.

**۲.نظام التشغيل OIS:**

نظام التشغيل هو عبارة عن حزمة من البرامج تتولى ادارة المكونات المادية للحاسب الالي مثل المعالج، والذاكرة، ووحدات التخزين، ووحدات الادخال والاخراج في الشبكة.

ان مكونات الحاسب المادية تتضمن تعقيدات فنية، ولا يستطيع المستخدم بسبب هذه التعقيدات، التعامل مع المكونات المادية مباشرة، ولذلك فان نظام التشغيل يساعد المستخدم في التواصل مع المكونات المادية للحاسب، وبالإضافة الى ذلك، يعتبر نظام التشغيل وسيط بين البرامج التطبيقية، وبين المكونات المادية، وبوجه عام يفسر نظام التشغيل الاوامر الصادرة من المستخدم، او من البرامج، الى لغة تفهمها المكونات المادية، وتنفذها، وبدون نظام التشغيل، لا يمكن للحاسب فهم تعليمات البرامج، ولا اوامر المستخدم، وبالتالي لا يمكنه تنفيذها.

يقوم نظام التشغيل بتوفير الاشراف، والادارة، والدعم، للعمليات التي تتم في الحاسب الالي، وتنسيق الاتصال بين مكوناته، ومن ذلك انه يتولى ادارة الذاكرة وتوفير وحجز المساحة الكافية للبرامج داخل الذاكرة، ويتولى ادارة المعالج، وجدولة تنفيذ العمليات والمهام، وتوزيعها على المعالجات في حالة وجود اكثر من معالج، والتنسيق بين المعالج، وبين اجهزة الادخال والاخراج، في حالة تطلبت العمليات اي دخل او خرج، وغير ذلك من المهام المتعلقة بالاشراف والتنظيم على العمليات وتنفيذ البرامج، وبحيث يمكن للمبرمج، او المستخدم، ان يركز جهوده في عمله فقط، بدون حاجة الى التعامل مع التعقيدات الفنية للحاسب.

**أ.تطور نظام التشغيل:**

عند بداية اختراع الحاسبات لم تكن هناك انظمة تشغيل، ولا برامج نظام، بل كان المبرمج هو الذي يتولى ادارة الحاسب ومكوناته، وكانت البرامج في ذلك الوقت تكتب بلغة الالة، اي بالشفرة الثنائية التي تفهمها المكونات المادية للحاسب.

وكان التعامل مع الحاسب في هذه الفترة غاية في الصعوبة، فقد كان يوجد بجوار الحاسب مهندس مختص، يقوم بادخال البرامج بعد تحويلها الى الشفرة الثنائية التي تفهمها الالة، ويمكننا ان نتصور وجود طابور امام هذا المختص او المشغل للحاسب، وكل واحد منهم يسلمه برنامجه لكي يقوم بتحويله الى لغة الالة ومن ثم ادخاله اليها.

بعد هذا تطور التعامل مع الحاسب من ناحيتين:

اولا: تم جمع العمليات والخطوات التفصيلية مثال عمليات الدخل والخرج، في مكتبة برمجية داخل الحاسب، بحيث يمكن للمبرمج كتابة امر واحد فقط ويقوم الحاسب بتنفيذ كل تلك العمليات.

ثانيا: تم عمل برامج مترجمات تفسر اوامر وتعليمات البرنامج، وتحولها الى الشفرة الثنائية، وبذلك استغنى المبرمجون عن المختص الذي يحول برامجهم الى الشفرة الثنائية، واصبح المبرمج يقوم بادخال اوامره مباشرة الى الحاسب، فتقوم المترجمات الموجودة في الحاسب بترجمة هذه الاوامر الى لغة الالة.

ثم حدثت قفزة هائلة في التعامل مع الحاسب باختراع الانظمة الرسومية، والتي تتكون من ايقونات ومربعات حوار، وتحولت شاشة الحاسب الى شاشة ملونة، مليئة بالمربعات والاشكال التي تسمى الايقونات او النوافذ WINDOWS، وبهذا التطور الكبير اصبح التعامل مع الحاسب ممكنا لكل الناس، ولم يعد مقصورا على المتخصصين.

**ب. مكونات نظام التشغيل:**

يتضمن نظام التشغيل ويندوز WINDOWS الكثير من البرامج التي تظهر في سطح المكتب، او على قائمة ابدأ، مثل متصفحات الانترنت، ومشغلات الوسائط، وبرامج الوورد، والرسام، والمفكرة، والساعة،...الخ، وتسمى هذه البرامج بالواجهة الرسومية لنظام التشغيل. وبالاضافة الى ذلك يتضمن نظام التشغيل برامج اخرى تعمل بشكل خفي عننا، وتسمى بنواة نظام التشغيل، وهي البرامج التي تتولى ادارة المكونات المادية للحاسب، مثل برنامج مدير المعالج، وبرنامج مدير الذاكرة، وبرنامج مدير الدخل والخرج...الخ. ونحن لا نرى هذه البرامج ولا نتعامل معها مباشرة، ووسيلة الاتصال بيننا وبينها هي الواجهة الرسومية، وعندما نتعامل مع برامج الواجهة الرسومية، ونطلب منها مهمة معينة من خلال الضغط على اي ايقونة، تتصل الواجهة الرسومية بنواة نظام التشغيل، والتي يقوم بتفسير الاوامر للمكونات المادية، وادارة عملية المعالجة الالكترونية التي تتم في العتاد المادي.

**واجهة المستخدم الرسومية**

**الغلاف ( سطر الاوامر )**

**النواة**

**المكونات المادية**

مكونات نظام التشغيل

وعلى هذا فان نظام التشغيل يحتوي على الاجزاء التالية:

**۱.النواة:** وتتولى ادارة مكونات الحاسب الالي المادية، وتنقسم الى خمسة برامج، وهي مدير المعالج، ومدير الذاكرة، ومدير اجهزة الدخل والخرج، ومدير الملفات، ومدير الشبكة.

**2. واجهات نظام التشغيل:** توفر واجهات نظام التشغيل للمستخدم الاتصال مع النواة، وهناك نوعين من واجهات نظام التشغيل، الرسومية، والنصية:

\_واجه المستخدم الرسومية GUT:

وهي تشتمل على الايقونات، والنوافذ، والقوائم التي نشاهدها في سطح المكتب. ويمكن للمستخدم ان يطلب امر معين، او ينفذ برنامج معين، عن طريق النقر بجهاز الماوس مرتين على الايقونة او النافذة، ومن امثلة واجهات التشغيل الرسومية، واجهة سطح المكتب.

\_واجهة الغلاف أومترجم الاوامر: وهذه الواجهة تسمح للمستخدم بالاتصال المباشر مع النواة، من خلال كتابة اوامر نصية، وسنتناول هذه الواجهة بالتفصيل في المبحث الخامس من الفصل الاول.

**2-برامج التطبيقات**

برنامج التطبيق هو الذي يتم اعداده من اجل مهمة معينة، او وظيفة محددة، من وظائف الاعمال، مثال ذلك، برنامج معالجة الكلمات الوورد، وبرنامج الجداول الالكترونية، وبرامج وقواعد البيانات، وبرامج المحاسبة، وبرامج البنوك، وبرامج التطبيقات التجارية، والانترنت، ونحو ذلك، وهذه البرامج هي التي يتفاعل معها المستخدم لتأدية نشاطاته. ويوجد منها انواع كثيرة لا يمكن حصرها، لانها تتطور باستحداث انشطة ومهام جديدة للشركات والمنظمات، الخاصة والحكومية، في مجالات الاعمال التجارية، والادارية، ونحوها

## المطلب الثالث: لغة الكمبيوتر

الحاسب الالي لا يتعامل مع الحروف، او الكلمات، او الارقام، او العلامات، التي نستخدمها نحن في لغتنا العادية، فللحاسب الالي لغة اخرى، تختلف عن لغتنا الانسانية التي نتعامل بها، وعلى الرغم من اننا نقوم بادخال البيانات الى الحاسب الالي على شكل حروف، الا ان الحاسب الالي يقوم بتحويلها الى لغة خاصة به، يتعامل بها ويفهمها، وتسمى لغة الالة، او اللغة الثنائية.

واللغة الثنائية هي عبارة عن نظام عددي ثنائي، يتكون من عددين فقط هما، الصفر والواحد (0،1). والسر في اختيار النظام الثنائي كلغة للحاسب الالي، هو ان الحاسب الالي جهاز الكتروني يعمل بالكهرباء، والكهرباء هي عبارة عن نبضة ولا نبضة، فالنبضة تمثل برقم واحد 1، ولا نبضة تمثل برقم 0، وبذلك يعد النظام الثنائي هو انسب النظم العددية للحاسب الالي.

ان الحاسب الالي يتكون من دوائر الكترونية، تضم الاف الترانزستورات، ويعمل الترانزستور على حالتين، موصلا للكهرباء (1)، او لا موصل (0). وهذه الدوائر الالكترونية التي يتكون منها الحاسب الالي هي عقل الحاسب الالي، وهي التي تقوم بجميع اعمال المعالجة، والحساب، وغيرها من وظائف الحاسب. وعندما نقوم بادخال البيانات الى الحاسب لمعالجتها، فان الحاسب الالي يقوم بتحويلها الى الشفرة الثنائية 0،1، ويقوم بمعالجتها وفق هذه الشفرة، ثم يرسلها الى جهاز الاخراج في اللغة الطبيعية التي نتعامل بها[[11]](#footnote-11).

فلا بد اذا لكي يتمكن الحاسب الالي من معالجة الحروف، والارقام، والكلمات، ان يكون لها نظير في لغة الحاسب او اللغة الثنائية، وبحيث يكون لكل حرف، ولكل رقم، تمثيل عددي يقابله في اللغة الثنائية.

**النظام الثنائي[[12]](#footnote-12):**

يقوم النظام الثنائي على رمزين فقط هما 0،1، وفي مقابل ذلك يتكون النظام العشري من عشرة رموز 0-9، ويتكون النظام الثماني من تسعة رموز 0-8.

وسنقارن فيما يلي بين هذه الانواع من الانظمة العددية، لنكون صورة اوضح للنظام الثنائي.

- في النظام العشري توجد عشرة رموز ؛.،۱، ۲،۳،٤، ٥، ٦، ٧، ٨،٩

ونعبر عن الاشياء بهذه الارقام، فاذا كان لدينا شيئين، نعبر عنهما بالرقم ۲، وهكذا الى العدد ٩، فاذا كان لدينا مجموعة من الاشياء اكثر من تسعة ٩، فاننا نستخدم للتعبير عنها تركيبة من عددين، او رمزين من هذه الرموز العشرة، فمثلا نستخدم تركيبة من العددين ۰، ۱ للتعبير عن الكمية عشرة (۱۰)، ونستخدم العددين ۱، ۲ للتعبير عن الكمية اثناعشر (۱۲)، وهكذا هلم جرا.

فاذا بعد العدد تسعة ٩، تكون الاعداد مركبة من الرموز العشرة مثل، ۱۰، ۱۱، ۱۲، ۱۳، وهكذا.

-بالنسبة للنظام الثماني فهو يحتوى على ثمانية رموز ۰\_٧، وهذا يعني ان النظام الثماني يتكون من ثمانية اعداد فقط ۰، ۱، ۲، ۳، ٤، ٥، ٦، ٧، وبالتالي لا يوجد فيه العددين ٨، ٩.

فاذا كان لدينا اشياء اكثر من سبعة، فاننا نستخدم تركيبة من عددين من هذه الرموز الثمانية، فاذا اردنا ان نعبر عن ثمانية اشياء نستخدم تركيبة من عددين هما ۱، ۰ (۱۰)، واذا اردنا ان نعبر عن تسعة اشياء، فاننا نستخدم تركيبة من العددين ۱، ۱ (۱۱).

وهذا معناه ان تسلسل الاعداد في النظام الثماني هو كالتالي: ۰، ۱، ۲، ۳، ٤، ٥، ٦، ٧، ۱۰، ۱۱، ۱۲، ۱۳، ۱٤، ۱٥، ۱٦، ۱٧، ۲۰، ۲۱، وهكذا

ويلاحظ على هذا التعداد ما يلي:

۱. ان الارقام ٨، ٩ مختفية من اعداد النظام الثنائي، فالنظام الثماني ينتهي العد فيه عند الرقم ٧، ثم يبدأ بتركيبات من الاعداد للتعبير عن الكميات التي تزيد عن العدد ٧، اما النظام العشري فان العد فيه ينتهي الى الرقم ٩، ثم يبدأ بتركيبات من الاعداد للتعبير عن الكميات التي تزيد عن ٩.

۲. ان الرقم ۱۰ في النظام الثماني، يقابل العدد ٨ في النظام العشري، والرقم ۳۰ يقابل الرقم ۲٤ في النظام العشري، وهكذا، فنستطيع ان نقول ان العدد ۳۰ هو التمثيل العددي الثماني للعدد ۲٤ في النظام العشري، والعدد ۱۰ هو التمثيل الثماني للعدد ٨ في النظام العشري، وهكذا.

-واذا انتقلنا الى النظام الثنائي، سنجد ان هذا النظام يتكون من رمزين فقط، هما الصفر والواحد.

وكما انه ينتهي العد في النظام العشري، عند العدد ٩، واذا احتجنا للتعبير عن كمية اكثر من ٩ نستخدم تركيبة من عددين

وينتهي العد في النظام الثماني عند العدد ٧، وعندما نريد الزيادة نستخدم تركيبة من عددين من نفس النظام.

فان النظام الثنائي، وبنفس الطريقة، ينتهي العد فيه عند الرقم ۱، واذا اردنا التعبير عن كمية اكبر من الواحد، نستخدم تركيبة من عددين من نفس النظام

فللتعبير عن شيء واحد في النظام الثنائي نستخدم العدد ۱، اما اذا اردنا التعبير عن شيئين، فاننا نستخدم تركيبة من عددين من الاعداد التي يتكون منها النظام الثنائي، وهي الصفر والواحد، وتكون التركيبة التي نستخدمها للتعبير عن شيئين هي ۱۰.

وهكذا بالنسبة للكميات الاخرى، على سبيل المثال، ۱ في النظام الثنائي يقابل ۱ في النظام العشري، و۱۰ في النظام الثنائي تقابل ۲ في النظام العشري، و۱۱ في النظام الثنائي تعبر عن ۳ في النظام العشري

۰، ۱، ۱۰، ۱۱

۰، ۱، ۲، ۳

ولكن نلاحظ اننا استنفدنا تركيبات اعداد النظام الثنائي عندما وصلنا الى الرقم ۱۱، والذي يعبر عن ثلاثة اشياء، او الرقم ۳ في النظام العشري، فكيف نعبر عن الكميات التي تزيد عن ثلاثة. اشياء؟

للتعبير عن الكميات التي تزيد عن ثلاثة، فاننا ننتقل الى مرتبة المئات ثم الالاف..الخ،كما نفعل بالضبط عندما نصل الى الرقم ٩٩، حيث نعبر عن الكمية التي تزيد عن ٩٩، بالانتقال الى مرتبة المئات، ثم الالاف، وهكذا.

وعلى هذا يكون العدد مائه ۱۰۰ هو الذي يعبر عن الكمية ٤ في النظام العشري، وهكذا

وبناء على ذلك فان العدد ۱۰ في النظام الثنائي هو التمثيل العددي الثنائي للرقم ۲ في النظام العشري، والعدد ۱۰۰ في النظام الثنائي هو التمثيل العددي الثنائي للرقم ٤ في النظام العشري، وهكذا.

يتميز النظام الثنائي بانه لا يوجد فيه سوى الرقمين ۰، ۱، ولذلك فان العد التصاعدي في النظام الثنائي، يتم بان نعد تصاعديا ابتداء من الصفر، مع اغفال جميع الاعداد غير الصفر والواحد ۰، ۱، ولذلك فاننا في حالة العد تصاعديا في النظام الثنائي، سنجد انفسنا نعد بالطريقة التالية:

۰، ۱، ۱۰، ۱۱، ۱۰۰، ۱۰۱، ۱۱۰، ۱۱۱......الخ 12.

ويمكن اجمال التقابل بين الانظمة الثلاثة على النحو التالي:

العشري: ۰، ۱، ۲، ۳، ٤، ٥، ٦، ٧، ٨،٩ ؛ ۱۰، ۱۱، ۱۲

الثماني: ۰، ۱، ۲، ۳، ٤، ٥، ٦، ٧، ۱۰، ۱۱، ۱۲، ۱۳، ۱٤

الثنائي: ۰، ۱، ۱۰، ۱۱، ۱۰۰، ۱۰۱، ۱۱۰، ۱۱۱، ۱۰۰۰، ۱۰۰۱، ۱۰۱۰، ۱۰۱۱، ۱۱۰۰، ۱۱۰۱، ۱۱۱۰، ۱۱۱۱

**تمثيل الحروف بالأعداد الثنائية:**

راينا ان الارقام العشرية تمثل في الانظمة الثنائية، بتركيبات تسلسلية من الصفر والواحد،

بالنسبة للحروف فيتم تمثيلها في النظام الثنائي بشكل مشابه لتمثيل الارقام ثنائيا، فيمثل الحرف A نفس شفرة الرقم ۱ وهي ۱، ويمثل الحرف B بالشفرة الثنائية للعدد ۲ وهي ۱۰، والحرف C بالشفرة الخاصة بالعدد ۳ وهي ۱۱، وهكذا.

ويميز الحاسب الالي بين الرقم والحرف من خلال ما يسمى بدليل المنطقة، وهي رقمين يوضعان قبل الشفرة، ويحدد من خلالهما، ان هذه الشفرة هي حرف او رقم. على سبيل المثال، الشفرة الثنائية 11، تكون رقما هو رقم 3 اذا سبقها الرقمين 00 ( 0011)، اما اذا سبقها 11 فتكون حرف C ( 1111 )، واذا سبقها الرقمين 10 تكون حرف L ( 1011 ) وهكذا، وهناك عدة انظمة، واكواد ثنائية مشهورة لتمثيل الاعداد، والحروف، ومن هذه الانظمة، نظام الكود الثنائي العشري BCD، والذي تمثل فيه الارقام والحروف على الشكل التالي[[13]](#footnote-13)13:

جدول دليل المنطقة للرموز

دليل المنطقة الرمز

0 0 9 \_ 0

1 1 I \_ A

0 1 R \_ J

1 0 Z \_ S

التمثيل العددي الثنائي للرموز دليل المنطقة

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1001 | 1000 | 0111 | 0110 | 0101 | 0100 | 0011 | 0010 | 0001 |  |
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 0 |
| I | H | G | F | E | D | C | B | A | 1 1 |
| R | Q | P | O | N | M | L | K | J | 1 0 |
| Z | Y | X | W | V | U | T | S |  | 0 1 |

**التمثيل الكهربائي للبيانات[[14]](#footnote-14):**

تناولنا في الفقرات السابقة التمثيل الثنائي للحروف والارقام، وبينا ان لكل رقم نظير من النظام الثنائي، وان هذا النظير الثنائي هو لغة الحاسب الالي.

والسبب الذي يجعل الحاسب الالي لا يفهم اللغة الثنائية، ولا يستطيع التعامل مع لغة البشر، هو ان الحاسب الالي جهاز او الة تعمل على الكهرباء، ومكون من دوائر الكترونية كهربائية، يسري فيها التيار الكهربائي، وكل مكونات الحاسب الالي من دوائر الكترونية، ومواصلات، واسلاك، تعمل على التيار الكهربائي، واذا اردنا ان نمثل الحروف كهربائيا داخل الحاسب، ونحولها كما هي الى اشارات كهربائية، فلن نستطيع ذلك، لان التيار الكهربائي عبارة عن سيل من الالكترونات، يمثل كل الكترون منه نبضة كهربائية، ولا يمكن ان يمثل اي شيء داخله الا على شكل نبضة ولا نبضة، قطع التيار ووصله، وانسب الانظمة العددية لتمثيل نبضات التيار الكهربائي، هو النظام العددي الثنائي، لان النبضة تمثل بالرقم ۱، ولا نبضة او قطع التيار يمثل بالرقم ۰

في بداية وجود الاتصالات الكهربائية، بحث العلماء عن شفرة وسيطة بين التيار الكهربائي، وبين الحروف، لكي يتمكنوا من وضع اشارات كهربائية تمثل الحروف الابجدية، وفي عام ۱٨۳٨ م ابتكر موريس شفرة وسيطة تناسب طبيعة الكهرباء، وهي عبارة عن مجموعة من الخطوط، والنقط، والفراغات، ووفقا لهذه الطريقة، فانه يجب تحويل الحروف الى هذه الخطوط والنقاط، والفراغات، وبحيث يعبر عن كل حرف، بخط معين او نقطة، او فراغ، ثم تمثل هذه الاشكال كهربائيا، في صورة نبضة، ولا نبضة، الخط يمثل بنبضة كبيرة، والنقطة بنبضة صغيرة، والفراغ بلا نبضة. وعلى هذا فانه عند ارسال رسالة، يقوم المرسل بتحويل كل حرف الى الشفرة الخاصة بموريس، ثم تحول شفرة الرسالة الى نبضات كهربائية، وعندما يتلقى الطرف الثاني الرسالة، فانه يقوم بتحويل النبضات الكهربائية الى خطوط، ونقاط، وفراغات حسب شفرة موريس، ثم يحول الشفرة المكونة من خطوط ونقاط، الى حروف ابجدية، هي الرسالة التي ارسلت اليه، وكانت شفرة موريس تتضمن كل حرف، وما يمثله من خطوط او نقاط او فراغات، فعلى سبيل المثال كان حرف E يمثل في شفرة موريس بنقطة واحدة، ولإرسال هذا الحرف، كان يتم تحويله الى نقطة، ثم ارساله على شكل نبضة قصيرة.

ومع ذلك فان هذا النوع من التمثيل قد واجه صعوبات كبيرة، تمثلت هذه والصعوبات في تغير الارسال، فقد كانت النبضة القصيرة تتغير اثناء ارسالها، ومرورها عبر الاسلاك، وتصل عند المستخدم نبضة طويلة مستمرة، مما يؤدي الى تداخل الحروف في الارسال، وصعوبة تفسيرها وقراءتها، الشكل التالي يبين ذلك[[15]](#footnote-15)15:

النبضة المرسلة

حالة النبضة عند استقبالها

سلسلة من النبضات المرسلة

حالة النبضات عند استقبالها

للتغلب على هذه الصعوبات، تم ابتكار التمثيل الثنائي للكهرباء، وفيه ياخذ التيار الكهربي حالتين ؛ تيار، ولا تيار، نبضة، ولا نبضة، وكان هذا هو سبب الاخذ بالنظام الثنائي، اذ ان هذا النظام يناسب حالتا، التيار، ولا تيار، فيمكن ان نعطي لحالة مرور التيار الرقم الثنائي ۱، ونعطي لحالة انقطاع التيار الرقم ۰، وبذلك ظهر ان النظام الثنائي هو الشفرة الاكثر ملائمة لطبيعة الكهرباء، وقد ادى الارسال بطريقة تيار، ولا تيار، او نبضة، ولا نبضة، الى ضبط الارسال، وعدم حدوث التداخلات والمشاكل السابقة.

وبهذه الطريقة، بدلا من ان نحول الحروف الى خطوط، ونقاط، فاننا سنحول كل حرف الى نظيره الثنائي، ثم نحول الشفرة الثنائية الى وحدات كهربائية من نبضات، ولا نبضات.

ومن هنا كانت فائدة النظام العددي الثنائي، وهو انه شفرة وسيطة بين الحروف الطبيعية، وبين الكهرباء، اذ انه من غير الممكن ان نحول الحروف والكلمات العادية التي نتخاطب بها الى كهرباء بطريقة مباشرة، وانما لا بد اولا ان نحولها الى شفرة ثنائية من الواحد ۱، والصفر ۰، ثم نحول الشفرة الثنائية الى نبضات كهربائية تمثلها داخل الحاسب الالي.

على سبيل المثال، عندما نضغط على حرف معين من لوحة مفاتيح الحاسب الالي، يوجد جهاز عبارة عن دائرة الكترونية داخل لوحة المفاتيح، يقوم بتحويل هذه الضغطة الى الشفرة الثنائية، الى نبضات كهربائية، ويدخل الحرف الى الحاسب الالي، على شكل نبضات كهربائية.

**تمثيل الاصوات[[16]](#footnote-16):**

الاصوات هي تغيرات في حجم الهواء، عند اذن السامع، بقياسات محددة، والذي يقوم باحداث هذه التغيرات في ضغط الهواء هي الحبال الصوتية التي في الحنجرة، عن طريق احداث انقباضات مختلفة، وعندما يمر الهواء المندفع من الرئتين عبر هذه الحبال، سيتسبب بمروره بينها باصدار الاصوات.

واذا كان الصوت هو تغير في ضغط الهواء، فانه يسهل جدا الاتيان به عن طريق قياس حجم هذا التغير، وسعة ضغط الهواء، ثم اعادة اصداره بهذه القياسات، وهذا ما تقوم به اجهزة الهاتف، واجهزة الحاسب الالي، حيث تقوم هذه الاجهزة بقياس تغيرات ضغط الهواء وتواترات الصوت للشخص المرسل، تسجل هذه القياسات على هيئة ارقام، تحول هذه الارقام الى الشفرة الثنائية، ثم تحول الى نبضات كهربائية، اذا كان الجهاز المرسل هو حاسب الي، او الى اشارات كهربائية، اذا كان الجهاز المرسل للصوت هو جهاز هاتف.

يتلقى الجهاز المستقبل هذه الاشارات، او النبضات، ثم يقوم بتحويلها الى شفرات ثنائية، ثم الى ارقام وقياسات لتغيرات ضغط الهواء، وتواترات الصوت، ثم يعيد تشكيل هذا الصوت وفقا للقياسات والتواترات المرسلة، وينطق به.

تتضمن القياسات التي ترسل من جهاز ارسال الاصوات، مقاييس معينة، ومحددة لكل حرف، من حيث النوع، والطبقة الصوتية، وغير ذلك، وترسل هذه المقاييس على هيئة ارقام ثنائية، ثم يعاد تكوين نفس الصوت، ونفس الحروف، في الجهاز المستقبل، وفقا لتلك المقاييس.

**تمثيل الصورة:**

تكون الصورة في الحاسب الالي على هيئة مجموعة من النقاط، فالنقطة (بيسكل. pixel) هي اصغر عنصر في الصورة، واصغر جزء من اجزائها، وفي حالة الصورة الملونة، تمثل كل نقطة في الصورة بعدة ارقام، رقم اللون، ورقم شدة الاضاءة، ورقم يمثل تدرج اللون، ورقم يمثل صفاء الصورة..الخ، تحول هذه الارقام الى شفرة ثنائية، ثم يتم تحويلها الى نبضات كهربائية ترسل عبر الاسلاك، ويعاد تشكيلها لدى الجهاز المستقبل وفقا لتلك الارقام والقياسات، كما يحدث في الاصوات[[17]](#footnote-17).

## المبحث الثاني: الاتصالات

يتمتع الحاسب الالي بقدرات هائلة في معالجة البيانات، ويمكنه ان يقوم بملايين العمليات، والاجراءات، في ثوان معدودة، ومع ذلك فان هناك مجال اخر لا يقل اهمية من مجالات استخدام الحاسب الالي، وهو مجال الاتصال عن بعد بشبكة الانترنت، وشبكات المعلومات الاخرى، ذلك انه بعد اكتشاف خدمة الويب، اصبحت شبكة الانترنت مكانا لكثير من الانشطة، التجارية، والاقتصادية، والاجتماعية...الخ، وكثير من المؤسسات والشركات، التجارية، والاقتصادية، انتقلت الى شبكة الانترنت، واتخذت لها مواقع على شبكة الويب، وبدأت في تقديم خدماتها، عبر موقعها في الانترنت، مثل البيع جملة، وتجزئة، وعرض الاخبار، وانتاج المعلومات، والصحف، والقنوات التلفزيونية، وقامت كثير من هذه المؤسسات، وخاصة البنوك، بتحويل عملياتها الى عمليات الكترونية، لاتاحة الفرصة للعملاء الانجاز اعمالهم عن بعد[[18]](#footnote-18).

لكن في موازاة هذا الانتشار الكبير للمؤسسات المالية، والتجارية، في الانترنت، ظهرت مخاطر كثيرة على العمل في مواقع الانترنت، وكان من اهم هذه المخاطر، الجرائم التي تتم باستخدام تقنية الانترنت، وبصفة خاصة جرائم السرقة التي تتم عبر الوسائل الالكترونية، كما سنرى فيما بعد.

## المطلب الاول: نظام الاتصال عن بعد

يقوم نظام الاتصال عن بعد على ربط الحاسب الالي بشبكة الانترنت، او الشبكات الاخرى الخاصة والعامة، بوسائل سلكية ولاسلكية، فيتم وصل الحاسبات الالية الخاصة بالأفراد بالأنترنت بواسطة كابلات من انواع مختلفة، وبما ان المعلومات الخارجة من الحواسيب او الداخلة اليها، هي نبضات ثنائية، فقد كان الاصل ان يتم مد كابلات رقمية بين الحواسيب المختلفة، لنقل النبضات الثنائية عبرها، لان تيار النبضات لا يستطيع المرور عبر اسلاك التلفون، فأسلاك التلفون معدة فقط لنقل الصوت على شكل موجات كهربائية،وليس نبضات، فلا تقبل خطوط الهاتف تيار النبضات، او ما يسمى بالتيار الرقمي، ولا يمكن لهذا التيار ان يمر من خلال هذه الخطوط.

ومع ذلك، فانه نظرا للتكلفة الباهظة لمد الكابلات الرقمية في المدن والشوارع، وتحت المباني، ولصعوبة ذلك، بل ومخالفته للقانون في بعض الدول، فقد استخدمت خطوط الهاتف لوصل الحاسبات الالية بشبكة الانترنت، وبالشبكات الخاصة والعامة الاخرى، وتم حل مشكلة اختلاف نوع التيار الكهربائي، بوضع محولات تتولى تحويل التيار الرقمي الى تيار تناظري، تقبله خطوط الهاتف، عند ارساله من الحاسب الالي، كما تتولى اعادته الى الشكل الرقمي عند وصوله الى الجهاز المستقبل، ويسمى هذا النوع من الاجهزة بالمودم modem [[19]](#footnote-19).

**وسائط الاتصال**

تنقسم وسائط الاتصال المستخدمة للاتصال بالأنترنت وشبكات المعلومات الى وسائل سلكية، ووسائل لاسلكية، حيث يتم وصل الحاسب الالي بالأنترنت اما عن طريق كابلات، او عن طريق وسائل اتصال لاسلكي.

**1\_الوسائل السلكية:**

الوسائل السلكية هي الوسائل الاهم في وصل الحاسب الالي بالأنترنت، وهىناك العديد من الانواع التي تتوفر منها بعضها قديم، وبعضها متطور وحديث، تعتبر الالياف الضوئية من احدث الكابلات او الوسائل السلكية، وأما اقدم هذه الوسائل فهي كابلات الاسلاك المجدولة. وفيما يلي نتناول انواع الكابلات القديمة والحديثة.

**1-كابل الاسلاك المجدولة او الازواج المجدولة (utp):**

هذا الكابل هو اقدم الوسائل التي استخدمت في الاتصال السلكي، وهو يتكون من سلكين نحاسين مجدولين أو ملفوفين حول بعضهما البعض، يستخدم الاول للأرسال والثاني للاستقبال، وهذا النوع من الاسلاك هو الذي يستخدم في خطوط الهاتف داخل المدن والمناطق السكنية، وكان في البداية عبارة عن زوج من الاسلاك فقط، الا انه فيما بعد تم تجميع كل حزمة منة في كابل واحد لاستيعاب عدد كبير من خطوط الهاتف، فأصبحت توجد منة كابلات تحتوي على زوجين من الاسلاك، واخرى على اربعة ازواج من الاسلاك المجدولة[[20]](#footnote-20).

****



واسلاك الهاتف المجدولة هي التي تستخدم غالبا لوصل الحاسب الالي بالأنترنت والشبكات الاخرى، ومع ذلك فان استخدامه في ارسال البيانات من الحاسوب الالي، او التنزيل من الانترنت، يثير ثلاث مشاكل، هي مشكلة الضوضاء والتشويش، ومشكلة ونوع التيار الكهربي الذي يقبله السلك، ومشكلة بطء الارسال ومحدودية البيانات، وسوف نتناولها باختصار على النحو التالي:

أ-الضوضاء والتشويش:

عندما ينتقل التيار الكهربي الممثل للبيانات والمعلومات عبر السلك فانه يثير مجال كهرومغناطيسي، هذا المجال يؤدي الى الاضرار بالأسلاك المجاورة، ويمكنه ان يؤدي الى تعطيل الاسلاك او التأثير في المعلومات التي تمر عبر تلك الاسلاك.

ولحل هذه المشكلة المتعلقة بالضوضاء والتشويش فانة تستخدم ثلاث تقنيات وتصاميم للأسلاك:

\_ التدريع اي تغليف الزوج المجدول من الاسلاك بطبقة معدنية رقيقة. \_المحورية وهي تغليف السلك النحاس بعدة طبقات من المعدن والبلاستيك.

\_وتقنية الازواج الملتفة وهي لف السلكين وجدلهما على بعضهما مما يؤدي الى توليد مجال كهربائي عازل للتشويش[[21]](#footnote-21).

ب-مشكلة نوع التيار الكهربائي في الاسلاك المجدولة:

اعدت اسلاك الهاتف المجدولة في الاساس لكي تنقل صوت الانسان، ولذلك فأنها صممت بحيث تستقبل الاشارات التناظرية الممثلة لهذا الصوت وليس الاشارات الرقمية، والفرق بين الاشارات التناظرية والاشارات الرقمية هو ان الاشارات التناظرية عبارة عن موجات كهربائية أي تيار مستمر من النبضات الكهربائية، واما الاشارات الرقمية فهي تيار كهربائي متقطع يتمثل في نبضة ولا نبضة، الواحد والصفر.

وبما ان الحاسب الالي جهاز رقمي يرسل المعلومات ويستقبلها في شكل اشارات، فانه يحتاج الى تحويل هذه الاشارات الى الشكل التناظري لكي تستطيع المرور في اسلاك الهاتف، ثم اعادتها الى الشكل الرقمي عند وصولها الى الحاسب الالي الهدف، وحتى عند وصولها الى الكابلات الرقمية الخاصة بالمسافات البعيدة.

ولحل هذه المشكلة يتم تركيب جهاز يسمى جهاز المودم يتولى تحويل الاشارات الرقمية الخارجة من الكمبيوتر الى اشارات تناظرية لكي تمر في اسلاك الهاتف، ثم يقوم بإعادتها الى الشكل الرقمي عند وصولها الى الكمبيوتر المستقبل[[22]](#footnote-22).

ج- محدودية السعة للأسلاك المجدولة:

من سلبيات الاسلاك المجدولة انها محدودة السعة وبطيئة، ولذلك فأنها غير كافية لا استخدامها في خدمة البيانات للحاسب الالي وبصفة خاصة خدمة الاتصال بالأنترنت، ولما كان اغلب المشتركين يستخدمون خطوط الهاتف للاتصال بالأنترنت فان شركات الاتصال، ورغبة منها في تقديم منتجات منافسة، عملت على معالجة مشكلة بطء التحميل من خلال ادخال خدمات رقمية لخطوط الهاتف المجدولة، وتقوم هذه الخدمات على اساس تقسيم خطوط الهاتف الى قناة صاعدة للارسال، وقناة نازلة للاستقبال، وجعل نسبة80%ألى 90% من سعة الخطوط الهاتفية للأرسال النازل على اعتبار ان معظم المستخدمون يحملون او يتلقون بيانات اكثر من البيانات التي يرسلون[[23]](#footnote-23).

**2-الكابل المحوري:coaxial cable**

يتكون الكابل المحوري من سلك نحاسي صلب محاط بمادة عازلة من المطاط، وفوق المادة العازلة يوجد غلاف معدني موصل من النحاس على شكل ظفيرة غالبا، ثم يغطى الضفيرة المعدنية غلاف بلاستيكي من التلفون والمطاط أو البلاستيك.



يقوم السلك النحاسي الذي هو قلب الكابل بنقل اشارات البيانات والمعلومات، واما الضفيرة المعدنية فتقوم بمنع التشويش والضوضاء عن السلك النحاسي الناقل للإشارات فهي بمثابة حاجز يقي السلك النحاس ويمنع عنه الاشارات والتشويشات الخارجية،ولذلك تسمى بالحجاب الواقي، كما انها في نفس الوقت تخفض من اشعارات الاشارات الداخلية.

وللكابل المحوري انواع مختلفة بعضها يستخدم للنقل الرقمي مثل الكابل ذو المقاومة 50، وبعضها يستخدم للنقل التشابهي وتلفزيون الكابل.

وقد سبق ان اشرنا الى ان الكوابل المجدولة تستخدم في انظمة الهاتف داخل المدن وفي المناطق المحلية، اما في المسافات البعيدة بين المدن والبلدان، فان خطوط الهاتف لا تستخدم الكوابل المجدولة وانما تستخدم الكابل المحوري، ويستخدم الكابل المحوري ايضا في شبكات الحاسب الالي المدنية man وفي تلفزيون الكابل، وفي استقبال الستالايت، ومن امثلة الكابل المحوري الكابل البحري الرابط بين فرنسا وانجلترا، والكابل القاري الرابط بين عدة دول[[24]](#footnote-24).

ويعتبر الكابل المحوري اكثر سرعة من الكوابل المجدولة، كما انه يوفر حماية افضل بكثير ضد التشويشات بالمقارنة بالأسلاك المجدولة.

**3\_كابل الالياف الضوئية[[25]](#footnote-25)**:

يشكل اكتشاف تقنية الالياف الضوئية ثورة حقيقية في عالم الاتصالات، وذلك لان الالياف الضوئية تتضمن قدرات هائلة في نقل البيانات تصل الى مليارات البتات في الثانية الواحدة، ويمكننا ان نتخيل حجم التطور الذي وصلت الية الاتصالات بدخول الالياف الضوئية اذا عرفنا ان الالياف الضوئية تنقل عشرات الملايين من المكالمات الهاتفية في الثانية الواحدة، بالمقارنة مع 400أربعة الف مكالمة فقط ينقلها اخر جيل من الكابلات المحورية قبل دخول الالياف الضوئية الى العمل.

على ان مميزات كابل الالياف الضوئية لاتقف فقط عند حد القدرات الهائلة في نقل البيانات، بل انها تمتاز ايضا بان لديها مناعة كامله ضد التشويش، وضد السرقة، وذلك لانها لا تلتقط الاشارات الكهربائية ولاتبثها[[26]](#footnote-26).

يتكون نظام الاتصال بالألياف الضوئية من ثلاث مكونات:

1. المنبع: وهو الذي يبث النبضات الضوئية وهو عبارة عن ثنائي تقنيه الليزر يقوم بتحويل الاشارة الكهربائية الى اشارة ضوئية مساوية لها.
2. وسط النقل وهو كابل الالياف.
3. الكاشف: وهو جهاز يتولى تحويل الاشارات الضوئية الواردة علية الى نبضات كهربائية، تمهيدا لا دخاله جهاز الحاسوب، وفي انظمة الاتصالات الهاتفية يوجد جهاز يتولى اعادة الاشارات الكهربائية بعد خروج من الكاشف الى شكلها الاصلي، فاذا كانت ممثله للصوت يقوم بإعادتها الى شكل موجات صوتيه.

واما كابل الالياف الضوئية نفسه فيتكون من عدة اجزاء وهي كالاتي:-

النواة الطبقة الكاسية



1. النواة: وتتضمن الالياف الزجاجية التي تنقل الضوء، آو النبضات الضوئية،وهي تنقلها على الشكل الثنائي وتمثل هذه النبضات، المعلومات والبيانات المرسلة داخل الكابل، ولما كانت الألياف البصرية موصله في اتجاه واحد فقط، فانه تستخدم مجموعات او حزم من الالياف الضوئية للأرسال واخرى للاستقبال.

تسمى الالياف البصرية الناقلة للضوء بالنواة او بالقلب او الصميم، وتسمى كذلك الالياف البصرية.

2 – الطبقة الكاسية:-

وهي عبارة عن طبقه من الزجاج تكسو الالياف الضوئية، ومهمتها منع تسرب الضوء الى خارج الالياف او النواة، وهي تقوم بأعاده توجيه اشارات الضوء الى داخل النواه اي الى الالياف الناقلة الضوء.

3 – الغلاف البلاستيكي للكابل:-

ومهمته حمايه الالياف من العوامل الخارجية مثل الحرارة والتمدد والثني والكسر.

* **مقارنه بين الكابلات بالنسبة لمخاطر الامن:**

تتفاوت انواع الكابلات من حيث معايير الامن والحماية التي تقدمها السرقة. فأقل هذه الكابلات من حيث مستوى معايير الامن هو الكابل المزدوج المجدول، لان هذا الكابل تتسرب منه الاشارات خارج السلك وبالتالي يمكن التقاطها من الغير.

ويأتي بعد هذا النوع من حيث درجه الامن الانواع التي يتم تغليفها بطبقه عازله من المعدن، لان هذه الطبقة تعمل على امتصاص الاشارات الداخلية أي المنبعثة من السلك وتنخفض منها، ويشمل ذلك بوجه خاص الكابل المحوري، ومع ذلك فأنه يمكن سرقه البيانات من الكوابل المحورية عبر تركيب أجهزه لتفريغ الاشارات منه (تسمى بعض هذه الأجهزة محللات البروتكولات).

واعلى درجات الحماية من السرقة توجد في كابلات الالياف الضوئية، وذلك لان التيار الكهربائي لا يمر فيها، وبالتالي فهي منيعة ضد السرقة، كما ان كابلات الالياف الضوئية لا تشع الا عند الوصلات، واذا تم تركيب جهاز لتفريغ الضوء منها الى الخارج فأن ذلك يسبب في وقف الكابل عن العمل واخفاق النظام[[27]](#footnote-27).

## المبحث الثالث: الشبكات

* **تمهيد:**

تناولنا فيما تقدم من هذا الفصل الطرق الرئيسية لوصل الحاسب الالي بشبكات المعلومات، وشبكات الانترنت، وهي الكابلات بأنواعها المختلفة. وبينا ان اغلب اتصال المستخدم او المستفيد بهذه الشبكات يتم عن طريق خطوط الهاتف.

ولكن؛ ماهي شبكات المعلومات؟ وما هو الانترنت؟ ومما تتكون الانواع المختلفة من الشبكات؟

سنتناول فيما يلي مفهوم الشبكة، ثم انواعها المختلفة ومكوناتها، ثم نتطرق لشبكه الانترنت.

**مفهوم الشبكة:-**

تتكون الشبكة من ربط حاسبين او اكثر، بواسطه كابلات سلكيه في الاغلب، بقصد المشاركة في الموارد والمعلومات.

وقد تكون الشبكة داخل غرفه واحدة مثل عدة اجهزة داخل مكتب واحد، وتتصل بطابعة واحده يستخدمها الجميع.

في حاله الشركات الصغيرة قد تكون الشبكة داخل مبنى واحد، وتضم عدة اجهزة في عدة مكاتب مرتبطة مع بعضها البعض.

والشركات والمؤسسات الكبيرة تكون مكاتبها موزعه عادة على عدة مدن داخل الدولة الواحدة، ويتم ربط الاجهزة الحاسبة في هذه المكاتب بشبكه واحدة من خلال خطوط الطلب الهاتفي، وقد تكون الشبكة شامله لعده فروع في عده دول، ويكون الربط بين هذه الاجهزة، في هذه الفروع، بواسطه انواع مختلفة من قنوات الاتصال، مثل خطوط الهاتف والكابلات المحورية والوسائط اللاسلكية.

على كل حال فأن الشبكة اذا كانت موزعه في مبنى واحد، او كانت موزعه على عده مباني في نطاق مدينه واحدة، فانها تسمى شبكه محليه.

اما اذا كانت الشبكة موزعه على عدة مدن داخل الاقليم الواحد، او كانت تربط بين مكاتب وفروع في عده دول، فأنها تسمى بالشبكة الواسعة[[28]](#footnote-28).

**المعلومات والشبكات:-**

نشأت الشبكات في البداية من أجل التشارك في الموارد، مثل الطابعات، والاقراص الصلبة، ونحو ذلك، وكان هذا النوع من المشاركة يتم غالبا داخل الغرفة الواحدة، او المبنى الواحد في عدد من المكاتب.

ولكن مع توسع الشبكات وانتشارها في المؤسسات المختلفة، مثل الجامعات ومراكز البحوث وغيرها من المؤسسات العلمية او الاجتماعية، تحولت الشبكات الى مشروعات تعاونية تستهدف نشر وبث المعلومات للمستفيدين في أي مكان، والمساعدة على التعليم والتعلم، وقد ادى هذا التحول الى ان تكون البيانات والمعلومات هي العنصر الرئيسي في الشبكات، والموارد الأولية والضرورية فيها، وخصصت المؤسسات لقواعد البيانات حاسبات خاصه قويه سميت مخدمات، وصار بإمكان المستفيدين من كل مكان التواصل مع هذه الحاسبات القوية للحصول على المعلومات والبيانات المخزنة فيها[[29]](#footnote-29).

وبالتالي اصبح الهدف الاساسي من الشبكات هو المشاركة في المعلومات، وسميت الشبكات بشبكه المعلومات

**انواع الشبكات:-**

**1-الشبكة المحلية ( Local Area Networks( LAN:-**

وهي التي تربط بين اجهزه الحواسيب داخل غرفه، او مكتب معين، او طابق او بناية، او مجموعه من المباني المجاورة القريبة من بعضها البعض، ولا تتجاوز مساحة الشبكة المحلية عدة كيلو مترات، ويستخدم هذا النوع من الشبكات في المباني الخاصة بالشركات والمؤسسات المختلفة مثل المؤسسات التجارية والصناعية والاكاديمية والصحية..الخ[[30]](#footnote-30)

ويعتبر الكيبل المتحد المحور coaxial cabl هو الاكثر استخداما في الشبكات المحلية، نظرا لما يوفره من سرعه واسعة في نقل البيانات والمعلومات، وبالإضافة الى الكيبل المتحد المحور تستخدم الشبكات المحلية الكيبل الثنائي المجدول Twisted pair canbl، كذلك الالياف الضوئية او الزجاجية optical fiber.

**2-الشبكة المدنية او الاقليمية MAN:-**

وهذه الشبكة تربط بين مجموعة من مباني المنظمة، في نطاق مدينه او اقليم، فهي اكبر من الشبكة المحلية من حيث المساحة الجغرافية التي تشملها، وقد تربط الشبكة المدنية بين مجموعة من الشبكات المحلية داخل مدينة واحدة، تستخدم الشبكات المدنية كابل الالياف الضوئية كوسيط اساسي لنقل البيانات.

**3-شبكات المناطق الواسعة wide Area Netwerk(WAN):-**

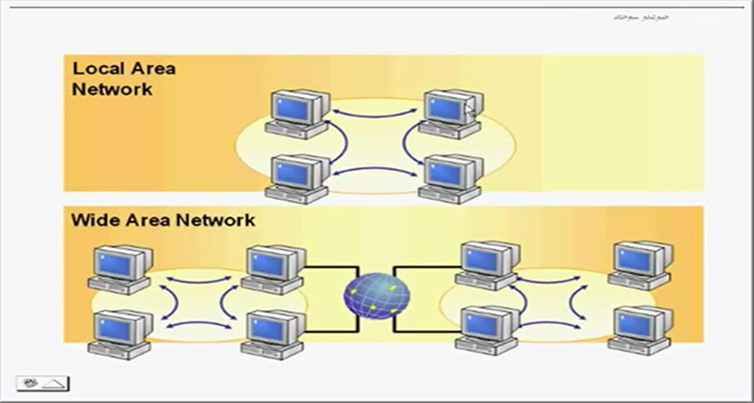
تمتد شبكة المناطق الواسعة فوق منطقة جغرافية كبيرة، على امتداد الدولة الواحدة، او عدة دول في قارة واحدة.

وتربط شبكة المناطق الواسعة بين شبكات محلية واقليمية مختلفة، لتكون شبكة واحدة على امتداد كامل لدولة، او عدة دول.

و تستخدم الشبكة الواسعة تقنية خطوط الهاتف، وتقنية المايكرويف والاقمار الصناعية لنقل البيانات، كما تستخدم اجهزة تسمى الموجهات للربط بين مختلف اجزائها.

يعتبر بعض الكتاب ان شبكة الانترنت هي نوع من انواع شبكات المناطق الواسعة[[31]](#footnote-31).

الشكل التالي يبين الشبكات المحلية والواسعة:



**4\_شبكة المؤسسات:-**

هي عبارة عن شبكة داخلية خاصة بشركة او مؤسسة ما، وقد تتكون شبكة المؤسسة من شبكة محلية في مبنى، او عدة مباني تتبع شركة واحدة في منطقة واحدة، وقد تتكون من شبكه واسعة WAN تربط شبكه مبنى الشركة او المؤسسة، بالشبكات الخاصة، أو بفروع الشركة المنشرة في مدن او دول اخرى، اي انها قد تتكون من عدة شبكات محلية ومدنية واسعة ومترابطة معا.

ما يميز شبكة المؤسسات هو انها تستخدم تكنولوجيا وخدمات الانترنت، وبالتالي تسهل تبادل المعلومات بين فريق الموظفين داخل المؤسسة، ولذلك يسمى هذا النوع من الشبكات بشبكات الانترانت بسب استخدامها هذه التكنولوجيا.

ونظرا لان شبكة المؤسسة او الانترانت تستخدم تكنولوجيا الانترنت، فانه يمكن وصلها بالانترنت لتحقيق عدة من الفوائد للشركة، واذا اتصلت عدد من شبكات الانترنت الخاصة بمؤسسات وشركات مختلفة مع بعضها البعض بواسطة الانترنت، فأنها تكون شبكة اكبر من الانترانت وتسمى شبكة الإكسترانت، وشبكة الاكسترانت هي شبكة تضم عدة شبكات انترانت متصلة مع بعضها البعض عبر الانترنت[[32]](#footnote-32).

**مكونات الشبكة**

ان اي شبكة تتكون من اجهزة وبرمجيات، وتشمل الاجهزة الحاسبات الالية، وادوات الوصل، والكابلات، واما البرمجيات فتشمل نظم التشغيل، والبرامج، والبروتكولات.

**أولا: المكونات المادية للشبكة hardware:-**

وهي عبارة عن اجهزة الحاسب الالي والتي يخصص واحد منها كخادم او ملقم server، يقدم خدمات مركزية لبقية الشبكة، وكذلك اجهزة ووحدات الربط بين الكابلات، ونظام الكابلات نفسه.

**1\_الخادم او الملقم server:**

لما كانت الشبكات عبارة من مشروعات تعاونية تستهدف المشاركة في البيانات والمعلومات، وفي الموارد، فأنه يتم تخصيص حاسب الي قوي وبموصفات عالية، توضع فيه قواعد البيانات والمعلومات التي يراد المشاركة فيها، واتاحة الوصول اليها، لجميع المستفيدين، ويسمى هذا الحاسوب بالخادم او الملقم server.

يتمتع الحاسوب الخادم / او الملقم serverبقدرات عالية من حيث المعالج والذاكرة ومساحة الاقراص الصلبة، وتوضع فيه برمجيات تسهل وتنظم للمستفيدين، الوصول الى قواعد البيانات والمعلومات الموجودة فيه، وتقوم المؤسسة او الشركة بوضع كل ما تريده من بيانات ومعلومات تهم الموظفين التابعين لها، او الزبائن والعملاء، داخل هذا الخادم، وعندما يرغب احد الموظفين التابعين للمنظمة في الحصول على بيانات او معلومات معينة، فأنه يتصل عبر جهاز حاسوبه بقواعد البيانات في الخادم server، ويحصل على المعلومات المطلوبة منة.

تسمى هذه الطريقة في العمل داخل الشبكات بطريقة العميلclient- الخادمserver، وهي اساس العمل في الشركات الكبيرة، وبمقتضاها يخصص حاسوب بموصفات عالية كخادم للحواسيب الاخرى المرتبطة بالشبكة، ولا يقتصر عمل الحاسوب الخادم server على الاحتفاظ بقواعد البيانات والمعلومات فقط، بل يتم ربط جميع موارد الشبكة ووصلها به، مثل الطابعات، والاتصالات، والملفات، وسواقات الاقراص الصلبة، ويكون لكل حاسوب مرتبط بالشبكة ان يحصل على اي من هذه الموارد، من خلال طلبها من الحاسوب الخادمserver، الذي يتولى ايصاله بقواعد البيانات او ربطة بالطابعة، او توفير الاتصال الخارجي له، او توفير خدمة تحميل الملفات...وهكذا.

والغالب ان يخصص حاسوب واحد قوي يتولى تقديم كافة الخدمات للشبكة، ولكن قد تخصص عدة حواسيب قوية للعمل كخادمات لا نواع مختلفة من الموارد، فيخصص خادم الطباعة، وخادم لقواعد البيانات، وخادم للاتصالات، وخادم للملفات، وخادم للبريد الالكتروني وهكذا.

ترتبط هذه الطريقة في عمل الشبكة بنظام التشغيل للشبكةopreating system، لان النظام التشغيل هو الذي يوفر برمجيات طريقة الخادم العميل، ويتيح الحاسوب العمل كخادم server [[33]](#footnote-33).

**2\_حاسبات المستفيدين والمرتبطة بالشبكة:-**

وهي الحاسبات الالية التي تكون الشبكة، ومن خلالها يمكن للمستفيدين التواصل مع جهاز الخادم server، والوصول الى البيانات والمعلومات الموجودة فيه، واستخدام الموارد الاخرى المتصلة بالخادم.

3\_**بطاقة الشبكة** **Network Interface cards NIcs:-**

لا يتم الاتصال بالحاسبات الالية في الشبكة بمجرد تمديد الكابلات بينها، او بينها وبين الخادم، بل لابد من وجود جهاز الكتروني اخر يسمى بطاقة الشبكة، يقوم بإنشاء هذا الاتصال بين الحاسبات المختلفة في الشبكة، ويتم تركيب بطاقة الشبكة الالكترونية في كل كمبيوتر، وتتولى هذه البطاقة انشاء الاتصالات بين الحاسب الالي وبين بقية الحاسبات الاخرى في الشبكة، سواء كانت حاسبات المستفيدين او الخادمات، ويتم الاتصال من خلال وصل كابل الشبكة الى هذه البطاقة الالكترونية، وتتولى هذه البطاقة ادارة عملية أرسال البيانات واستقبالها، فتقوم البطاقة في جهاز المرسل بأرسال البيانات عبر الكابلات في الشبكة، وتقوم بطاقة الحاسب المستقبل باستلام البيانات الواردة الى الكمبيوتر عبر الكابل.

****

بطاقة الشبكة عبارة عن لوحة دائرية الكترونية تحتوي على الكثير من الدوائر الالكترونية التي تقوم بوظائف اتصال الشبكة، كما تحتوي بطاقة الشبكة على برامج تشغيلية تتولى القيام بعض بروتوكولات الارسال. ومن اهم وظائف البطاقة الشبكة القيام بعملية تجزئة البيانات الى حزم، واضافة الترويسات الخاصة بعنوان المرسل وعنوان المستقبل اليها، كما سنرى فيما بعد، وتقوم بطاقة او كرت الشبكة بهذه الوظائف من خلال الدوائر الالكترونية والبرامج الموجودة فيها، والتي تم اعدادها وصناعتها حسب مواصفات البروتكولات[[34]](#footnote-34).

الصورة التالية لبطاقة شبكة:



وفي الشبكات اللاسلكية التي تستخدم فيها موجات موجات الراديو والاشعة تحت الحمراء، فان بطاقة الشبكة تستخدم هوائيات لاستقبال لاتصال بدلا عن الكابلات[[35]](#footnote-35).

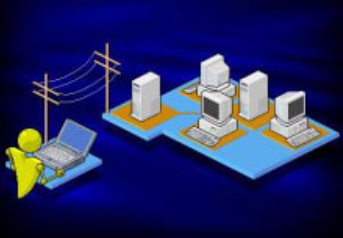
**4-وسائط الارسال:-** رأينا فيما تقدم انه عندما نريد الاتصال بالأنترنت وشبكات المعلومات، فان الاتصال يتم عبر خطوط الطلب الهاتفي، ويعتبر الاتصال عبر خطوط الهاتف هو الاساس الذي يستخدم لعمل اتصال بالشبكة الواسعة التي تغطي عدة مدن، او عدة دول داخل القارة الواحدة.

وتستخدم شبكة المعلومات المختلفة ايضا الكابلات المحورية، وكابلات الالياف الضوئية لعمل قنوات اتصال بين الاجهزة الداخلة في الشبكة.

وفي الحقيقة فانه عندما يتصل الحاسوب الخاص بنا بالأنترنت، فانه يصبح جزء من شبكة، هي شبكة مزود خدمة الانترنت في المنطقة الواقع فيها.

وعادة يتم الاتصال بين العميل ومزود خدمة الانترنت عبر خطوط الطلب الهاتفي، اما الاتصال بين مزود الخدمة والشبكات الاخرى فيتم عن طريق كابلات الالياف الضوئية او الكابلات المحورية.

وقد تستخدم الشبكات وسائط الاتصال اللاسلكي وهي الموجات الرادوية، او الاشعة تحت الحمراء، ويكثر استخدام هذا النوع من الوسائط في الشبكات الواسعة وشبكات الانترنت[[36]](#footnote-36)، الشكل التاي يبين احدى هذه الشبكات:



**5-أجهزة الوصل Connectivity Devices:-**تستخدم ادوات الموصل للربط بين شبكتين مختلفتين معا، او للربط بين الكابلات التي تمتد عبر مسافات بعيدة، وتؤدي ادوات الوصل مهام متعددة، فبعضها مثل الموجهات Routers والقناطرBridges تقوم بتنظيم مرور البيانات عبر الشبكات المختلفة، وتوجيه كل حزمة من البيانات الى العنوان او الحاسب المرسلة اليه من بين الشبكات المختلفة، والى الشبكة التي يوجد بها هذا الحاسب، اما المعيدات او المكررات Repeaters فتستخدم عادة في الشبكات التي تمتد لمسافات بعيدة، حيث ان اشارات البيانات المارة عبر مسافات بعيدة قد تضعف او تتجزأ، فيقوم المكرر باعادة الاشارة كما هي وتقويتها، لتواصل رحلتها الى العنوان ( الحاسب والشبكة ) الموجهة اليه.

**ثانيا: المكونات البرمجية**

1. **نظام تشغيل الشبكات (NOS):-**

النموذج السائد لنظام التشغيل هو نموذج زبون او عميل \_ مخدم، والذي يتم فيه تخصيص كمبيوتر واحد يسمى SERVAS لأداء وظائف الشبكة والخدمات المركزية فيها، مثل خدمة الملفات، وخدمة قواعد البيانات، وخدمة الاتصالات، وخدمة البريد الالكتروني، في حين ان الكمبيوترات الاخرى المنضمة الى الشبكة، تستفيد من المخدم، وتسمى زبون او عميل.

ويتكون نظام تشغيل نظام الشبكات من مجموعة من البرامج بعضها يوضع في جهاز المستفيدين SHELL وبعضها يوضع في جهاز الخادم Servas

يتولى نظام التشغيل لشبكة NOS القيام بالمهام والوظائف التي تقدمها الشبكة، مثل خدمة الملفات، وخدمة قواعد البيانات...الخ. كما يكون مسؤولا عن التعرف على الاجهزة المشتركة في الشبكة معها.

1. **برامج العميل:-**

تعمل هذه البرامج على مساعدة المستفيد، والذي يسمى بالعميل، في الوصول الى الخادم Server، والمشاركة في الموارد والبيانات المخزنة فيه، كما تجعل هذه البرامج الموارد البعيدة الموجودة في الخادم Server، وكانها موارد محلية، وتشمل هذه البرامج:

\_ برنامج مغير الوجهة: وهو يقوم بتغيير وجهة الطلبات الصادرة من جهاز العميل لتذهب الى جهاز الخادم Server، وبدون هذا البرنامج ستذهب الطلبات الصادرة من العميل الى المعدات الدخلية للحاسب وليس الى الخادم.

\_ برامج طبقة النقل: وهي التي تقدم بتحميل هذه الطلبات الى بطاقة الشبكة الموجودة في جهاز المستفيد، والتي تقوم بتهيئتها وإرسالها الى جهاز الخادم عبر الكابلات [[37]](#footnote-37).

وفي حالة اذا ما كانت الشبكة تتضمن مخدم ويب الانترنت، أو الانترانت، فانه لابد من توافر برامج معينة داخل جهاز المستخدم او العميل، منها برنامج المستعرض الذي يستعرض صفحات او مواقع الويب، ومن انواعه الشهيرة برنامج Mezilla،وبرنامج- internet Explor، والمستعرض هو برنامج عميل يتصل بخوادم الويب في شبكة الانترنت، ويرسل اليها الطلبات، ويتلقى الردود، ومن برامج العميل ايضا برامج الوصول الى قواعد البيانات، وبرمجيات البريد الالكتروني، وبرامج نقل وتحميل الملفات، وكل واحد من هذه البرامج هي برامج عميل، وقد تأتي برامج العميل كجزء من نظام التشغيل، وقد توزع وتباع كمنتج مستقل[[38]](#footnote-38).

1. **برامج الخادم او الملقم Server [[39]](#footnote-39):-**

في اغلب الاحيان ينظر الى المخدمات او الملقمات على انها اجهزة كمبيوتر كبيرة، لكن المخدم في الحقيقة هو برنامج تطبيقي، يمكن الاجهزة المشتركة في الشبكة من المشاركة في مورد معين من موارد الشبكة، فهناك برنامج لمخدم الطباعة، وبرنامج لمخدم الملفات، وبرنامج لمخدم قواعد البيانات،.... الخ، وقد يخصص كمبيوتر واحد لخدمة معينة، كان يعمل خادم طباعة مثلا، لكن الاغلب ان توضع عدة برامج مخدمات في حاسوب واحد.

من اشهر انظمة تشغيل الملقمات، او المخدمات، نظام ويندوز سرفر 2003م، ويوجد منه عدة اصدارات، وقد خصصت ميكروسوفت اصدار خاص منة ليعمل كنظام تشغيل لملقم الويب نظرا لاهمية مخدم الويب، ويتيح هذا النظام للزبائن الحصول على كافة خدمات الويب، مثل نشر مواقع الويب وبرامج الويب المتنوعة، وغير ذلك من خدمات الويب.

وهناك اصدارات اخرى لنظام ويندوز سرفر 2003م، وهي اصدارات عامة لعدة مخدمات، وليس فقط لخدمة واحدة كملقم الويب، مثل اصدار ستاندرد، وهو يعمل كنظام تشغيل لملقم متعدد المهام، حيث يوفر برامج مخدمات الطباعة، والملفات، والاتصالات، والويب للمشاركين في الشبكة.

1. **بروتوكولات الشبكة:-**

البروتوكولات هي عبارة عن آلية قياسية عامة تنظم سير عملية الاتصالات داخل الشبكة، والهدف الاساسي لتصميم الية البروتوكولات هو انشاء نظام اتصالات قياسي تستطيع فيه المعدات المصنعة من الشركات المختلفة، الاتصال مع بعضها البعض.

ان معدات الشبكة لا تستطيع الاتصال ببعضها، وتبادل المعلومات فيما بينها، الا اذا كانت متوافقة تماما مع بعضها البعض، وهذا يعني انه لابد ان تكون جميع معدات الشبكة مصنعة من شركة واحدة لكي تستطيع اجراء الاتصالات، وتبادل البيانات،وبحيث يكون لدينا شبكة IBM، او شبكة ابل....الخ، ولحل هذه المشكلة صممت البروتوكولات التي تشكل الية قياسية عامة تتضمن مواصفات ومعايير يمكن اعتمادها من قبل كل الشركات المصنعة، وتسهل بالتالي استخدام معدات واجهزة من شركات مختلفة، داخل الشبكة الواحدة، من خلال اتباع تلك البروتوكولات والمواصفات والمقاييس العامة عند اعداد وتصنيع الاجهزة، والبرامج.

والطراز المعتمد للبروتوكولات هو طراز OSI الذي قامت بإعداده منظمة المواصفات القياسية الدولية (OSI)، وتضمن الطراز OSI تقسيم عملية الاتصالات بين الحواسيب في الشبكة الى سبع طبقات، وهي الطبقة المادية، وطبقة وصل البيانات، وطبقة الشبكة، وطبقة النقل، وطبقة جلسة العمل،وطبقة العرض، وطبقة التطبيقات، وكل طبقة من هذه الطبقات تصف جزء محدد من عملية الاتصال وتبادل البيانات.

ويتولى القيام بمهام كل طبقة اجهزه وبرامج معدة من قبل الشركات المصنعة، فالطبقة المادية مثلا تشمل الكابلات ووسائط النقل للبيانات، وطبقة وصل البيانات تقوم بها بطاقة الشبكة.... وهكذا

وبناء على ما سبق فانة يتم اعداد جميع مكونات الشبكة المادية والبرمجية لتنفيذ هذه البروتوكولات، وفقا للمقاييس التي تضمنتها. يلاحظ هنا ان برامج البروتوكولات ليست هي نظام التشغيل، لكنها مع ذلك تأتي في اكثرها كجزء منه، وبعضها يقيم في اجهزة الربط بعيدا عن نظام التشغيل مثل برامج الموجه، وبرامج بطاقة الشبكة التي تسمى السواقات، اما برامج نظام التشغيل فتقيم جميعها في جهاز الكمبيوتر التي يعمل الخادم Server وفي جهاز العميل Client.

## المبحث الرابع: الانترنت enternet

**ماهية الانترنت؟**

شبكة الانترنت هي عبارة عن شبكة كبيرة تربط بين الاف الشبكات المحلية والشبكات الواسعة وشبكات المؤسسات والمراكز الخاصة والعامة والاكاديمية، في البداية نشأت شبكة الانترنت في المجال العسكري في العام 1969م( ولم تكن تسمى بهذا الاسم بعد) وكانت عبارة عن مشروع انشاء شبكة تربط اربعة من اجهزة الحاسب الالي في عدد من الولايات الامريكية، واشرفت على انشاء هذه الشبكة وكالة مشروع الابحاث المتقدمة Arpanet التابعة لوزارة الدفاع الامريكية [[40]](#footnote-40).

تالفت شبكة اربانت Arpanet في البداية من اربعة حواسيب كبيرة[[41]](#footnote-41)، واعتمدت على بروتوكول Tcp\ip لتنظيم حركة نقل تبادل المعلومات بين اجهزة الحاسب الالي المختلفة التي تضمنتها، بعد ذلك بدأت العديد من الجهات الاكاديمية من جامعات ومراكز ابحاث بالارتباط بهذه الشبكة، فاصبحت شبكة اربانت تضم العديد من الحاسبات الخاصة بالمؤسسات الاكاديمية مراكز الابحاث.

خلال هذه الفترة لم تكن Arpanet هي الانترنت، وفي العام 1983م انقسمت Arpanet شبكتين: شبكة Arpanet وخصصت للاستعمال المدني مثل الابحاث، وشبكة Milint وخصصت للاستعمال العسكري، وكانت كلا الشبكتين متصلتين معا بما يسمح بتبادل المعلومات بينها، وسمي هذا الاطار الذي يجمع الشبكتين بالأنترنت Internet، ثم نشأت شبكات اخرى تعليمية وبحثية، وكانت شبكات منفصلة عن شبكة الانترنت ونشات لأغراض تعليمية، ثم ما لبثت ان انظمت الى شبكة الانترنت، ومن اهم تلك الشبكات شبكة nsfnet التي انشاتها المؤسسة القومية الامريكية للعلوم، وقد حلت هذه الشبكة محل شبكة اربانت في العام 1990م، فصارت شبكة nsfnet هي العمود الفقري هو اعتمادها غلى بروتوكول لشبكة انترنت بدلا عن اربانت خلال الاعوام 90-95م، ثم توسعت انترنت بعد ذلك توسعا هائلا داخل الولايات المتحدة الامريكية وخارجها، وكانت تشرف عليها ابتداء من العام 1990م المؤسسة القومية الامريكية للعلوم [[42]](#footnote-42).

اصبحت انترنت الان تضم الكثير من الشبكات داخل الولايات المتحدة الامريكية وخارجها، والذي ادى الى هذا الانتشار الواسع لشبكة انترنت هو اعتمادها على بروتو كول Tep\ip القياسي الذي سمح الاجهزة ومعدات شبكية مصنوعة من شركات ومصادر مختلفة، بالاتصال فيما بينها.

هناك شركات امريكية كبرى حاولت ان تجعل من الشبكات الخاصة بها شبكات تضاهي شبكة الانترنت، وتنافسها، مثل شبكة شركة IBM وشبكة SITA، وشبكة رويترز ROUETER، وشبكة امريكا اونلاين AMENICAM ONLIN ، وشركات اخرى، لكن محاولتها لم تنجح، واضطرت الى الارتباط بشبكة الانترنت لتتمكن من تقديم خدماتها [[43]](#footnote-43).

**خدمة الويب WORLD WID WEB(WWW)** [[44]](#footnote-44):

تقوم شبكة الانترنت على نموذج تشغيل الزبون Clint \_المخدم Server ، وتوجد فيها الالاف من اجهزة المخدمات Server.التي تتبع شركات ومؤسسات علمية، وتجارية مختلفة، وتتضمن اجهزة المخدمات الكثير من المعلومات والملفات والمنشورات الخاصة بالمؤسسات التابعة لها، وفى البداية كان يتم الحصول على المعلومات من هذه المخدمات من خلال ارسال كمبيوتر العميل او الزبون رسالة الى المخدم او الملقم، وانتظار الرد.

ولكن نظرا لنمو الانترنت الذي اصبح يتكون من ملايين الاجهزة، فقد وجدت صعوبة في الحصول على المعلومات بهذه الطريقة، فنشات نتيجة لذلك خدمة الويب او الشبكة العنكبوتية الدولية WORLD WID WEB(WWw) لتساعد الباحثين والمستفيدين في الحصول على المعلومات.

خدمة الويب هي عبارة عن لغة برمجية تقوم بعرض المعلومات الموجودة في المخدمات، على شكل نصوص مكتوبة، واصوات، وصور، وفيدوهات، ورسوم متحركة، اى ان خدمة الويب تحول المعلومات من شفرات برامج الى واجهة رسومية، فيها رسوم وصور وفيديوهات ونصوص، توضع هذه الواجهات الرسومية في صفحة تسمى صفحة المكان او الموقع، وتكتب الصفحة او الموقع بلغة تسمى html.

وقد تم انشاء برامج لقراءة هذه اللغة تسمى مستعرضات رسومية مثل mozilla \_internet explorer، تتولى قراءة لغة html، وتفسيرها، وتحويلها الى وجهة رسومية في جهاز الزبون او المستخدم تتضمن النصوص والصور والفيديو والصوت وكافة اشكال المعلومات.

و تتضمن خدمة الويب ما يسمى بالصفحات المرجعية name page وهى قائمة تظهر لك في الويب تتضمن عناوين صفحات ومواقع، عندما تنقر للبحث عن معلومة معينة في المتصفح، كالقائمة التي تظهر في محرك البحث جوجل عند البحث عن معلومة او شيء معين.

كما تتضمن خدمة الويب ما يسمى بالوصلات المرجعية links او الروابط، وهي عبارة عن روابط داخل موقع او صفحة ويب معينة، تنقلنا الى صفحة او موقع اخر يتضمن معلومات مرتبطة، ويسمى هذه النظام بالنصوص المحورية المرجعية Hxpenr text ، وبمقتضى هذا النظام فان الموقع يظهر لنا كوحدة واحدة او موقع واحد، ومع ذلك فان الصفحات التي يتكون منها قد لا تكون في مكان واحد، فقد تكون واجهة الموقع في مخدم داخل مصر او اليمن، وتكون أجزاءه الاخرى التي تدل عليها الروابط في اماكن اخرى من العالم في اوروبا او امريكا، فليست كل وصلات وروابط الموقع في جهاز واحد كما قد يبدوا لنا حينما تتصفح الموقع، بل هي موزعة على اجهزة اخرى ولكن نظام الويب يعرضها لنا كأنها في جهاز واحد.

**انشاء الموقع:-**

تتكون خدمة الويب WORLD WID WEB(WWW) من الاف من حواسيب الخدمة او الملقمات المنتشرة في انحاء العالم، والتابعة لشركات تجارية، او مؤسسات اكاديمية او علمية، وتضم هذه الحواسيب معلومات ضخمة ومتنوعة في صورة مواقع ويب wep [[45]](#footnote-45).

هناك طريقتين لا نشاء الموقع في الويب:

الاولى:- هي اعداد جهاز ملقم Server ووصله بالأنترنت، وهذه الطريقة مكلفة ولا تقوم بها الا الشركات التجارية الكبرى.

الثانية:- حجز مساحة في احدى الملقمات لانشاء موقع فيها، فهناك شركات تقوم بإنشاء ملقمات ثم تبيع مساحات مخصصة من هذه الملقمات للأفراد والشركات الصغيرة ليقوموا بأنشاء مواقع لهم فيها، تسمى هذه الشركات شركة استضافة المواقع، او متعهدي الايواء، وتتولى هي ادارة المواقع الخاصة بالافراد والشركات الموجودة في الملقم التابع لها.

**البحث عن المعلومات في الويب web:-** لتسهيل البحث عن المعلومات في الانترنت ثم ابتكار ما يعرف بعنوان الموقع العالمي universal Resource location ويعرف اختصار باسم(URL )، وهذا العنوان هو عنوان موقع المواد او المعلومات التي نبحث عنها، فيكفي ان يكتب هذا العنوان على المتصفح للوصول الى مكان المعلومات التي نريدها.

كما تم ابتكار برامج خاصة تتجول نيابة عنا في الانترنت بحثا عن المعلومة وتسمى هذه البرامج محركات البحث مثل محرك البحث Yahoo ومحرك البحث Google

## الجزء الثاني

## مراحل القرصنة الالكترونية

## تمهيد

على خلاف الجرائم التقليدية، فان جريمة القرصنة المعلوماتية تتم وفقا لمنهجية منظمة تتضمن عدد من المراحل والخطوات المتتالية التي يقوم بها المجرم حتى يصل الى هدفه، وهذه المراحل والخطوات اصبحت بمثابة مناهج او نماذج عامة، يتبعها القراصنة بوجه عام لدخول نظام الحاسب الالي، بصرف النظر عن اهدافهم، اي سواء كانوا قراصنة اخلاقيين وخبراء امن، او هكر مجرمين، وقد تم استخلاص هذه المراحل من خلال مراجعة دقيقة لا عمال الاختراق التي قام بها كبار الهكر في العالم.

تتكون مراحل القرصنة بوجه عام، بحسب ما تواضع وتعارف عليه مجتمع القراصنة، من خمس مراحل**[[46]](#footnote-46)**:-

1. الاستطلاع او جمع المعلومات

reconnaissance or information gathering

1. مسح المنافذscanning
2. الدخول الى النظام gaining access
3. الحفاظ على الدخول maintaining access
4. تغطية وتنظيف الاثار covering track

وهذه الخطوات الخمس يجب ان تؤدي بالترتيب، لان النتائج المتحصلة من كل مرحلة تستعمل في انجاز المرحلة التالية وصولا الى مرحلة الدخول وارتكاب جريمة السرقة، وبدون هذا الترتيب لا يستطيع المجرم اداء جريمته بطريقة ناجحة[[47]](#footnote-47).

المرحلة الاولى وهى مرحلة الاستطلاع هي المرحلة الاكثر عمومية في هذه المراحل الخمس، ويقوم الجاني فيها بجمع كل المعلومات الممكنة عن النظام مهما كانت تبدو تافهة او عديمة الاهمية، فكم من الحالات التي كانت تبدو فيها بعض المعلومات تافهة او عديمة الاهمية، تحولت فيما بعد الى عنصر حاسم في انجاز عملية الاختراق والوصول معلومات النظام[[48]](#footnote-48).

في المراحل التالية يبدا الجاني بخطوات اكثر تحديدا ويركز على طرق ومسارات محددة، مثل نقاط الدخول، الوصول الى النظام، والاستيلاء على حسابات المستخدمين، وهكذا، لذلك يصور بعض الكتاب هذه المراحل على شكل مثلث مقلوب يبدا واسعا رحبا ثم ينتقل بالتدرج نزولا الى التحديد والتركيز.

تمثل هذه المراحل والخطوات في الحقيقة تجزئة لعملية ظلت معقدة وغامضة لسنوات عدة، وهى عملية قرصنة نظام الحاسب الالي، ولذلك فان لها اهمية كبيرة من منظور مجتمع امن المعلومات، لانها تساعد على فهم واتقان اساليب تقنيات الجناة، وبالتالي وضع اجراءات الحماية اللازمة لكل مرحلة منها.

المبحث الاول: مرحلة الاستطلاع **[[49]](#footnote-49)**

**reconnaissance**

يقصد بمرحلة الاستطلاع جمع المعلومات عن المنظمة الهدف، او بالتحديد شبكة المنظمة الهدف، سواء كانت هذه المنظمة بنك او شركة...الخ.

فقبل ان يقوم الجاني باختراق نظام المعلومات في منظمة او مؤسسة ما فانة يقوم اولا بالتحضير والاعداد لهذا الاختراق من خلال جمع كل المعلومات الممكنة والمتوفرة عن شبكة المنظمة التي يريد اختراقها، ويمكن تشبيه هذه المرحلة بمرحلة التحضير للسطو على بنك معين، فالعصابة التي تخطط للسطو على بنك معين تبدأ اولا بالتحضير لارتكاب الجريمة من خلال اجراء واستطلاع وبحث عن البنك مداخله ومخارجه، ومواقع المال، واجهزة الرقابة والحراسة...الخ، ثم تقوم بارتكاب الجريمة، وهذا يتماثل مع ما يتم في مرحلة الاستطلاع.

والمعلومات التي يقوم الجاني المعلوماتي بتجميعها في مرحلة الاستطلاع تساعده في امور كثيرة، مثل تحديد الاهداف ذات القيمة العالية في المنظمة المستهدفة، وتحديد مواقع وجود المعلومات المطلوبة، الحصول على بيانات يمكن من خلالها بدء الهجوم مثل عناوينip للحواسيب الموجودة في المنظمة، ونوع نظام التشغيل...الخ، فكل هذه المعلومات تسهل للجاني ارتكاب الجريمة.

وبوجه عام، فان هذه المرحلة تتميز بالسعة وعدم التحديد، ويقوم فيها الجاني بجمع كل المعلومات عن المنظمة مهما كانت تبدو له تافهة، ويستخدم في ذلك مصادر مختلفة للمعلومات في شبكة الانترنت او على الواقع، فهي نوع من البحث الشامل الغير محدد عن المعلومات. وتعتبر مرحلة الاستطلاع ايضا من اهم مراحل القرصنة، لأنها تحدد الاهداف القيمة، وطرق الدخول الى نظام المنظمة، والمعلومات المهمة، ولذلك فإنها تعتبر الخطوة الاولى للمجرم المعلوماتي من وجهة نظر مجتمع القراصنة وخبراء الامن الالكتروني، والجاني الذي ينجح في هذه المرحلة يكون احتمال نجاحه اكيد في المراحل اللاحقة، وبعد ان يقوم الجان بجمع المعلومات في هذه المرحلة يستطيع ان يركز جهوده ووقته على اهداف محددة وذات قيمة في المنظمة، وان يقتصر نشاطه على نطاق محدد وصولا في نهاية المطاف الى اختراق النظام والاستيلاء على المعلومات والقيم المالية الموجودة فيه.

وفي هذه المرحلة لا يتم الاتصال الالكتروني المباشر بالهدف، ولذلك فان الادوات والطرق المستخدمة فيها لا تتصل الكترونيا بنظام الحاسب الالي المستهدف، بل يتم جمع المعلومات من خلال مصادر عامة متوفرة في الانترنت، او من خلال اساليب التفاعل المباشر مع الموظفين، من دون المساس بنظام الحاسب المستهدف، وهذه الخاصية هي التي تميز هذه المرحلة في الحقيقة بانها مرحلة تحضير للجريمة لا تنفيذ لها، لان الاتصال المباشر بنظام الحاسب الالي يعني فعليا بدا تنفيذ الجريمة، والانتقال من التحضير الى التنفيذ، ولذلك فان هذه المرحلة لا تدخل في المفهوم القانوني والشرعي للركن المادي. نموذجيا تتضمن هذه المرحبة نوعين من البحث:

1- وactive recon

2- passive recon

\***اهداف مرحلة الاستطلاع: reconnaissance targets**

تهدف مرحلة الاستطلاع الى تكوين نظرة عامة شاملة لنظام الحاسب الالي المستهدف، والمنظمة التي ينتمي اليها ذلك النظام، بغرض ايجاد طرق اقتحام النظام المعلوماتي للمنظمة والدخول اليه، وصولا الى سرقة الاموال المخزنة فيه، أو ارتكاب اي جريمة اخرى ضد النظام، وبصفة عامة يمكن القول ان مرحلة الاستطلاع تهدف الى ما يلي:-

1. جمع المعلومات عن بيئة النظام المعلوماتي المستهدف، والبنية المعمارية التي يتكون منها.
2. الكشف عن نقاط الضعف في النظام، وافضل الطرق لاستغلالها.
3. التعرف اكثر عن الجوانب الامنية، والتفاصيل الدقيقة للنظام الهدف، مثل انظمة الوصول عن بعد، والمنافذ، وانواع الخدمات، وطرق واساليب الحماية والامن، والانظمة الامنية التي تتبعها المنظمة......الخ.

ا**نواع المعلومات Information typs**

تتميز مرحلة الاستطلاع بالشمولية والسعة، بمعنى انه لا يوجد معلومات محددة يجب البحث عنها خلال هذه المرحلة، بل ان الجاني يقوم بإجراء البحث عن كل المعلومات المتاحة، وعليه ان يلتقط كل معلومة عن النظام الهدف سوء كانت على شكل اجزاء صغيرة ومقتطفات، او على شكل مجموعات متكاملة، وسوء بدت له تافهة او مهمة، ثم يقوم بعد ذلك بتركيبها او تجميعها مع بعضها ودراستها وتحليلها، وهذه مبادئ مستقرة في مجتمع القراصنة، لان المعلومات التي تبدو غير هامة في هذه المرحلة قد تكون حاسمة في نجاح المراحل اللاحقة للدخول الى النظام، كما ان المعلومات التي تكون غير مفيدة بسبب انها متفرقة ومبعثرة، تكون اكثر اثارة واهمية عند تجميعها، ولذلك فالقاعدة المستمرة عند المخترقين هو عدم اغفال أي معلومة توجد في الطريق عن النظام الهدف.

ومع ان القاعدة في هذه المرحلة هي الشمولية في البحث، فان هناك مجموعات محددة من المعلومات يجب ان يحصل عليها المخترق خلال هذه المرحلة، ويمكن تصنيف هذه المعلومات على النحو التالي:-

1. معلومات عن شبكة المنظمة:

مثل اسم الميدان للمنظمة واسماء الميادين للشبكات الداخلية الفرعية للمنظمة، وعناوين IP ، كتل الشبكة، البروتوكولات والخدمات، جدار النار، موقع المنظمة على الانترنت والموقع السري ان وجد، وخريطة الشبكة ومعماريها.

1. معلومات عن النظام:

مثل نظام او انظمة التشغيل في المنظمة، ملصقات النظام، برتوكول البريد smmp، نظام الوصول عن بعد، كلمات السر password اسماء المستخدمين والمجموعات، جداول الموجهات، الية التحقق من الصحة.

1. معلومات عن المنظمة:

مثل تفاصيل الموظفين كالعناوين وارقام التلفونات، دليل اسماء وتلفونات الشركة، موقع ويب الخاص بالشركة والمنظمة، عناوين البريد الالكتروني.

* **طرق جمع عن المعلومات:**

يتم جمع المعلومات في مرحلة الاستطلاع بواسطة بعض ادوات القرصنة المخصصة للبحث في الانترنت، وتنقسم ادوات جمع المعلومات بشكل عام الى تطبيقات، والى مواقع ويب، واساس عمل كل هذه الادوات هو القيام بعمليات بحث مفتوحة في مصادر عامة شتى على شبكة الانترنت، مثل الاخبار والمقالات والمجموعات الاخبارية وشركات التسجيل وخوادم اسماء النطاقات...الخ.

وتوجد في كل الادوات المخصصة لجمع المعلومات، خطوات محددة يقوم بها الجاني، سواء كان يستخدم اداة او برامج معينة، او كان يستخدم موقع من مواقع الويب الخاصة بالبحث، يمكن اجمال هذه الخطوات بالاتي:-

1. الدخول على الموقع او التطبيق، وفي حالة الموقع يقوم الجاني بكتابة اسم الموقع على محرك البحث، او نسخ الرابط على المتصفح، ثم فتح صفحة الموقع، وفي حالة الاداة يتم تنزيل او تركيب الاداة اولا، ثم فتح صفحة الاداة.
2. كتابة اسم الشركة على نافذة البحث المختارة في صفحة الموقع او الاداة، وضغط زر البحث.
3. يقوم الموقع او الاداة بالبحث وجلب جميع البيانات والمعلومات المتوفرة في الانترنت عن الشركة الهدف على شكل تقرير.
4. يقوم الجاني بمراجعة تقرير المعلومات وتحليله ودراسته واستخلاص المعلومات المفيدة منه، مثل عناوينIP، ارقام الموظفين وارقام التلفونات، ونظام التشغيل، خادم اسماء النطاق....الخ.
5. يقوم الجاني بهذه الخطوات في عدة ادوات ومواقع، وينتقل بين الادوات والمواقع المختلفة بحثا عن اكبر قدر من المعلومات.
6. يقوم الجاني بحفظ هذه المعلومات اما الكترونيا في مجلد او ملف، او كتابتها وتسجيلها على الاوراق.

**1-البحث في مواقع الويب:-**هناك العديد من المواقع التي تجوب الانترنت بحثا عن المعلومات، ومع ذلك فإن الموقع الاهم الذي يجب ان نبحث عن المعلومات فيه هو موقع المنظمة او المؤسسة الهدف، وتعتبر صفحة المنظمة على الانترنت مستودع لكثير من المعلومات الهامة عنها، والتي لا غنى عنها لعملية الاختراق، وسوف نتناول فيما يلي البحث في موقع المنظمة ثم البحث عن بعض المواقع الاكثر شهرة الخاصة بجمع المعلومات.

1- **البحث في موقع المنظمة:**

تتضمن صفحة الويب الخاصة بالمنظمة او الشركة المستهدفة كثير من المعلومات عن بنية النظام الحاسوبي المتبع فيها، ولذلك فان الجاني يبدا في جمع المعلومات من موقع المنظمة على الانترنت، ومن اهم المعلومات التي يحصل عليها الجاني من خلال موقع الشركة على الانترنت ما يلي[[50]](#footnote-50):-

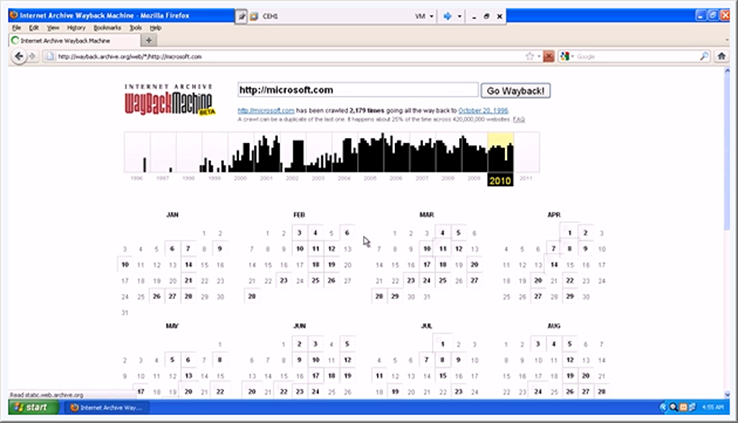
1. البرمجيات المستخدمة واصدارها.
2. نظم التشغيل المستخدمة.
3. معلومات الاتصال مثل اسماء وارقام الهاتف، وعناوين البريد الإلكتروني، وموقع المشرف.
4. خوادم الويب المستخدمة واصدارها، ومنصة السكربت.
5. الموقع الجغرافي للشركة او المنظمة الهدف.
6. سياسات الامن او الخصوصية التي تشير الى انواع اليات الامن الموضوعة.
7. الارتباطات الى خوادم اخرى والكينونات والشركات المرتبطة.
8. شيفرة المصادر HTML واكواد الانشاء والتي من خلالها نحصل على الكثير من المعلومات مثل العناوين الداخلية والروابط، وبنية نظام الملفات والمجلدات، وعادة ما يعمل المخترق على نسخ المواقع الالكتروني للمنظمة الهدف الى جهازه، لكي يتمكن من دراسة محتويات الموقع بعمق اكثر وخاصة شفرات المصدر HTMI، ويتم نسخ الموقع الالكتروني من خلال عدد من ادوات القراصنة ومن اهمها واشهرها اداة

HTTrack والتي تقوم بنسخ الموقع الالكتروني كاملا وتحميله الى مجلد محلي في جهاز المخترق بكافة صفحاته وملفاته، وتقوم هذه الاداة ببناء كافة المجلدات وصفحات TTTML والصور وغيرها من الملفات الخاصة بالموقع، في المجلد المحلي الخاص بالجاني المخترق. وبالتالي يتيح له دراسة صفحات ومكونات الموقع وتحليلها في جهازه والحصول على اكبر قدر من المعلومات منها.

2- **البحث في موقع ارشيف http\\archive org [[51]](#footnote-51):** موقع ارشيف هو مخزن لصفحات الويب الخاصة بالشركات، ويتضمن كل صفحات الويب التي انشاتها كل شركة منذ بداية انشاء موقعها والى الان، وبالتالي فانة يتضمن كل التطورات والتحديثات التي حدثت في الموقع، وكل الاصدارات الحديثة والقديمة له، هذا يسمح للجاني المخترق بجمع المعلومات، واستكشاف نقاط الضعف والثغرات التي كانت في الاصدارات السابقة للموقع، والتي تم ترقيعها او لم يتم.

ويعمل موقع الارشيف من خلال كتابة اسم الشركة في خانة البحث وضغط الزر، وعندها يقوم الموقع بجلب جميع الصفحات منذ انشاء الموقع ويرتبها حسب التاريخ اليوم الشهر والسنة، ويستطيع الجاني استعراض الصفحة التي يريدها من خلال الضغط على تاريخ معين

فيدخلك الى الصفحة التي كانت موجودة في ذلك التاريخ، وتقوم بدراستها وتحليلها.



**3- البحث في موقع Net craft:-**

موقع Net craft هو احد اهم مواقع البحث عن المعلومات حول المنظمات والمؤسسات، ويقدم هذا الموقع كثير من المعلومات ومن اهمها تحديد نظام التشغيل خادم للويب osi web serves الخاص بالمنظمة، ونأخذ صفحة الموقع الشكل الاتي:

****

ولاستخدام هذا الموقع نقوم بفتح صفحة الويب الخاصة بالموقع ونكتب اسم الشركة او المنظمة الهدف في الحقل what is ونضغط زر البحث، وعندها يعيد لنا الموقع تقرير بالمعلومات عن المنظمة، ومن اهمها نوع نظام تشغيل الويب، وعناوين ip، وتحديد خوادم اسماء النطاقات DNS [[52]](#footnote-52).

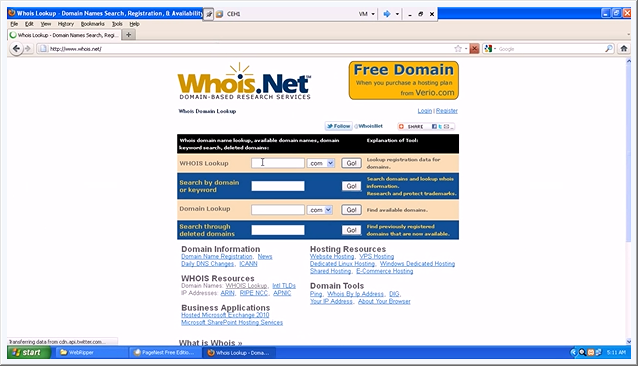
**4-البحث في موقع Whois:-**

Whois هي عبارة عن قواعد بيانات متعددة تتضمن معلومات التسجيل الخاصة بالشركات، وتعتمد الية البحث في whois على استيراد المعلومات من سجلات تسجيل اسماء وارقام الانترنت، فمن المعروف ان مؤسسة ican تتطلب من كل شركة او منظمة ان تقوم بتسجيل اسم المجال الخاص بها لتضمن ان شركة او منظمة واحدة فقط تستخدم هذا الاسم، وعندما تقوم اي شركة او منظمة بتسجيل اسم الميدان، فأنها تقدم معلومات تودع في قواعد بيانات Whois، ومن اهم هذه المعلومات اسم الميدان او المجال اي اسم الشركة على الانترنت، عناوين ip، اسم الشخص القائم بالتسجيل وارقام الهاتف وعناوين البريد الالكتروني الخاص به، معلومات الاتصال الاداري الاخرى، اسماء الملقمات والسيرفرت التابعة للشركة، اسماء خوادم Dns، معلومات عن مسئولين الشركة وعناوينهم وارقامهم[[53]](#footnote-53).

تقوم الية البحث في whois باستيراد هذه المعلومات وغيرها من سجلات التسجيل وجلبها الى من يطلبها، وقد كانت ادوات البحث الخاصة بWhois في البداية ضمن نظام تشغيل unix، الا انها تطورت الان واصبحت تستخدم في عدد من انظمة التشغيل، والالية الاسهل والافضل في البحث داخل قواعد بيانات Whois هي الدخول الى موقعها على الانترنت، وعندما نقوم بفتح صفحة الموقع في الانترنت نكتب عنوان الشركة او المنظمة المستهدفة بالاختراق في خانة البحث، ثم نضغط زر البحث، وعندها يقوم الموقع بعرض تقرير كامل بالمعلومات عن المنظمة، يتضمن اسماء ملقمات Dns، ومعلومات عن شخص القائم بالتسجيل، وغير ذلك من المعلومات الخاصة بتسجيل المنظمة التي سبق الاشارة اليها[[54]](#footnote-54).

هناك اليات بحث متقدمة في الموقع تستطيع تحويل اسماء ملقمات Dns الى عناوينIP والعكس، وتستخدم هذه الاليات عندما تكون المعلومات التي تم جلبها تقصر فقط على اسماء ملقمات ال DNS دون ارقامها [[55]](#footnote-55).

تعتبر المعلومات التي تجلبها قواعد بيانات Whois في غاية الاهمية للقيام بعملية اختراق الانظمة وقرصنتها، ولايمكن القيام بعملية القرصنة والاختراق دون هذه المعلومات، الشكل التالي يبين صفحة الموقع:



5-**البحث في نظام DNS**: يعتبر البحث في نظام DNS والمعروف بنظام اسماء النطاقات اولوية عليا بالنسبة للقراصنة الذين يخترقون اجهزة الكمبيوتر ومواقع المنظمات، ذلك انهم يستطيعون من خلال قواعد بيانات هذا النظام الحصول على عناوين IP للمنظمات واسماء النطاقات المقابلة لها، وسوف نوضح فيما يلي فكرة نظام DNS وطرق الحصول على المعلومات من قواعد البيانات الخاصة بهذا النظام، وذلك نظرا لأهمية هذا النظام البالغة في المراحل اللاحقة للاختراق.

* **فكرة ظهور نظام DNS:-**

تستخدم عناوين الانترنت بوجه عام لتسهيل الوصول الى اجهزة الكمبيوتر المتصلة بشبكة الانترنت، والولوج الى مواقع المنظمات والشركات في الويب، في البداية كان كل حاسب الي متصل بشبكة الانترنت يملك رقم فريد يميزه ويعرف به داخل الشبكة، وكان يسمى هذا الرقم بعنوان IP "IP ADRESS" [[56]](#footnote-56)، وهو عبارة عن رقم يتكون من اربع مجموعات ارقام، تفصل بينها نقاط، ويشير الى عنون جهاز الكمبيوتر المحدد، مثل 128- 54- 16- 1 [[57]](#footnote-57)، وتماثل هذه الارقام ارقام الهاتف التي تتكون من عدد من الارقام تشير الى جهاز الهاتف المطلوب.

ووفقا لهذا النظام، فانه اذا اراد المستخدم الوصول الى موقع معين على شبكة الانترنت، كان عليه ان يحفظ الارقام التي تشير الى هذا الموقع[[58]](#footnote-58)، لكن تذكر هذه الارقام وحفظها لم يكن سهلا، وكان يشكل صعوبة كبيرة في التعامل مع المواقع عبر الانترنت، لذلك اخترع مطوروا الانترنت مفهوم جديد للعنونة وهو مفهوم اسماء المضيفاتHOST NAME، ووفقا لهذا المفهوم الجديد، يقوم المسؤولون بتعيين اسماء مناسبة للكمبيوتر في الشبكة، وتحويلها الى عناوين ip عند الحاجة، وهذا يشابه ما تقوم به عندما تحفظ ارقام الهاتف في اجهزة التلفونات المحمولة، حيث اننا نعرف هذه الارقام على شكل اسماء، لكن عند الاتصال يتحول الاسم عند الضغط علية الى الرقم.

كان اسم المضيف host name عبارة عن اسم يمثل كمبيوتر، وفي البداية كان يتم تخزين اسماء المضيفات في ملف نصي يدعى host في كل كمبيوتر، وكان هذا الملف النصي host يحتوي ايضا على عنوان ip المقابل لاسم المضيف والمقترن به[[59]](#footnote-59)، إي ان الملف host كان عبارة عن لائحة او جدول، يتضمن اسم كل مضيف ورقم الip الخاص به، وعندما كان يريد إي جهاز كمبيوتر التخاطب مع جهاز او موقع اخر بأرسال الطلبات او الرسائل، فانه كان يأخذ عنوان ip الخاص باسم المضيف من الملف host ويقوم بالأرسال على هذا العنوان، اي ان الملف hostكان بمثابة رجل في الوسط يقوم بتحويل العنوان الاسمي الى عنوان ip قبل الارسال.

في البداية كان كل مستخدم يختار اسم مضيف خاص به، وكان المستخدمون يبلغون بعضهم بالأسماء الجديدة ليضيفوها الى جداولهم في الملف host، لكن مع بدء شبكة الانترنت بالنمو قرر المسؤولون في الانترنت انشاء سجل مركزي لأسماء المضيفات، وتم اختيار المؤسسة sri لصيانة ملف host المركزي، وكان على مسئولوين الانظمة المنتشرة في ارجاء شبكة الانترنت ارسال اسماء مضيفاتهم الجديدة الى مؤسسة sri التي تتولى اضافتها الى السجل الرئيسي، وكان مستخدمو الشبكة يحملون هذا الملف الرئيسي دوريا للحصول على احدث الاصدارات.

لكن مع تواصل نمو شبكة الانترنت اصبح هذا النظام غير ملائم، فقد زادت عدد الاضافات الى الجداول الرئيسي بشكل هائل، كما حدث ازدحام كبير في الشبكة نتيجة قيام كل المستخدمين تحميل الملف الرئيسي الى اجهزتهم، وبالإضافة الى ذلك حدثت مشكلة كبيرة عندما بدء المستخدمون يختارون اسماء لمضيفاتهم كان يستخدمها اشخاص اخرون، وحدثت نزاعات كثيرة حول اسماء المضيفات، ونتيجة لهذه المشاكل الكبيرة قرر مطورو هذا الانترنت انشاء نظام اخر لتلافي كل هذه المشاكل، وكان هذا النظام هو نظام DNS.

استهداف نظام DNS امرين رئسيين:-

1. تلافي تكرار الاسماء وما ينشأ عنه من نزاعات.
2. تلافي الازدحام من خلال انشاء قاعدة بيانات موزعة لملف host، بحيث يتم تخزين بيانات اسماء المضيفين وارقامهم في ملقمات أو خوادم منتشرة في كافة ارجاء شبكة الانترنت، وهذا يعني ان بيانات اسماء المضيفين وارقام IP لن تكون موجودة في مكان رئيسي واحد، بل ستوزع على الملقمات في كل الانترنت، ولتحقيق هذه الاهداف انشأ مطوروا DNS مفهوم الميدان Domain، والميدان هو عبارة عن كيان اداري يتألف من مجموعة مضيفات (اجهزه كمبيوتر مضيفه )، وكل ميدان له ملقمات اسماء DNS، تتضمن كل معلومات الاسماء وعناوين IP الخاصة بها في نطاق ذلك الميدان، وتعتبر ملقمات او خوادم الاسماء (DNS) في ميدان معين هي المكان الرسمي الذي تخزن فيه معلومات الملف host التي تتعلق بكل الأجهزة التابعة للميدان، وهو المصدر الرسمي للمعلومات عن ذلك الميدان[[60]](#footnote-60).

يخزن ملقم DNS الخاص بميدان معين معلومات اسماء المضيفات وارقام IP التابعة لهذا الميدان في سجلات تسمى سجلات موارد، وهذه السجلات تشمل الانواع الرئيسية الاتية[[61]](#footnote-61):-

1. سجل A host: ويتضمن هذا السجل اسم المضيف ورقم IP الخاص به، وفي حاله تلقيه طلب السؤال عن اسم معين فانه يعيد اليه رقم IP الخاص بهذا الاسم.
2. سجل MX: وهو يتضمن عنوان IP لجهاز الكمبيوتر الذي يقوم بمعالجة حركة البريد الالكتروني الوارد الى الميدان.
3. سجل NS ويتضمن عناوين IP لجمع ملقمات DNS الموجودة في الميدان
4. سجل PTR ويتضمن اسماء المضيفات المطابقة لعناوين IP، ويعالج هذا السجل طلبات لمعرفة الاسم الخاص برقم IP معين، حيث انه يرد باسم المضيف المطابق لعنوان IP. أي انه يقوم بعملية تحويل من IP الى الاسم.

* مشكلة تعيين الاسماء:

بموجب نظام DNS فانة اصبح من الممكن ان يتكرر اسم المضيف في اكثر من ميدان، من دون وجود أي تضارب او تنازع، حيث يشترط ان يكون اسم المضيف فريدا وغير مكرر في ميدانه فقط، وقد ترتب على اضافة الميادين ان الاسم او العنوان الالكتروني اصبح يتكون من جزئين: اسم المضيف + اسم الميدان، واسم المضيف هو اسم لكمبيوتر محدد "سيرفر "، واما اسم الميدان فهو غالبا اسم لشبكة خاصة بشركة او منظمة ما.

* **البحث في DNS:**

يعتبر نظام الDNS مثل وعاء من الذهب بالنسبة للقراصنة والمخترقين، والسبب في ذلك انه يحتوي على لائحة كاملة بأسماء الكمبيوترات التابعة لشبكة المنظمة الهدف، وعناوين IP القابلة لها، ومن خلال هذه العناوين يستطيع الجاني كسب الوصول الى أي جهاز في الشبكة واختراقه[[62]](#footnote-62).

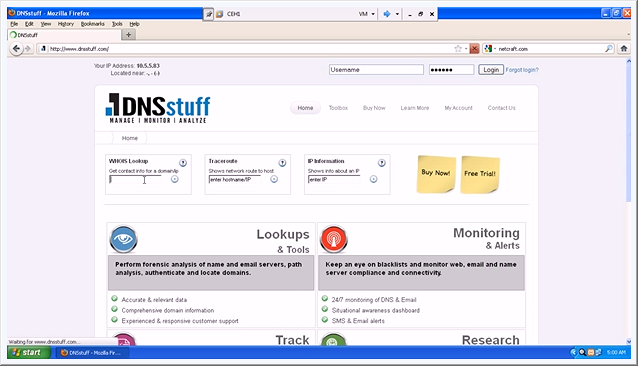
بالاضافة الى ذلك فانة خادم DNS التابع للمنظمة يتولى ترجمة اسماء النطاقات وعناوين IP التي تم تجميعها من مرحلة الاستطلاع، الى اسماء أو الى عناوين IP بحسب ما يريد الجاني.

وتسمى عملية استخراج المعلومات من خادم DNS بعملية استجواب DNS، وتتم عملية الاستخراج هذه بطريقتين، البحث في الموقع والادوات، والقيام بعمليات نقل المنظمة، نتناول الطريقتين فيما يلي:

1. **البحث في المواقع[[63]](#footnote-63):-**

هناك العديد من المواقع التي توفر امكانية البحث في خوادم DNS، مثل موقع IP TOOL - DNS tools -DNS stuff، ويتميز موقع ip tools بوجود خيارات وخصائص للبحث تتضمن البحث في كل انواع سجلات DNS، فيمكن للجاني عند دخوله الى صفحة الموقع ان يضع اسم الشركة في خانة البحث، ثم يقوم بتحديد خيار أي سجل من سجلات DNS من القائمة المنسدلة، مثل سجل A أوسجل MX، ثم يضغط زر البحث وعندئذ يعيد الموقع كامل المعلومات عن المنظمة التي يتضمنها السجل المحدد.

الشكل التالي يبين صفحة الموقع DNS stuff الذي يوفر امكانية البحث في عدة مواقع منها موقع DNS:



**ب- عمليات نقل المنطقة[[64]](#footnote-64):-**

السبب الذي تم لأجله توزيع قاعدة بيانات DNS على خوادم متعددة في انحاء العالم هو تخفيف الحمل عن الخادم الرئيسي والحد من عمليات الاختناق في الشبكة، ولنفس هذا السبب فان الشركات والمنظمات تعمل على نشر خوادم ثانوية لDNS الى جانب خادم DNS الرئيسي، وذلك من اجل تخفيف الحمل عن الخادم الرئيسي وعن شبكة المنظمة، والذي ينشأ نتيجة تكرار طلبات التحميل لملف قاعدة البيانات.

يحتفظ خادم DNS الثانوي بنسخة كاملة من قاعدة البيانات الموجودة في الخادم الرئيسي، ولكن هذه النسخة هي للقراءة فقط وغير قابلة للتعديل او التحديث، ولذلك فان الخادم الثانوي يقوم بتحديث قاعدة البيانات الموجودة فيه دوريا من الخادم الرئيسي، من اجل استيعاب التعديلات والاضافات الجديدة في الاسماء والارقام، ويتم هذا التحديث كل خمسة عشر دقيقة من خلال طريقتين:

-طريقة AXFr: وفي هذه الطريقة فانه عند حدوث أي تعديلات او اضافات في الخادم الرئيسي يأخذ الخادم الثانوي نسخة كاملة جديدة من كل قاعدة البيانات الخاصة بالمنطقة، وهكذا مع كل تعديل او اضافة.

-طريقة IXFR:في هذه الطريقة فان الخادم الثانوي يأخذ فقط الفروقات والتعديلات من الخادم الرئيسي.

* **كيف تتم عملية نقل المنطقة:**

يقوم الجاني في عملية نقل المنطقة بانتحال شخصية الخادم الثانوي ويقوم بتحميل نسخة كاملة من قاعدة بيانات الخادم الرئيسي للDNS، على اساس انها لتحديث قاعدة البيانات في الخادم الثانوي، ولكنها في الواقع تذهب اليه، ويتمكن بهذه الطريقة من الاحتيال من الحصول على قاعدة بيانات ال DNS الكاملة للمنطقة، ويستخدم الجاني في هذه العملية عدد من الادوات مثل الاداة Dig، ووالاداة Nslood up [[65]](#footnote-65).

وبمجرد ان يقوم الجاني بتحميل نسخة ال DNS فانه يصبح لدية كافة اسماء وارقام IP لأجهزة الشبكة الداخلية، ومخطط كامل لتركيب وبنية الشبكة، وطبعا هذه المعلومات تعد ثروة كبيرة لا تقدر بثمن بالنسبة للمخترق.

6-**البحث من خلال الاداةTraceroute:-**

وهي تطبيق او برنامج يستكشف بنية شبكة المنظمة، ومسارات الوصول المهمة داخلها، وذلك من خلال تتبع الطريق الذي تسلكه الرسالة داخل الشبكة، وتعتمد اداة Tracer out على تقنية رسائل ICMP، وهى رسائل معلوماتية لا تحمل بيانات وانما تستخدم فقط للتبليغ عن الاخطاء، او للاستعلام عن الانظمة المتصلة الفعالة، تتضمن رسائل ICMP قيمة اشبه بالعداد، وعندما يقوم برنامج **Traceroute** بإرسال رسالة ICMP يحدد قيمة معينة مثلا 100، بعدها تمر الرسالة على كل موجة او جهاز على الشبكة، وكلما مرت بموجة يقوم هذا الموجة بإنزال قيمة العدد بمقدار 1، في نهاية المطاف يمثل العدد الذي نقص من قيمة العداد، عدد الموجهات والاجهزة الموجودة في الشبكة، والنتيجة النهائية التي يحصل عليها الجاني من هذه العملية هو تكوين لائحة بالموجهات، واجهزة الوصول مثل جدران النار وموجهات تصفية الرزم، التي تتضمنها الشبكة، وكذلك تحديد المدة الزمنية بين كل موجه والاخر، ومعلومات اخرى تتصل بذلك، ويستطيع المخترق من خلال هذه النتائج ان يقوم ببناء تصور حول تخطيط الشبكة، وبنيتها، ومسارات الوصول داخلها[[66]](#footnote-66).

تعرض اداة Tracerout هذه النتائج على شكل وثبات والسبب في ذلك ان الموجه هو جهاز يعالج الرسالة التي تمر به على شكل وثبة، حتى انه يختار قصر مسارات الوصول الى جهة معينة على حسب عدد الوثبات، وهناك ادوات Tracerout متقدمة مرئية، تعرض النتائج في صورة اشكال ورسوم ومن هذه الادوات اداة Tracerout VISual ip وهي تعرض شبكة المنظمة وسلسلة الموجهات التابعة لها على شكل خريطة تبين مواقع اجهزة الشبكة والمسافات والمعلومات الاخرى.

## المطلب الثاني: مرحلة المسح scanning

**مفهوم عملية المسح:-**

تهدف مرحلة المسح scanning الى التعرف على الانظمة الحية التي تعمل على الشبكة، والخدمات (التطبيقات والبرامج )التي تشغلها.

ويضيف البعض خطوة اخرى الى هذه المرحلة وهي التعداد والذي يقصد به تحديد اسماء المنظمة والمستخدمين وملفات وقنوات المشاركة التي تعمل على النظام الهدف.

بينما يعتبر البعض الاخر ان التعداد يشكل مرحلة مستقلة من جملة مراحل اخرى.

والارجح ان التعداد يعتبر مرحلة مستقلة، ولذلك فإننا سوف نقتصر في هذا المبحث على المسح فقط، وسنتناول التعداد في مبحث مستقل

ويمكن ان نقسم مرحلة المسح الى الخطوات الاتية:

1. التعرف على الانظمة الفاعلة host live
2. مسح المنافذ port scaning

* **التعرف على الانظمة الفعالة** **Host live**

يتم التعرف على الانظمة الفعالة والقابلة للوصول عبر الانترنت من خلال ارسال رسالة من نوع Icmp الى عنوان ip للنظام الهدف، في حالة اذا استجاب النظام الهدف لهذه الرسالة، فإننا نعرف ان هذا النظام متصل وفعال، ونبدأ بالخطوة 2 وهي البحث عن منافذ للدخول اليه، ويتطلب استيعاب خطوة التعرف على الانظمة الفعالة الالمام ببعض العناصر وهي:-

1. عنوانip
2. تقنية رسائل ICMP
3. اداة ارسال الرسائل PING
4. **مفهوم عنوان IP:-**

عندما يتصل حاسب الي بالأنترنت فانه يجب ان يكون له عنوان يعرف به في هذه الشبكة، بحيث يتلقى البيانات وانواع الخدمات والاتصالات التي تقدمها شبكة الانترنت، على هذا العنوان، ويسمى عنوان الحاسب الالي الذي يتم التعامل والتخاطب مع الحاسب عليه بعنوان IP، ويتكون هذا العنوان من رقم الجهاز ورقم الشبكة التي ينتمي اليها هذا الجهاز، والاصل ان عنوان IP تمنحه شركة متخصصة غير ربحية تسمى ICAN وذلك لتفادي حدوث أي تكرار او نزاعات في هذه العناوين، الا ان هذه الشركة قد فوضت مؤسسات اقليمية ودولية في انحاء العالم بمنح هذه العناوين، وقد اصبح الاغلب انه يتم الحصول على عناوين IP من مزودي خدمات الانترنت، وهي المؤسسات الحكومية أو الخاصة التي تزود خدمة الانترنت للمستخدمين في كل بلد او مدينة، سواء كان هؤلاء المستخدمين شركات او افراد.

عنوان IP الذي يمنحه مزود الخدمة نيابة عن مؤسسة ايكان قد يكون عنوان ثابت دائم، وقد يكون عنوان موقت، والعنوان الثابت يمنحه مزود الخدمة الى الشركات ومؤسسات المال التي تحتاج الى اتصال دائم بالأنترنت، اما عنوان IP المؤقت فيمنحه مزود الخدمة للحواسيب التي تتصل بالأنترنت لفترة محددة ومؤقتة، حيث يستطيع اكثر من حاسوب آلي ان يستخدم هذا العنوان للاتصال بالأنترنت، وغالبا ما يمنح هذا النوع المؤقت من العناوين لحواسيب الافراد الذين لا يحتاجون لاتصال دائم بالأنترنت[[67]](#footnote-67).

ب-تقنية رسائل ICMP:-

ذكرنا فيما سبق ان رسائل ICMP هي رسائل معلوماتية تستخدم للتبليغ عن الاخطاء، وهذه هي احدى وظائف ICMP، واما الوظيفة الثانية فهي الاستعلام.

**1-التبليغ عن الاخطاء:**

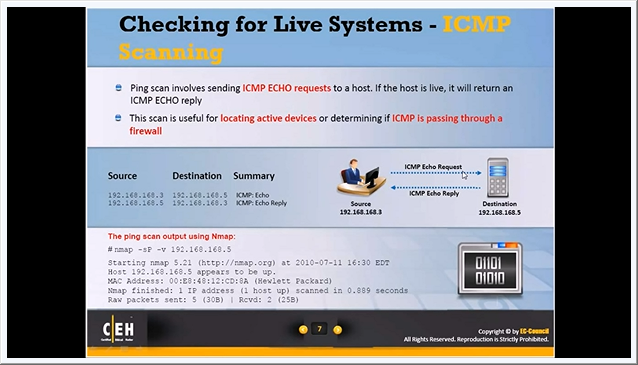
الوظيفة الرئيسية لرسائل ICMP هي التبليغ عن الاخطاء من مختلف الانواع، وهى تستخدم من قبل الاجهزة الوسطية التي تربط بين اجزاء الشبكة (الموجهات مثلا) لتبليغ النظام المرسل بوجود خطأ من نوع ما في عملية الارسال، مثل عدم امكانية الوصول الى النظام المرسل اليه، او وجود عنوان غير صحيح الرسالة، او امتلاء ذاكرة الموجه بالرسائل مما يجعله يرسل رسالة ICMP الى النظام المرسل من اجل ابطاء سرعة ارساله، او غير ذلك من الاخطاء، ويلاحظ هنا ان هذا النوع من الرسائل هو عبارة عن رد فعل على مشكلة حدثت في عملية الارسال، ويقوم بتوليد هذه الرسائل الاجهزة الوسطية مثل الموجهات[[68]](#footnote-68).

2**-رسائل الاستعلام:**

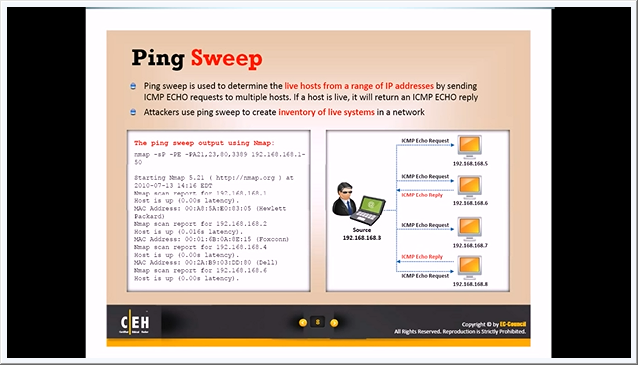
اما الوظيفة الثانية لرسائل ICMP فهي نقل طلبات المعلومات والردود عليها من نظام الى اخر، وهذا النوع من الرسائل يولده نظام الجهاز المصدر نفسه، وليس الاجهزة الوسطية، ومن اهم انواع هذه الرسائل ما يسمى برسائل طلب الصدى ورد الصدى، وتتضمن هذه الرسائل السؤال نظام معين فعالا ام لا،، اي عما اذا كان نظام ما متصل يعمل على الشبكة ام لا، وهذه الرسائل كما قلنا يستطيع ان يولدها الجهاز المصدر، ويستخدم لذلك اداة تسمى PING تأتي مع طقم بروتوكولات Tcp/ip وتستخدم لمراقبة وقياس اداء الشبكة.

* **الاداة Ping:-**

تقوم اداة ping بتوليد رسالة طلب الصدى وارسالها الى النظام الهدف، وتكن رسالة طلب الصدى من نوع Echo، وهي تسال النظام الهدف ما اذا كان لازال فعالا؟، وفي حالة ما اذا كان النظام الهدف فعالا ومتصلا بالأنترنت فانه يجيب برسالة من نوع Echo reply ومعنى هذه الرسالة: نعم انا فعال، اما في حالة ما اذا كان النظام غير فعال فانه يأخذ مهلة ولا يرد، وفي هذه الحالة اما يكون النظام الهدف في حالة ايقاف التشغيل، او في حالة عدم الاستجابة[[69]](#footnote-69).

****

يتطلب هذا النوع من المسح من الجاني استخدام اداة ping لكل كمبيوتر على حدة، بحيث ان الاداة عندما تتلقى الرد او الجواب من الكمبيوتر الاول ينتقل الجاني الى الكمبيوتر الثاني وهكذا، وهذا الامر قد يكون مناسبا لشبكة صغيرة، اما الشبكات الكبيرة فان المسح بهذه الطريقة سيستغرق ساعات وايام، ولذلك فانه في الشبكات الكبيرة تستخدم اداة متطورة اكثر وهىping sweep، وادوات اخرى مماثلة، وتقوم اداة ping sweep بإرسال عدة طلبات icmp في وقت واحد الى عدة اجهزة في الشبكة وتنتظر الرد، والاجهزة التي تكون فعالة وتعمل على الشبكة هي فقط التي سوف ترد [[70]](#footnote-70).

****

تعرض الادوات التي تستخدم المسح المتوازي الخرج في شكل قائمة بالأجهزة المفحوصة وبجوار كل منها علامة تبين ما اذا كان فعالا ام لا.

وفي الادوات ذات الواجهات النصية كأداة fping يعرض الخرج على شكل قائمة بعناوين ip، وبجوار كلا منها كلمة live بالنسبة للانظمة الفعالة.

* **الخطوة الثانية: مسح المنافذ**

تهدف عملية مسح المنافذ الى التعرف على المنافذ المفتوحة في النظام الهدف، وبالتالي الخدمات العاملة التي تنصت على تلك المنافذ، ويمثل المنفذ المفتوح خدمة عاملة على النظام مثل خدمة تلنت، او خدمة ftb، او غير ذلك من الخدمات، وبعد اكتشاف المنافذ المفتوحة يقوم الجاني باستغلال أي منفذ مفتوح لاختراق النظام المستهدف، ولفهم خطوة مسح المنافذ فانه يجب علينا الالمام ولو بشكل موجز بأساسيات برتوكولات الشبكة ونظام العنونة في هذه البروتوكولات لنها تتصل مباشرة بهذه العملية، وسوف نوضح ذلك في الفقرات التالية:

**مبادئ البروتوكولات[[71]](#footnote-71):-**

البروتكول بوجه عام هو آلية الاتصال المتعارف عليها او المتفق عليها بين طرفين، او عدة اطراف، فمثلا الية تحقيق الاتصال بين شخصين يودان الحديث مع بعضهما هي المصافحة بينهما، والية تحقيق الاتصال بين مكتب البريد عبر رسائل البريد هي وضع الرسالة في مظروف وعنونته وختمة بطوابع، وهكذا.

وفي مجال الحاسب الآلي فان بروتوكولات الشبكة يقصد بها الية تحقيق الاتصال بين كمبيوتر شبكي، وبين كمبيوتر اخر او عدة كمبيوترات متصلة بالشبكة، تأخذ الية الاتصال بين كمبيوتر واخر داخل الشبكة شكل مراحل او طبقات متدرجة، تتكون من برامج ومعدات مختلفة داخل الجهاز المرسل، والجهاز المستقبل، فعلى سبيل المثال عندما يريد المستخدم ارسال رسالة بالبريد الالكتروني الى مستخدم اخر متصل بنفس الشبكة او بشبكة اخرى، او عندما يكتب احد المستخدمين عنوان موقع ما على المتصفح او محرك البحث، ويضغط زر البحث او زر الوصول الى الموقع، فان الرسالة او طلب الموقع لا يذهب مباشرة الى النظام الوجهة، بل يمر نزولا بكومة من الطبقات داخل جهاز الحاسب الالي المرسل، وتتكون هذه الطبقات من برامج ومعدات، يقوم كلا منها بأداء وظيفة ومهمة معينة في الرسالة او طلب الاتصال الخارج من الجهاز من اجل تهيئته للأرسال عبر الاسلاك الى النظام الموجهة. تسمى آلية الاتصال بين كمبيوتر واخر عبر الشبكة ببروتوكولات الشبكة، وهى لازمة في كل اتصال داخل الشبكة، حتى ولو كانت الشبكة تتكون من حاسبين اثنين فقط، فلابد من اتباع هذه الآلية من اجل اجراء اتصال بين حاسبين اثنين في شبكة أو أكثر، ويتم اتباع البروتوكولات واليات الاتصال من خلال قيام الشركات المصنعة بصناعة المعدات والبرامج وفق مواصفات هذه البروتوكولات، بحيث يؤدي كل برنامج وكل واحدة من المعدات، الوظائف المرسومة له في بروتوكولات الشبكة بكل دقة، وفي النهاية تشكل هذه الاليات كومة او مكدس من الطبقات تمتد من بطاقة الشبكة الى البرنامج التطبيقي الذي يستعمله المستخدم مباشرة.

اهم نماذج هذه الطبقات، وتحديد وظائفها، هو نموذج osi المرجعي، ووفقا لهذا النموذج، فان طبقات البروتوكولات داخل كل حاسب الي تنقسم الى سبع طبقات على النحو التالي:

1. طبق البرامج ( Application)
2. طبقة التقديم Presentation))
3. طبقة الجلسة Session) )
4. طبقة الارسال والنقل (Transport)
5. طبقة الشبكة (network)
6. طبقة وصلة البيانات او ربط البيانات (Duta link)
7. الطبقة المادية Physical))

واكثر هذه الطبقات وخاصة العليا هي عبارة عن برامج موجودة في نظام التشغيل، وبعضها كالطبقة المادية هي عبارة عن معدات واسلاك.

تزود هذه الطبقات العديد من الوظائف ولكن الوظيفة الاهم هي تحضير رسالة البيانات وتحزيمها وتهيئتها للأرسال، فعلى سبيل المثال عندما يقوم المستخدم بكتابة رسالة البريد الالكتروني، فانه بعد الانتهاء من كتابة الرسالة يقوم بضغط زر ارسال، وهنا فان الرسالة لا تذهب عبر قناة مباشرة الى النظام المرسل اليه، بل تمر نزولا في مكدس او كومة من طبقات البروتكولات داخل الجهاز المرسل، على شكل رسالة بيانات، وتقوم الطبقات الموجودة في الجهاز المرسل بتجهيز هذه الرسالة للأرسال، واهم العمليات التي تقوم بها طبقات البروتوكولات هي تجزئة الرسالة الى حزم أو وحدات من البيانات، وتغليف الحزم او وحدات البيانات وعنونتها.

فمثلا عندما يولد برنامج تطبيقي طلبا معينا، وليكن مثلا برنامج البريد الالكتروني، فانة بروتوكول طبقة البرامج يقوم بتحزيم الطلب، وهو هنا رسالة البريد الالكتروني في شكل وحدة بيانات، ويرسلها الى طبقة النقل على النحو التالي:

طلب البرنامج

البرنامج\_\_\_\_\_\_\_\_\_\_\_\_طلب البرنامج

التقديم\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

الجلسة\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

الارسال\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

الشبكة\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

وصلة البيانات\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

المادية\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

­­عندما تصل وحدة البيانات الى طبقة الارسال او النقل تقوم طبقة النقلTCP بإضافة راس الى وحدة البيانات، وتصبح وحدة البيانات الواردة من طبقة البرنامج هي الحمولة في الطلب الجديد.

**طلب البرنامج**

البرنامج\_\_\_\_\_\_\_\_\_\_\_\_\_\_طلب البرنامج

التقديم\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

الجلسة\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

الارسال\_\_\_\_الراس\_\_\_\_\_الحمولة\_\_\_\_

الشبكة\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

وصلة البيانات\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

المادية\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

بعد ان يضيف بروتكول طبقة الارسال رأس الى حمولة البيانات، يمرر وحدة البيانات الجديدة نزولا الى طبقة الشبكة، وعندها يقوم بروتكول طبقة الشبكة باضافة راس امام رأس طبقة الإرسال، وعندها تصبح وحدة البيانات المكونة من طلب البرنامج الاصلي ( رسالة البريد الالكتروني )، ورأس طبقة الارسال، هي الحمولة في وحدة البيانات الجديدة الخاصة بطبقة الشبكة.

البرامج\_\_\_\_\_\_\_\_\_\_\_ \_\_ طلب البرنامج

التقديم\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_

الجلسة\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

الارسال\_\_\_ الرأس \_\_\_\_\_ الحمولة

الشبكة\_\_ الراس \_\_\_الحمولة\_\_\_\_\_\_\_\_

وصلة البيانات\_ \_ \_\_

المادية\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

بعد ذلك تمرر طبقة الشبكة وحدة البيانات الجديدة الى الطبقة التي تحتها وهي طبقة ربط البيانات، وهذه المرة تقوم طبقة ربط البيانات بإضافة راس وتذييل الى وحدة البيانات.

البرامج\_\_\_\_\_\_\_\_\_\_\_\_ \_ طلب البرنامج

التقديم\_\_\_\_\_\_\_\_\_ \_\_\_\_ \_\_\_\_\_\_\_\_\_

الجلسة\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

الارسال\_\_\_ \_\_\_\_ الرأس \_ الحمولة

الشبكة\_\_\_\_\_\_\_ الرأس \_\_\_\_\_الحمولة\_

وصلة البيانات\_ الرأس الحمولة \_\_\_ التذييل

المادية\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

بعد ذلك يتم تحويل رزمة البيانات النهائية النهائية الى اشارات ملائمة لوسط الارسال، فاذا كانت وسط الارسال كابل الياف ضوئية فانه يتم تحويل الرزمة الى نبضات ضوئية صالحة للمرور في كابل الألياف، واذا كان كابل الارسال هو كابل كهربائي تناظري فانه يتم تحويل وحدة البيانات الى اشارات تناظرية صالحة للمرور عبر الكابل الكهربائي، وهكذا، وتسمى العملية التي يضيف لها كل بروتوكول معلومات وراس الى وحدة البيانات التي يتلقاها من الطبقة التي فوقة بعملية تغليف البيانات، وعندما تصل رسالة البيانات (وهي في هذا المثال رسالة بريد الإلكتروني) الى الجهاز المستقبل، تقوم طبقة البرتوكولات في الجهاز المستقبل بعملية معاكسة، حيث تقوم كل طبقة بإزالة راس التغليف الذي أنشأته الطبقة المناظرة لها في جهاز المرسل، حتى تصل الى المستخدم المرسل اليه كما هي عندما جهزت من طبقة البرنامج في الجهاز المرسل، أي تصل اليه فقط وحدة البيانات الاصلية بدون الاضافات والرؤوس والتذييلات.

ولذلك فان المستخدم النهائي الذي يتعامل مع طبقة التطبيقات، سواء كان مرسلا أو مستقبلا، لا يشعر ولا يرى ما تقوم به هذه الطبقات من اعمال تجهيز وتغليف وارسال، فأعمال ووظائف طبقات البروتوكولات هي وظائف مخفية عن المستخدم، وكل ما يراه المستخدم هو المنتج الاصلي.

* **نظام العنونة داخل البروتوكولات ومفهوم المنافذ:**

الان بعد ان تم تجهيز وحدة البيانات وتغليفها وايصالها الى الطبقة المادية او طبقة الاسلاك، كيف تعرف وحدة او رسالة البيانات هذه وجهتها والنظام المرسلة اليه؟

عندما يتم تمرير وحدة البيانات الى طبقة الشبكة، فان طبقة الشبكة تقوم باضافة راس اليها، الراس الذي تضيفه طبقة الشبكة هو عنوان ip للجهاز المرسل اليه او النظام الوجهة، وتسير وحدة البيانات في الاسلاك الى حين ان تصل الى الجهاز الذي يحمل عنوانIP الذي وضعته طبقة الشبكة، في الطريق هناك اجهزة وسطية تسمى الموجهات هي التي تقوم بقراءة العنوان وتوجيه الرسالة الى عنوان الجهاز ووجهتها من خلال جداول عناوين الاجهزة الموجودة في الموجهات.

وعندما تصل رسالة أو وحدة البيانات الى الجهاز المرسل اليه تظهر مشكلة اخرى، وهى كيف تتوجه هذه الرسالة الى البرنامج المحدد داخل الجهاز المتلقي من بين الحجم الكبير للبرامج الموجودة في نظام الحاسب، ونظام التشغيل الذي يعمل فيه؟

للاجابة عن هذا السؤال فانه يجب ان نتذكر ان وحدة او رسالة البيانات التي يتم ارسالها من المستخدم يتم تمريرها اولا الى طبقة الارسال، وان طبقة الارسال TCP تقوم بإضافة رأس اليها، ان الرأس الذي تضيفه طبقة الارسال TCP يتضمن عنوان البرنامج المرسلة اليه وحدة البيانات، وعلى ذلك فان رسالة البيانات تصل اولا الى عنوان IP للجهاز المتلقي، ثم تتوجه بعد ذلك الى عنوان البرنامج او الخدمة المرسلة اليه، فاذا كانت وحدة البيانات عبارة عن رسالة بريد الالكتروني فإنها تتوجه الى عنوان برنامج البريد الالكتروني الموجود في النظام المتلقي، واذا كانت عبارة عن طلب اتصال مع خدمة الويب فإنها تتوجه الى عنوان خدمة الويب داخل الحاسب الالي المتلقي.... الخ، وتسمى عناوين البرامج والخدمات داخل الحاسب الآلي بالمنافذ، وتوجد في كل نظام منافذ متعددة بحسب عدد البرامج والخدمات المشغلة في هذا النظام.

ولتقريب الصورة يمكن تشبيه الحاسب الالي بشركة كبيرة يوجد بها عدد كبير من المكاتب المختلفة، وعندما يريد أي شخص مثل زبون معين الاتصال بالشركة فانة يقوم اولا بالاتصال برقم التحويلة العام للشركة، ثم يقوم موظف التحويلة بإحالته الى رقم اخر يمثل مكتب معين الذي يريده، فرقم الشركة العام او رقم التحويلة يمثل عنوان IP للجهاز، وأرقام المكاتب تمثل عناوين البرامج والخدمات، او المنافذ.

يبين الشكل التالي اتصال من برنامج معين في الحاسب رقم 1 الى برنامج اخر في الحاسب رقم 2 [[72]](#footnote-72):

برامج

طبقة النقل منفذ

طبقة الشبكة عنوانip

الطبقة المادية

برنامج

طبقة النقل

طبقة الشبكة

الطبقة المادية

منفذ

عنوانip

**حاسب رقم 2 حاسب رقم 1**

* **آلية ربط البرامج الخدمات بالمنافذ:**

عندما يريد الجاني ان يرسل رسالة الى برنامج معين مثل برنامج تلنت، او برنامج مخدم الملفات FTB، اوغير ذلك من البرامج، فكيف يعرف ان هذا البرنامج او المخدم مربوط الى منفذ معين؟

يتم ربط الخدمات والبرامج الى منافذ محددة آليا بواسطة نظام التشغيل، فهو الذي يقوم بربط كل خدمة او برنامج الى منفذ محدد، مثلا مخدم الملفات FTP يربط الى المنفذ رقم21 وبرنامج تلنت يربط الى المنفذ رقم23.

وبعض المنافذ تكون ثابتة دوما، بمعنى ان نظام التشغيل يربط الخدمة او البرامج الى منفذ محدد دائما في كل مرة يتم فيها تشغيل الحاسب الالي، مثلا مخدم الملفات يتم دائما ربطة بالمنفذ رقم 21ومخدم الويب يتم دائما ربطة بالمنفذ رقم 80، ويستخدم هذا الاسلوب بالنسبة للبرامج والخدمات التي تحتاج دائما الى اتصال مستمر، والى توفير خدماتها طوال اليوم، مثل مخدم الملفات ومخدم الويب، وفي هذه الحالة تمثل هذه الارقام عناوين او منافذ ثابتة لا تتغير، ويتم حفظ هذه العناوين في ملفات واماكن معروفة في نظام التشغيل، فاذا اراد الجاني ان يعرف البرنامج والمنفذ الخاص به فانه يستطيع معرفة ذلك بالرجوع الى هذه الملفات، ومن امثلة ذلك الملف ect/services على نظام unx والذي يستعرض البرامج والخدمات التي تم ربطها بشكل دائم الى منافذ معينة، وارقام هذه المنافذ، هذا بالنسبة للخدمات والبرامج التي تحتاج الى خدمة الاتصال طوال اليوم، اما بالنسبة للخدمات النادرة الاستخدام فان ربطها الى منفذ معين طوال اليوم يستهلك طاقة الحاسب الالي، بالاضافة الى ان الاكثار من المنافذ المفتوحة طوال الوقت يسمح للجناة بالاختراق والدخول من أي منفذ من هذه المنافذ، أي انه يسهل مهمة الجاني ويصعب عملية الحماية، ولذلك فانه غالبا يتم اللجوء الى مخدم وكيل يرتبط بهذه المنافذ ذات الخدمات النادرة، وعندما يتلقى المخدم الوكيل اي طلب اتصال لبرنامج معين على عنوان الخدمة، فان المخدم الوكيل يقوم بإنشاء اتصال بين العميل وبين البرنامج او الخدمة النادرة المطلوبة.

غالبا ما يتم التعرف على عناوين او منافذ الخدمات من خلال برنامج يسمى مخدم الاسماء name server اومخدم الدليل Derectory server، ويتضمن هذا البرنامج قاعده بيانات داخلية تحتوي على الخدمات مع ارقام المنافذ الخاصة بها، فاذا اراد مستخدم معين معرفة عنوان او منفذ خدمة معينة، فانه يرسل رسالة الى مخدم الاسماء او الدليل يحدد فيها اسم الخدمة، فيرد علية مخدم الاسماء بالعنوان او المنفذ الخاص بهذه الخدمة، وفي هذا النموذج فانه عندما يتم انشاء خدمة جديدة، فان عليها ان تسجل نفسها عند مخدم الاسماء معطية اياه اسم الخدمة، وعنوان او رقم المنفذ الخاص بها، ويضيف مخدم الاسماء هذه المعلومات الى قاعدة بياناته الداخلية[[73]](#footnote-73).

يوضح الجدول التالي بعض الخدمات الشائعة يستخدمها المحترفون للاختراق مع ارقام المنافذ الخاصة بها[[74]](#footnote-74):

|  |  |
| --- | --- |
| Service | Pert number |
| ftp data trimester | 20 |
| ftp contrd | 21 |
| SsH | 22 |
| TELENT | 23 |
| Smtp (e-mail) | 25 |
| DNS | 53 |
| HTTP | 80 |
| HTTPS | 4 43 |

* **تحديد المنافذ في بروتكول TCP:**

تتضمن برمجيات tcp/ip لائحة بالمنافذ الاكثر شيوعا داخل ملف نصي يسمى services، وهذه اللائحه اعدتها مؤسسة (lana) لتعيين ارقام الانترنت ونشرتها على موقعJena org/assignment/port Number و، وعندما تصل وحدة البيانات الى النظام المتلقي تقوم برامج Tcp/ipالموجودة فيه بقراءة حقل رقم المنفذ في الوحدة، ثم تسلم وحدة البيانات الى البرنامج او الخدمة المقترن بذلك المنفذ [[75]](#footnote-75).

**كيف يتم الاتصال بمنفذ معين:**

عندما يريد الجاني ارسال رسالة الى المنفذ معين فانه يستعمل تركيبة من عنوان ip ورقم المنفذ، فيقوم اولا بكتابة عنوان ip للجهاز، ثم يضع نقطتين ثم يقوم بكتابة رقم المنفذ، مثال على ذلك:

192-168-2-10:21

رقم المنفذ عنوانip

وفي معظم الحالات يكون عناوين URLعبارة عن اسماء من مجالات اسماء DNS، وليس عناوين IP، وفي هذه الحالات يتم كتابة اسم الدومين ثم نتبعه بنقطتين ثم رقم المنفذ كالتنسيق السابق، مثلا العنوان السابق سيكون على الشكل التالي:

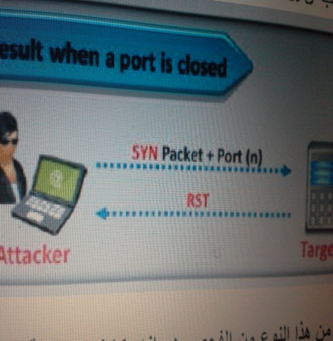
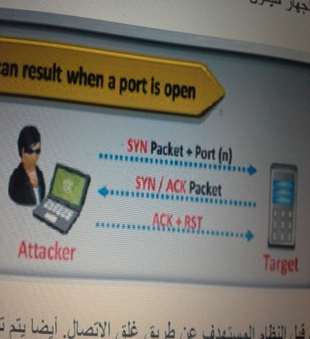
FTP-datum com:21

رقم المنفذ اسم النظام في DNS

وعندما نكتب عنوان URT فانه لا يحتاج عادة الى تحديد رقم منفذ، لان معظم البرامج تفترض انك تريد الاتصال بالمنفذ المشهور، فمثلا في متصفح الانترنت تتصل كل العناوين URL التي تكتبها الى المنفذ 80 وهو المنفذ الشائع لملقم ويبHTTP، وارقام المنافذ الشائعة هي في الغالب تستخدم في الملقمات او خوادم الشركات والمؤسسات، لان هذه الملقمات هي التي تحتاج الى اتصال وخدمات دائمة طوال اليوم، وبالتالي تحتاج الى عناوين وارقام منافذ ثابتة، اما بالنسبة لبرنامج العميل وهو برنامج الجاني في هذه الحالة، فانه يستخدم منافذ عشوائية سريعة الزوال، لأنه لا يحتاج الى اتصال دائم، وينتقي برنامج العميل عادة رقم منفذ بشكل عشوائي يسمى رقم منفذ سريع الزوال لاستعماله اثناء الاتصال بأحد الملقمات، وبما ان ارقام المنافذ المشهورة من الشائعات التي تديرها مؤسسة LANA هي فقط من1-1023، فان ارقام المنافذ العشوائية التي يستخدمها برنامج العميل او برنامج الجاني تحمل دائما قيما اكبر من 1024، وعندما يتلقي الملقم وحدة البيانات من برنامج العميل فانه يعرف رقم المنفذ العشوائي من حقل المنفذ المصدر في راس TEP، وبالتالي يرسل رده على طلب العميل على هذا المنفذ.

* **التعرف على البرامج او الخدمات العاملة:**

اشرنا فيما تقدم ان نظام التشغيل يقوم آليا يربط البرامج والخدمات بالمنافذ الشائعة لها، وعندما يتم ربط برنامج او خدمة معينة بالمنفذ الشائع لها يصبح هذه الخدمة في حالة انتظار لاي اتصال من اى عميل، ويطلق على البرامج المربوطة الى المنافذ الخاصة بها انها في حالة انصات، وقد ذكرنا فيما تقدم انه لا يتم ربط كل الخدمات او البرامج بالمنافذ الخاصة بها لان ذلك يستنفذ طاقة النظام، بالاضافة الى انه يسهل اختراق النظام من قبل الجناة، ولكي يتمكن الجاني من معرفة أي الخدمات مربوطة الى المنفذ الخاص بها وبالتالي في حالة عمل او انصات، فانه يستخدم ما يسمى بالمصافحة الثلاثية، تتألف عملية المصافحة الثلاثية من تبادل ثلاث رسائل بين جهاز العميل وبين المنفذ المحدد في جهاز الملقم، في البداية يرسل جهاز العميل رسالة SYN الى المنفذ المحدد وينتظر تلقي الجواب او الرد من ذلك المنفذ في الملقم، اذا كان المنفذ في حالة انصات أي جاهز للاتصال فانه يعيد جواب برسالة ACT/SYN، ومعنى هذه الرسالة ان البرنامج او الخدمة تعمل غلى المنفذ وجاهزة للاتصال، أو بعبارة اخرى ان المنفذ مفتوح للدخول، اما اذا رد الملقم برسالة RST/ACT فان ذلك يشير عادة الى ان المنفذ لا ينصت أي مغلق، بمعنى ان الخدمة او البرنامج المحدد لا يعمل على نظام الهدف[[76]](#footnote-76)، يوضح الشكل التالي هذه العملية:



* **تقنية رسائلSYN:**

رسائل هذه التقنية لا تحمل أي بيانات، وهي تستخدم من قبل خدمات وبرامج بروتكول tcp للتحقق من صحة الاتصال قبل البدء بإرسال أو تلقي البيانات بين اجهزة الحاسب الآلي، ويتميز برتكولtcp بانه بروتكول اتصالي المنحى، ومعنى انه اتصالي انه قبل اجراء أي تبادل للبيانات يقوم هذا البرتوكول انشاء قناة اتصال بين البرنامج المرسل وبين البرنامج المتلقي، وذلك للتأكد من ان البرنامج المتلقي يعمل وبالتالي جاهز لتلقي البيانات، ولذلك فان خدمات وبرامج tcp مثل البريد الالكتروني، والويب، وخدمة الملفات،وغيرها، تقوم دائما بإنشاء الاتصال قبل تبادل أي بيانات.

جوهر عملية انشاء الاتصال هو التأكد من وصول البيانات الى النظام المتلقي من خلال تلقى اشعار بالوصول، ذلك ان بعض وحدات البيانات المرسلة قد تفقد في الطريق، او تتعرض للإتلاف، او التشويه، وعندئذ تستخدم تقنية رسائل syn لتلاقي هذه الحوادث من خلال ضبط عملية الارسال، ويتم ضبط عملية الارسال على النحو الاتي:

1. يعرف البرنامج المرسل ان البرنامج المتلقي فعال ويعمل وقادر على تلقي او تحميل البيانات.
2. يقوم البرنامج المتلقي والمرسل بوضع ارقام تسلسلية لعملية الارسال، بحيث تحمل كل وحدة بيانات رقم معين.
3. في حالة عدم وصول وحدة البيانات معينة من النظام المتلقي يعرف ذلك من خلال فارق الارقام الواردة الية، واذا وجد إي نقص في سلسلة الارقام يقوم بأشعار البرنامج المرسل بذلك، فيقوم البرنامج المرسل بإعادة ارسال وحدة البيانات المفقودة.
4. يتم ارسال وحدات البيانات عبر الاسلاك بطريقة غير مرتبة ولذلك يستخدم النظام المتلقي الارقام التسلسلية لإعادة تجميع وحدات البيانات بالشكل الصحيح [[77]](#footnote-77).

* **ادوات مسح المنافذ:**

**التقنية**: تقوم ادوات مسح المنافذ بأرسال حزم syn الى المنفذ في النظام الهدف وتنتظر الجواب، فاذا كان المنفذ مفتوح فانه يرسل اشارة موافقة على طلب الاتصال هي اشارة ACT/SYN، اما اذا كان المنفذ مغلق فانة يغلق الاتصال مباشرة.

بعض ادوات المسح تقوم بمسح المنافذ التي يتم تحديدها وكتابتها من قبل الجاني ، ولكن الادوات الاكثر شهرة مثل NMUP تقوم بمسح المنافذ الشائعة والمشهورة افتراضيا داخل الجهاز الهدف، هناك ادوات كثيرة للقيام بعملية مسح المنافذ وتعتبر NMUP من افضل واشهر الادوات ويستخدمها المخترقون بمختلف اختصاصهم واغراضهم، ولذلك فسوف نقتصر على تناول هذه الاداة.

* **الاداة NMUP:**

الاداة NMAPهي كما قلنا افضل واقوى ادوات مسح المنافذ واكثرها شهرة، وعند وضع عنوان IP في اداةNMAP وتشغيلها على النظام الهدف تقومNMAP بمسح المنافذ المشهورة والشائعة افتراضيا وهي الف منفذ شائع مشهور، ولكن يمكنك تحديد خيار المسح لكل المنافذ في النظام الهدف، وبالتالي لن تقتصر NMAP على المنافذ الشائعة في النظام، ولكن ستقوم بمسح كل المنافذ الموجودة في النظام[[78]](#footnote-78).

يمكن لnmap ايضا ان تقوم بمسح شبكة بأكملها حيث يمكن ببساطة تحديد نطاق المسح بين عنوانين ip، فتقوم NMAP بمسح العنوانين معهما جميع الانظمة الموجودة على الشبكة والتي تقع بين العنوانين[[79]](#footnote-79)، مثلا:

192-168-1-1 الى 192-168-1-254

في حالة اذا كانت الانظمة عشوائية وغير مرتبة، فانه يمكن ان تقوم NMAP بمسح الانظمة الهدف من خلال استخراجها من أي ملف نصي مكتوبة فيه، ولذلك فانة يمكن بسهولة كتابة العناوين في ملف نصي وترك NMAP تقوم بمسح هذه العناوين من خلال هذا الملف النصي.

**نتائج مسح NMAP:**

الخرج الذي تعيده NMAP يتضمن انواع عديدة من المعلومات مثل:

1. المنافذ المفتوحة والخدمات العاملة عليها.
2. اصدارات البرامج والتطبيقات.
3. نوع نظام التشغيل.
4. بعض نقاط الضعف المشهورة مثل الاباتش.
5. تحديد مالك العملية هل هو مستخدم اوحساب مدير[[80]](#footnote-80).

## المبحث الثالث: مرحلة التعداد

\***تمهيد:**

يقوم الجاني في مرحلة الاستطلاع بجمع معلومات عن النظام الهدف، ومن اهم المعلومات التي يجب ان يقوم بجمعها بالاضافة الى عناوينip، حسابات المستخدمين والمدراء، وترجع اهمية هذه الحسابات الى ان انظمة التشغيل الشبكية تعتمد آلية امان تسمى آلية التحقق من الصحة، وبمقتضى هذه الآلية فانه لا يمكن الدخول الى أي نظام تشغيل شبكي الا بواسطة اسم مستخدم وكلمة مرور، ولذلك فان الجاني لا يمكنه ان يذهب بعيدا فوق طبقة tcp للنظام الهدف الا اذا كان لديه اسم مستخدم صالح وكلمة مرور، وفي الاحوال التي لا يتمكن فيها الجاني من الحصول على اسماء المستخدمين او المدراء في مرحلة الاستطلاع، فانه يلجا الى ما يسمى بالتعداد، ويختلف التعداد عن مرحلة الاستطلاع ومرحلة مسح المنافذ في مستوى التدخل، اذ ان التعداد يتطلب اتصال مباشر ونشط مع النظام.

**مفهوم التعداد:**

التعداد هو عملية جمع وتصنيف اسماء المستخدمين والمشاركات والخدمات وموارد الشبكة[[81]](#footnote-81)، ويأتي التعداد بعد عملية مسح المنافذ ويتم فيه اجراء اتصالات واستعلامات نشطة الى النظام الهدف لغرض كسب معلومات الحسابات[[82]](#footnote-82)، وهذا الاتصال النشط الذي يتم في التعداد هو الذي يميزه عن مرحلة مسح المنافذ، وبما ان تقنيات التعداد تتصل بنظام التشغيل فإنها تختلف بحسب نوع نظام التشغيل المستخدم في النظام الهدف، لذلك سنتناول فيما يلي نوعين من التعداد، تعداد ويندوز وتعداد يونكس

**اولا: تعداد ويندوز**

هناك نوعين من التعداد في نظام التشغيل ويندوز، تعداد الجلسة الخالية، وتعداد برتوكول الادارة البسيط SNMP.

**1- تعداد الجلسة الخالية**

يقصد بالجلسة الخالية الدخول على النظام الهدف من دون اسم مستخدم او كلمة مرور.

تتطلب آلية التحقق من الصحة في نظام التشغيل ويندوز وجود حساب مستخدم وكلمة مرور للدخول الى النظام، ولكن يمكن للجاني الدخول الى نظام ويندوز واستخراج معلومات منه من دون حاجة الى حساب مستخدم من خلال بعض نقاط الضعف الموجود في نظام ويندوز، وهي خدمات Netbios وsmp، وهما تعتبران من الخدمات القياسية في النظام، ونقطة الضعف في هذه الخدمات انها يتيح الاتصال المباشر وتاسيس جلسة بدون كلمة مرور واسم المستخدم، كما انها تقوم باعادة معلومات حول النظام حتى للمستخدمين الغير مخولين عبر المنافذ القياسية لها وهي ، 135،137،139 والمنفذ 445، ولذلك فان الجاني يقوم بإرسال طلب انشاء جلسة خالية الى احد المنافذ الخاصة بهذه الخدمات مع عنوان ip، وبدلا عن ان يكتب اسم المستخدم وكلمة المرور، يقوم فقط بكتابة علامة داخلها فراغ هكذا" "، واذا نجح الجاني بإنشاء جلسة الاتصال، فانه يحصل على قناة مفتوحة يمكن بعدها ان يستخدم ادوات وتقنيات مختلفة تقوم باستخراج ثروة من المعلومات عبر هذه القناة، اهمها حسابات المستخدمين وموارد المشاركة في النظام[[83]](#footnote-83).

تعداد الجلسة الخالية هو نوعين رئيسيين، تعداد NETBIOS وتعداد SMP

**النوع الاول: تعداد NETBIOS:-**

**مفهوم خدمة NETBIOS:** هي خدمة تعيين اسماء لأجهزة الكمبيوتر في الشبكة المحلية تقابل عناوين IP لهذه الاجهزة، وهذه الخدمة هي خدمة خاصة بنظام التشغيل ويندوز، وتستخدم فقط في شبكات ويندوز، وتشبه هذه الخدمة نظام اسماء النطاق DNS من حيث انها تتضمن اسماء للأجهزة مقابلة لعناوين IP، الا ان العناوين الاسمية في نظام DNS تستخدم لتعريف جهاز الكمبيوتر في شبكة الانترنت بأكملها، ولذلك فهناك منظمات مركزية تمنح هذه العناوين لضبط عمليه منح العناوين الاسمية وتلافي التكرار، واما العناوين الاسمية لخدمة NETBIOS فهي تعرف الاجهزة في الشبكة المحلية فقط، بمعنى ان اسم NETBIOS يستخدم لتعريف جهاز معين لأغراض الاتصال بين الاجهزة في شبكة محلية ولا يصلح للاستخدام في الانترنت، فخدمة NETBIOS لا يمكنها الاتصال بالأنترنت، ولذلك اذا ارادت أي شبكة تستخدم NETBIOS ان تتصل بالأنترنت فان عليها ان تضيف نظام DNS الى جانب NETBIOS او بدلا عنه، في انظمة التشغيل Windows الحديثة قل الاعتماد على هذا النظام وانشات هذه الانظمة ما يسمى بالدليل النشط، ومع ذلك فانة بقى يستخدم في نطاق الشبكة المحلية [[84]](#footnote-84).

تعمل خدمة NETBIOS على المنافذ 135، 137، 138، 139، واذا وجد الجاني احد هذه المنافذ يعمل فانه يحاول مباشرة انشا جلسة الاتصال واستخراج المعلومات منه، لذلك فان هذه الخدمة هي اول خدمة يحاول الجاني استغلالها.

تعيد خدمة NETBIOS عبر واجهة برمجية خاصة الكثير من المعلومات للمستخدم ولو كان مجهولا وغير مخول، ومن اهم هذه المعلومات اسماء المستخدمين، انواع المشاركات، واذونات الوصول الخاصة بالمستخدمين، وغير ذلك من المعلومات المهمة.

**ادوات تعداد NETBIOS:-**

هناك العديد من الادوات التي تستخدم لتعداد NETBIOS وهذه الادوات تعتمد على سطر الاوامر أي واجهة النصية، ومن اهم هذه الادوات NBSTAT، NBTSCANوهي تقوم باستخراج جدول الاسماء من NETBIOS وتفريغه الى جهاز الجاني وذلك عن طريق انشاء جلسة خالية او حتى بدون جلسة خالية[[85]](#footnote-85).

**النوع الثاني: تعداد smp:**

**مفهوم خدمة smp:** هي خدمة مشاركة الملفات في نظام التشغيل windows، وتتولى هذه الخدمة ادارة الملفات وتنظيم عملية الوصول الى الملفات الموجودة في الملقم، فاذا اراد المستخدم الوصول الى ملف معين في ملقم الملفات، فانه يستخدم رسائل smp التي تقوم بإنشاء جلسة اتصال بين الجهازين، وتحقق من صحة الوصول الى الملف[[86]](#footnote-86).

تتضمن خدمة مشاركة الملفات smp: تحديد انواع المشاركات، اعطاء اسماء للمشاركات المختلفة، وتحديد اذونات الوصول 1، وهي تعمل على المنافذ 139او445، ونقطة الضعف في هذه الخدمة انها تتضمن – كخدمة NETBIOS واجهة برمجية تعيد معلومات غنية عن النظام عن طريق المنافذ 445او tcp 139، حتى الى مستخدمين غير مسجلين، والخطوة الاولى للوصول الى الواجهة البرمجية الخاصة بهذه الخدمة هي من خلال انشاء جلسة فارغة في احد المنافذ 445 or tcp 139 التي يتبين انها منصتة من خلال عملية مسح المنافذ السابقة، بعدها يحصل المهاجم على قناة اتصال مفتوحة مع هذه الخدمة ويستطيع نهب اقصى حد ممكن من المعلومات باستخدام تقنيات وادوات مختلفة، ومن هذه المعلومات، المشاركات والمستخدمين والمجموعات ومفاتيح التسجيل، ونحو ذلك[[87]](#footnote-87).

**ادوات تعداد smp:-**

كما في NETBIOS، فان هناك ادوات عدة يمكن ان تنفذ تعداد smp، ومن اهم هذه الادوات على الاطلاق اداة dumpsec، والتي تستخدم لتعداد المشاركات من خلال انشاء جلسة خالية بسيطة، وهي تستطيع استخراج لائحة بالمستخدمين وامتيازاتهم، واذونات المشاركات سواء كانت هذه المشاركات مخفية او غير مخفية[[88]](#footnote-88).

**2-تعداد SNMP**

**مفهوم snmp [[89]](#footnote-89):-**

Snmp هو عبارة عن بروتكول يسمى بروتكول الادارة البسيط، يستخدم لجمع المعلومات محددة عن مكونات الشبكة مثل الويب، والخدمات والاجهزة الوسطية مثل الموجهات....الخ.

بروتكول snmp آلية تتضمن عدة عناصر تعمل من اجل جمع المعلومات، المكون الاهم في هذه الالية هو برامج الوكلاء، وهي عبارة عن برامج توزع على كل مكونات واجهزة الشبكة، ويقوم كل برنامج من هذه البرامج بجمع معلومات عن الجهاز الذي هو فيه، ومن هذه المعلومات اسماء المستخدمين والمشاركات وحالة الاتصال ونحو ذلك، وبعد ان يقوم البرنامج الموجود في الجهاز بجمع هذه المعلومات يقوم بتخزينها في قاعدة بيانات فرعية في ذات الجهاز تسمى قاعدة بيانات mib، وترسل قواعد بيانات mib بصفة دورية الى وحدة ادارة وتحكم قد تكون جهاز كمبيوتر او برنامج مخدم [[90]](#footnote-90)، يمثل البرنامج الوكيل الموجود في كل جهاز من اجهزة الشبكة الطرف المرسل للمعلومات، ويسمى بمحطة agent، ويعمل هذا البرنامج على المنفذ "161"UDP.

المكون الثاني في الية SNMP هو نظام الاداة او الموقع المركزي في الشبكة الذي ترسل الية دوريا قواعد بيانات MIB والمعلومات الاخرى المطلوبة، ونظام الادارة هو عبارة عن حاسب مركزي يشغل احد البرمجبات الخاصة بإدارة SNMP، وعادة يوجد نظام ادارة وحيد ل SNMP في كل مجموعة من المضيفات (الحواسيب) وتسمى هذه المجموعة بالجمعية (Community)، وتقسيم خدمة snmp الى جمعيات (مجموعات) يساعد على ادارة الشبكات الضخمة والكبيرة من خلال تجزئتها الى عدة جمعيات لكل جمعية نظام ادارة snmp مستقل.

العنصر الثالث والاخير في بروتكول snmp هو الرسائل التي يستخدمها هذا البروتكول لنقل الاستعلامات والردود، ورسائل snmp يستخدمها نظام الادارة لطلب معلومات محددة من الوكلاء (برامج المحطات المضيفات ) agent، من انواع هذه الرسائل الرسالة get وهي تطلب معلومات محددة، والرسالة next get وهي تطلب معلومات اضافية للمعلومات المرسلة، دائما الذي يطلب المعلومات عن حالة وسجل المكونات هو نظام الادارة، اما المحطة agent فهي التي تجيب وترد على هذه الطلبات، الرسائل التي يرسلها نظام الادارة هي عبارة عن اوامر يصدرها نظام الادارة، ويتم تبادلها على المنفذ 161، وعندما ما ترد المحطات Agent على الاستعلامات تجلب المعلومات المطلوبة من قواعد mip الموجودة فيها وترسلها الى المنفذ 161 لنظام ادارة أو مدير SNMP.

وتتضمن قواعد MIP، انواع مختلفة من المعلومات منها على سبيل المثال:

1. المشاركات SHARS
2. المستخدمين USERS
3. تسجيل الخولLOGEN
4. جلسات العمل SESSIONS
5. الاحصائيات STATICALL

**كيف يعمل التعداد SNMP:-**

كما تقدم فان كل مجموعة من الاجهزة والحواسيب التي تتضمن برامج الوكلاء يكون لها خدمة او نظام ادارة SNMP واحد مستقل، وذلك لتسهيل ادارة الشبكات الكبيرة، وتسمى المجموعة التي تتبع نظام ادارة SNMP بالجمعية، وتدعى الجمعية بالاسم الخاص بها، والاسم الافتراضي الخاص بالجمعية هو Public، وجميع المكونات داخل خدمة snmp واحدة تنتمي لهذا الاسم، ولذلك جميع البرامج الوكيلة داخل الاجهزة تستجيب بشكل افتراضي الى اي طلب يستخدم اسم الجمعية الافتراضي Public، ولذلك فإنه يمكن للجاني ان يستخدم اسم الجمعية الافتراضي لأرسال طلب بالمعلومات التي يريدها وسترد عليه البرامج الوكيلة بالمعلومات المطلوبة من قواعد MIP، واذا تم ضبط الاعدادات على اسم خاص للجمعية فان هذا يوفر سريه محدودة، لان البرامج الوكيلة agents لن تستجيب الا للطلبات الواردة من اعضاء هذه الجمعية ذات الاسم الخاص، ومع ذلك فان خدمة SNMP تظل عرضة لعملية انتحال ( ip spoofing )ipحيث يمكن للجاني ان ينتحل عنوان ip الخاص بالمدير او بأحد اعضاء الجمعية ثم يطلب المعلومات التي يريدها وسيحصل عليها من برامج الوكلاء[[91]](#footnote-91).

خدمة SNMP لا تتمتع باي نوع من انواع الامان والسرية، فالبيانات غير مشفرة، ولا توجد أي طريقة لمنع شخص ما من الدخول الى الشبكة واستكشاف اسماء وعناوين الجمعيات والاعضاء، وبالتالي انتحال أي عنوان منها وتلفيق طلبات مزورة باسمه الى برامج الوكلاء.

يستخدم الجناة في تعداد SNMP عدة ادوات تقوم بإرسال الطلبات وفقا لأي من التقنيات السابقة وجلب المعلومات الخاصة بأسماء المستخدمين ومشاركتهم، ومن هذه الادوات برنامج استعراض SNMP والمسمى SNMP URIL، كذلك برنامج الاستعراض الرسومي ip Net werk prowser [[92]](#footnote-92)، واداة oputils، وعدد اخر من الادوات.

**ثانيا: تعداد يونيكس**

هناك نوعين رئيسيين من التعداد في نظام التشغيل unix، تعداد المشاركات، وتعداد المستخدمين والمجموعات.

**1\_تعداد المشاركات:-**

1. **تعداد NFS:** خدمة NFS هي آلية مشاركة الملفات في نظام Lunix. unix، وتعمل هذه الالية على اساس نظام عميل \ملقم، وتتكون من برنامج يوجد في جهاز المستخدم ويسمى عميل، وبرنامج الملفات الموجود في الملقم او الخادم والذي يتضمن الملفات المشتركة، ويصل المستخدمين الى الملفات المشتركة الموجودة في الملقم عن طريق تثبيت برنامج العميل في اجهزتهم، حيث يتيح لهم هذا البرنامج فتح الملفات الموجودة في الملقم كما لو كانت موجودة ومخزنة لديهم في الجهاز.

ويلاحظ انه وفقا لنظام NFS فإن الملفات لا يتم فتحها في الملقم، وانما عند دخول المستخدم الى النظام تظهر له دلائل ملفات المشاركة، ويقوم الملقم بتزويد الملف الى جهاز العميل حيث يقوم بفتحه في جهازه وليس في الملقم[[93]](#footnote-93)57.

**ادوات تعداد NFS:** يعمل نظام ملفات NFS على المنفذ 2049، وعندما يكتشف الجاني من خلال عملية مسح المنافذ ان هذا المنفذ في حالة انصات، فانه يستخدم اداة من الادوات التي تستخدم لاستعراض دلائل ملفات هذا النظام، ومن هذه الادوات الاداة Showmount، وتقوم اداةshowmount بأمرين:

الاول: عرض قائمة بمجلدات المشاركة من خادم NFS [[94]](#footnote-94).

والثاني: سرد الاجهزة التي تصل الى الملفات المشتركة في النظام.

**ب\_تعداد SAMBA:**

سامبا هي مجموعه من البرامج التي تعتمد البروتكول smp، وهي تمكن انظمة التشغيل غير ويندوز من الاتصال باستعمال هذا البروتكول، ويتم تثبيت برامج sampa في ملقم يونيكس او ليونيكس، وهي توفر خدمة مشاركة الملفات والطباعة، وتمكن المستخدمين من الوصول الى الملفات الموجودة على الملقم كما لو كانت في ويندوز[[95]](#footnote-95).

**الادوات المستخدمة:** يمكن تعداد الملفات في ملقم samp في نظام التشغيل unix اوlunix باستخدام الادوات المذكورة سابقا في تعداد smp في ويندوز.

**ج\_تعداد SNMP:**

في الانظمةUnix وlunix التي تشغل بروتكول snmpفانه يمكن تعداد المشاركات في هذه الانظمة باستخدام الاسم الافتراضي للجمعية public على نحم ما تقدم في تعداد snmp في نظام ويندوز، ومن الادوات التي تستخدم في تعداد snmpفي unix وlunix الاداة snmp walk وهي تأتي مع العديد من حزم sampa unix.

**2\_تعداد المستخدمين والمجموعات:-**

هناك ادوات عديدة تستخدم لتعداد المستخدمين والمجموعات في نظام unix اوlunix وهذه الادوات هي عبارة عن اوامر تنفذ على نظام unixوlunix، ومن امثلتها:

1. **الاداةfinger:-**

الاداة finger هي من اقدم الادوات التي تقدم معلومات عن المستخدمين في نظام لتشغيل unix، وتقوم هذه الاداة بتعداد المستخدمين، كما انها تقوم بعرض ملف او مجلد hom الذي يتضمن المستخدمين وقت الدخول، ووقت الخمول، وتأتي اهمية ملف hom في انه يعطي فكرة عن المدير او حساب الجهاز في يونيكس والذي يقوم بعملية المراقبة[[96]](#footnote-96)، كذلك فان معلومات الملف قد تستخدم في عملية الهندسة الاجتماعية، وتنصت الخدمة finger على المنفذ 79، وعندما يكتشف الجاني ان المنفذ 79 في حالة انصات فانه يقوم بكتابة الامر finger ثم بعدها يظهر ناتج هذا الامر، ويتضمن هذا الناتج اسم تسجيل الدخول، الترمنال، وقت تسجيل الدخول، ووقت الخمول قائمة المستخدمين على المضيف الهدف[[97]](#footnote-97).

**ب- الاداة rpcclient**:

وتستخدم هذه الاداة لتعداد المستخدمين في نظام lunix، وهى اداة من ادوات الملقم sampa، وعند طباعة الامر rpcclient تقوم الاداة بعرض اسماء المستخدمين وبرامج Rpc المسجلة على المضيف، وتعمل هذه الخدمة غلى المنفذ القياسي 139 وهو منفذ خدمة sampa.[[98]](#footnote-98)

## المبحث الرابع: الدخول الى النظام

الدخول الى النظام الضحية يتم اما عن طريق كسر كلمة المرور في احدى خدمات الاتصال عن بعد، أو عن طريق استغلال ثغرة أو منطقة ضعف برمجية في جدار النظام الهدف، الطريقة الاولى لا صعوبة فيها ويمكن تشبيهها بكسر الابواب والنوافذ، اما الطريقة الثانية الخاصة باستغلال الثغرات البرمجية فهي اصعب في التحديد، لأنها احيانا تبدوا كأنها ثغرة مفتوحة في الجدار يمر عبرها الجاني، واحيانا اخرى تبدوا كأنها منطقة ضعيفة في جدار النظام يقوم الجاني بخرقها والدخول منها، واختيار هذا التكييف او ذاك يترتب عليه بلا شك آثار خطيرة بالاعتبار الشرعي بشأن توافر شرط هتك الحرز.

**المطلب الاول**

**كسر كلمة المرور**

من خلال المراحل السابقة الاستطلاع، المسح، التعداد، يكون الجاني قد تمكن من جمع معلومات كثيرة ومهمة عن الهدف، ومن اهم هذه المعلومات حسابات المستخدمين والمجموعات، التطبيقات والخدمات، الاتصال عن بعد، نوع انظمة التشغيل، وهذه المعلومات هي معلومات اساسية ولازمة للدخول الى النظام الهدف والسيطرة على موارده.

في البداية فان الجاني يستخدم أي برنامج من برامج الاتصال عن بعد من اجل الوصول الى النظام الهدف، فالوصول الى أي كمبيوتر بعيد لا يتم الا من خلال برامج محددة توفر خدمة الاتصال عن بعد، وتقوم هذه البرامج بأرسال طلب الاتصال الى النظام الهدف وتنتظر الجواب، وتتضمن انظمة التشغيل ويندوز ويونيكس الكثير من البرامج المعروفة التي توفر وظيفة الاتصال عن بعد، ومنها على سبيل المثال برنامج تلنت telent، وبرنامج خادم الملفات ftp، برنامج الويب web،...الخ، وقد كان بعض هذه البرامج يأتي مستقلا في الماضي، اما الآن فإنها تأتي ضمن باقة برامج بروتكول Tcp/ip التي تأتي مدمجة مع انظمة التشغيل الحديثة، وبوجه عام تتكون برامج الاتصال عن بعد مثل التلنت telent والFTP من مكونين برمجيين، المكون الاول يسمى العميل او الزبون وهو يوجد في جهاز المستخدم، والمكون الثاني يسمى الخادم او الملقم وهو يوجد في سيرفرا المؤسسة او الشركة، وعندما يريد الجاني الاتصال بالنظام الهدف يدون عنوان ipاو اسم الجهاز للنظام الهدف في مربع البرنامج، ثم يرسل طلب الاتصال الى ذات البرنامج في الخادم او الملقم[[99]](#footnote-99) ، غالبا بطلب البرنامج الموجود في الملقم من المستخدم "وهو هنا الجاني" اسم مستخدم وكلمة مرور لكي يمكنه من انشاء الاتصال والدخول الى الخادم، واذا كان الجاني قد حصل على لائحة حسابات المستخدمين من خلال مراحل الاستطلاع والتعداد، فانه يدون اسم المستخدم ثم يقوم بمحاولة تخمين كلمة المرور من اجل ان يتمكن من الدخول الى النظام الهدف، وهناك ادوات عديدة تساعد الجاني في تخمين كلمة المرور كما سنرى لاحقا.

اذا نجح الجاني في تخمين كلمة المرور باستخدام أي اداة من ادوات كسر كلمة المرور فانه سيتمكن من الدخول الى النظام الهدف، ومع ذلك فان هذا الدخول يعتبر من حيث الاثر كلا دخول، لان الوصول الى موارد النظام وخاصة المعلومات الحساسة لا يتاح للمستخدمين العاديين، فمهما استطاع المستخدم الدخول الى الجهاز الهدف فانه لن يتمكن من الوصول الى الملفات الهامة في النظام، لان انظمة التشغيل تقصر حقوق الوصول الى الملفات والمعلومات الحساسة على مدير النظام فقط، او من يمنحه مدير النظام صلاحية الوصول الى ملف معين او قراءته او تحميلة او نقلة، فاذا حاول المستخدم وهو هنا "الجاني " البحث عن ملف معين مهم فانه لن يجده لان النظام التشغيل يخفي الملفات الهامة عن المستخدمين العاديين، وحتى اذا تمكن من الوصول الى الملف الهدف فانه لن يتمكن من فتح الملف وقراءته او تحميلة او نقلة او نسخة، لان هذه الصلاحيات يخولها نظام التشغيل لمدير النظام فقط administor، او لمن يمنحة مدير النظام هذه الصلاحية[[100]](#footnote-100).

لذلك فان الجاني بعد ان يتمكن من الدخول الى النظام الهدف فانه يعمل على رفع حسابة الى امتياز مدير النظام، اما من خلال اضافة نفسة الى مجموعة المدراء، او من خلال انشاء حساب مدير جديد، او بأي طريقة من الطرق، وتسمى هذه العملية بهجوم رفع الامتياز، وبمجرد ان يحصل الجاني على امتياز مدير فان جميع موارد النظام وملفاته الهامة تصبح تحت رحمته وفي متناول يده.

وفقا لما تقدم سيتم تناول الدخول عبر خدمات الاتصال عن بعد على خطوتين رئيسيتين: الاولى كسر كلمات مرور هذه الخدمات، والثانية هجوم رفع الامتياز.

**الخطوة الاولى: كسر كلمة المرور لخدمات الاتصال عن بعد:**

وفقا لهذه الطريقة فان الجاني يقوم بمهاجمة شبكة خدمات الاتصال عن بعد العاملة في النظام الهدف، في البداية يقوم الجاني بعملية مسح منافذ على النظام الهدف من اجل معرفة المنافذ المفتوحة في هذا النظام، اذا اكتشف الجاني ان احد المنافذ مفتوحة فان ذلك يعني ان خدمة ما في خدمات الاتصال عن بعد في حالة عمل وتنصت على هذا المنقذ، عندها يقوم الجاني بمهاجمة هذه الخدمة ومحاولة الاتصال بها، وتسال الخدمة المتصل اولا عن اسم المستخدم وكلمة المرور، فجميع خدمات الاتصال عن بعد تتطلب مستوى من السرية والامان يتمثل باسم المستخدم وكلمة المرور، وبما ان الجاني لدية قائمة بأسماء المستخدمين جمعها من المراحل السابقة، فانه يدون اسم المستخدم ثم يبدا عملية تخمين كلمة المرور، وهناك العديد من الادوات التي تساعد الجاني في تخمين كلمة المرور بصورة مؤتمتة، ومن اشهر هذه الادوات الاداة هيدراhydra والاداة ميدوسا medusa، وتسمى هذه الادوات ادوات كسر كلمة المرور على الانترنت، وتعتمد هذه الادوات على تجربة تركيبات مختلفة من اسم المستخدم وكلمة المرور محفوظة في ملف لديها، وعند استخدام أي اداة من هذه الادوات فان الجاني يقوم بتسجيل عنوانip للنظام الهدف ونوع الخدمة المطلوب الاتصال بها، وعند ذلك ترسل الاداة تركيبة من اسم المستخدم وكلمة المرور الى الخدمة، اذا كانت هذه التركيبة خاطئة، او كان احد الامرين: اسم مستخدم او كلمة المرور غير صحيح، فان الاداة تعرض رسالة خطأ ويفشل الدخول، تقوم الاداة بعد ذلك بإرسال تركيبة اخرى من اسم مستخدم وكلمة مرور، ثم يتكرر هذا الامر الى ان تنجح الاداة في العثور على كلمة المرور الصحيحة او تستنفذ كل التخمينات الموجودة فيها [[101]](#footnote-101).

- **التلصص على كلمة المرور:** في بعض الحالات يمكن للمهاجم ان يحصل على الدخول الى النظام الهدف من خلال السطو على بيانات تسجيل الدخول التي تمر عبر اسلاك الشبكة، عندما يتبادلها المستخدمون الشرعيون مع الملقمات لتسجيل دخولهم.

بعض الخدمات ضعيفة الامان وتمرر معلومات عبر الشبكة على هيئة نص عادي مقروء بشريا، وبالتالي يمكن للجاني استعمال اداة sniffer لالتقاط هذه المعلومات وبخاصة معلومات تسجيل الدخول لأي مستخدم واستعمالها بالتالي في الحصول على دخول غير شرعي الى النظام، ومن امثلة الخدمات التي لا تستعمل التشفير وتمرر معلوماتها كنص عادي: خدمة ftp وخدمةsmtp وخدمة http [[102]](#footnote-102).

وحتى في الخدمات التي تستعمل تقنيات التشفير، فان هناك ادوات متخصصة تقوم بالتقاط بيانات الدخول التي يرسلها المستخدمون الشرعيون عبر الشبكة، ثم تقوم بفك تشفيرها عبر استخدام تقنية الهندسة العكسية، ومن هذه الادوات الاداة lophcracke [[103]](#footnote-103).

**الخطوة الثانية: هجوم رفع الامتياز:**

في بعض الحالات قد يتمكن للجاني من الدخول الى النظام الهدف باسم مدير النظام ويحصل على كل الامتيازات على النظام، ويتمكن من السيطرة عليه والوصول الى أي معلومات يريدها، وهذه الحالات تحدث اما لنجاح الجاني في التلصص على كلمة المرور لمدير النظام اثناء مرورها عبر الشبكة، واما لكون كلمة المرور الخاصة بمدير النظام كلمة سهلة يسهل تخمينها وكسرها، ولكن الغالب هو ان الجاني يدخل الى النظام باسم مستخدم عادي وليس باسم مدير النظام،لان كلمة المرور الخاصة بمدير النظام تكون معقدة صعبة الكسر، وتحتاج الى فترات طويلة لتخمينها بخلاف كلمات المرور الخاصة بالمستخدمين العاديين، فالمستخدم العادي يلجأ غالبا الى اختيار كلمات مرور سهلة يسهل علية حفظها، مثل الكلمات التي تتعلق باسمة او اسماء اقربائه او الهوايات او الاشياء التي يحبها او نحو ذلك، وهذه الكلمات يسهل تخمينها وكسرها من قبل المهاجم باستخدام ادوات الكسر التي تعتمد على قواميس من الكلمات المحفوظة بها جمعت من قبل شركات، او مهاجمين اخرين، خلال عدة سنوات.

وعندما يدخل المهاجم الى النظام بحساب مستخدم عادي فانه لن يتمكن من الوصول الى الملفات الهامة والحساسة الموجودة فيه، اما لأنه لايراها اصلا، واما لأنه لا يستطيع فتحها، ويرجع ذلك الى سياسة الامان التي تتبعها انظمة تشغيل الشبكات، والتي تقصر صلاحية فتح الملفات \_ وحتى رؤيتها \_ على مدير النظام فقط او مستخدمين محددين ومعينين، وبوجه عام فان انظمة تشغيل الملقمات تعتمد على سياسة امان من عدة عناصر على النحو التالي[[104]](#footnote-104):

1. تحديد انظمة تشغيل الشبكات المستخدمين الذين يحق لهم الدخول الى نظام التشغيل، ويتم ذلك من خلال خاصية تعرض عند تركيب نظام تشغيل الشبكة تترك وتتيح لمدير النظام خيار تحديد مستخدمين معينين للاتصال بالنظام، او عدم تحديد مستخدمين معينين وترك الحق في الدخول مفتوح لأي شخص، وعندما يختار مدير النظام مستخدمين محددين فانه يقوم بتسجيلهم على نظام التشغيل ولا يتمكن أي شخص غيرهم من الدخول الى النظام، ولذلك فان على المهاجم ان ينتحل أي اسم من اسماء المستخدمين المسجلين، ويحاول كسر كلمة مروره ليتمكن من الدخول الى النظام.
2. يحدد نظام التشغيل لكل مستخدم من المستخدمين الذين تم تسجيلهم في الشبكة دورا محددا سواء بالنسبة للملفات، او بالنسبة لعمليات محددة، فمثلا قد يمنح النظام مستخدم معين حق قراءة ملف او ملفات محددة وعندها لا يملك الوصول الى أي ملف اخر غير ما حدد له، ولا يمتلك حق اخر غير القراءة مثل حقوق التعديل او الكتابة، وقد يمنح مستخدم آخر حق القيام بإجراء او عملية محددة، وعندها لا يمكنه القيام باي اجراء اخر، وهكذا.
3. بالنسبة لكل ملف او برنامج فان نظام التشغيل يتيح تحديد حقوق الوصول الى هذا الملف او البرنامج، مثل تحديد الاشخاص الذين يمكنهم الوصول الى الملف او البرنامج بحيث لا يستطيع غيرهم الوصول اليه، كما انه حتى بالنسبة للمستخدمين الذي يحق لهم الوصول الى ملف معين، فان نظام التشغيل يتيح تحديد صلاحيه كل مستخدم بالنسبة لهذا الملف، هل هي قراءة فقط ام قراءة مع كتابة ام تحكم كامل وهكذا، كذلك يتيح نظام التشغيل جعل بعض الملفات مخفية وغير مرئية للمستخدمين.

معايير لسياسة الامان هذه موجودة بوجه عام في انظمة التشغيل ويندوز ويونيكس، مع بعض الاختلافات التي يقتضيها اختلاف طبيعة النظامين، وبالنتيجة لذلك فان أي مهاجم ينجح في انتحال اسم مستخدم معين والدخول الى النظام الهدف سواء كان ويندوز او يونيكس، لن يتمكن من تحقيق الاهداف التي يريدها، ولن يستطيع الوصول الى الملفات والمعلومات الهامة، ولذلك فان المهاجم سوف يلجا الى طريقة تساعده على الحصول على الامتيازات اللازمة للسيطرة على النظام وبالتالي الوصول الكامل لكل الملفات التي يريدها، وتسمى طرق الحصول على هذه الامتيازات بهجوم رفع الامتياز، وقد يسعى المهاجم الى رفع امتيازه افقيا، أي بالحصول على امتيازات مستخدم اخر اكثر منه صلاحية في الحقوق والاجراءات، ولكن الغالب في العمل هو ان يسعى المهاجم الى الحصول على امتيازات مدير النظام من اجل تحقيق السيطرة الكاملة على النظام الهدف، والحصول على كل المعلومات الموجودة فيه، وهناك ادوات وطرق عديدة تستخدم لرفع الامتياز، وهي تختلف من نظام تشغيل الى اخر، وسنقتصر علي تناول طرق رفع الامتياز الرئيسية المرتبطة باختراق نظام التشغيل ويندوز.

**الطريقة الاولى: استخدام ادوات رفع الامتياز**

ا**لأدوات getadmin والاداة sechele**

**التقنية المستخدمة:** التقنية التي تستخدمها هذه الادوات هي الارتباط بعملية تمتلك امتيازات مدير النظام، ومن ثم ادراج شيفرة خبيثة في هذه العملية واستغلال الامتياز الخاص بالعملية لتشغيل الشيفرة الخبيثة المدرجة، وهذه الشيفرة الخبيثة تعمل عند تشغيلها على اضافة اسم المستخدم الى مجموعة المدراء Administrator، وبالتالي يصبح المستخدم الذي انتحله المهاجم احد مدراء النظام ويستطيع بسهولة الوصول الى كافة المعلومات والملفات الواردة فيه.

ان صلاحية انشاء العمليات والاجراءات في أنظمة تشغيل الشبكات مقصورة على مدير النظام فقط، او من يفوضه مدير النظام بالقيام بعمليات محددة، وعندما يقوم مدير النظام بإنشاء عملية معينة مثلا انشاء جداول للبيانات ويريد تفويض احد المستخدمين بقراءة الجداول او اضافة او حذف احد الصفوف او الاعمدة، فان العملية التي يقوم بها هذه المستخدم المفوض لا تنفذ وفقا لحقوقه هو، ولكن تنفذ وفقا لامتيازات المدير او الشخص الذي انشأ العملية، فاذا قام المستخدم بحذف أو اضافة أحد الصفوف، فإن ذلك يجري وينفذ بإمتيازات مدير النظام لا بامتيازاته هو، فالقاعدة ان أي اجراء يقوم به المستخدم المفوض مثل القراءة او التعديل او الحذف، ينفذ بامتيازات مالك العملية ومنشأها، فاذا كان مدير النظام هو الذي انشأ العملية فان المستخدم ينفذها بامتيازات مدير النظام لا بامتيازاته هو[[105]](#footnote-105)، وهذه الثغرة يستطيع المستخدم استغلالها من اجل ادراج شيفرات خبيثة داخل هذه العملية وتنفيذها بامتيازات المدير[[106]](#footnote-106)، ومن اهم هذه الشيفرات الخبيثة، الشيفرة التي تعمل على اضافة اسم المستخدم المنتحل من قبل المهاجم الى مجموعة مدراء النظام، فهذه الشيفرة تنفذ كان مدير النظام هو الذي قام بها لانها تنفذ بامتيازاته.

طريقة ترقية الامتياز عن طريق ادراج شيفرة في عملية ذات امتيازات اصبحت منهجية عامة يستخدمها الهاكر، اما بأنفسهم او بواسطة ادوات معينة، ولكن بالنسبة للأدوات فان استخدامها يتطلب صلاحية معينة مثل صلاحية تحميل الاداة وتنفيذها داخل الجهاز، وهذه الصلاحية لا يملكها عاده المستخدم العادي الذي ينتحله المهاجم، وبالتالي يحتاج المهاجم الى وسائل اخرى لتحميل الادوات واستخدامها، ومن هذه الوسائل خدمات مشاركة الملفات الموجودة في الجهاز، والتي تسمح بشكل افتراضي بكل الصلاحيات من قراءة وتنفيذ وتحميل.

1. **الاداة getadmin:**

وهي عبارة عن برنامج صغير يضيف مستخدم الى مجموعة المدراء المحلية administrators من خلال ادراج شيفرة ذكية ضمن عملية تمتلك امتياز اضافة مستخدمين الى مجموعة المدراء.

وبما ان امتيازات المدير لازمة لفعل أي شيء داخل النظام الهدف فان المهاجم سيجد صعوبة في تنفيذ هذه الاداة عن بعد، ولكن يمكنه تنفيذ هذه الاداة من خلال تحميلها الى دليل قابل للكتابة مثل خدمة ftp التي تأتي مع سماحيات افتراضية في الكتابة والتنفيذ، وهذا يتطلب وجود خطا في اعدادات تكوين نظام التشغيل بما يسمح بترك مثل هذه السماحيات الافتراضية [[107]](#footnote-107).

1. **الاداة sechole:**

تقوم الاداة sechole بوظيفة مماثلة للأداة getadmin فهي تضيف المستخدم الى مجموعة المدراء local Administrator، وهى تستخدم نفس التقنية: الارتباط بعملية ذات امتياز ثم تشغيل شيفرة ضمن تلك العملية تقوم بإضافة المستخدم الحالي الى المجموعة Administrator [[108]](#footnote-108)، والعملية التي تمتلك امتياز اضافة مستخدم الى مجموعة المدراء هي عملية مدير نظام،لان مدير النظام هو وحدة الذي يمتلك هذه الصلاحية.

وتحتاج هذه الاداة الى امتيازات المدير لتحميلها وتنفيذها على النظام الهدف، ولكن يمكن تشغيل الاداةsechole عن بعد باستخدام الادلة والخدمات القابلة للكتابة، ومن هذه الخدمات ملقم معلومات الانترنت IIS من مايكروسفت، حيث يشتمل هذا الملقم على خدمةftp وhttp وهو يمتلك سماحيات افتراضية بالقراءة والكتابة والتنفيذ، ولذلك يمكن تحميل الاداة secholeالى احد دلائل IIS وتنفيذها بواسطته[[109]](#footnote-109).

**استخدام بعض الخدمات في تثبيت ادوات رفع الامتياز:**

هناك العديد من الخدمات التي توفر للمستخدمين القدرة على تحميل وتثبيت ملفات وبرامج عن بعد، في النظام الهدف، فمثلا اذا تمكن الجاني من كسر كلمة المرور والدخول الى خدمة نقل الملفات ftp فان هذه الخدمة تضع تحت تصرفه عدد من اوامر نظام الملفات في جهاز الملقم، ومن اهمها الصلاحيات والسماحيات الخاصة بجلب الملفات من النظام الهدف الى جهاز الجاني، او تحميل الملفات من جهاز الجاني الى النظام الهدف وتثبيتها عليه، مع صلاحيات وسماحيات هامة اخرى،، واما الخدمة تلنت telnet فهي تسمح للجاني بتحميل أي برامج الى النظام الهدف وتنفيذها عليه، وكذلك البحث عن أي ملفات مهمة موجودة فيه[[110]](#footnote-110)، كذلك خدمة http تمكن المستخدم ايضا من تحميل البرامج والملفات على ملقم ويب wep وتنفيذها عليه.

هذه السماحيات والامكانيات في تحميل البرامج والملفات والادوات على النظام الهدف تأتي مع هذه الخدمات بشكل افتراضي، وعادة ما تترك على حالها بسبب اخطاء في تكوين النظام، وهى بعض الوسائل التي قد يستخدمها الجاني لتحميل ادوات رفع الامتياز السابقة وتنفيذها على النظام الهدف، وتأتي بعض هذه الخدمات مع ملقم معلومات ميكروسوفت iis مع السماحيات افتراضية لها.

**الطريقة الثانية:** **استخدام برنامج طروادة**

تعمل تقنية برنامج طروادة المستخدمة في هجوم رفع الامتياز على اساس خداع مدير النظام بجعله ينفذ برنامج صغير يرفع امتيازات المهاجم، وهو يظن انه ينفذ برنامج اخر من البرامج المفيدة داخل نظام التشغيل، وفي هذه الحالة يتنكر البرنامج الضار والمؤذي والذي يرفع الامتيازات تحت اسم احدا برامج وادوات نظام التشغيل، بحيث لا يستطيع مدير النظام التمييز بينه وبين البرنامج الاصلي، فيقوم بالضغط عليه وتنفيذه وهو يظن انه البرنامج الاصلي الذي يريده، وهذه التقنية منهجية عامة تتبعها معظم فيروسات الحاسب الالي، وهي تعتمد على نقطة ضعف في اسماء ملفات البرامج في انظمة التشغيل، وتتمثل نقطة الضعف هذه من طريقة تعامل نظام التشغيل مع الملفات التنفيذية EXE او COM التي تخزن فيها معظم البرامج والتطبيقات، فعندما يكتب مدير النظام او المستخدم اسم ملف معين يبحث نظام التشغيل عنه اولا في الملفات التنفيذية التي تنتهي ب COM، فاذا لم يجده فانه يبحث في الملفات التي تنتهي ب EXE، فاذا لم يجده ينتقل الى الملفات التي تنتهي باللاحقة FAT، وهذه الخاصية في البحث عن الملفات يستغلها القراصنة والمهاجمون من خلال انشاء ملف باسم مشابه لاحد الملفات التي تنتهي EXE، ولكن مع تغيير اللاحقة الى COM لينفذ اولا قبل الملف الاصلي، فاذا كتب مدير النظام، او أي مستخدم اخر، اسم الملف فان نظام التشغيل يستدعي اولا الملف الذي يحمل هذا الاسم وينتهي ب COM (وهو هنا الملف الزائف)، فاذا لم يجده فانه يبحث عن ملف بهذا الاسم في الملفات التي تنتهي ب EXE [[111]](#footnote-111).

يمكن للمهاجم مثلا ان ينشئ البرنامج تحت اسم مشابه لملف redgit وهو احد ملقمات في نظام تشغيل ويندوز، ويضع داخل الملف الزائف برنامج يرفع امتيازه وتضيفه الى مجموعة المدراء، ولكنة يغير الملاحقة EXE الى اللاحقة COM ليصبح COM REDGIT وبالتالي عندما ياتي مدير النظام ويكتب redgit في مربع البحث في سطر الاوامر، يبدا نظام التشغيل بالبحث عن هذا الاسم من الملفات التي تنتهي باللاحقة com ويجلب اليه لملف redgit com، فاذا قام المدير بالضغط عليه وتنفيذه، يتم تنفيذ برنامج المهاجم، ويتم اضافة المهاجم الى مجموعة المدراء rators. Administ[[112]](#footnote-112).

واذا كان الملف الاصلي ينتهي باللاحقة com فان المهاجم يستطيع ان يغير ويعدل اسم الملف الاصلي الى con بالn، وينشئ ملف زائف ينتهي بcom، وبالتالي يتم تنفيذ الملف الزائف وليس الاصلي.

وتوفر في خدمة ftp للمهاجم صلاحيات كثيرة من اهمها صلاحية تعديل اسماء ملفات النظام.

ويلاحظ ان ملف البرنامج الزائف يتم تنفيذه خلال ثوان قليلة ثم بعد ذلك ينتقل التنفيذ الى البرنامج الاصلي، وبذلك لا يشعر المستخدم او مدير النظام بانه قام بتنفيذ البرنامج الزائف او الفيروس.

* **الحصول على ملف كلمة المرور SAM**

اذا نجح المهاجم في الوصول الى مستوى مدير نظام محلي فان ذلك سوف يمكنه من السيطرة بدرجة كبيرة على احد انظمة الملقمات المحلية في شبكة المنظمة الهدف، ومع ذلك فان شبكة المنظمة تتكون من عدد من الملقمات المحلية والتي يعمل كل منها غالبا على اجهزة كمبيوتر مستقلة، وكسب السيطرة على احد هذه الملقمات لا يعني سوى كسب السيطرة على فرع صغير من الشبكة الكلية للمنظمة، ولذلك فان المهاجم لايزال بحاجة الى الوصول الى مستوى اداري اعلى من مستوى مدير محلي يمكنه من السيطرة على كل موارد وملقمات الشبكة، وفي انظمة تشغيل ويندوز سيرفر يمكن ان تحقق الوصول الكامل لكل موارد وملقمات الشبكة من خلال ما يسمى بوحدة تحكم الميدان، وهى عبارة عن ملقم مستقل يتولى التحكم في الوصول الى كل عناصر ومكونات شبكة المنظمة، وتخزن فيه كافة الحسابات وانواع كلمات المرور ومعلومات اخرى عن كافة البرامج والاجهزة التي في الشبكة الكلية للمنظمة، والسيطرة على وحدة تحكم الميدان تعني وضع الشبكة كلها تحت رحمة المهاجم وفي متناول يديه، ولذلك فان المهاجم سوف يتوجه في المرحلة التالية الى اختراق وحدة تحكم الميدان من خلال انتحال اسم أي مستخدم او مدير يكون له حساب صالح في وحدة تحكم الميدان، وبطبيعة الحال يوجد عدد من المستخدمين او المدراء في النظام المحلي يكون لهم حسابات في وحدة تحكم الميدان، يخزن نظام ويندوز كافة لوائح المستخدمين وكلمات المرور لكل ملقم في ملف خاص يسمى sam، وبما ان نظام ويندوز يخزن كافة حسابات المستخدمين ولوائح كلمات المرور الخاصة بالنظام المحلي في هذا الملف، فإن البحث فيه سيكشف بلا شك عن مستخدمين محليين لهم اعتمادات لدى وحدة تحكم الميدان، وبالتالي فان على المهاجم ان يقوم بالحصول على ملف SAM وان يحاول كسر تشفيره والبحث داخله.

بالإضافة الى ما تقدم فان ملف SAM يتضمن جميع حسابات الخدمات والبرامج التي تعمل في النظام المحلي، وبالتالي فان كسر هذا الملف يمكن المهاجم من السيطرة الى كافة الخدمات والبرامج في النظام المحلي ونشر نفوذة وأدواته داخل هذا النظام، لهذا فان كسر SAM هو طريقة للحصول على امتيازات اعلى في النظام المحلي.

1. **مفهوم الملف SAM:**

تخزن انظمة تشغيل ويندوز لوائح المستخدمين وكلمات المرور في النظام المحلي داخل ملف يسمى SAM، ولوائح المستخدمين هذه هي التي يتم اعدادها عند تركيب نظام تشغيل الشبكة وتثبيته في جهاز الكمبيوتر.

وبما ان هذا الملف يحتوي على معلومات حساسة فهو يحاط بإجراءات حماية غير عادية، فيتم تشفير محتوياته بأحدث تقنيات التشفير.وهو غير قابل للقراءة حتى من مدير النظام Administrators، ولا يقبل الفتح والعرض بالبرامج العادية، بل يحتاج لفتحه برامج مثل برامج الهاكر، كما انه يتم دائما اقفاله عند بداية تشغيل النظام حتى لا يتمكن أي شخص من الوصول اليه اثناء عمل النظام.

1. **طرق سحب الملف SAM:**

على الرغم من هذه الاجراءات والميزات الامنية فانه يمكن الوصول على ملف SAM بعدة طرق:

أ\_اعادة التشغيل الى نظام تشغيل بديل: يمكن تجاوز تامين الملف SAM من خلال تحميل نظام تشغيل اخر على نفس الجهاز، وبما ان تامين الملف SAM في ويندوز يعمل فقط وقت عمل نظام تشغيل وينتهي عند اطفاءه، فانه اذا ظل ويندوز في حاله ايقاف لن يعمل القفل على الملف ويمكن بالتالي الوصول الى الملف واستخراجه من خلال نظام التشغيل البديل[[113]](#footnote-113).

وتتطلب هذه الطريقة الوصول المادي الى الجهاز الهدف لتركيب نظام التشغيل الجديد عليه من خلال القرص الضوئي.

ويلاحظ انه من خلال اعادة التشغيل الى نظام تشغيل اخر حذف حساب مدير النظام Administrators وانشاء حساب مدير نظام جديد على النظام الهدف خاص بالمهاجم، وبالتالي فهو يعد من طرق رفع الامتياز الذي يستخدمه المهاجم الموجود في الشبكة المحلية لرفع امتيازه الى مدير النظام79[[114]](#footnote-114).

ب\_سحب النسخة الاحتياطية للملف SAM: فعندما يتم تشغيل اداة اصلاح القرص الصلب يتم تلقائيا عمل نسخة احتياطية لملف SAM في المجلد Repair [[115]](#footnote-115)80، وتقوم اداة كسر كلمة المرور بسحب هذه النسخة ومحاولة فك تشفيرها.

ج\_استخراج بيانات الملف SAM: يمكن لمدير النظام استخراج وقراءة البيانات الخام لملف SAM، الغير قابله للعرض والفتح، من خلال بعض الادوات والبرامج التي تعمل بامتياز وصلاحيات مدبر النظام مثل الاداة LOPHT CRACK.

د\_التلصص على الشبكة: حيث يمكن التلصص على بيانات اسم المستخدم وكلمة المرور اثناء تبادلها في الشبكة لا جراء المصادقة على دخول المستخدمين [[116]](#footnote-116).

* **الادوات المستخدمة في سحب SAM:**

اداة Lophtcrack تقوم بسحب الملف SAM الخام عن بعد او سحب النسخة الاحتياطية، وتقوم ايضا بالتلصص على البيانات لمصادقة الدخول للمستخدمين والتقاطها اثنا مرورها عبر الشبكة، تعمل هذه الاداة بامتيازات مدير النظام، وعن بعد.

ايضا الاداة Pwdump2 تقوم بالحصول على الملف سام واستخراج بياناته عن بعد، ولكن يجب تنفيذها بشكل محلي عبر واجهة تخاطبيه او موجه اوامر النظام البعيد[[117]](#footnote-117).

* **كسر تشفير الملف SAM:**

1. **تقنيات كسر التشفير:**

هناك ثلاث تقنيات اساسية مستخدمة في فك تشفير الملفات بوجه عام، ومنها الملف SAM، وهذه التقنيات هي: هجوم القاموس، الهجوم الهجين، هجوم القوة المجردة.

* **هجوم القاموس:A dictionary Attack:-**

يعتمد هذا النوع من الهجوم على محاوله تخمين كلمة المرور من خلال البحث عنها في قوائم او قواميس تتضمن الاف الكلمات، واحيانا الملايين، وهذه القواميس تم اعدادها وتجميعها من قبل الهكر والمتسللين وبعض مواقع الانترنت خلال فترات طويلة تصل الى عدة سنوات، وعادة ما تتضمن هذه القواميس الكلمات المرتبطة بحياتنا الشخصية وهواياتنا، واعمالنا، والاشياء التي نحبها، وكل ما هو محتمل ان يستخدمه الشخص العادي ككلمة مرور عندما يسجل في النظام، وتقتصر منهجية هذا الهجوم على البحث في الكلمات التي توجد في القاموس ومحاولة تراكيب مختلفة لها، فلا تشمل محاولة تراكيب من ارقام ورموز، ولذلك فان هذا الهجوم يستخدم ضد كلمات المرور السهلة ولا يستخدم ضد كلمات المرور القوية والصعبة التي تحتوي على ارقام ورموز، وبعض هذه القواميس تأتي مخزنة في ادوات كسر كلمات المرور أي ان كل اداة تمتلك قاموس او عدة قواميس خاصة بها، كما يمكن تحميل الكثير من ملفات القواميس من بعض مواقع الانترنت ومن ثم تغذية ادوات كسر المرور بهذه القواميس المحملة [[118]](#footnote-118).

* **الهجوم الهجين Hybrid attack:-**

اذا فشل المهاجم في العثور على كلمة المرور من خلال هجوم القاموس فانه يحاول تقنيه اخرى تعتمد على اضافة رموز او ارقام الى كلمات المرور، او استبدال بعض الحروف بأرقام او رموز، وتسمى هذه التقنية بالهجوم الهجين Hybrid attack، وهي تعتمد على ملف القاموس الا انها تغير في كلمات القاموس اما بالإضافة لرموز وارقام، او التبديل، مثلا بعض الاشخاص قد يضيف رقم (1) الى كلمة السر الخاصة به ليجعلها قويه اكثر، وهنا فان تقنية الهجوم الهجين مصممة للعثور هذه الانواع المميزة من كلمات المرور[[119]](#footnote-119).

* **هجوم القوة الغاشمة: 13rute-farce attack:-**

وهذا الهجوم يجرب كل التراكيب المحتملة من الحروف الكبيرة والحروف الصغيرة والارقام والرموز، ولذلك فهو ابطأ الانواع الثلاثة بسبب العدد الكبير من التراكيب التي تتطلبها حروف كلمة المرور[[120]](#footnote-120)، وفي كثير من الاحيان يكون هذا الهجوم غير عملي لا نه يحتاج الى فترة طويلة قد تمتد الى سنوات [[121]](#footnote-121).

1. **الادوات المستخدمة:**

**الفرق بين ادوات كسر الخدمة عن بعد وادوات كسر SAM:**

تعتمد ادوات كسر التشفير بوجه عام على البحث في قواميس من الكلمات، وتخمين مئات او الاف الكلمات والتراكيب المختلفة للحروف والرموز والارقام حتى تتمكن من العثور على كلمة المرور الصحيحة، ومع ذلك فان ادوات كسر الخدمة عن بعد لا تحتاج لتنفيذها الى صلاحيات مدير النظام، بل يمكن لأي شخص استخدامها في الهجوم، وبمجرد ان يجد المهاجم اسم مستخدم صالح وعنوان ip يمكنه المباشرة في الهجوم على الخدمة المحددة بهذه الادوات، اما ادوات كسر SAM فهي تحتاج الى امتياز مدير النظام من اجل استخدامها وتنفيذها عن بعد، وبعض هذه الادوات يتطلب فضلا عن ذلك ان يتم تنفيذه بشكل تفاعلي اي من خلال موجة اوامر، وفيما عدا هذه الفروق فان جميع ادوات كسر التشفير تشترك في نفس المنهجية، سنتناول فيما يلي كمثال اداة كسر الملف سام Lophtarack SAM.

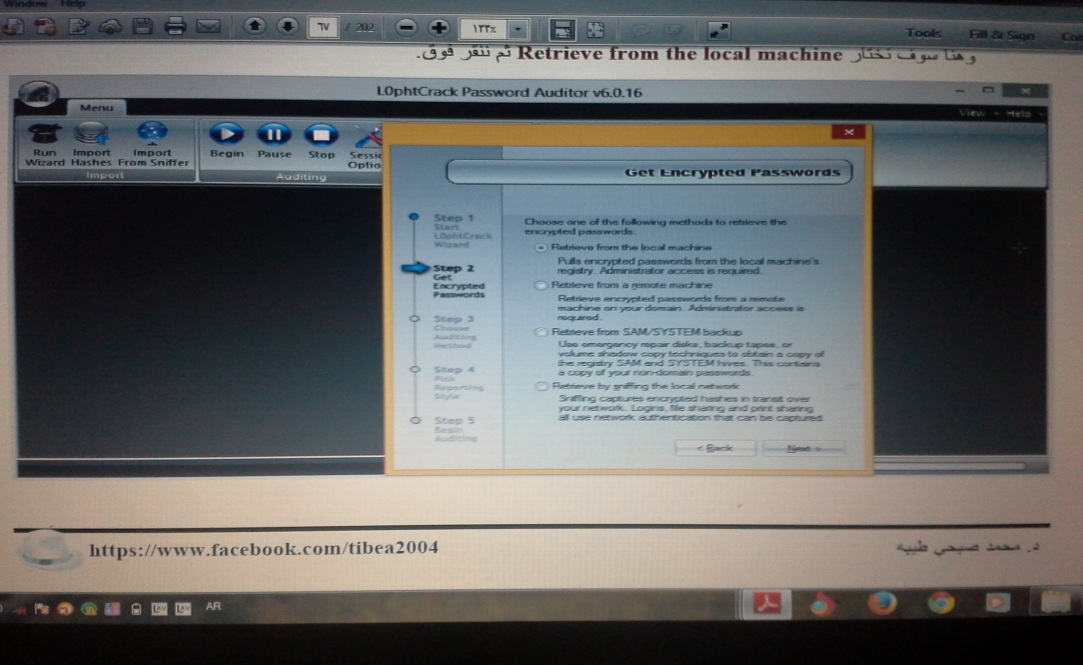
- **الاداة Lophtcrack:** وهذه الاداة تحتاج الى امتياز مدير النظام لتنقيذها وهى تعمل على النظام المحلي كما تعمل عن بعد، وتقوم باستيراد الملف سام SAM من الجهاز، او من حركة المرور في الشبكة، ومحاولة كسر تشفيره، وتعرض هذه الاداة اربع خيارات لسحب الملف سام SAM على النحو التالي:-

1- سحب الملف سام SAM من النظام المحلي.

2-سحب الملف سام SAM عن بعد.

3-سحب الملف سام SAM من النسخة الاحتياطية.

يمثل الشكل التالي الصفحة مع هذه الخيارات:

****

وبعد ان تقوم اداة Lophreack باستخراج الملف SAM بأحد الطرق السابقة التي تم تحديدها، تعرض الاداة خيارات الانواع الثلاثة للهجوم الخاص بكسر التشفير: هجوم القاموس، والهجوم الهجين، وهجوم القوة الغاشمة، وعند قيام المهاجم بتحديد اي نوع منها تقوم الاداة بكسر التشفير للملف SAM باتباع الطريقة التي حددها المهاجم، تستغرق الاداة في جهود فك التشفير 24 ساعة تقربيا في المتوسط [[122]](#footnote-122).

**خاتمة للفصل:**

تناولنا في هذا البحث عملية الدخول الى انظمة الكمبيوتر من خلال خدمات الاتصال عن بعد، وبينا ان خدمات الاتصال عن بعد تؤمن عادة باسم مستخدم وكلمة مرور، وان الدخول الى النظام سوف يبدا بمحاولة تخمين كلمة المرور لهذه الخدمات، وتسمى هذه العملية بعملية كسر الخدمات عن بعد، هذه العملية نمطية في ويندوز ويونيكس لان النظامين يتضمنان برتكول TCP الذي يطبق هذه الخدمات، بعد ذلك سيجد المهاجم نفسة بحاجة الى رفع الامتياز الى مستوى مدير النظام ليملك الحق الكامل في الوصول الى الملفات، يسمى هذا بهجوم رفع الامتياز، وبما ان المقصود هو اعطاء فكرة عامة عن كيف يعمل المهاجم، فقد اقتصرنا على تناول طرق رفع الامتياز في ويندوز كمثال، المطلب القادم سيتناول انشاء الله نظام يونيكس كمثال.

**المطلب الثاني**

**الدخول عبر ثغرات البرمجية**

- الثغرات البرمجية هي: عيوب او هفوات في تصميم البرنامج او في البيئة التي يعمل البرنامج ضمنها [[123]](#footnote-123).

وتوجد الثغرات البرمجية نتيجة اخطاء المبرمج اما عند تصميم وكتابة البرنامج، او عند تطويره وتحسينه بغرض زيادة فاعليته، فغالبا ما يتم تصميم البرنامج بسرعة بدافع تلبية احتياجات السوق او المنافسة او ارضاء للمدراء دون مراعاة شروط الامن، مما يؤدي الى حدوث اخطاء برمجية تسبب في هذه الثغرات[[124]](#footnote-124)، كما انه في بعض الحالات يعدل المبرمج برنامج ما بسرعة لتوسيع وظيفته وتحسين اداءة، ومع ان هذا التحسين والتوسيع يجعل البرنامج اكثر رواجا وشعبية فانه يزيد من تعقيده مما يزيد فرص الهفوات والعيوب ايضا[[125]](#footnote-125)، وفي كل الاحوال يبحث المهاجم عن هذه الثغرات، وعندما يتمكن من العثور عليها وايجادها يقوم باستغلالها من خلال تهريب برنامج خبيث عبرها الى النظام الهدف، ويعمل هذا البرنامج الخبيث على تمكين المهاجم من الدخول الى النظام ومن ثم السيطرة عليه، او يمكنه من سحب معلومات او ملفات حساسة من ذلك النظام.

في مجال الانظمة المعلوماتية يمكن للجاني استغلال الثغرات البرمجية ليتمكن من الدخول الى النظام الهدف، ومن ثم السيطرة الكاملة عليه والاستيلاء على كافه مواردة، او على مواردة الحساسة والهامه، كما يمكنه استغلال هذه الثغرات اما لسحب معلومات وملفات هامة وقيمة من النظام الهدف.

وبما ان الثغرات الامنية هي اخطاء برمجية والمبرمجين بشر معرضين للأخطاء في بعض الاحيان، فانه ستوجد الكثير من الثغرات في البرامج، وعادة تكون الاخطاء البرمجية غير مرئية للمبرمج عند تصميم البرنامج، ولا تكتشف اثنا التنفيذ الطبيعي للبرنامج، ولكن تكتشف بعد وقوع الهجوم، ويسارع بعدها المبرمجون الى ترقيعها، وهناك اخطاء اصبحت شائعة جدا وتوجد في كل مكان تقريبا وبما ان هذه الاخطاء شائعة وتتكرر في كثير من الاماكن فقد تم تطوير تقنيات عامة لاستغلالها من قبل المهاجمين، ويمكن استخدام هذه التقنيات العامة في مجموعات متنوعة من الحالات، ومن الثغرات البرمجية الشائعة ما يسمى بفيض الذاكرة المؤقتة Baffer overflow وهجوم سلاسل الصيغة Format string [[126]](#footnote-126).

**الفرع الاول**

**هجوم فيض الذاكرة المؤقتة**

Buffer overflew

* **مفهوم فيض الذاكرة المؤقتة:**

المخزن المؤقت او الBuffer مجموعة محددة من المواقع المتجاورة في الذاكرة [[127]](#footnote-127)، أي سلسة محددة من الخانات المتتابعة داخل الذاكرة، ويطلق ايضا على المخزن المؤقت داخل الذاكرة اسم المصفوفة array، والمصفوفات هي اكثر انواع المخازن المؤقتة شيوعا في لغات البرمجة ++c – c المستخدمة في اعداد أكثر برامج انظمة التشغيل، والشكل التالي يمثل مصفوف داخل الذاكرة[[128]](#footnote-128):-

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

الشكل السابق هو عبارة عن مربعات يمثل كل منها موقع داخل الذاكرة، وهي متشابهة ومتراصة على شكل صف، ولذلك تسمى بالمصفوفة، تخزن في هذه المصفوفة من المواقع المتتابعة مجموعة البيانات التابعة لبرنامج ما، ومن المفترض ان تكون البيانات التي تخزن في هذه المواقع المتتابعة مساوية لها في الحجم او اقل منها، ولكن اذا تم ادخال بيانات بأحجام كبيرة الى هذه المصفوفة، فان البيانات ستزيد وتفيض الى خارج هذه المواقع مما يؤدي الى انهيار البرنامج، يشبه ذلك ما لو وضعت كمية من الماء داخل كأس اكبر من حجم هذا الكاس، فان الماء سيفيض من الكاس الى الاماكن المجاورة.

على سبيل المثال البرنامج الذي يطلب من المستخدم ادخال البريد الالكتروني، او كلمة مرور، يملك مخزن مؤقت في الذاكرة محدود بحجم وطول معين، ويمكنه تخزين مجموعة من الكلمات هي الاسماء او الارقام التي ستقوم بإدخالها، لكن اذا قام احد المهاجمين بإدخال مجموعة ضخمة من الاحرف، الف حرف مثلا، بدلا من البريد الالكتروني، فان هذه المجموعة الضخمة من الاحرف سوف تملأ المخزن المؤقت الخاص بالبرنامج وستفيض منه الى الاماكن الاخرى داخل الذاكرة، وبما ان كل بيان جديد يخزن في أي موقع في الذاكرة المؤقتة يؤدي الى مسح البيانات السابقة التي كانت موجودة في هذا الموقع ويحل محلها، فان هذا الفيض سيتسبب في الكتابة في المواقع المجاورة للمخزن المؤقت الخاص بالبرنامج، من خلال استبدال البيانات الموجودة في هذه المواقع بالأحرف الفائضة من المخزن المؤقت في المثال السابق، وقد تكون بعض الاحرف الفائضة برنامج خبيث يدسه المهاجم بين سلسلة الاحرف التي سببت الفيض، ويمكنه من الدخول الى النظام، وبالتالي سيؤدي وصول هذا البرنامج الخبيث الذاكرة الى تنفيذه وتمكين المهاجم من الدخول الى النظام والسيطرة عليه[[129]](#footnote-129).

يرجع امكانية حدوث فيض الذاكرة المؤقتة Buffer overflew الى عدم وجود آلية او وظيفة داخل لغة c، c++ تفحص الدخل الى البرنامج وتتحقق من حجمة وتحدد له حجم معين او طول ثابت، أي لا يوجد في هذه اللغة ما يضمن ان لا يكون حجم البيانات المدخلة او المنسوخة اكبر من حجم المخزن المؤقت الخاص ببرنامج ما [[130]](#footnote-130)، فلغة c، c++ تترك المسؤولية عن سلامة البيانات الى المبرمج، فاذا لم يكن المبرمج حذرا فانه يقع في هذا الخطأ اثناء تصميم البرنامج[[131]](#footnote-131) ، وبما ان لغة c، c++ هي المستخدمة في تصميم معظم برامج وخدمات انظمة التشغيل مثل ويندوز ويونيكس، فان هذا العيب شائع جدا في هذه الانظمة.

2**-فهم تقنيات الفيض**

فهم هجوم الفيض وكيفية حدوثة واستغلاله يحتاج الى فهم عدد من التقنيات والمراحل التي يعمل بواسطتها، مثل الذاكرة، والبرمجة، وحجز الذاكرة، والمتغيرات، ونحو ذلك.

**اولا الذاكرة:-**

كما قد يتذكر القارئ من الفصل التمهيدي ان ذاكرة الكمبيوتر تنقسم الى ثلاثة انواع:

1. ذاكرة الرام RAM او ذاكرة التنفيذ: وهي الذاكرة التي تنفذ فيها جميع العمليات والبرامج داخل الحاسب، ويلاحظ ان الذي ينفذ في الذاكرة كل مرة هو برنامج واحد فقط، ولكن بسبب السرعة يظن انه ينفذ عدة برامج في المرة الواحدة.
2. ذاكرة الROM: وهى الذاكرة التي تخزن فيها البرامج الدائمة الخاصة بنظام الحاسب مثل برنامج الاقلاع وبرنامج الدخل والخرج.
3. الذاكرة الاحتياطية: وهى التي يخزن فيها المستخدم بياناته وبرامجه التي يريد الاحتفاظ بها بشكل دائم داخل الكمبيوتر، وهى اما ذاكرة مغناطسية مثل القرص الصلب، او ذاكرة ضوئية مثل الفلاش.

والذاكرة الرام RAM تسمى ذاكرة التنفيذ لان الكمبيوتر لا ينفذ أي برنامج الا اذا تم إحضاره الى هذه الذاكرة، وهي المهمة هنا بالنسبة لفهم عملية الى الفيض، وبالتالي هي التي ستكون موضع البحث في الفقرات التالية.

* **مكونات الذاكرة RAM:**

في حقيقتها فان الذاكرة RAM هي عبارة عن شريحة الكترونية تحتوي على ملايين الترانزستورات المحفورة عليها، يعمل كل ترانزستور كمكثف يخزن بنبضة كهربائية واحدة، وهذه الترانزستورات مرتبة بجانب بعضها البعض على هيئة صفوف، بالنسبة للمبرمج او المستخدم العادي فانه يمكنه تخيل هذه الترانزستورات على شكل صفوف من الخلايا، مثل صفوف صناديق البريد الموجودة في مكاتب البريد، او صفوف خانات الكتب في المكتبات العامة، او حتى صفوف خلايا النحل، في كل خلية من خلايا ذاكرة الكمبيوتر يتم تخزين نبضة واحدة فقط، وبما ان الاعداد الثنائية 0،1 هي المستخدمة في تمثيل النبضات الكهربائية داخل الذاكرة، العدد 1 يمثل نبضة والعدد 0 يمثل عدم وجود نبضة –فانه يمكن القول ان كل خلية من هذه الخلايا تخزن رقم ثنائي واحد فقط اما 1 او0، ويسمى العدد او الرقم الثنائي الواحد الذي يتم تخزينه في خلية الذاكرة بت BIT اختصارا لكلمة Binary digit التي تعني رقم ثنائي[[132]](#footnote-132).

ومع ان الخلية تستطيع تخزين عدد ثنائي واحد اما 1 واما 0، فان ذلك لا يكفي لتخزين الحروف ومجموعات الاعداد، ذلك ان الحرف الواحد عندما يتم ترجمته الى الشفرة الثنائية فانه يترجم في الشفرة الثنائية الى مجموعة من الواحدات والاصفار، ولذلك فان الحروف ومجموعة الاعداد تحتاج الى مجموعة من خلايا الذاكرة لتخزينها، ولهذا السبب يتم التعامل مع خلايا الذاكرة كمجموعات وليس على اساس كل خلية، وتسمى المجموعة الواحدة من الخلايا بالبايت Bite )) ، ويتضمن البايت ثمان خلايا او ثمانية بتات، ويكون لكل بايت عنوان عبارة عن رقم معين وفريد داخل الذاكرة بحيث يتم الوصول اليه عن طريق هذا العنوان، ويوضع العنوان في اول خلية من خلايا البايت، وعندما يريد المعالج نسخ معلومات من بايت معين، فانه يصل اول خلية في البايت ثم ينسخها مع الخلايا السبع التي تليها[[133]](#footnote-133)، فالتعامل ما بين المعالج والذاكرة او ما بين المبرمج والذاكرة يتم على اساس البايت، وليس على اساس البت.

الشكل التالي يبين عناوين الذاكرة:

الذاكرة الرئيسية خانة في الذاكرة

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

البايت

ثمانية خانات، وهو

الوحدة الرئيسية

للتعامل مع الذاكرة

عنوان البايت التسلسلي

2 1 بايت واحد

|  |  |
| --- | --- |
| أ | م |

الخانات التي يتكون منها البايت تسمى بت وعددها ثمان كل خانه بت واحد

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

0

1 عنوان البايت

2

* **المتغيرات Variabls:**

ان وحدة التخزين الاساسية التي يتعامل معها الكمبيوتر والمبرمج هي البايت، لكن البيانات المستخدمة في البرنامج قد تكون اكبر من بايت واحد وتتطلب 2، أو 4، أو 8 بايت لتخزينها في الذاكرة[[134]](#footnote-134)، وبالتالي فانه يجب ان يتم جمع عدة بايتات كافية لتشكل وحدة كافية لتخزين البيانات التي تحتاج اكثر من بايت، ويتم جمع عدة بايتات تحت اسم واحد باستخدام ما يسمى بالمتغيرات، حيث ان المتغير يخبر الكمبيوتر بحجز مساحة تتكون من عدة بايتات للبيانات المطلوبة للبرنامج، والمتغيرات هى اسماء معينة بحجز مواقع في الذاكرة قد تصل الى حجم 8 بايت من اجل تخزين البيانات فيها[[135]](#footnote-135).

الشكل التالي يبين متغيرات 2بايت،4بايت:

الذاكرة متغير من نوع char 2بايت =16بت

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

الذاكرة متغير من نوع بايت عدد ثمان بتات

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

متغير من نوع int عدد 4 بايت ويساوي 32بت

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

---------------- Nit ----------------

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

-----------------------------------

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

الذاكرة

ويمكن القول ان المتغيرات تستخدم كعنصر رئيسي في كل البرامج تقريبا، وهي نوع من انواع تنظيم الذاكرة لتتسع تخزين البيانات التي يتجاوز حجمها بايت واحد، وبمجرد ان تقوم بالضغط على أي برنامج بزر الماوس او بزر انتر ينتقل البرنامج الى الذاكرة ويقوم المتغير بحجز مكان في هذه الذاكرة لتخزين البيانات التي تجرى عليها عمليات البرنامج، وتكون الذاكرة الخاصة بالبيانات منظمة ومقسمة على شكل متغيرات، اي مواقع تزيد حجمها على البايت الواحد، والغالب ان تكون البيانات الموجودة في الذاكرة مدخلة من قبل المستخدم، وعند ادخال المستخدم أي بيانات الى البرنامج تذهب الى متغير معين وتخزن فيه، ثم تجرى العمليات بين المتغيرات وتخزن النتائج في متغير جديد تمهيدا لعرضها على الشاشة [[136]](#footnote-136).

بعض المتغيرات يكون من بايت واحد مثل المتغير Byte، وبعض المتغيرات يتكون من اكثر من بايت، الشكل التالي يبين انواع المتغيرات:

|  |  |
| --- | --- |
| المتغير | الحجم |
| Byte | 8 Bit |
| Short | 16 Bit |
| Int | 32 Bit |
| Long | 64 Bit |
| Float | 32 Bit |
| Double | 64 Bit |
| Char | 16 Bit |
| String | Bit - |
| Boolean | 1 Bit |

يمكن القول ان المتغيرات عبارة عن وعاء يمكن ان نضع فيه قيمة معينه او بيانات معينه، وهذا الوعاء يتغير حجمة حسب القيمة التي سوف توضع فيه، الشكل التالي يوضح هذه الفكرة[[137]](#footnote-137) 106:

: 

ويلاحظ من الشكل انه اذا كان هناك وعاء مخصص للأرنب فانه لا يستطيع باي حال من الاحوال ان يحمل شيء كبير بحجم الزرافة مثلا[[138]](#footnote-138)، وهذه الفكرة تناظر فكرة المتغير، فيجب علينا ان نختار حجم المتغير بما يناسب كمية البيانات التي نريد وضعها فيه، وبعد ان نختار نوع المتغير من الانواع السابقة في الجدول، يجب علينا ان نعطي للمتغير اسم بمثابة عنوان له، ذلك اننا بعد ان نقوم باستخدام المتغيرات يختفي عنوان البايت ولا نتعامل معه، بل نتعامل مع اسم المتغير الذي يشمل مجموعه من البايتات يتم التعامل معها كواحده واحده، تماما كما يتم التعامل مع البتات الثمانية كبايت واحد، هناك طرق اخرى لتنظيم البيانات والتقسيمات داخل الذاكرة، ومن هذه الطرق ما يسمى بالمصفوفات.

**المصفوفات ARary:-**

المصفوفة هي عبارة عن سلسلة محددة او وصف من المتغيرات المتجاورة والمتتابعة داخل الذاكرة[[139]](#footnote-139).

الشكل التالي يبين مصفوفة[[140]](#footnote-140):

متغير

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

4 3 2 1 0 فهرس المصفوفة

**الغرض من المصفوفة:**

تستخدم المصفوفة لعدة اغراض:-

1-تخزين البيانات التي تحتاج لتخزينها الى حجم اكبر من حجم المتغيرات، مثلا المتغير من نوع shar يستطيع تخزين حرف واحد فقط، لكن اذا اردنا تخزين كلمة او عبارة كاملة فأننا نحتاج الى سلسلة متتابعة من المتغيرات من نوع shar.

وتسمى هذه السلسلة من المتغيرات shar مصفوفة حروف، الشكل التالي يمثل مصفوفة من نوع shar [[141]](#footnote-141):

مصفوفة من سبعة متغيرات

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | M | a | R | G | O | R | p |

متغير حرفي واحدshar

2-ايضا عناصر المصفوفة تكون موضوعه بجوار بعضها في الذاكرة بشكل صف متتابع ومتسلسل في حين ان المتغيرات لا تكون كذلك، بل توضع المتغيرات متفرقة في أي مكان في الذاكرة، مثلا عند تخزين درجات الطلاب نحتاج الى متغيرات متباينة لتخزين رقم تعريف لطالب واسمه الاول واسمة الاخير ودرجته، وهذه المتغيرات من انواع مختلفة بعضها حرفية وبعضها عددية، وعند تخزين البيانات فيها تكون متفرقة في اماكن مختلفة داخل الذاكرة وغير مرتبة، وبالتالي نحتاج للحصول على هذه البيانات الى نسخها من كل مكان على حدة، اما اذا خزنا هذه البيانات في مصفوفة واحدة فان المتغيرات والبيانات التي فيها ستكون بجوار بعضها البعض وستشكل سجلا لكل طالب، يمكن الحصول عليه ونسخه كاملا بمجرد الوصول الى عنوان العنصر الاول في المصفوفة[[142]](#footnote-142).

3-تستخدم المصفوفة ايضا عند الحاجة الى استعمال عدد ضخم من المتغيرات، كما لو اردنا مثلا تخزين درجات خاصة بألاف الطلاب ثم جمعها، فسنحتاج عندئذ الى كتابة الاف المتغيرات داخل البرنامج وكتابة الاف الاسماء لها بحيث يكون لكل متغير اسم، وهذا يشكل عبء ضخم على المبرمج في الكتابة، وفي ادخال البيانات، وفي جمعها، ولذلك نستخدم مصفوفة واحدة باسم واحد، بدلا من كتابة كل هذه المتغيرات، ويمكننا حينها ادخال جميع بيانات الطلاب الى المصفوفة، واجراء العمليات المطلوبة من جمع وغيره بكل سهولة[[143]](#footnote-143)

**تقنية عمل المصفوفة:**

تشتمل المصفوفة على عدد من المتغيرات يحدد في البرنامج من قبل المبرمج، وتسمى هذه المتغيرات عناصر المصفوفة، ويكون للمصفوفة عنوان او اسم واحد يحمله كل عنصر في المصفوفة، ويكون لكل عنصر رقم فهرسة بجوار اسم المصفوفة يميزه عن بقية العناصر. ويبدا رقم الفهرسة من الصفر ثم 3،2،1،.... الخ، بحسب حجم المصفوفة وعدد عناصرها، ويمكن للمبرمج ان يحدد أي حجم للمصفوفة بحسب حاجة البرنامج[[144]](#footnote-144)، وعند تنفيذ البرنامج ينتقل البرنامج الى الذاكرة وتقوم المصفوفة بحجز اماكن تخزين في الذاكرة بحسب عدد العناصر التي حددها المبرمج في المصفوفة[[145]](#footnote-145)، الشكل التالي يبين تقنية عمل المصفوفة[[146]](#footnote-146):

مصفوفة اسمها"a" وهي مكونة من اربع متغيرات

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

a اسم المصفوفة

5 4 3 2 0

المتغير يسمى عنصر المصفوفة وهو يحمل رقم معين، وبجانبه اسم المصفوفة، مثلا المتغير الاول يحمل الرقم 0 واسم المصفوفة a، فيكتب هكذا ( a0)، المتغير الثاني يكتب هكذا ( 2a )، وهكذا.

عندما يتم نسخ بيانات المصفوفة فان المعالج يذهب الى عنوان العنصر الاول في المصفوفة وينسخه وينسخ معه على التوالي العناصر الاخرى للمصفوفة[[147]](#footnote-147).

**المكدسة:**

المكدسة هي مصفوفة من المتغيرات وتتميز عن المصفوفة العادية بانها تخزن البيانات بطريقة الداخل اولا هو الخارج اخرا، تشبه المكدسة كدسة الاطباق والتي تكون فيها مجموعة اطباق مرصوصة فوق بعضها البعض، فالطبق الذي تضعه اولا يكون اسفل الكدسة، والطبق الاخير يكون اعلى الكدسة، فاذا اردت الحصول على الطبق الاول فيجب عليك اخذ جميع الاطباق التي تسبقه الى ان تصل اليه، ولا يوجد طريقة للحصول على الطبق الاول الا برفع الاطباق التي فوقه[[148]](#footnote-148).

الشكل التالي يبين مصفوفة عادية ومكدسة[[149]](#footnote-149):

|  |
| --- |
| احمد |
| علي |
| حسن |

المصفوفة

|  |
| --- |
| B(0) |
| B(1) |
| B(2) |
| B(3) |
| B(4) |
| B(5) |
| B(6) |

اسم المصفوفة هو B، وعناصرها تبدأ ارقامها من الصفر الى الرقم 6 وكل عنصر يحمل اسم المصفوفة مع رقمه، الجدول المقابل الذي يحتوي على الأسماء هو محتويات المصفوفة ابتداء من المتغير 0 الى المتغير 3 ، الشكل السابق هو الشكل العادي للمصفوفة، أما المكدسة فيتم التخزين فيها بطريقة عكسية، الشكل التالي يبين نموذج الكدسة:

كدسه

|  |
| --- |
| حسن |
| علي |
| احمد |

|  |
| --- |
| 2 |
| 1 |
| 0 |

محتويات المصفوفة

فهرس المصفوفة

هذا الشكل هو للمصفوفة B بعد نقلها الى الكدسة، ويلاحظ عليه ان كل محتويات المصفوفة B ترتب عكسيا، بطريقة الاخير يدخل اولا، والاول يدخل آخرا، وعند الاسترداد نبدأ من الاول ثم نصل الى الاخير.

توجد الكدسة في كل برنامج[[150]](#footnote-150)، واي برنامج ينتقل الى الذاكرة يقوم بحجز جزء من الذاكرة ليعمل كمكدسة للبرنامج[[151]](#footnote-151)، اما بقية المساحة المخصصة في الذاكرة فهي تتوزع على ثلاثة قطاعات: قطاع النص وهذا القطاع يتضمن تعليمات واوامر البرنامج، وقطاع البيانات وهو الذي تخزن فيه المتغيرات والمخازن المؤقتة او المصفوفات، بالإضافة الى قطاع الكومة[[152]](#footnote-152)، والذي يقوم بحجز هذه المساحة داخل الذاكرة من اجل البرنامج هو نظام التشغيل، فعندما نقوم بالضغط على ملف البرامج داخل القرص الصلب، او على ايقونته الموجودة في سطح المكتب، يقوم نظام التشغيل اليا بتحميل البرنامج الى الذاكرة من اجل تنفيذه، ويقوم مدير الذاكرة بحجز المساحة المناسبة للبرنامج داخل الذاكرة، يسمى البرنامج الموجود في الذاكرة عملية، فالعملية هي برنامج يتم تنفيذه داخل الذاكرة [[153]](#footnote-153).

**الغرض من الكدسة:**

تستخدم الكدسة للاحتفاظ بتدفق التنفيذ وسياقة عند حدوث انتقال من برنامج رئيسي الى برنامج فرعي او ثانوي[[154]](#footnote-154).

هناك العديد من المهام النمطية التي تتكرر في كثير من البرامج، مثل مهمة المصادقة على عملية الدخول الى البرنامج، والدوال الرياضية مثل دوال ايجاز الجذر التربيعي او جيب الزاوية...الخ، وهذه المهام النمطية يتم اعدادها برامج نمطية موحدة لها، بحيث يمكن استعمالها من مجموعة من البرامج والخدمات الرئيسية بدلا من اعدادها وكتابتها داخل كل برنامج رئيسي، فبرامج الدوال الرياضية يمكن استخدامها من قبل كل برنامج يقوم بعمليات رياضية او حسابية، وكذلك برنامج المصادقة على الدخول بكلمة مرور واسم مستخدم يمكن استعماله من قبل مجموعة كبيرة من البرامج الرئيسية والخدمات الهامة، ويتم استعمال هذه البرامج من خلال ما يسمى بالاستدعاء او النداء، فعندما يصل البرنامج الرياضي الحسابي الرئيسي في تنفيذه الى مرحلة يحتاج فيها الى ايجاد جذر تربيعي لرقم معين مثلا، فانه يستدعي البرنامج الثانوي الخاص بإيجاد الجذر التربيعي والذي يوجد عادة في مكتبة مستقلة تحتوي على البرامج الثانوية الرياضية، وعندما يستدعي البرنامج الخاص بالجذر التربيعي فان نظام التشغيل ينقل التحكم اليه، ويقوم بإخراج البرنامج الرئيسي من الذاكرة ويدخل برنامج الجذر التربيعي بدلا عنه، وعندما ينتهي برنامج الجذر من مهمته يعيد نظام التشغيل البرنامج الرئيسي الى الذاكرة ويخرج البرنامج الفرعي، ولكي يستطيع البرنامج الرئيسي ان يكمل التنفيذ من حيث توقف قبل إخراجه، فانه يستخدم المكدسة، وتساعد الكدسة البرنامج الرئيسي على العودة الى الاجراء او التعليمية او الخطوة التي تلي مباشرة عملية ايجاد الجذر في تسلسل تعليمات البرنامج الرئيسي، وبالتالي يمكن للبرنامج الرئيسي ان يوصل التنفيذ ويكمل سياقة من دون ان يتأثر بعملية القطع والاخراج من الذاكرة[[155]](#footnote-155).

يتم تخزين نص العملية او البرنامج الرئيسي، واخر عنوان لها في الكدسة، وعندما ينتهي المعالج من تنفيذ البرنامج الثانوي ويعود الى البرنامج او العملية الرئيسية، يستخرج النص واهمه العنوان الخاص بالتعليمية او الخطوة التالية من المكدسة، وعند التخزين في المكدسة فان اخر التعليمات والبيانات هي التي تدخل اولا الى مصفوفة الكدسة ثم الذي يليها وهكذا وصولا الى اولى البيانات والتعليمات والتي تكون في اخر او اعلى الكدسة، وعندما يعود المعالج الى العملية الرئيسية يستعيد البيانات ابتداء من اعلى الكدسة التي فيها البيانات واجراءات البرنامج الاولى وصولا الى اسفل الكدسة وهي التي فيها اخر الاجراءات التي تمت في البرنامج، وهذا هو المقصود بعبارة ان الداخل اولا هو الخارج اخرا [[156]](#footnote-156).

**طريقة التخزين في الكدسة:**

عندما يتم استدعاء البرنامج الثانوي او الفرعي تدفع الى المكدسة نص وبنية البرنامج الرئيسي، وبعد ذلك يدفع الى المكدسة العنوان الراجع وهو عنوان التعليمية او الاجراء الذي يلي البرنامج الثانوي والذي يجب ان يتم تنفيذه بعد الانتهاء من البرنامج الثانوي، ثم يدفع الى المكدس بنية ونص البرنامج الثانوي فوق البرنامج الرئيسي والعنوان الراجع، وبالتالي تصبح المكدسة مكونة على الترتيب من بنية البرنامج الرئيسي ثم العنوان الراجع ثم بنية البرنامج الفرعي[[157]](#footnote-157)، ويسمى ذلك باطار المكدس ويكون على الشكل التالي[[158]](#footnote-158):

مكدس البرنامج الثانوي

العنوان الراجع

مكدس البرنامج الرئيسي

مكمكمكمك

عندما يتم الانتهاء من تنفيذ البرنامج الثانوي يتم ازالة اطار المكدس الخاص بالبرنامج الثانوي (أي بنية ونص البرنامج الثانوي ) من المكدسة، ويتم اعادة المعالج الى العنوان الراجع لتنفيذ التعليمية التالية في البرنامج الرئيسي.

**-هجوم فيض المكدس:**

يمكن تقسيم هجوم فيض المكدس الى مرحلتين:

في المرحلة الاولى

يستخدم المهاجم بعض الادوات مثل لغةPerl لتوليد متتاليات من الاحرف على شكل سلسة، بحيث تكون هذه السلسلة اكبر من حجم المخزن المؤقت للبرنامج الذي يطلب إدخال البيانات من المستخدم، مثلا يستخدم المهاجم سلسة من حرفA ثم يضع في نهاية السلسلة شفرة برنامج خبيث مثل برنامج موجه اوامر، او أي برنامج تحكم آخر، وعندما يتم ادخال هذه السلسلة الى الذاكرة المؤقتة للبرنامج عبر مربع الادخال المخصص للبيانات المطلوبة، تفيض السلسلة عن المخزن المؤقت الخاص بالبرنامج الى موقع اخر في الذاكرة، ويقوم برنامج موجه الاوامر الموجود في نهاية السلسلة بحجز مكان له في الذاكرة.

وفي المرحلة الثانية:

يقوم المهاجم بإرسال سلسلة اخرى من الاحرف الى المكدسة الخاصة باي برنامج يتم تنفيذه داخل الذاكرة، وتتضمن هذه السلسلة في نهايتها عنوان مكان التخزين الذي يوجد فيه البرنامج الخبيث كموجه الاوامر، او اي برنامج خبيث للتحكم في الذاكرة، تمر هذه السلسلة من الاحرف عبر مصفوفة المكدس وتملأ خاناتها ببيانات عشوائية من الاحرف حتى تصل الى موقع العنوان الراجع الخاص بالمكدس، وعندها تكتب او تضع بدلا من العنوان الراجع عنوان البرنامج الخبيث الخاص بالمهاجم، وبمجرد ان ينتهي المعالج من تنفيذ البرنامج الثانوي يذهب الى العنوان الراجع الخاص بالبرنامج الرئيسي داخل المكدسة ويقوم بتنفيذه، ولكن عندما يكون المهاجم قد غير العنوان الراجع الى العنوان الذي يريده، فان المعالج يذهب الى عنوان البرنامج الخبيث الخاص بالمهاجم ويقوم بتنفيذه، ولا يذهب الى التعليمة او المهمة التالية في البرنامج الرئيسي كما كان يجب، ويؤدي تنفيذ البرنامج الخبيث كموجة الاوامر الى تمكين المهاجم من السيطرة على الجهاز الضحية وتوجيه اوامر اليه وسرقة أي معلومات منه[[159]](#footnote-159).

يعبر الشكل التالي عن كيفية حدوث هجوم فيض المكدس:

فيض من الحروف يملأ

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

مكدس البرنامج الثانوي

DDDDDDDDDDDDDDDDDDD

العنوان الراجع:

الفيض يصل الى

العنوان الراجع ويكتب فيه

برنامج المهاجم.

يساعد المهاجم على البرامج في هذا الهجوم امرين:

الاول: ان الكمبيوترات الحديثة لا تعمل اي تمييز حقيقي بين التعليمات والبيانات، فاذا وجد المعالج أي تعليمات في الاماكن المخصصة للبيانات داخل الذاكرة فانه يقوم بتنفيذها[[160]](#footnote-160)، وهذه الخصيصة هي التي تجعل هجوم الفيض ينجح، لان هجوم الفيض يعتمد على ادخال البرنامج الى اماكن تخزين البيانات داخل الذاكرة، مثل المتغيرات والمصفوفات (المخازن المؤقتة)، اما قطاع الشيفرة او التعليمات الخاص بالبرنامج داخل الذاكرة فهو للقراءة فقط، وغير قابل للكتابة عليه، وبالتالي لا يمكن ادخال أي تعليمات او برنامج في مكانة.

الامر الثاني: هو وجود ادوات تمكن المهاجم من معاينة الذاكرة، وهذه الادوات تعرض ذاكرة البرنامج اثناء التنفيذ واماكن المتغيرات والمخازن المؤقتة الخاصة بالبرنامج داخل الذاكرة، وتقوم بحساب المسافات بينها والتي تكون مجموعة من البايتات التي تفصل بين كل متغير او مخزن وبين الاخر، مما يساعد المهاجم على تحديد حجم سلسلة الاحرف اللازمة لملأ الاماكن والمواقع بين متغير وآخر، أو مخزن مؤقت وآخر والوصول الى المكان المطلوب من الذاكرة[[161]](#footnote-161)، فمثلا في فيض المكدس عندما يريد المهاجم الكتابة فوق العنوان الراجع، فانه يقوم بمعاينة ذاكرة المكدس من اجل تحديد حجم سلسلة الاحرف اللازمة لملأ الاماكن التي تسبق هذا العنوان، ومن ثم يقوم بتوليد السلسلة المناسبة ويضيف الى نهايتها العنوان الجديد الذي يريد ان يكتبه محل العنوان الراجع في نهاية السلسلة، مع ملاحظة انه يمكن ان يتكرر كتابة العنوان الجديد في نهاية السلسلة الى عشر مرات لضمان وصول العنوان الجديد الى مكان العنوان الراجع بالضبط [[162]](#footnote-162).

**الفرع الثاني**

**هجوم سلاسل الصيغة**

**تعريف سلاسل الصيغة:**

سلاسل الصيغة هي مجرد سلسلة من الحروف، ذات تتابع خروج، يطلب من البرنامج ادخال المتغيرات المكتوبة بصيغة معينة، في مكان تتابع الخروج[[163]](#footnote-163).

تتكون سلسلة حروف الصيغة من مجموعة من الحروف يبدا كل منها بإشارة بالمائة %، الجدول التالي يبين هذه الحروف[[164]](#footnote-164):

|  |  |  |
| --- | --- | --- |
| البارامتر | نمط الدخل | نمط الخرج |
| D% | قيمة | عشري |
| U% | قيمة | عشري دون اشارة |
| X% | قيمة | ست عشري |
| S% | مؤشر | سلسلة محارف |
| N% | مؤشر | عدد البايتات المكتوبة حتى الان |

**-وظيفة سلاسل الصيغة:**

ان المتغيرات الموجودة داخل الذاكرة والتي تخزن فيها البيانات تختلف من حيث نوع البيانات التي تخزن فيها، بعض المتغيرات تخزن فيها اعداد صحيحة فقط، سواء كانت هذه الاعداد تمثل ارقام او حروف، من امثلة هذه المتغيرات المتغير int فهذا المتغير هو متغير اعداد صحيحة يمكن ان تخزن فيه ارقام مثل 96 أو64، ولكن لا يمكن ان نخزن فيه أي عدد عشري مثل 7،39، واذا حاولنا ان تخزن العدد العشري في متغير من نوع int، فان المتغير سوف يحذف الفاصلة العشرية وما بعدها، ويخزن فقط العدد الصحيح، وبالتالي سوف يخزن العدد العشري 7،39 في متغير من نوع int في الصورة 7 فقط.

وبعض المتغيرات تقبل تخزين اعداد عشرية بالإضافة الى الاعداد الصحيحة ومن امثلة هذه المتغيرات dubl- float، فهذه المتغيرات تقبل ان يخزن فيها اعداد صحيحة واعداد عشرية[[165]](#footnote-165).

جوهر المشكلة هو انه اذا اراد برنامج معين اخراج ارقام تحتوي على علامة عشرية، فانه سوف يحتاج الى حجز متغيرات جديدة اخرى في الذاكرة من نوع flat اوdual لتخزين هذه الارقام ثم اخراجها الى الشاشة، مما يزيد في كمية التعليمات داخل البرنامج ويزيد مساحة الذاكرة المخصصة له، وبالمثل اذا اراد البرنامج تخزين اعداد عشرية فانه سيحتاج الى انشاء متغيرات جديدة تزيد في حجم البرنامج وتشغل مساحة اكبر من الذاكرة[[166]](#footnote-166).

تستخدم سلاسل الصيغة لحل هذه المشكلة، اذ يمكن استخدام رموز سلاسل الصيغة كأماكن او عناصر تنوب عن المتغيرات وتحل محلها في اخراج اعداد تختلف عن نوع المتغير، أي اخراج الاعداد الموجودة في المتغير بصيغة مختلفة، فيمكن لرموز سلاسل الصيغة ان تخرج العدد الصحيح الموجود في المتغير int في صيغة عشرية، من دون حاجة الى انشاء متغيرات جديدة من نوع اخر لتخزين هذا العدد في صورة عشرية، فعندما نريد مثلا ايجاد الجذر التربيعي للعدد الصحيح الموجودة في المتغير int ويكون الناتج عدد عشري، فيمكن من خلال استخدام رمز الصيغة d% خراج الصيغة العشرية الناتجة من دون انشاء متغير جديد من النوع العشري نخزن فيه هذا العدد العشري ثم نخرجه الى الشاشة، وعندما نريد ايجاد الشفرة الثنائية لهذا العدد، فيمكن من خلال استخدام رمز الصيغة x% اخراج الشفرة الثنائية الى الشاشة من دون حاجة الى متغير آخر يقبل تخزين ومن ثم اخراج هذا النوع من الشفرات الثنائية، وخلاصة القول ان رموز سلاسل الصيغة تعمل على اخراج صيغ مختلفة للاعداد الموجودة في المتغيرات من دون حاجة الى زيادة التعليمات او انشاء مواقع ومتغيرات اخرى تحجز مساحة كبيرة من الذاكرة[[167]](#footnote-167).

- **البرامج التي تستخدم مع سلاسل الصيغة[[168]](#footnote-168):**

يعتمد هجوم سلاسل الصيغة على دوال الاخراج والادخال، وهذه الدوال عبارة عن برامج ثانوية نمطية موحدة يتم استخدامها من قبل جميع البرامج الرئيسية التي تحتاج الى ادخال واخراج.

توجد برامج الادخال والاخراج في مكتبات برمجية خاصة داخل الحاسب الالي، وعندما يريد برنامج رئيس القيام باي ادخال او اخراج فانه يستدعي برنامج الادخال او برنامج الاخراج من المكتبة للقيام بهذا الادخال، ويتم الاستدعاء من خلال كتابة اسم المكتبة التي يوجد فيها برنامج الادخال والاخراج، بالإضافة الى اسم البرنامج.

ومع ان دوال او برامج الادخال والاخراج هي برامج نمطية موحدة تستعمل من قبل كافة البرامج، وتستخدم تقنية واحدة، الا ان اسمائها واسماء المكتبات البرمجية التي توجد فيها تختلف من لغة الى اخرى، على سبيل المثال في لغة c، c++ تكون هذه الدوال كالاتي[[169]](#footnote-169):

|  |  |  |
| --- | --- | --- |
| الاختلافات | لغةc) ) | ولغة C ++)) |
| اسم المكتبة | #include<studio> | #include<iostream> |
| اسم دوال الادخال | Scanf | Cin |
| اسم دوال الاخراج | Print | Cout |

**هجوم سلاسل الصيغة:**

يمكن تصنيف هجوم سلاسل الصيغة الى نوعين من الهجوم: هجوم اخراج المعلومات وهو يقوم بسحب المعلومات من النظام الهدف، وهجوم الادخال وهو يقوم بإدخال شفرات او برامج خبيثة الى النظام الهدف للسيطرة عليه.

**النوع الاول: هجوم اخراج المعلومات**

لكي نفهم هجوم اخراج المعلومات عبر سلاسل الصيغة فإننا نحتاج اولا الى معرفة كيف يعمل برنامج الاخراج، ثم طريقة استخدامه في هجوم سلاسل الصيغة.

* **برنامج الاخراج printf [[170]](#footnote-170):**

هو برنامج فرعي يقوم بغرض محتويات اى متغير في الذاكرة، ولكي يتم عرض محتويات أي متغير والمعلومات او البيانات الموجودة فيه باستخدام برنامج printf، يتم كتابة اسم برنامج الاخراج printf وبجانبه اسم المتغير على النحو التالي:-

(اسم المتغير)printf

يكتب اسم المتغير بين قوسين

مثلا اذا كان يوجد متغير في الذاكرة يحتوي على عدد 80 واسمه number، فانه يمكن عرض محتويات هذا المتغير على الشاشة عبر برنامج الاخراج printf بكتابته على النحو التالي:

Printf (number)

عندما ينفذ البرنامج سوف يظهر العدد80 على شاشة الحاسب، والذي حدث في هذه الحالة هو ان برنامج الاخراج قام بأرسال محتويات المتغير number الى الشاشة عبر قناة الخرج.

الشكل التالي بين هذه العملية:

888

متغير قناة الخرج الشاشة

**استخدام برنامج printf في الهجوم:** ان اخراج البيانات من أي متغير في الذاكرة الى الشاشة يتم بكتابة اسم البرنامج printf ثم بجانبه اسم المتغير، ولكن عندما نريد اخراج البيانات من المتغير باستخدام احد رموز سلاسل الصيغة فأننا نكتب رمز الصيغة قبل المتغير على الشكل التالي [[171]](#footnote-171):

Printf (% d number)

متغير رمز الصيغة برنامج الاخراج

يبدا برنامج الاخراج print بنقل المعلومات الى الشاشة ابتداء من اليمين وعلى شكل متتابع، عندما يصادف برنامج brintf علامة % فانه يتوقع ان يأتي بعد هذه العلامة المتغير التابع لرمز الصيغة[[172]](#footnote-172)، وعندما يجد البرنامج هذا المتغير وهو هنا المتغير number يقوم بقراءته ونقل محتوياته وعرضها على الشاشة على نمط رمز الصيغة % d، وليس على نمط المتغير، فاذا كان المتغيرnumber من نوع صحيح int فان برنامج الاخراج يعرض المعلومات على نمط رمز الصيغة %d، وهو النمط العشري، أي ان يخرج البيانات من المتغير بالصيغة العشرية عبر الرمز %d[[173]](#footnote-173).

يمكن وضع اكثر من رمز صيغة في برنامج الاخراج وفي هذه الحالة يجب ان تكون المتغيرات الموجودة في برنامج الاخراج تساوي عدد رموز الصيغة، ويقوم برنامج الاخراج printf بإخراج محتويات كل متغير الى الشاشة الحاسب الالي بحسب نمط رمز الصيغة الذي يتبعه هذا المتغير، فاذا كان عدد رموز الصيغة في برنامج الاخراج ثلاثة رموز فانه يجب ان تتضمن برنامج الاخراج ايضا ثلاثة متغيرات بحيث يكون لكل رمز صيغة متغير يتبعه، وهذا التطابق بين عدد رموز الصيغة وبين عدد المتغيرات التابعة لها امر ضروري لكي يعمل البرنامج بشكل صحيح، لكن اذا كان يوجد لدينا ثلاثة رموز صيغة ومتغيران فقط، بمعنى ان رمز الصيغة الثالث ليس له متغير تابع له في برنامج الاخراج فما الذي سيحدث؟

في هذه الحالة فان برنامج الاخراج printf سوف يسحب المحتويات والبيانات من المكان الذي كان يجب ان يكون المتغير الثالث موجودا فيه داخل الذاكرة[[174]](#footnote-174)، ذلك انه في حاله وجود رمز سلاسل الصيغة وليكن d %مثلا في برنامج الاخراج printf من دون وجود متغير تابع له، فان برنامج الاخراج سوف يبحث عشوائيا عن أي متغير في مكان ما من الذاكرة ويخرج محتوياته الى الشاشة الحاسب الالي، ولو لم يكن هذا المتغير مخصص للتابع الموجود في برنامج الاخراج[[175]](#footnote-175).

Printf (olo d )

اذا لم يجد البرنامج Printf متغير بعد رمز d % فانه سوف يذهب الى الذاكرة ويسحب محتويات أي متغير ويخرجه على نمط d %

ان أي رمز صيغة يقابله برنامج الاخراج printf يجب ان يأتي بعده المتغير التابع له، فاذا لم يجد برنامج الاخراج متغير بعد رمز الصيغة فإنه يبحث عشوائيا عن أي متغير اخر في الذاكرة، ويطبعه على نمط الرمز، وهذا الامر يترتب عليه نتائج في غاية الخطورة، اذ يمكن لمهاجم ان يكتب مجموعة كبيرة من رموز الصيغة في برنامج الاخراج ولا يضع لها متغيرات تقابلها كما في الشكل التالي:

............... %d وd % وd %و d %و d %) printf

في هذه الحالة فان برنامج الاخراج سوف يقوم بجلب محتويات عدد كبير من المتغيرات من الذاكرة مساوي لعدد الرموز، ويعرضها على شاشة الجاني، مما يعني كشف معلومات حساسة قد توجد في تلك المتغيرات، مثل اسماء المستخدمين، وكلمات المرور، واي بيانات مهمه اخرى، وكلما زاد عدد رموز الصيغة المكتوبة في برنامج الاخراج printf، كلما زادت مساحة الذاكرة التي سيكشفها البرنامج للمهاجم وبالتالي كمية المعلومات التي سيحصل عليها[[176]](#footnote-176).

**كشف محتويات المكدسة:**

راينا فيما تقدم انه عندما يستدعي أي برنامج ثانوي فان هذا البرنامج يخزن في المكدسة فوق البرنامج الرئيسي والعنوان الراجع، وفي هذه الحالة يشمل التخزين في المكدسة جميع مكونات البرنامج الثانوي من وسائط ومتغيرات وتعليمات، وبما ان عائلة برنامج printf هي من البرامج الثانوية التي تستدعي من المكتبة، فانه عندما يستدعي احد برامج عائلة printf تنتقل الوسائط والمتغيرات التي في البرنامج وتخزن على المكدسة، كما يحدث عند استدعاء اى برنامج ثانوي اخر، واذا كانت المتغيرات التي تمرر للبرنامج printf قليلة جدا اقل من رموز الصيغة فان برنامج printf سوف يستولي على القيمة التالية من المكدسة[[177]](#footnote-177)، ويستخدمها للرمز الذي لا يوجد له متغير، فاذا تم استخدام عدد كبير من رموز الصيغة %x بدون وجود متغيرات تابعة لها، فان ذلك سيؤدي في نهاية المطاف الى الاستيلاء على القيم التالية المخزنة في المكدسة وكشف محتوياتها للمهاجم.

**النوع الثاني: هجوم الادخال**

تستخدم سلاسل الصيغة ايضا في تشغيل برامج وشفرات خبيثة داخل ذاكرة النظام الهدف، ويتم ذلك من خلال تبديل الرمز المستخدم في برنامج print الى الرمز n %[[178]](#footnote-178)، يستخدم هذا الرمز لادخال البيانات والكتابة على المتغير الذي يأتي بعده، وهذا على عكس رموز الصيغة السابقة التي تخرج وتعرض البيانات الموجودة في المتغيرات التي تليها، واذا حددنا الرمز n %في البرنامج print فان هذا الرمز يتوقع متغير تابع له، وسوف يدخل الشفرات والبيانات ويكتبها في هذا المتغير[[179]](#footnote-179)، وهذا يعني انه يمكن لنا ان ندخل برنامج خبيث او أي شفرة تحكم الى أي موقع في الذاكرة باستخدام رمز الصيغة n%.

يتم الادخال عبر ال رمز n %بالصيغة التالية:

اسم المتغير (control) وn% AAAAA)PRINTF

فخرف الA هو مثال عن الشفرة او البرنامج الذي سيتم إدخاله، ثم يليه رمز الصيغة n % ثم يليه اسم المتغير الذي سيتم ادخال البرنامج او الشفرة اليه.

ومن اجل تشغيل البرنامج الذي قمنا بإدخاله الى الذاكرة، نقوم بالكتابة فوق العنوان الراجع في المكدس، ونغير العنوان الراجع ليشير الى عنوان البرنامج الذي قمنا بإدخاله، وبهذه الطريقة نتمكن من اعادة توجيه التنفيذ الى العنوان الذي نريده داخل الذاكرة[[180]](#footnote-180).

ويتم الوصول الى العنوان الراجع من خلال استخدام رمز الصيغة x % والذي سوف يقوم بالمرور عبر كل المتغيرات والوسائط داخل المكدسة حتى يصل الى العنوان الراجع[[181]](#footnote-181).

ايضا فان اشارة الدولار توفر لنا الوصول المباشر الى اى متغير في الذاكرة بدلا من المرور الية بشكل تسلسلي[[182]](#footnote-182)، ويمكن من خلال كتابة اشارة الدولار بجانب اسم المتغير الذي يخزن فيه العنوان الراجع ان يصل مباشرة الى العنوان الراجع، ونكتب فوقة العنوان الذي نريد ونجعل المعالج يقفز الى تنفيذ هذا العنوان.

**تعديل اساليب الامان في الذاكرة:**

يمكن استخدام رمز الصيغة n % لا دخال تعديلات على القيم المخزنة في الذاكرة من اجل تغيير اساليب واجراءات اساسية لأمان بعض البرامج، على سبيل المثال، برنامج يخزن كلمة المرور لبعض الامتيازات الادارية في الذاكرة، هنا يمكن بواسطة استخدام رمز الصيغة n % ان نعدل كلمة المرور هذه الى كلمة خالية مما يتيح الوصول الى تلك الامتيازات الادارية بكلمة مرورها فارغة (أي بلا كلمة مرور)، ايضا رقم التعريف لID ورقم تعريف المجموعات Grub ID هي قيم قد تكون اهداف جيدة اذا كان البرنامج يمنح او يلغي الوصول الى بعض الموارد، او يغير مستوى امتيازاته، بطريقة تعتمد على قيم في الذاكرة، اذ يمكن ادخال تعديلات عشوائية محل تلك القيم لتعطيل وشل امن البرنامج[[183]](#footnote-183).

احيانا عند مهاجمة شبكة فان كل ما تريد ان تعمله هو تحطيم او كسر خدمة محددة على سبيل المثال اذا كانت تؤدي هجوم يتضمن تحليل او تخريج اسماء، ربما تريد كسر خدمة اسماء النطاق DNS، فاذا كانت الخدمة قابلة للإصابة بمشكلة سلاسل الصيغة، من المحتمل ان تكسرها بسهولة جدا[[184]](#footnote-184).

**الفرع الثالث**

**الادوات**

**اداةMetasploit**

* **Metasploit:**

هي اداة من اهم ادوات الاختراق، وهى الاداة المثالية للقراصنة حتى انها تقوم بالاختراق كما في الافلام، أي بضغطة زر[[185]](#footnote-185).

وتتميز Metasploit بانها ليست مجرد اداة فقط، بل هي مشروع او اطار يضم كل الادوات او البرامج الخاصة بالاختراق، وهذه الادوات والبرامج تم المزج بينها داخل Metasploit وفق قواعد محددة، وتم داخل Metasploit اتمتة جميع المهام العادية الروتينية، والمهام المعقدة، التي تطلبها عملية الاختراق[[186]](#footnote-186)، والواقع ان هذه الأتمتة الشاملة لمهام الاختراق هي التي تجعل الاختراق سهلا عبر Metasploit ويبدو كما في الافلام.

**مفهوم الاختراق عبر Metaspleit**: يتم الاختراق عبر Metasploit من خلال اطلاق الexploit وإرساله الى النظام الهدف[[187]](#footnote-187)، وال exploit هو وسيلة الاختراق وهو كود مخصص يقوم عند أرساله الى نظام الضحية باختراق منطقة ضعف في جدار النظام وينفذ الى داخل النظام حاملا معه برنامج تحكم، وبعد ادخال برنامج التحكم الى النظام الهدف يقوم هذا البرنامج بتمكين المهاجم من تنفيذ اوامره عليه، واحيانا يكسبه السيطرة الكاملة على النظام، يسمى برنامج التحكم الذي يرسل ال expect بالبايلود payload، وهو انواع كثيرة اشهرها برامج الابواب الخلفية أو احصنة طروادة، وبرامج الshell وهو موجة الاوامر.

يمكن توضيح هذه العملية اكثر بالرجوع الى هجوم فيض الذاكرة، حيث تمثل ال exploit سلسلة الحرف A التي ترسل الى المخزن المؤقت وتحدث الفيض، اما ال payload فهو الشيفرة الخبيثة التي يتم ارسالها في نهاية سلسلة الحرف A، والتي تمكن المهاجم من السيطرة على النظام عند تنفيذها، ان عملية هجوم فيض الذاكرة هو نوع من انواع ال exploit لكن الاختلاف هو ان ال Metasploit تقوم بأتمتة هذه العملية بالنسبة للمهاجم، من ناحية انها تقوم باكتشاف منطقة الضعف، وتوفر الكود لExploit المناسب لاختراقها، وكذلك برنامج التحكم والسيطرة الpayload الذي يمكن إدخاله مع الExploit لكسب السيطرة الجزئية او الكلية على النظام الهدف.

**الوحدات الرئيسية في Metasploit:-**

تتكون Metasploit من العديد من الوحدات البرمجية التي تكون كل واحدة منها مسؤولة عن مهمه او عمل معين في اطار عملية الاختراق، ومع ذلك فانه لأغراض هذا الكتاب سنتناول ثلاث وحدات رئيسية تعتبر كافية لإعطاء الفهم الكافي لطبيعة الاداة Metasploit وهذه الوحدات هى exploit والpayload، والinterface.

1-**وحدة exploit: exploit** هي اكواد مخصصة تستفيد من عيوب وثغرات امنية في النظام الهدف[[188]](#footnote-188)، ان كل كود exploitمسؤول عن استغلال نقطة ضعف محددة[[189]](#footnote-189)، وعندما يتم ارسال كود exploit معين الى النظام الهدف فان هذا الكود يخترق النظام من نقطة الضعف هذه، اي من نقطة الضعف المسئول عنها، تتضمن ال Metasploit عشرات من exploit المخصصة لاختراق نقاط ضعف وعيوب امنية محددة في انظمة التشغيل والخدمات والبرامج المختلفة[[190]](#footnote-190)، ومن اجل استخدام ال Metaspleit يجب ان نكتشف اولا نقاط الضعف وعيوب الامن في النظام الهدف، ثم بناء على ذلك نختار ال exploit المخصصة لها ونرسلها لاختراق النظام من خلال العيوب ونقاط الضعف المكتشفة، ال exploit الشائعة تتضمن، عيوب فيض الذاكرة Buffer.

يتيح ال Metasploit ايضا انشاء اكواد exploit جديدة تناسب أي نقاط ضعف او عيوب امنية يتم اكتشافها في المستقبل[[191]](#footnote-191) 162، في بداية انشاءMetaspleit لم تكن تتضمن هذا العدد الكبير من أكود ال exploit، ففي العام 2003م اطلقت اول نسخة من ال Metasploit وكانت هذه النسخة تتضمن فقط 11، احد عشر، كود exploit، ثم في العام 2004م اطلقت نسخة بديلة منها تضمنت 19 كود exploit فقط ولكن اضيف الى هذه النسخة 27 من برامج التحكم والسيطرة الpayload [[192]](#footnote-192)، ومنذ ذلك الحين اخذت Metasploit في التطور الى ان وصلت الى ماهي علية الان.

يشبه المتخصصون ال expliet بزناد البندقية المنطلق، أي انها بمثابة اطلاق الزناد على نقطة ضعف في النظام الهدف، لكنها لا تتضمن أي برنامج تحكم او سيطرة متقدمة[[193]](#footnote-193)، فبرامج التحكم والسيطرة يتم توفيرها بواسطة وحدة اخرى هي وحدة البايلود payload

* **وحدة البايلود payload:**

بمجرد ان تكون قد اطلقت الزناد على نقطة الضعف فان الخطوة التالية هي ان تنفذ بعض العمل على جهاز الضحية، ويتمثل هذا العمل في تثبيت برامج تحكم اضافية، مثل موجة الاوامر، وبرامج الابواب الخلفية[[194]](#footnote-194)، تسمى برنامج التحكم هذه payload، ان ال payload هي برامج اضافية يتم تثبيتها على النظام الهدف بمجرد نجاح تنفيذ ال exploit واختراق النظام[[195]](#footnote-195)، وتتضمن هذه البرامج الاضافية الاجابة عن السؤال ماذا احتاج الان لكي يكون لي تحكم وسيطرة على الآلة، هناك انواع عديدة من برامج ال payload ولكن ال payload الاكثر شعبية يتضمن اضافة مستخدمين جدد، فتح ابواب خلفية، وتحميل برامج جديدة على الالة الهدف[[196]](#footnote-196).

ان ال payloads هي متغيرة ولا ترتبط بexploit محدد، وتقوم الاداة Metaspleit بالمزج بين exploitو،payload وارسالهما معا الى النظام الهدف، ويتم ذلك بصورة أوتوماتكية بمجرد الوصول الى نقطة الضعف في هذا النظام.

3-**واجهات استخدام Metasploit:-**

هناك العديد من الواجهات الخاصة ب metasploitتتضمن الواجهة النصية والواجهة الرسومية Gut، ومن هذه الواجهات الاصدارArmitag ارميتاج، وهو واجهة رسومية قويه وتوفر للمستخدم تفاعل كامل.

## المبحث الخامس: نسخ البيانات والمعلومات

نسخ البرامج والبيانات هو المرحلة النهائية في جريمة القرصنة الالكترونية، وهو الهدف المقصود منها، وقبل أن نتناول عملية النسخ التي تتم للبرامج والبيانات يجب أن نمهد لذلك بالإشارة الى اماكن التخزين في نظام الكمبيوتر، لأنها من الامور الضرورية لفهم الصورة الكاملة لجريمة قرصنة البيانات والبرامج.

**اماكن التخزين:**

عندما ينجح المهاجم في الدخول الى نظام الكمبيوتر الضحية، فانه يبدا بالبحث داخل هذا النظام عن البيانات والبرامج التي يريد نسخها والاستيلاء عليها، ولا يقوم المهاجم بالبحث عشوائيا في كل النظام، بل توجد اماكن معينة يخزن فيها كل نوع من البيانات والبرامج داخل نظام الكمبيوتر، وهذه الاماكن هي مجلدات النظام والتي تأتي كجزء من نظام التشغيل. فعندما يتم تخزين البيانات او البرامج داخل نظام الكمبيوتر، يذهب كل نوع منها الى المجلد الخاص به من مجلدات النظام. وسوف نتناول فيما يلي انواع واسماء المجلدات التي تخزن فيها البيانات والبرامج داخل نظامي التشغيل ويندوز ويونيكس.

**اماكن التخزين في نظام التشغيل ويندوز**[[197]](#footnote-197): في نظام التشغيل ويندوز توجد جميع المجلدات التي تخزن فيها البيانات في المجلد c ، والمجلد c او القرص c هو المجلد الجذر في ويندوز، وهو الذي يستضيف نظام التشغيل.

اماكن التخزين التي توجد في ويندوز تسمى بنية الدليل، وهي تشمل عدة مجلدات تتوزع عليها انواع البيانات التي يتم تخزينها في نظام الكمبيوتر. وعندما ينجح المهاجم في اقتحام ودخول جهاز يعمل بنظام ويندوز، فانه يبحث عن هدفه في هذه المجلدات، فالبرامج مثلا يتم تخزينها في المجلد program files ضمن المجلد الجذر c ، وبيانات المستخدم يتم تخزينها في المجلد users ضمن المجلد الجذر c ، وفيما يلي جدول بأهم مجلدات التخزين داخل المجلد الجذر c:

C\:

program files \: وتوجد فيه جميع ملفات البرامج الخاصة بالمستخدم.

: \program data وتوجد فيه كل بيانات البرامج.

\users: وتخزن فيه بيانات المستخدمين.

: \public وتخزن فيه ملفات المشاركة

windows\: وتخزن فيه ملفات النظام

boot\: وتخزن فيه الملفات التمهيدية للنظام، اي ملفات الاقلاع.

المجلدات الفرعية لمجلد المستخدم users:

Users\

: \Desktop ويتضمن ملفات واختصارات الملفات والبرامج

Documents\: وهو الموقع الافتراضي للمستندات

Downloads\: وهو الموقع الافتراضي لحفظ كل محتويات التنزيلات

Music\: وهو الموقع الافتراضي الذي توجد فيه الصوتيات الخاصة بالمستخدم.

Pictures\: وهو الموقع الافتراضي لملفات الصور

Videos\: وهو الموقع الافتراضي لملفات الفيديو او الفيديوهات الخاصة بالمستخدم

Searches\: وهو الموقع الافتراضي لحفظ عمليات البحث.

Appdata\: وهو الموقع الافتراضي الذي تخزن فيه بيانات البرامج، والشفرات الثنائية للبرامج.

**اماكن التخزين في يونيكس[[198]](#footnote-198):** المجلد الجذر في انظمة يونيكس هو المجلد root وهذا المجلد يحتوي على كافة المجلدات الموجودة في النظام والتي تخزن فيها انواع البيانات المختلفة، وهو يعتبر بمثابة المجلد c\: في ويندوز. يتضمن المجلد الجذر في انظمة يونيكس المجلدات الاساسية التالية:

Root\:

\Dv: وهذا المجلد يتضمن كل الاجهزة المرتبطة بنظام التشغيل، مثل محركات الاقراص المرنة والصلبة والطابعات.. الخ، ويوجد ملف لكل جهاز من هذه الاجهزة داخل المجلد dv ، وهذا الملف هو نقطة الاتصال بالجهاز، ويمكن من خلال هذا الملف اجراء العمليات على الجهاز. على سبيل المثال يمكن من خلال الملفات الخاصة بمحركات الاقراص المختلفة، نسخ هذه الاقراص كاملة.

: \Homeيتضمن المجلدات الخاصة بالمستخدمين، فنظام يونيكس ينشئ لكل مستخدم مجلد يكون بمثابة المنزل له، او بمثابة الملعب الخاص به، ويمكنه ان يعمل داخله ما يحلو له، مثل تحميل البرامج والملفات او حذفها او نحو ذلك. فيكون للمستخدم علي مجلد باسم aly ويكون للمستخدم محمد مجلد باسم mohammed وهكذا. ويكون لكل مستخدم ان يقوم بكافة العمليات من قراءة وتحميل وحذف وكتابة داخل مجلده فقط، ولا تكون له اي صلاحية على مجلدات الاخرين، وعندما يسجل المستخدم دخوله الى النظام، فان النظام يضعه على المجلد الخاص به، واذا اجرى عملية بحث عامة داخل النظام عن ملف او برنامج معين، فان النظام يبحث عن هذا الملف او البرنامج داخل مجلده فقط، واذا لم يكن موجودا، فان عملية البحث تعيد النتيجة بانه غير موجود، ولو كان موجودا في مجلد تابع لمستخدم اخر

وهذ يمنع عمليات التخريب والعبث في النظام من قبل المستخدمين

Opt\: يستخدم هذا المجلد لتخزين البرامج وحزم التطبيقات المضافة التي لا تكون جزءا من التثبيت الافتراضي للنظام، وملفات البرمجيات التجارية التي تثبت على النظام.

\Root: هذا هو مجلد المنزل لمدير النظام، وجميع المجلدات الاخرى في النظام بما فيها المجلدات الخاصة بالمستخدمين الاخرين، تابعة لهذا المجلد، ويستطيع مدير النظام من خلال هذا المجلد ان يجري كافة العمليات من.فتح وحذف وتقييد وتثبيت ونحو ذلك، على كافة المجلدات في النظام. فهو يملك صلاحية مطلقة على كل النظام. وهذا على عكس المجلدات الخاصة بالمستخدمين الموجودة في المجلد الرئيسي home فان كل مستخدم هناك لا يملك اي صلاحية الا على مجلده فقط.

User \: هذا المجلد هو اكبر مجلد في نظام يونيكس، وتوجد فيه البيانات والبرامج الخاصة بالمستخدمين، مثل برامج الالعاب برامج.........الخ وهو يتضمن عدة مجلدات منها:

User\bin: وهذا المجلد يتضمن برامج المستخدم المثبتة على نظام يونيكس، وتوجد فيه الاف البرامج القابلة للاستخدام.

User\doc: هذا المجلد هو الدليل المركزي للمستندات، وتقع المستندات في المسار user\shar\doc والمرتبط من هنا في هذا المجلد.

User\shar: يحتوي هذا المجلد على.جميع البيانات المشتركة بين برامج المستخدم الموجودة في المجلد user\bin مثل المستندات، الايقونات، الملفات الصوتية، الخطوط، خلفيات الشاشة.. الخ.

tmp\: تستخدم هذه الملفات للتخزين المؤقت للبيانات من قبل البرامج اثناء عملية تشغيلها.

وعادة ما يتم ضبط انظمة التشغيل على مسح محتويات هذه الملفات المؤقتة التي تنشئها البرامج، عند كل اعادة تشغيل للنظام.

Var\: ويحتوي على البيانات المتغيرة التي تتغير باستمرار مثل، الايميلات او رسائل البريد الالكتروني، بنوك المعلومات، المخازن المؤقتة للبيانات مثل مخازن البيانات الخاصة بالطباعة، سجلات الدخول، وغير ذلك من البيانات التي تتغير باستمرار.

**تقنية النسخ: سطر الاوامر:**

ما هو سطر الاوامر؟

سطر الاوامر هو عبارة عن برنامج له واجهة على شكل مربع نص صغير، ويستخدم لتوجيه الاوامر الى نظام التشغيل لكي يقوم بمهمة معينة مثل تشغيل برنامج معين او نسخ بيانات،،وعندما نريد استخدام برنامج سطر الاوامر فإننا نقوم بكتابة الاوامر التي نريد اصدارها الى النظام في داخل المربع الخاص بالبرنامج، ويأخذ برنامج سطر الاوامر عند فتحه الشكل الاتي:

والاوامر التي نكتبها في مربع البرنامج هي عبارة عن كلمات معينة يفهمها نظام التشغيل، وكل كلمة تعني بالنسبة للنظام ان يقوم بمهمة معينة، مثلا الكلمة cp تعني بالنسبة للنظام ان يقوم بعملية نسخ وهكذا، ويجب ان يكون المهاجم على معرفة والمام بهذه الكلمات لكي يتمكن من استخدامها في تنفيذ هجومه.

يعتاد اكثر المستخدمين على برنامج النوافذ windows والذي يرمز فيه للبرامج والمجلدات والملفات بأيقونات واشكال رسومية، وهذا البرنامج يسمى بالواجهة الرسومية، ويستخدم بواسطة سطح المكتب الذي يضم مجموعة من الرموز والرسومات التي تمثل الملفات والأجهزة والبرامج، والتي يمكن فتحها او تشغيلها بمجرد النقر على هذه الرموز.

اما برنامج سطر الاوامر فهو يسمى بالواجهة النصية، ويكون على شكل مربع نص، يكتب فيه المستخدم الامر، ثم يضغط الزر enter، فيقوم الجهاز بتنفيذ الامر.

كان برنامج سطر الاوامر هو السائد قبل ظهور الواجهة الرسومية، وبما ان برنامج سطر الاوامر يحتاج الى الالمام بالأوامر المختلفة، فقد كان من الصعب على المستخدم العادي ان يستعمله، وبالتالي حال ذلك دون الانتشار الكبير للكمبيوتر.

تمكن العلماء بعد ذلك من اختراع الواجهة الرسومية، والتي مثلت فيها الاوامر بأيقونات واشكال سهلة، واصبح بإمكان المستخدم النقر على تلك الايقونات وسحبها ونسخها، واجراء كافة العمليات عليها بسهولة بالغة، مما ادى الى انتشار الكمبيوتر بحجم هائل في كل انحاء العالم

مع ذلك فقد بقي استخدام برنامج سطر الاوامر من قبل المتخصصين الذين لدبهم المام به، بسبب انه اكثر كفاءة من الواجهة الرسومية في تنفيذ المهام الصعبة والمعقدة، ومعظم ادوات الهاكر والمهاجمين تتضمن برنامج سطر الاوامر، ويتم تنفيذها عن طريق هذا البرنامج.

يوجد برنامج سطر الاوامر في انظمة التشغيل وفي ادوات الهاكر، والاوامر الاساسية في هذا البرنامج موجودة في كل هذه الانظمة والادوات.

**طريقة كتابة الاوامر[[199]](#footnote-199) 170:**

عندما يقوم المهاجم بتشغيل برنامج سطر الاوامر، فإنه يكتب الاوامر التي يريد تنفيذها داخل مربع النص الخاص بالبرنامج، مثلا في نظام تشغيل لينكس اذا اراد المهاجم نسخ ملف فإنه يكتب الامر التالي:

Cp item1 item2

اي انسخ المجلد item1 الى المجلد item2.

واذا اراد نقل ملف يكتب الاتي:

Mv item1 item2

اي انقل المجلد item1 الى المجلد item2

واذا اراد عرض الملفات الموجودة في مجلد ما داخل الجهاز يكتب حرف Is بجانب اسم المجلد داخل مربع النص الخاص بسطر الاوامر..... وهكذا.

Is item1

اي اعرض محتويات المجلد item1.

**نسخ البرامج والملفات من النظام البعيد:**

لكي يتمكن المهاجم من الوصول الى النظام البعيد ونسخ البيانات والمعلومات منه، فانه يستخدم اولا احد برامج الاتصال التي تسمح له بالاتصال بجهاز الضحية، بعض هذه البرامج تكون محمية بكلمة المرور، وبعضها يكون غير محمي، بالنسبة للبرامج المحمية فانه الدخول عبرها الى النظام واستخدام سطر الاوامر لنسخ البيانات والبرامج يكون بعد كسر الحماية او اختراقها باي طريقة من طرق الاختراق.

اما بالنسبة للبرامج الغير محمية فانه يمكن الدخول عبرها الى النظام البعيد عن طريق كتابة اسم البرنامج في مربع سطر الاوامر وضغط زر enter وبعد ان يتم الاتصال يقوم المهاجم بكتابة اوامر النسخ في السطور التالية من مربع النص، مثلا الاتصال ببرنامج خادم الملفات ftb في الجهاز الخادم البعيد server يكون على الشكل الاتي[[200]](#footnote-200):

FTB Fileserver

**البيانات المستهدفة للسرقة:**

البيانات التي يستهدفها الجناة عادة من عملية اختراق نظام الضحية تشمل عدة انواع اهمها على الاطلاق هي البيانات المالية، وسوف نتناول فيما يلي بعض انواع البيانات المستهدفة للنسخ والقرصنة من قبل الجناة.

**1\_سرقة البيانات المالية للهوية الشخصية:**

تعتبر البيانات المالية الخاصة بالهوية الشخصية من اكثر البيانات التي تتعرض للنسخ والسرقة، وتتضمن هذه البيانات رقم بطاقة الائتمان، ورقم الحساب، ورقم الضمان الاجتماعي، ويمكن للجاني من خلال الاستيلاء على هذه البيانات ارتكاب جرائم اقتصادية متنوعة، بالاضافة الى ان الجاني يمكنه بيع هذه البيانات لمجرمين آخرين، وتحقيق الربح منها مباشرة من دون حاجة الى ارتكاب جرائم اضافية بواسطتها. وبمجرد الحصول على هذه البيانات فان الجاني يمكنه ان يستخدمها في ارتكاب مجموعة متنوعة من الجرائم الاقتصادية.

على سبيل المثال يمكن للجاني ان يستخدم رقم بطاقة الائتمان في شراء البضائع من الانترنت، الحصول على الخدمات، فتح حسابات ائتمان جديدة، فتح حساب هاتف او شبكة لاسلكية او الاشتراك في خدمات الكهرباء، والتدفئة، كابل التلفزيون، اي نفقات او رسوم من استخدام رقم البطاقة.

اما رقم الحساب البنكي فيمكن للجاني ان يستخدمه في تسوية مدفوعاته واجراء تحويلات الكترونية غير مشروعة، وطلب القروض، فتح حسابات بنكية جديدة، اصدار شيكات مزيفة، استنزاف الحساب بعمليات مالية مختلفة.

واما رقم الضمان الاجتماعي فانه يساعد الجاني في الحصول على الاعانات الحكومية، استرداد الاموال من الضرائب، الحصول على وثائق من الحكومة او على وظيفة....الخ.

توجد البيانات المالية للاشخاص عادة في قواعد البيانات التابعة للبنوك والشركات التجارية والمؤسسات المختلفة التي يتعامل معها الافراد. ويرجع ذلك الى ان الشركات والمؤسسات التجارية تسجل ارقام بطاقات الائتمان في قواعد بياناتها عند كل عملية شراء، ولذلك فان المهاجم يمكنه ان يحصل على هذه بيانات مالية مختلفة للافراد من خلال اختراق انظمة الكمبيوتر التابعة لهذه الشركات والمؤسسات.

**2-سرقة الودائع:**

سرقة الودائع الالكترونية تتم عن طريق الدخول الى نظام الحاسب الالي في البنوك ومن ثم القيام بعمليات تحويل ونقل ودائع مالية من حساب الى اخر. ويقوم الجاني في هذه الحالة باجراء قيود كتابية من حساب الى اخر، وهذه القيود تمثل ودائع مالية، تنتقل من حساب الى اخر، اي انها اموال تنتقل من حساب الى اخر.

**3-نسخ المعلومات:**

تشمل المعلومات المقالات والابحاث والكتب والصوت والصور والفيديو، وتخزن هذه الانواع المختلفة من المعلومات في انظمة الكمبيوتر داخل قواعد بيانات، وقد كانت قواعد البيانات التقليدية تخزن النصوص فقط، اما التطبيقات الحديثة لقواعد البيانات فبامكانها ايضا تخزين الصوت والصور ومقاطع الفيديوا مثل موقع اليوتيوب الذي يخزن فيه الصوتيات ومقاطع الفيديو[[201]](#footnote-201)، ومع ان كثير من المعلومات متاح للتحميل والنسخ مجانا من الانترنت، الا ان منها ما يقتضي رسوما مالية مقابل السماح بنسخه وتنزيله، مثال ذلك الكتب الالكترونية التي تباع بسعر معين، وتستلزم دفع هذا الثمن قبل تنزيلها، وكذلك بعض المقالات المنشورة الكترونيا في بعض انظمة الكمبيوتر لا يسمح بقرا ءتها الا بعد دفع مبالغ رمزية، وكذلك الافلام والصوتيات وغيرها.

**4-نسخ البرامج:**

اكثر البرامج التي تتعرض للنسخ هي برامج الالعاب، وبرامج الاعمال التجارية، والسبب في ذلك هو ارتفاع تكلفة هذه البرامج، ولذلك يقوم الجناة بنسخ هذه البرامج وقرصنتها، ثم يعيدون بيعها باثمان زهيدة، بحالتها او بعد ادخال بعض التحويرات عليها.

يتطلب نسخ البرنامج اولا كسر كلمة المرور الخاصة به، ومن ثم تنزيله الى جهاز الجاني، والذي يتم تنزيله الى جهاز الجاني هو نسخة البرنامج فقط، اما الاصل فهو يبقى لدى المجني عليه، ومع ذلك فان نسخ برنامج معين يفقد المصنف له حقه في بيع هذه البرنامج والحصول على ارباح منه تعادل الجهد المبذول في اعداده، لان المستهلكين يقبلون على النسخة المسروقة لانخفاض ثمنها، ويعرضون عن شراء النسخة الاصلية.

## اهم مراجع الكتاب

**اولا: المراجع الفنية:**

1. **مراجع الحاسب الالي والشبكات:**
2. اساسيات الحاسب الالي، محمد احمد فكيرين، بيروت / لبنان، دار الراتب الجامعية، 1993م
3. مفاهيم الكمبيوتر الاساسية، وليام س ديفيز، ترجمة مؤسسة الابحاث اللغوية، 1987 م.
4. موسوعة الكمبيوتر الميسرة، انطوان بطرس، لبنان، مكتبة لبنان، 1994 م.
5. مكونات الميكروكمبيوتر التقنية، مظهر طابل، دار الراتب الجامعية، 1985 م.
6. مكونات الحاسب وتجميعه، المؤسسة العامة للتعليم الفني والتدريب المهني، المملكة العربية السعودية،
7. مقدمة الى نظرية المعلومات، الرموز، الاشارات، الضجيج، جون ر بيرس، ترجمة فايز فوق العادة
8. الحاسب شرح تعليمي مبسط، سامي الرماحي، الدار العربية للعلوم.
9. مفاهيم نظام التشغيل، كتاب الكتروني، عبد الرحمن احمد محمد عثمان، الطبعة الثانية، مارس 2013 م
10. ، شبكات المعلومات والاتصالات، عامر ابراهيم قنديلجي، ايمان فاضل السامرائي، الاردن، دار المسيرة، ط1، 2009م.
11. تكنولوجيا الاتصالات وشبكات المعلومات، محمد محمد الهادي، القاهرة، المكتبة الاكاديمية، 2001 م
12. شبكات الحاسب، النظرية والتطبيق، مصطفى محمد مشلح، لبنان، شعاع للنشر والعلوم، الطبعة الاولى 2008 م
13. طقم التدريب على الشهادة +Network الاصدار الثاني، محترفي تكنولوجيا المعلومات،، ترجمة مركز التعريب والبرمجة، لبنان، الدار العربية للعلوم ناشرون، ط1، 2001م
14. بروتكول IP/TCP الدليل الكامل، احمد خالد المحمد، لبنان، شعاع للنشر والعلوم، الطبعة 1999 م.
15. زدني علما: انترنت، ارنود دوفور، ترجمة منى ملحيس، نبال إدلبي، بيروت، الدار العربية للعلوم، 1998 م
16. الانترنت والعولمة، بهاء شاهين، القاهرة، عالم الكتب، 1999 م.
17. التكنولوجيا الرقمية، نيكولاس نيجروبونت، ترجمة سمير ابراهيم شاهين، مصر، مركز الاهرام للترجمة، ط1، 1998م
18. **مراجع في البرمجة:**
19. كشف اسرار البيانات \_ دليل التعلم الذاتي، جيم كيوغ، كين ديفيدسون، لبنان، مركز التعريب والبرمجة، الدار العربية للعلوم، الطبعة الاولى، 2005 م
20. البرمجة بلغة c++، جون ر هيوبارد، ترجمة محمد ابراهيم العدوي، ومحمد السيد ابو الوفا، مصر، الدار الدولية للاستثمارات الثقافية، ط1، ج1، 2000 م،
21. الخطوات الاولى في التحليل والبرمجة، جان بيار لوران، ترجمة محمد الحجار، لبنان، المؤسسة الجامعية للدراسات والنشر والتوزيع، ط1، 1987 م،
22. المعالجات الدقيقة، البرمجة والمواجهة والتطبيق، محمد ابراهيم العدوي، مصر، الدار الدولية للاستثمارات الثقافية، ط1، 2000 م
23. برمجيات الحاسب الالي، لغة الجافا، سلوى محمد محمد كسير، هدى غريب علي محمد النجدي، مصر، وزارة التربية والتعليم
24. كتاب الاكسير، سلطان محمد الثبيتي، نسخة الكترونية مجانية
25. خطوة بخطوة لتعلم لغة c،c++، حسين احمد طالب الربيعي، كتاب الكتروني
26. احترف اوراكل خطوة بخطوة، نجوى الخباز، سوريا، شعاع للنشر والعلوم، ط1، 2004 م.

**ثانيا: المراجع المتخصصة في الاختراق:**

1. **المراجع العربية:**
2. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، جويل سكامبري، ستيوارت ماك كلور، جورج كيرتز، لبنان، مركز الترجمة، الدار العربية للعلوم، الطبعة الثانية، 2001
3. الهكر الاخلاقي، محمد طيبة، كتاب الكتروني متاح على موقع المهندسين العرب
4. القرصنة، الفنون \_ الاساليب \_ التدابير، نجوى مصطفى الخباز، لبنان، شعاع للنشر والعلوم، الطبعة الاولى 2009 م
5. تشريح الفيروسات، البنية -الية العمل \_ الحماية، فادي حجار، لبنان، شعاع للنشر والعلوم، 2003 م.
6. امن المعلومات بلغة ميسرة، خالد بن سليمان الغثبر، محمد بن عبدالله القحطاني، مركز التميز لامن المعلومات، ط1، 2009 م.
7. **كورسات الفيديو:**
8. دورة الهكر المتقدم، محمد طيبة، فيديو، اليوتيوب، تم نشره في 29‏/09‏/2015
9. دورة الهكر الاخلاقي، محمد هاني، فيديو، اليوتيوب، تم تحميله في 27‏/08‏/2011
10. دورة الهكر الاخلاقي، محمود عاطف، فيديو، على موقع اليوتيوب،تم نشره في 17‏/06‏/2014
11. صيحة الحق، دروس مرئية عن الشبكات، فيديو، اليوتيوب، تم تحميله في 17‏/10‏/2008
12. سنة اولى كمبيوتر، مقدمة عامة في اساسيات الكمبيوتر، ابراهيم عبد الحميد، اليوتيوب، تم نشره في 3/3/2012 م.

**ج. المراجع الانجليزية:**

1. Graves،kimberly، CEH-Certified Ethical Hacker Study Guide، SYBEX، WILEY، 2010
2. Engebretson، patrick، the basic of hacking and penetration، syngress، 2011
3. Baloch، Rafay، ethical hacking and penetration testing guide، crc 2015.
4. Burns،Bryan، *Jennifer Stisa Granick، Steve Manzuik Paul Guersch، Dave Killion، Nicolas Beauchesne، Eric Moret Julien Sobrier، Michael Lynn، Eric Markham Chris Iezzoni، and Philippe Biondi،Security Power Tools ، orelly، 2007،*
5. the shellcoder،s Handbook، anley، chris،John Heasman، Felix “FX” Linder، Gerardo Richarte، Wiley، 2007
6. Harper، Allen،Shon Harris،Jonathan Ness،Chris Eaqle،Gideon Lenkey،Terron Williams، gray hat hacking، Third Edition، Mc Graw Hill، 2011
7. scambray، joel، stuart mc clure، hacking exposed windws، third edition، mc graw hill، 2008
8. the top 5 cyber crimes،aicpa، october 2013
9. Kennedy، David، Jim O’Gorman، DevonKearns،and Mati Aharoni، Metasploit، san Francisco،، no starch press، 2011
10. Zdziarski، Jonathan، Hacking and Securing ios Applications، O،REILLY، 2012
11. Handbook on Identity\_ related crime، UNODC، New York، 2011
12. Nguyen، Binh، Linux Filesystem Hierarchy، Version 0.65،2003

المحتويات

[شكر وتقدير 2](#_Toc476644946)

[مقدمة 3](#_Toc476644947)

[الجزء الأول 7](#_Toc476644948)

[مقدمة عن الحاسب الالي 7](#_Toc476644949)

[المبحث الاول 7](#_Toc476644950)

[الحاسب الآلي 7](#_Toc476644951)

[المطلب الثاني: البرمجيات 18](#_Toc476644952)

[المطلب الثالث: لغة الكمبيوتر 26](#_Toc476644953)

[المبحث الثاني: الاتصالات 40](#_Toc476644954)

[المطلب الاول: نظام الاتصال عن بعد 41](#_Toc476644955)

[المبحث الثالث: الشبكات 51](#_Toc476644956)

[المبحث الرابع: الانترنت enternet 67](#_Toc476644957)

[الجزء الثاني 73](#_Toc476644958)

[مراحل القرصنة الالكترونية 73](#_Toc476644959)

[تمهيد 74](#_Toc476644960)

[المبحث الاول: مرحلة الاستطلاع 76](#_Toc476644961)

[المطلب الثاني: مرحلة المسح scanning 98](#_Toc476644962)

[المبحث الثالث: مرحلة التعداد 124](#_Toc476644963)

[المبحث الرابع: الدخول الى النظام 138](#_Toc476644964)

[المبحث الخامس: نسخ البيانات والمعلومات 206](#_Toc476644965)

[اهم مراجع الكتاب 219](#_Toc476644966)

1. مفاهيم الكمبيوتر الاساسية، ص 2. [↑](#footnote-ref-1)
2. نظم المعلومات الادارية، ص29\_31. [↑](#footnote-ref-2)
3. مكونات الحاسب وتجميعه، ص4، وما بعدها. [↑](#footnote-ref-3)
4. مقدمة في الحاسبات الالكترونية ونظم الاختزان والاسترجاع، ص 15، 16، مكونات الحاسب وتجميعه، ص2، مفاهيم الكمبيوتر الاساسية، ص20. [↑](#footnote-ref-4)
5. اساسيات الحاسب الالي، ص15\_55، ص58 \_ 60، موسوعة الكمبيوتر الميسرة، ص34، 38. [↑](#footnote-ref-5)
6. اساسيات الحاسب الالي، ص31. [↑](#footnote-ref-6)
7. مفاهيم الكمبيوتر الاساسية، ص19. [↑](#footnote-ref-7)
8. اساسيات الحاسب الالي، ص44، 45، مكونات الحاسب وتجميعه، ص23، 24، مقدمة في الحاسبات الالكترونية، ص 21، 22. [↑](#footnote-ref-8)
9. موسوعة الكمبيوتر الميسرة، ص 32، 34، مفاهيم الكمبيوتر الاساسية، 92. [↑](#footnote-ref-9)
10. انظر المراجع التالية:

    - نظم المعلومات الادارية، ص295، ص 298 – 302، ص308،

    - مفاهيم الكمبيوتر الاساسية، ص 100 – 102،

    - تطور نظام التشغيل، بحث على موقع https:www.facebook.com efhamcomputer.

    -افهم كمبيوتر، بدأ تشغيل الحاسب، بحث على موقع https:www.facebook.com efhamcomputer.

    - نظم التشغيل الالكتروني، كتاب الكتروني متاح على الانترنت.

    - مفاهيم نظام التشغيل، كتاب الكتروني، ص 15 – 17، ص19 – 22. [↑](#footnote-ref-10)
11. الحاسب الآلي، الكمبيوتر، ص 22، 23، اساسيات الحاسب الالي، ص 35، موسوعة الكمبيوتر الميسرة، 39،40. [↑](#footnote-ref-11)
12. الحاسب، شرح تعليمي مبسط، ص112، 113، التكنولوجيا الرقمية، ص 23. [↑](#footnote-ref-12)
13. اساسيات الحاسب الالي، ص39. [↑](#footnote-ref-13)
14. مقدمة الى نظرية المعلومات، الرموز، الاشارات، الضجيج، ص42 -46، ص91 – 92. [↑](#footnote-ref-14)
15. مقدمة الى نظرية المعلومات، 45،46. [↑](#footnote-ref-15)
16. مقدمة الى نظرية المعلومات، ص178، 179. [↑](#footnote-ref-16)
17. التكنولوجيا الرقمية، ص141، 142. [↑](#footnote-ref-17)
18. تكنولوجيا الاتصالات وشبكات المعلومات، ص23، وما بعدها. [↑](#footnote-ref-18)
19. شبكات الحاسب، النظرية والتطبيق، ص93، 94، 97، 101، شبكات المعلومات والاتصالات، ص 91، 92، الاتصالات وشبكات المعلومات، بحث مقدم للاكاديمية العربية في الدنمارك، ماهر محمود غنيم، ص 4. [↑](#footnote-ref-19)
20. شبكات المعلومات والاتصالات، ص 93، 94، شبكات الحاسب، النظرية والتطبيق، ص60 – 62. [↑](#footnote-ref-20)
21. الاتصالات وشبكات المعلومات، ص 7، 8، الشبكة المحلية للمعلومات، ص 34. [↑](#footnote-ref-21)
22. شبكات الحاسب، النظرية والتطبيق، ص 101. [↑](#footnote-ref-22)
23. شبكات الحاسب، النظرية والتطبيق، ص110، 111. [↑](#footnote-ref-23)
24. شبكات المعلومات والاتصالات، ص93 -95، شبكات الحاسب، النظرية والتطبيق، ص62 [↑](#footnote-ref-24)
25. شبكات المعلومات والاتصالات، ص96 -101، شبكات الحاسب، النظرية والتطبيق، ص64، 66، 67. [↑](#footnote-ref-25)
26. الدليل الجديد لترابط الحواسيب، ص126، دورة دراسية شاملة لامتحان ميكروسوفت في الشبكات، كتاب الكتروني، ص 89 – 90. [↑](#footnote-ref-26)
27. الدليل الجديد لترابط الحواسيب، ص126. [↑](#footnote-ref-27)
28. راجع: شبكات المعلومات والاتصالات، ص23، شبكات الحاسب، النظرية والتطبيق، ص10. [↑](#footnote-ref-28)
29. شبكات المعلومات والاتصالات، 24ص – 26. [↑](#footnote-ref-29)
30. شبكات المعلومات والاتصالات، ص54، 55. [↑](#footnote-ref-30)
31. شبكات المعلومات والاتصالات، ص59. [↑](#footnote-ref-31)
32. تكنولوجيا الاتصالات وشبكات المعلومات، ص142، شبكات المعلومات والاتصالات ص61،62. [↑](#footnote-ref-32)
33. تكنولوجيا الاتصالات وشبكات المعلومات ص145، 146، الشبكة المحلية للمعلومات، ص21 – 23، الدليل الجديد لترابط الحواسيب ص 46، وما بعدها. [↑](#footnote-ref-33)
34. تكنولوجيا الاتصالات وشبكات المعلومات، ص148. [↑](#footnote-ref-34)
35. تكنولوجيا الاتصالات وشبكات المعلومات، ص149. [↑](#footnote-ref-35)
36. تكنولوجيا الاتصالات وشبكات المعلومات، ص149. [↑](#footnote-ref-36)
37. الشبكة المحلية للمعلومات، ص51 -57. [↑](#footnote-ref-37)
38. شبكات الانترانت، بنيتها الاساسية وانعكاساتها على المؤسسات، ص 103، وما بعدها، طقم التدريب على الشهادة Network+، ص 380. [↑](#footnote-ref-38)
39. طقم التدريب على الشهادة Network+، ص 354، 358، 360. [↑](#footnote-ref-39)
40. الانترنت: استثمار المستقبل، 321. [↑](#footnote-ref-40)
41. زدني علما: انترنت ، ص40. [↑](#footnote-ref-41)
42. زدني علما: انترنت، ص42، مبادئ Internet ، ص 18. [↑](#footnote-ref-42)
43. الانترنت: استثمار المستقبل، ص31. [↑](#footnote-ref-43)
44. تكنولوجيا الاتصالات وشبكات المعلومات، ص، شبكات الحاسب، النظرية والتطبيق، ص37، وما بعدها، الانترنت والعولمة، ص 169 – 173. [↑](#footnote-ref-44)
45. الانترنت والعولمة، ص47. [↑](#footnote-ref-45)
46. راجع في هذه المراحل:

    CEH-Certified Ethical Hacker Study Guide، sybex، wiley، 2010،p 52**\_**

    ، the basic of hacking and penetration، syngress، 2011،p29،30،31**\_**

    \_الهكر الاخلاقي، كتاب الكتروني متاح على موقع المهندسين العرب،ج1، ص14، 15. [↑](#footnote-ref-46)
47. the basic of hacking and penetration، p 11 [↑](#footnote-ref-47)
48. the basic of hacking and penetration، p 11،12 [↑](#footnote-ref-48)
49. راجع في هذه المرحلة:

    Graves،kimberly، CEH-Certified Ethical Hacker Study Guide،p 33-39

    Engebretson، patrick، the basic of hacking and penetration،،p16-18 [↑](#footnote-ref-49)
50. الهكر الاخلاقي، ج2 ص33،45، القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص 26، 27 [↑](#footnote-ref-50)
51. الهكر الاخلاقي، ج2 ص55 وما بعدها ، فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة. [↑](#footnote-ref-51)
52. the basic of hacking and penetration،p31

    فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة. [↑](#footnote-ref-52)
53. CEH-Certified Ethical Hacker Study Guide،p،42

    االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص26. [↑](#footnote-ref-53)
54. CEH-Certified Ethical Hacker Study Guide،p،42

    فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة. [↑](#footnote-ref-54)
55. the basic of hacking and penetration،p،29 [↑](#footnote-ref-55)
56. زدني علما: انترنت، ص23. [↑](#footnote-ref-56)
57. الانترنت: استثمار المستقبل، ص36. [↑](#footnote-ref-57)
58. السياسة الجنائية في مواجهة جرائم الانترنت، ص247. [↑](#footnote-ref-58)
59. طقم التدريب على الشهادة Network+، ص409. [↑](#footnote-ref-59)
60. طقم التدريب على الشهادة Network+، 410 -412. [↑](#footnote-ref-60)
61. فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة، طقم التدريب على الشهادة Network+، ص411، وما بعدها. [↑](#footnote-ref-61)
62. the basic of hacking and penetration،p،32-34 [↑](#footnote-ref-62)
63. فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة [↑](#footnote-ref-63)
64. فيديو كورس الهكر الاخلاقي، محمود عاطف، الحلقة الثالثة. [↑](#footnote-ref-64)
65. فيديو كورس الهكر الاخلاقي، محمود عاطف، الحلقة الثالثة. [↑](#footnote-ref-65)
66. راجع في ذلك:

    طقم التدريب على الشهادة Network+، ص148، ص290 وما بعدها، ص561 وما بعدها.

    القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص11، وما بعدها.

    فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة. [↑](#footnote-ref-66)
67. لمزيد من التفاصيل، راجع:

    شبكات الحاسب، النظرية والتطبيق، ص475 – 490،

    طقم التدريب على الشهادة Network+، ص 224، 225. [↑](#footnote-ref-67)
68. طقم التدريب على الشهادة Network+، 291، 292 [↑](#footnote-ref-68)
69. راجع: شبكات الحاسب، النظرية والتطبيق، 491، طقم التدريب على الشهادة Network+

    CEH-Certified Ethical Hacker Study Guide [↑](#footnote-ref-69)
70. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص11، وما بعدها.

    فيديو كورس الهكر الاخلاقي، محمد هاني، الحلقة الثالثة. [↑](#footnote-ref-70)
71. المراجع الاساسية لهذه الفقرة هي:

    شبكات الحاسب، النظرية والتطبيق.

    طقم التدريب على الشهادة Network+. [↑](#footnote-ref-71)
72. هذا الشكل مأخوذ مع تصرف وتحسين من: شبكات الحاسب، النظرية والتطبيق، ص541. [↑](#footnote-ref-72)
73. شبكات الحاسب، النظرية والتطبيق، ص540 – 543. [↑](#footnote-ref-73)
74. the basic of hacking and penetration،p،45 [↑](#footnote-ref-74)
75. طقم التدريب على الشهادة Network+، ص 269. [↑](#footnote-ref-75)
76. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص59، طقم التدريب على الشهادة Network+، ص259. [↑](#footnote-ref-76)
77. طقم التدريب على الشهادة Network+، ص259. [↑](#footnote-ref-77)
78. الهكر الاخلاقي ج4 ص3. [↑](#footnote-ref-78)
79. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص64. [↑](#footnote-ref-79)
80. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات،ص66. [↑](#footnote-ref-80)
81. CEH-Certified Ethical Hacker Study Guide،p،81 [↑](#footnote-ref-81)
82. CEH-Certified Ethical Hacker Study Guide،p،81 [↑](#footnote-ref-82)
83. CEH-Certified Ethical Hacker Study Guide،p،83 [↑](#footnote-ref-83)
84. طقم التدريب على الشهادة Network+، ص422، 423، دورة شاملة لامتحان ميكروسوفت، ص 211. [↑](#footnote-ref-84)
85. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص95 – 97، الهكر الاخلاقي، ج4، ص259 وما بعدها.

    HACKING EXPOSED WINDWS، THIRD EDITION، MC GRAW HILL، 2008،p 78 [↑](#footnote-ref-85)
86. طقم التدريب على الشهادة Network+، 363. [↑](#footnote-ref-86)
87. hacking exposed windws،p85 [↑](#footnote-ref-87)
88. hacking exposed windws [↑](#footnote-ref-88)
89. بروتكول IP/TCP الدليل الكامل، ص207 – 211. [↑](#footnote-ref-89)
90. طقم التدريب على الشهادة Network+، ص540. [↑](#footnote-ref-90)
91. الهكر الاخلاقي ج4، ص269. [↑](#footnote-ref-91)
92. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص102، 103. [↑](#footnote-ref-92)
93. طقم التدريب على الشهادة Network+، ص376، 377. [↑](#footnote-ref-93)
94. الهكر الاخلاقي ج4، ص278. [↑](#footnote-ref-94)
95. طقم التدريب على الشهادة Network+، ص5 [↑](#footnote-ref-95)
96. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص127، 128،الهكر الاخلاقي ج4، ص275 [↑](#footnote-ref-96)
97. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص128، الهكر الاخلاقي ج4ص276. [↑](#footnote-ref-97)
98. الهكر الاخلاقي ج4، ص277. [↑](#footnote-ref-98)
99. بروتكول IP/TCP الدليل الكامل، ص235، طقم التدريب على الشهادة Network+، ص498. [↑](#footnote-ref-99)
100. صيحة الحق، دروس مرئية عن الشبكات، الجزء 13. [↑](#footnote-ref-100)
101. the basic of hacking and penetration،p،67 [↑](#footnote-ref-101)
102. ehical hacking and penetration testing guide، crc،2015، p164،165 [↑](#footnote-ref-102)
103. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص178، 179. [↑](#footnote-ref-103)
104. صيحة الحق، دروس مرئية عن الشبكات، ج13. [↑](#footnote-ref-104)
105. احترف اوراكل خطوة بخطوة، ص 1223. [↑](#footnote-ref-105)
106. قراصنة قواعد البيانات بلا اقنعة، ص20 – 26. [↑](#footnote-ref-106)
107. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، 188، 189. [↑](#footnote-ref-107)
108. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص190. [↑](#footnote-ref-108)
109. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص190 – 192. [↑](#footnote-ref-109)
110. زدني علما: انترنت، ص59، 76، 77. [↑](#footnote-ref-110)
111. ،تشريح الفيروسات، البنية -الية العمل \_ الحماية، ص 34، 40. [↑](#footnote-ref-111)
112. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص197، تشريح الفيروسات، البنية - الية العمل \_ الحماية، ص 53. [↑](#footnote-ref-112)
113. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص201، الهكر الاخلاقي، ج5، 313. [↑](#footnote-ref-113)
114. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص380. [↑](#footnote-ref-114)
115. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص201. [↑](#footnote-ref-115)
116. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص201، الهكر الاخلاقي، ج5، ص353. [↑](#footnote-ref-116)
117. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص201، 202. [↑](#footnote-ref-117)
118. CEH-Certified Ethical Hacker Study Guide،p،100

     الهكر الاخلاقي، ج5، ص322. [↑](#footnote-ref-118)
119. CEH-Certified Ethical Hacker Study Guide،p،100 [↑](#footnote-ref-119)
120. CEH-Certified Ethical Hacker Study Guide،p،100 [↑](#footnote-ref-120)
121. القرصنة، الفنون \_ الاساليب \_ التدابير، ص517. [↑](#footnote-ref-121)
122. االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص203، 205، الهكر الاخلاقي، ج5. [↑](#footnote-ref-122)
123. القرصنة، الفنون \_ الاساليب \_ التدابير، ص143 [↑](#footnote-ref-123)
124. القرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص350. [↑](#footnote-ref-124)
125. القرصنة، الفنون \_ الاساليب \_ التدابير، ص145. [↑](#footnote-ref-125)
126. القرصنة، الفنون \_ الاساليب \_ التدابير، ص147. [↑](#footnote-ref-126)
127. the shellcoder،s Handbook، anley، chris، Wiley، 2007،p،12 [↑](#footnote-ref-127)
128. البرمجة بلغة c++، ص191. [↑](#footnote-ref-128)
129. راجع في ذلك: االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، ص349.

     القرصنة، الفنون \_ الاساليب \_ التدابير، ص148.

     the shellcoder،s Handbook، anley، chris، Wiley، 2007،p،12 [↑](#footnote-ref-129)
130. the shellcoder،s Handbook، Wiley،p،12 [↑](#footnote-ref-130)
131. القرصنة، الفنون \_ الاساليب \_ التدابير، ص148. [↑](#footnote-ref-131)
132. مكونات الحاسب وتجميعه، ص23 -26، اساسيات الحاسب الالي، ص 30 -33. [↑](#footnote-ref-132)
133. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص11. [↑](#footnote-ref-133)
134. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص4. [↑](#footnote-ref-134)
135. برمجيات الحاسب الالي، ص19. [↑](#footnote-ref-135)
136. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص4، كتاب الاكسير، نسخة الكترونية مجانية، ص16 -18. [↑](#footnote-ref-136)
137. برمجيات الحاسب الالي، لغة الجافا، ص19. [↑](#footnote-ref-137)
138. برمجيات الحاسب الالي، لغة الجافا، ص19. [↑](#footnote-ref-138)
139. راجع في المصفوفات الكتب التالية:

     كشف اسرار البيانات \_ دليل التعلم الذاتي، ص31، وما بعدها.

     كتاب الاكسير، ص53، وما بعدها.

     البرمجة بلغة c++، ص191

     the shellcoder،s Handbook [↑](#footnote-ref-139)
140. البرمجة بلغة c++، ص191. [↑](#footnote-ref-140)
141. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص34. [↑](#footnote-ref-141)
142. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص16، 32، 33. [↑](#footnote-ref-142)
143. برمجيات الحاسب الالي، لغة الجافا، 69، البرمجة بلغة c++، 192. [↑](#footnote-ref-143)
144. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص31، وما بعدها، البرمجة بلغة c++، ص191. [↑](#footnote-ref-144)
145. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص36. [↑](#footnote-ref-145)
146. البرمجة بلغة c++، ص191. [↑](#footnote-ref-146)
147. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص33. [↑](#footnote-ref-147)
148. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص51، 52، القرصنة، الفنون \_ الاساليب \_ التدابير، ص91، 92. [↑](#footnote-ref-148)
149. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص52. [↑](#footnote-ref-149)
150. كشف اسرار البيانات \_ دليل التعلم الذاتي، ص51. [↑](#footnote-ref-150)
151. المعالجات الدقيقة، البرمجة والمواجهة والتطبيق، مصر، الدار الدولية للاستثمارات الثقافية، ط1، 2000 م، ص 335. [↑](#footnote-ref-151)
152. القرصنة، الفنون \_ الاساليب \_ التدابير، ص90. [↑](#footnote-ref-152)
153. مفاهيم نظام التشغيل، ص194 -197. [↑](#footnote-ref-153)
154. القرصنة، الفنون \_ الاساليب \_ التدابير، ص158. [↑](#footnote-ref-154)
155. راجع في ذلك الكتب التالية:

     الخطوات الاولى في التحليل والبرمجة، ص61 – 64، مفاهيم نظام التشغيل، ص123، 124.، القرصنة، الفنون \_ الاساليب \_ التدابير، ص158. [↑](#footnote-ref-155)
156. انظر المراجع التالية:

     المعالجات الدقيقة، البرمجة والمواجهة والتطبيق، ص335.

     انظمة تشغيل الميكروحاسبات، ص25.

     القرصنة، الفنون \_ الاساليب \_ التدابير، ص91، 92. [↑](#footnote-ref-156)
157. القرصنة، الفنون \_ الاساليب \_ التدابير، ص159 – 163. [↑](#footnote-ref-157)
158. الفنون \_ الاساليب \_ التدابير، ص164. [↑](#footnote-ref-158)
159. القرصنة، الفنون \_ الاساليب \_ التدابير، ص 149 – 173. [↑](#footnote-ref-159)
160. the shellcoder،s Handbook،p 4،pal:1 [↑](#footnote-ref-160)
161. راجع في شرح هذه الادوات: القرصنة، الفنون \_ الاساليب \_ التدابير، ص37، 38، وص42، وما بعدها [↑](#footnote-ref-161)
162. القرصنة، الفنون \_ الاساليب \_ التدابير، ص165 – 169. [↑](#footnote-ref-162)
163. القرصنة، الفنون \_ الاساليب \_ التدابير، ص65. [↑](#footnote-ref-163)
164. القرصنة، الفنون \_ الاساليب \_ التدابير، ص66. [↑](#footnote-ref-164)
165. راجع في انواع المتغيرات وكيفية استخدامها: كشف اسرار البيانات \_ دليل التعلم الذاتي، ص6 - 12، وما بعدها، كتاب الاكسير، ص16، 17. [↑](#footnote-ref-165)
166. the shellcoder،s Handbook،p 62 [↑](#footnote-ref-166)
167. the shellcoder،s Handbook،p 62،64 [↑](#footnote-ref-167)
168. القرصنة، الفنون \_ الاساليب \_ التدابير، ص68. [↑](#footnote-ref-168)
169. ، خطوة بخطوة لتعلم لغة c،c++، كتاب الكتروني، فقرة رقم 1015. [↑](#footnote-ref-169)
170. البرمجة بلغة c++، ص10 -12. [↑](#footnote-ref-170)
171. gray hat hacking، Third Edition، Mc Graw Hill، 2011، p 226. [↑](#footnote-ref-171)
172. gray hat hacking،p 228 [↑](#footnote-ref-172)
173. القرصنة، الفنون \_ الاساليب \_ التدابير، ص67. [↑](#footnote-ref-173)
174. القرصنة، الفنون \_ الاساليب \_ التدابير، 209،

     gray hat hacking،p 228 [↑](#footnote-ref-174)
175. the shellcoder،s Handbook، p 65 [↑](#footnote-ref-175)
176. the shellcoder،s Handbook، p 65،66 [↑](#footnote-ref-176)
177. the shellcoder،s Handbook، p 68 [↑](#footnote-ref-177)
178. the shellcoder،s Handbook، p 68 [↑](#footnote-ref-178)
179. the shellcoder،s Handbook، p 66 [↑](#footnote-ref-179)
180. the shellcoder،s Handbook، p75 [↑](#footnote-ref-180)
181. القرصنة، الفنون \_ الاساليب \_ التدابير، ص222. [↑](#footnote-ref-181)
182. القرصنة، الفنون \_ الاساليب \_ التدابير، ص223. [↑](#footnote-ref-182)
183. the shellcoder،s Handbook، p68 [↑](#footnote-ref-183)
184. the shellcoder،s Handbook، p69 [↑](#footnote-ref-184)
185. the basic of hacking and penetration،p 70 [↑](#footnote-ref-185)
186. Metasploit، san Francisco،، no starch press، 2011، pxxii [↑](#footnote-ref-186)
187. الهكر الاخلاقي، ج5، ص296. [↑](#footnote-ref-187)
188. Metasploit، p 8 [↑](#footnote-ref-188)
189. security power tools ، orelly، 2007، p 193 [↑](#footnote-ref-189)
190. Security Power Tools، p 193 [↑](#footnote-ref-190)
191. قناة المحترف على اليوتيوب، مقدمة الى الميتاسبلويت، الجزء الاول، الحلقة رقم 929. [↑](#footnote-ref-191)
192. Metasploit، pxxii [↑](#footnote-ref-192)
193. Security Power Tools، p 194 [↑](#footnote-ref-193)
194. Security Power Tools، p 194 [↑](#footnote-ref-194)
195. the basic of hacking and penetration، p 73 [↑](#footnote-ref-195)
196. the basic of hacking and penetration، p 71 [↑](#footnote-ref-196)
197. دورة الهكر المتقدم، فيديوهات على موقع اليوتيوب، الحلقة الحادية عشرة. [↑](#footnote-ref-197)
198. linux filsystem hierarchy، verson 0.65 13inh nguyen، p: 6 – 88. [↑](#footnote-ref-198)
199. ، سطر اوامر لينكس، ترجمة عبداللطيف محمد اديب ايمش، كتاب الكتروني، حلب، بدعم من وادي التقنية،2014 م، ص26 – 29 [↑](#footnote-ref-199)
200. سطر اوامر لينكس، ص14، 34، 36. [↑](#footnote-ref-200)
201. محاضرات في مبادئ قواعد البيانات، فهد آل قاسم، ص3. [↑](#footnote-ref-201)