السرقة الإلكترونية

وحكمها في الإسلام

أحمد محمد عبد الرؤوف المنيفي

شبكة الألوكة
www.alukah.net

السرقة الإلكترونية

وحكمها في الإسلام

أحمد محمد عبد الرؤوف المنيفي
وكيل نيابة جبلة / اليمن
ahmedalmoniefy@yahoo.com

قال تعالى:

(ونزلنا الكتاب تبياناً لكل شيء)

النحل: ٨٩

الإهداء

إلى روح والديّ

رحمهما الله تعالى

شكر وتقدير

أشكر زوجتي التي تحملت معي عناء السفر والاقامة بعيداً عن الأهل والاحبة في سبيل إعداد هذا الكتاب.

أشكر القائمين على **شبكة الألوكة** الذين اتاحوا لي نشر أبحاثي على موقع الشبكة الإلكتروني، واستطعت بفضل الله تعالى ثم بفضلهم أن أخرج هذه الأبحاث الى الجمهور في اخراج جميل، وأسأل الله تعالى ان يجزيهم عن ذلك خير الجزاء، وأن يبارك جهودهم في خدمة الباحثين ونشر للعلم.

اشكر المواقع الإلكترونية التي احتفت بكتابي الأول، "منهج الحكم على المصلحة التي لا نص فيها "، الذي صدر عبر شبكة الألوكة، وعلى وجه الخصوص موقع منتدى علماء المسلمين الذي نشر نبذة عن الكتاب واتاحه للتحميل من صفحة المنتدى، وموقع الملتقى الفقهي في شبكة رسالة الاسلام الذي عرض الكتاب وكتب مقدمة جميلة عنه.

اشكر الأستاذ والقاضي الفاضل عبد القوي الخراساني الذي تعلمت منه الاتقان في العمل وقدم لي كل الرعاية والتشجيع اثناء اعداد هذه الأبحاث.

اشكر عمي الحاج عبد الغني المنيفي على يد العون التي مدها لي ولا يزال، وعلى فضله الذي لا ينكر علي وعلى اسرتي.

أشكر أخواتي الرائعات اللواتي قدمن لي كل المساعدة وفي مقدمتهن أختي أم سامح التي قدمت لي المساعدة والرعاية اثناء تواجدي في بعض المدن لاعداد هذه الأبحاث.

مدخل الى الدراسة

الحمدلله الذي بنعمته تتم الصالحات، والصلاة والسلام على سيدنا محمد أشرف المرسلين وخاتم النبيين، وبعد

تساؤلات الدراسة:

تحاول هذه الدراسة الاجابة على التساؤلات التالية:

١. ماهي جريمة السرقة الالكترونية، وما هي التعاريف التي اوردها الفقه القانوني الحديث لها، وما هي خصائصها المميزة لها.

٢. -كيف تتم السرقة الالكترونية، وهل تتكون من خطوات ومراحل متعددة، واذا كانت تتكون من مراحل، فما هي هذه المراحل، وما هو التكييف الشرعي لكل مرحلة منها.

٣. كيف عجزت القوانين الجنائية التقليدية عن مواجهة جريمة السرقة الالكترونية، وما هي المشاكل القانونية التي اعاقت تطبيقها.

٤. ما هو موقف الشريعة الاسلامية من جريمة السرقة الالكترونية، وهل تنطبق احكام السرقة في الشريعة الاسلامية على السرقة الالكترونية، وكيف يتم تطبيق الاركان والشروط المكونة للسرقة الحدية على هذه الجريمة المستحدثة، مثل هتك الحرز والاخذ والعلم والخفية ونحوها، وهل يمكن ان توجد نظائر معلوماتية لهذه العناصر، فيوجد مثلا الحرز المعلوماتي والاخراج المعلوماتي، وهكذا.

دوافع الدراسة:

١-الاضرار الناجمة عن السرقة الالكترونية:

الخسائر الناجمة عن جرائم السرقة والاحتيال المعلوماتية وصلت الى مبالغ ضخمة وهائلة لم يسبق ان وصلت اليها الجرائم التقليدية، فقد بلغت الخسائر الاجمالية لهذه الجرائم، في بعض الاحيان مليارات الدولارات، وهي تزداد سنويا بنسبة كبيرة تصل الى الضعف، وهذا الحجم الكبير من الخسائر يرجع الى انتقال معظم النشاط الاقتصادي والتجاري الى شبكة الانترنت، بالإضافة الى الانتشار الكبير لأجهزة الحاسوب، والموبايل، والمعدات الرقمية على مستوى العالم.

ووفقا لتقرير صادر عام ٢٠١٣م عن معهد المحاسبة العامة cpas في الولايات المتحدة الامريكية، كانت الخسائر التي لحقت بالشركات التجارية نتيجة للجرائم المعلوماتية بأجمالي مبالغ ٢،٧مليار دولار في العام ٢٠١٠م، ارتفعت الى ٣،٤مليار دولار في العام ٢٠١١م، وقد ذكر التقرير قائمة بأعلى الجرائم المعلوماتية الاكثر ارتكابا، وهي خمس انواع من السرقات المعلوماتية هي كالتالي:-

١-سرقة المبالغ المعادة من الضرائب Tad-re fund fraud

١- سرقة حسابات الشركات Corporate account Takeo6er

٢- سرقة البيانات الشخصية(المالية) Identity Theft

٣- سرقة البيانات الحساسة theft of sensiti6e data

٤- سرقة الممتلكات والمنتجات الفكرية Theft of intellectul property

ويلاحظ من هذه القائمة ان جرائم السرقات المعلوماتية تحتل النسبة الاعلى من الجرائم التي تعرضت لها الشركات الامريكية، وهي التي سببت ذلك القدر الهائل من الخسائر، وقد نقل التقرير عن دراسة اعدها معهد pnemen أن الشركات المشاركة في الدراسة عانت المتوسط من ١٠٢ هجوم سيبيري ناجح في العام ٢٠١٢م، مقابل ٧٤ هجوم اجرامي معلوماتي في العام ٢٠١١م، وان٥١% من كبار المدراء التنفيذيين ذكروا ان شركاتهم تمت مهاجمتها، اما يوميا، أو كل ساعة كما جاء في الدراسة الخاصة بالمعهد ان سرقات بطاقات الائتمان ارتفعت نسبة ٣٢%من العام ٢٠٠٩م الى العام ٢٠١٠م

وان الخسائر المالية للشركات التي شملتها الاستطلاع في دراسة العام ٢٠١٢م بلغت في المتوسط ٨،٩مليون دولار في السنة، ماعدا شركة واحدة بلغت خسائرها ٤٨ مليون دولار في السنة، وان هذه الخسائر كانت بنسبة ارتفاع ٦%عن العام ٢٠١١م[١].

٢- عجز الدول عن المواجهة الجنائية للجريمة:

عندما ظهرت جرائم السرقات الالكترونية لم تستطع الدول مواجهة هذه الجرائم من خلال قواعد القانون الجنائي التقليدية، وذلك بسبب وجود مشاكل وعقبات كبيرة امام تطبيق قواعد القانون الجنائي على هذا النوع من الجرائم المستحدثة، ذلك ان قواعد السرقة في القانون التقليدي بنيت على المال العادي المادي وليس المعنوي، وبالتالي من الصعب تطبيقها على المال المعلوماتي الذي يعد من الاموال المعنوية لا المادية وكان من اثر ذلك ان المشرع ذهب في كثير من الدول الغربية

---

[١] the top 5 cyber crimes،aicpa، october 2013، p 4، 5، 6

الى سن قوانين جديدة لمواجهة جرائم المعلومات ضمن حقوق الملكية الفكرية، والاسرار الصناعية، والعلامات التجارية، اعترافا منه بعدم ملائمة القانون الوضعي التقليدي للتطبيق عليها.

٣- اهمية ايجاد الحكم الشرعي للسرقة الالكترونية:

في ضوء عجز القانون الجنائي التقليدي عن مواجهة الجرائم الالكترونية، وعدم ملائمة قواعده للتطبيق عليها، كان لا بد من بيان موقف الشريعة الاسلامية من هذه الجريمة لعدة اسباب:

١- الاجابة عن التساؤل الذي يراود الكثيرين من الغيورين على الشريعة والمهتمين بتطبيقها عن كيفية تطبيق احكام السرقة في الشريعة الاسلامية على السرقة الالكترونية، وما مدى انطباق كل حكم وكل عنصر في هذه الاحكام على وقائع الانواع الحديثة من السرقات المعتمدة على الحاسب الالي.

٢- اظهار محاسن الشريعة ومدى تفوقها على القوانين الوضعية التي عجزت عن مواجهة جريمة السرقة الالكترونية، واثبات ان الشريعة الاسلامية صالحة لكل زمان ومكان، وانها كفيلة بالوفاء بحاجات المسلمين في التشريع مهما تطورت الوسائل والمخترعات والتقنيات التي تاتي بها الازمنة والعصور المتعاقبة.

٣- مساعدة الدول التي تأخذ باحكام الشريعة الاسلامية وتطبقها على انزال هذه الاحكام بجريمة السرقة الالكترونية، وذلك من خلال بيان كيفية انطباق كل حكم وكل عنصر من عناصر النموذج الشرعي لاحكام السرقة على الجوانب المختلفة لعملية السرقة الالكترونية، حتى يسهل على هذه الدول تطبيقها أو اعداد

تشريع خاص بها مستمد من احكام الشريعة الاسلامية، وبحيث تستغني عن استيراد أي تشريعات وضعية جديدة لمواجهة هذا النوع الحديث من الجرائم.

اهداف الدراسة:

يحاول البحث ان يحقق الاهداف التالية:

١- بيان ماهية جريمة السرقة الالكترونية، وشرح الخصائص المختلفة لها والتي تميزها عن بقية الجرائم.

٢- كشف الطريقة التي تتم بها جريمة السرقة الالكترونية، والخطوات المتبعة في ارتكابها، والمراحل التي تتكون منها، وإعطاء التكييف الشرعي لكل مرحلة من مراحلها.

٣- بيان عجز القوانين الوضعية التقليدية عن مواجهة جريمة السرقة الالكترونية، والمعوقات التي حالت دون تطبيق هذه القوانين على السرقة الالكترونية.

٤- بيان تفوق الشريعة الاسلامية على القوانين الوضعية وان أحكامها تنطبق على جريمة السرقة الالكترونية، وذلك من خلال دراسة تطبيق احكام السرقة في الشريعة على السرقة الالكترونية وانزال كل حكم شرعي على وقائع وعناصر الجريمة، مثل ركن الأخذ وشروط المالية والحرز ومدى تحقق الخفية في هذه الجرائم.

الاضافة العلمية:

١-كشف الكتاب عن المنهجية التي يتبعها القراصنة والمجرمون في الهجوم على شبكة او نظام الشركة الضحية، وشرح المراحل التي تتكون منها هذه المنهجية، وحاول اعطاء تكييف شرعي لكل مرحلة منها، وقد اضاف الكتاب مرحلة

أخيرة لهذه المنهجية لم تتضمنها المراجع العالمية المتخصصة في الاختراق، وهي مرحلة نسخ المعلومات والبرامج، وذلك على اعتبار ان نسخ المعلومات هو النتيجة المقصودة من جريمة السرقة الالكترونية، كما أعاد تأطير نوع من انواع الدخول الى الحاسب الآلي هو الدخول عبر الثغرات البرمجية، وأعطاه التكييف الشرعي.

٢-قدم الكتاب ولاول مرة في العالم العربي حسب علم المؤلف دراسة علمية شاملة عن تطبيق احكام الشريعة الاسلامية على السرقة الالكترونية، ومدى انطباق عناصر النموذج الشرعي للسرقة الحدية على جوانب السرقة الالكترونية، فبينت مدى انطباق ركن الاخذ على نسخ المعلومات والبيانات، وكيفية انطباق شروط السرقة المالية والحرز والخفية على جريمة السرقة الالكترونية، واعتمدت الدراسة في ذلك على النصوص الشرعية والمراجع والمؤلفات الاصلية لعلماء المسلمين.

خطة الدراسة:

بإذن الله ستكون خطة الدراسة على النحو التالي:

الفصل التمهيدي: مقدمة عن الحاسب الآلي

الفصل الأول: السرقة الالكترونية

المبحث الأول: تعريف السرقة الالكترونية وخصائصها

المبحث الثاني: مراحل السرقة الالكترونية

الفصل الثاني: الأحكام الشرعية للسرقة الالكترونية

المبحث الأول: عدم ملائمة القانون الوضعي للسرقة الالكترونية

المبحث الثاني: مدى ملائمة احكام الاسلام للسرقة الالكترونية

تمهيد: مصادر احكام السرقة في الاسلام.

المطلب الأول: ركن الاخذ

المطلب الثاني: شروط السرقة (المالية والحرز)

المطلب الثالث: الخفية

المبحث الثالث: تطبيقات السرقة الالكترونية.

وهذه الدراسة تم اعدادها سواء في جوانبها الفنية أو الشرعية بمنهج اسلامي خالص يعتمد على رد الفروع الى الأصول، والجزئيات الى الكليات، وتم تطبيق كثير من المبادئ والقواعد التي وردت في كتاب منهج الحكم على المصلحة في إعداد هذا الكتاب، وقد تمثل هذا التطبيق في رد الادوات والبرامج والجوانب الفنية الجزئية في الاختراق الى منهجيات عامة، تصلح لتطبيق احكام الشريعة الاسلامية عليها، وكذلك رد الأحكام الشرعية الجزئية الى اصولها الكلية وقواعدها العامة.

وفي الأخير أحمد الله تعالى الذي لولا فضله ونعمته علي وتوفيقه لما استطعت ان اكتب هذا الكتاب.

أحمد محمد عبدالرؤوف المنيفي

الفصل التمهيدي

مقدمة عن الحاسب الالي

الحاسب الآلي:

يعرف الحاسب الالي بانه الة وظيفتها قبول البيانات ومعالجتها لتحويلها الى معلومات [1].

ويتكون الحاسب الالي من معدات مادية وبرمجيات نتناولها فيما يلي:

أ. الوحدات المادية في الحاسب الالي:

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:

[1] مفاهيم الكمبيوتر الاساسية، ص ٢.

١.وحدات الادخال:

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

٢.وحدات الاخراج:

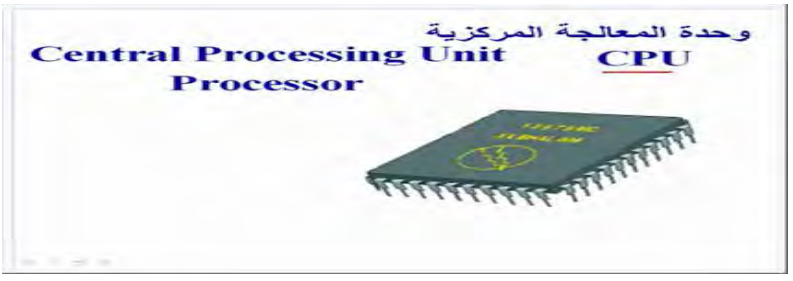
وهي التي تقوم بإظهار نتائج العمليات التي يقوم بها الحاسب الالي، ومن امثلة وحدات الاخراج ؛ شاشة الحاسب، الطابعة، السماعات.

٣.وحدة أو صندوق النظام:

يتضمن صندوق النظام وحدة المعالجة المركزية cpu، والذاكرة الرئيسية، ومكونات اخرى تركب جميعها على شريحة تسمى اللوحة الام، كما يتضمن صندوق النظام الاقراص الصلبة التي نحفظ فيها البيانات بصورة دائمة وتسمى بالذاكرة الاحتياطية مثل: C، D..الخ.

أ.وحدة المعالجة المركزية cpu

المعالج هو عبارة عن 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 وهي دوائر الكترونية، تنفذ الاعمال الحسابية، مثل الجمع والطرح والاعمال المنطقية مثل المقارنة، ووحدة اخرى للتحكم تنسق وتتحكم في عمليات الحاسب الالي[1]

الذاكرة الرئيسية:main memory:

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 [2].

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

---

[1] اساسيات الحاسب الالي، ص١٥_٥٥، ص٥٨ _ ٦٠، موسوعة الكمبيوتر الميسرة، ص٣٤، ٣٨.

[2] اساسيات الحاسب الالي، ص٣١.

التي تحمل العنوان المحدد، وعندما يجد العنوان يجلب البيانات او تعليمة البرنامج من هذا العنوان. ديفيز [1].

انواع الذاكرة [2]:

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، الشكل التالي بذاكرة الرام:

وذاكرة الرام RAM 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.

كما انه يمكن القراءة منها، والكتابة عليها، الا ان الكتابة على الذاكرة تؤدي الى محو البيانات السابقة، ويحل محلها البيانات والكتابة الجديدة.

---

[1] مفاهيم الكمبيوتر الاساسية، ص١٩.

[2] اساسيات الحاسب الالي، ص٤٤، ٤٥، مكونات الحاسب وتجميعه، ص٢٣، ٢٤، مقدمة في الحاسبات الالكترونية، ص ٢١، ٢٢.

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.

ب. البرمجيات

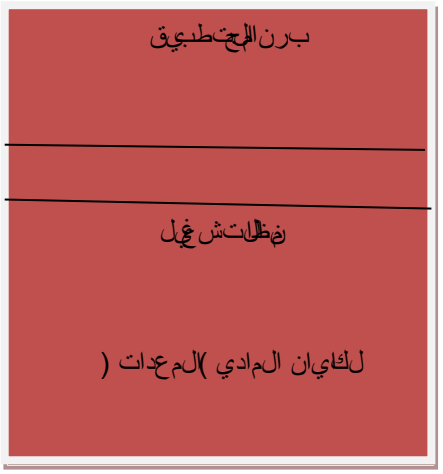
يشبه البعض العلاقة بين المعدات المادية للحاسوب، وبين البرامج، بالعلاقة بين الروح والجسد، ولا شك ان هذا التشبيه يخالف الواقع، اذ الروح من خلق الله، وهي سر من الاسرار التي يعجز البشر عن فهمها، ومع ذلك فان هذا المثال يقرب الى الذهن فكرة الصلة بين المعدات والبرامج، وذلك ان المكونات والمعدات المادية بدون 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[1]



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،

[1] موسوعة الكمبيوتر الميسرة، ص ٣٢، ٣٤، مفاهيم الكمبيوتر الاساسية، ٩٢.

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، ومن أشهر أنظمة التشغيل نظام تشغيل ويندوز windows.

الشبكات

١. 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 فإن 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 [١].

---

[١] شبكات المعلومات والاتصالات، ص٢٣، شبكات الحاسب، النظرية والتطبيق، ص١٠.

٢. 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[١].

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

٣. انواع الشبكات:-

أ. 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

---

[١] شبكات المعلومات والاتصالات، ٢٤ – ٢٦.

الخاصة بالشركات والمؤسسات المختلفة مثل المؤسسات التجارية والصناعية والاكاديمية والصحية...الخ[1].

ب. **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.

ت. **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.

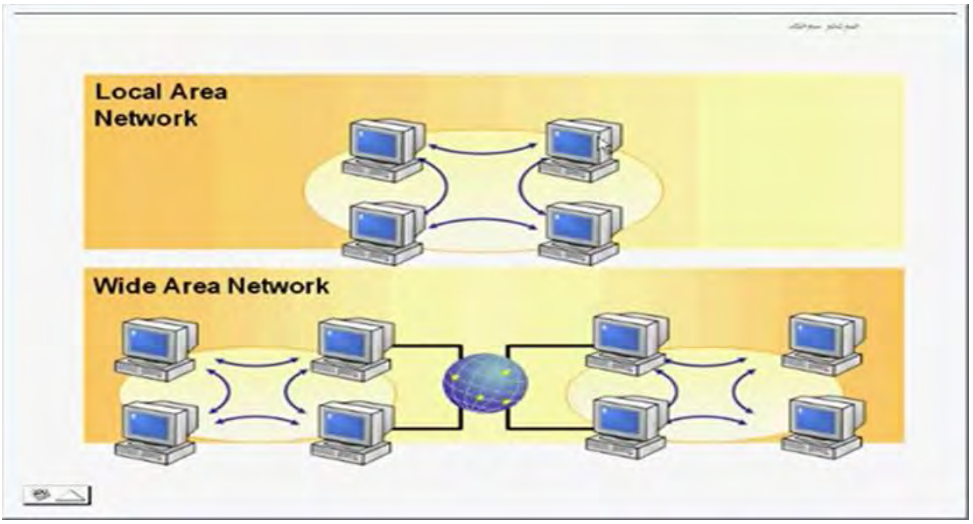
يعتبر بعض الكتاب ان شبكة الانترنت هي نوع من انواع شبكات المناطق الواسعة[2].

الشكل التالي يبين الشبكات المحلية والواسعة:

---

[1] شبكات المعلومات والاتصالات، ص٥٤، ٥٥.

[2] شبكات المعلومات والاتصالات، ص٥٩.



ث. 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 [1].

٤. وسائط الارسال:-

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 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 [2].

---

[1] تكنولوجيا الاتصالات وشبكات المعلومات، ص١٤٢، شبكات المعلومات والاتصالات ص٦١،٦٢.

[2] تكنولوجيا الاتصالات وشبكات المعلومات، ص١٤٩.

٥. 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.

٦. الانترنت enternet:

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 ١٩٦٩م(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[١].

---

[١] الانترنت: استثمار المستقبل، ٣٢١.

، 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.

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 ١٩٩٠م، فصارت شبكة nsfnet هي العمود الفقري هو اعتمادها غلى بروتوكول لشبكة انترنت بدلا عن اربانت خلال الاعوام ٩٠-٩٥م، ثم توسعت انترنت بعد ذلك توسعا هائلا داخل الولايات المتحدة الامريكية وخارجها، وكانت تشرف عليها ابتداء من العام ١٩٩٠م المؤسسة القومية الامريكية للعلوم [١].

اصبحت انترنت الان تضم الكثير من الشبكات داخل الولايات المتحدة الامريكية وخارجها.

خدمة الويب WORLD WID WEB(WWW):

تتكون خدمة الويب world wid web(www) من الاف من الحواسيب الكبيرة (المخدمات 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 [٢].

---

[١] زدني علما: انترنت، ص٤٢، مبادئ Internet، ص ١٨.

[٢] الانترنت والعولمة، ص٤٧

وهناك طريقتين لا نشاء الموقع في الويب:

الاولى:- هي اعداد حاسب ملقم Serber 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.

لتسهيل البحث عن المعلومات في الانترنت ثم ابتكار ما يعرف بعنوان الموقع العالمي uniBersal Resource location ويعرف اختصار باسم(URL)، وهذا العنوان هوعنوان 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.

الفصل الأول

السرقة الالكترونية

المبحث الاول

تعريف السرقة الالكترونية

وخصائصها

تمهيد

ان جريمة السرقة المعلوماتية هي جزء من ظاهرة اجرامية حديثة هي ظاهرة اجرام المعلومات، او الاجرام المعلوماتي، وقد نشأت ظاهرة الجريمة المعلوماتية بفعل التطور المذهل في تقنيات الحاسب الالي والاتصالات، والتزاوج الذي حصل بينهما، والذي ادى الى ظهور ابرز ابتكارات القرن العشرين وهي شبكة الانترنت العالمية world wid web.

قدمت شبكة الانترنت للإنسانية فوائد جمة في شتى مناحي الحياة، وعلى وجه الخصوص فيما يتعلق بالتجارة الالكترونية، وقطاعات الاعمال، والقطاعات المصرفية، وذلك عبر الخدمات المتعددة التي توفرها الانترنت، والتي من اهمها برنامج الويب الذي اتاح لهذه القطاعات انشاء مواقع لها في الانترنت، والتواصل مع عملائها، واداء الخدمات عبر هذه المواقع، وكذلك برنامج البريد الالكتروني الذي اتاح تبادل الرسائل بين اجزاء متباعدة من العالم بسرعة فائقة، وغير ذلك من الخدمات.

وبالتوازي مع هذه الخدمات الهائلة التي قدمتها شبكة الانترنت، نشأت ايضا على شبكة الانترنت مخاطر حديثة، وغير مألوفة، تمثل اهمها في استغلال هذه

التقنية في الولوج عن بعد الى الحواسيب الالية الخاصة بالأفراد وبالمؤسسات، وارتكاب جرائم السرقة والتخريب فيها. وعلى الرغم من ان الجرائم المعلوماتية تأخذ اشكالا عدة وانواع مختلفة مثل جرائم التخريب والاتلاف والسرقة وخيانة الامانة...الخ، فان هذه الانواع المختلفة تلتقي عند عناصر مشتركة، تعتبر بمثابة خصائص مميزة للجرائم المعلوماتية بوجه عام، وسنتناول فيما يلي تعريف الجرائم المعلوماتية بوجه عام والتعريف المختار للسرقة الالكترونية، ثم نعرض لأهم الخصائص المميزة للسرقة الالكترونية.

- **تعريف الجرائم المعلوماتية**

تعددت تعريفات الجرائم المعلوماتية تعددا كبيرا حتى احصى بعض الباحثين لها اكثر من ثلاثمائة تعريف، ويبدو ان هذا التعدد في التعاريف يرجح من ناحية الى كون الجرائم المعلوماتية هي ظاهرة حديثة، والصلة بينها وبين نظريات القانون الوضعي التقليدية هي الصلة ضعيفة، او تكاد ان تكون منقطعة، كما سنرى في الفصول التالية من هذا الكتاب، كما يرجع هذا التعدد من ناحية اخرى الى اختلاف المجالات والتخصصات التي انطلق منها الباحثون في هذا النوع من الجرائم، مثل المجالات الجنائية والمدنية ونحوها.

وقد جرى بعض الباحثين على رد هذه التعريفات الى فئات رئيسية نتناولها بإيجاز على النحو التالي[1]:-

١ـ تعريفات تعتمد على وسيلة ارتكاب الجريمة، وهذه التعريفات تقوم على اساس ان كل جريمة ترتكب بواسطة الكمبيوتر، او تقنية المعلومات هي جريمة

[1] راجع في هذه التعاريف: قانون العقوبات ومخاطر تقنية المعلومات، ص٤٩ وما بعدها، الجرائم المعلوماتية، ص ٨٦ وما بعدها، بحث جرائم الكمبيوتر والانترنت ص٤ وما بعدها.

معلوماتية، ومن ابرز هذه التعريفات تعريف الفقيه الالماني Tied emann الذي عرف الجائم المعلوماتية بانها " السلوك الغير مشروع (او الضار-بالمجتمع) الذي يرتكب باستخدام الحاسب"

وكذلك تعريف مكتب تقييم التقنية في الولايات المتحدة لجريمة الحاسب الالي بانها "الجرائم التي تلعب فيها البيانات الكمبيوترية، والبرامج المعلوماتية، دورا رئيسيا، أي ان البرامج والبيانات تستخدم كأدوات في ارتكابها ".

ب_ تعريفات تعتمد على موضوع أو محل ارتكاب الجريمة، وهو المعلومات المخزنة في الحاسب الالي، ووفقا لهذه الفئة من التعريفات فان الجريمة المعلوماتية ليست هي التي ترتكب باستخدام الحاسب الالي، او الشبكات، او ادوات تقنية المعلومات الاخرى، وانما هي الجريمه التي تقع على المعلومات الموجودة في الحاسب الالي، وتستهدفها بالنسخ، او التزوير، او الاتلاف، وسواء تمثلت هذه المعلومات في قيم واصول مالية، او برامج وقيم معلوماتية اخرى كالأبحاث والابتكارات،.....الخ.

ومن ابرز التعريفات في هذه الفئة تعريف روز نبلات.Rosenblatt وخبراء اخرين جريمة الحاسب بانها" نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه".

ج_ تعريفات تعتمد على توافر المعرفة بتقنية المعلومات، ووفقا لهذه التعريفات فانه يلزم وجود صفة شخصية لدى المجرم وهي معرفتة بتقنية المعلومات، فاذا توافرت لدى المجرم هذه المعرفة، فإننا نكون بصدد جريمة معلوماتية، ومن امثلة هذا النوع من التعريفات تعريف –Dabid Thompson لجريمة الحاسب بانها "أية جريمة يكون متطلبا لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية

الحاسب"، وكذلك لتعريف a salary بانها "فعل غير مشروع تكون المعرفة بتقنية المعلومات اساسية لمرتكبه".

دـ تعريفات مختلطة: وهي تعريفات لا تقتصر على معيار واحد فقط في تعريف الجريمة المعلوماتية، بل تجمع بين اكثر من معيار، ومن امثلة التعريفات المختلطة تعريف الجريمة المعلوماتية بأنها (جريمة يستخدم الحاسب كوسيلة، أو اداة لارتكابها، أو يمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها).

أو تعريفها بأنها (أي ضرب من النشاط الموجه ضد، أو المنطوي على إستخدام، نظام الحاسب)

ومن ابرز واشهر هذه التعريفات التعريف البلجيكي للجريمة المعلوماتية، والذي اوردته بلجيكا في تقريرها الخاص بإستبيان الغش المعلوماتي الذي اجرته منظمة التعاون الاقتصادي والتنمية عام ١٩٨٢ م بأنها (كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة، أو غير مباشرة، عن تدخل تقنية المعلومات).

التعريف المختار للسرقة المعلوماتية:

جريمة السرقة المعلوماتية هي نوع من انواع الجرائم المعلوماتية التي ترتكب بواسطة الكمبيوتر، وتقع على النظام المعلوماتي ككل، وبالتالي فهي تنطوي بوجه عام على ذات الصفات والخصائص التي تتمتع بها الجرائم المعلوماتية، ومع ذلك فان جريمة السرقة المعلوماتية تتميز عن بقية جرائم المعلومات الاخرى بانها تقع فقط على المعلومات التي لها قيم مالية، او تلك التي تتجسد في شكل اصول مالية.

و يمكن بوجه عام تعريف جريمة السرقة المعلوماتية بانها: (اخذ المعلومات والبرامج المخزنة في الحاسب الالي، أو المنقولة عبر وسائط الاتصال، باستخدام ادوات تقنية المعلومات)، وسر اختيار لفظ الاخذ في التعريف ان هذا اللفظ له مدلول عام في

احكام السرقة في الفقه الاسلامي يتسع ليشمل كل خصائص السرقة المعلوماتية، كما سنرى في موضعه

- **الخصائص العامة للسرقة المعلوماتية**

تتمتع جريمة السرقة المعلوماتية بعدد من الخصائص هي في الحقيقة من نتائج ذلك التطور الهائل في تقنية المعلومات والاتصالات، ومن اهم هذه الخصائص:

١-التنفيذعن بعد:-

تتميز جريمة السرقة المعلوماتية بان تنفيذها يتم عن بعد والجاني في مكان بعيد عن مكان الجريمة وعن مكان المال المسروق، ذلك انه بفعل تقنية المعلومات فان الجاني لا يحتاج لتنفيذ جريمته الى التواجد في مكان الجريمة وموضع المال المسروق، بل يمكنه الوصول الى المعلومات باستخدام تقنية الاتصال عن بعد، عبر الشبكات ووسائط الاتصال التي، وبعد ان يصل الى المعلومات عن طريق هذه التقنيات، يمكنه ان يقوم بنسخها والاستيلاء عليها[١].

٢_عابرة للحدودTransnotiaral:-

ولان جريمة السرقة المعلوماتية يتم تنفيذها عن بعد فإنها لا تتقيد بحدود الزمان والمكان، ولا تعترف بالجغرافيا، بل يمكن ان يكون الجاني في دولة في احدى القارات ويرتكب جريمة على احد الانظمة الحاسوبية الموجودة في دولة اخرى في قارة اخرى، فقد الغت تقنية الشبكات والاتصالات الحاسوبية حدود المكان والزمان بين الدول، وهدمت بالتالي مبدا الاقليمية الذي تقوم علية قواعد

[١] بحث الجرائم الالكترونية، ص١٩،٢٠، جرائم الكمبيوتر والانترنت، ص١٠٤، ١٠٥.

الاختصاص الجنائي الدولي، وقوانين الاجراءات الجنائية، وقد ترتب على ذلك نشوء الكثير من مشاكل الاختصاص والاجراءات التي لا يمكن حلها الا بتعاون وجهود مشتركة من مختلف دول العالم[1]

٣-خفاء الجريمة:-

أي ان جريمة الحاسوب جريمة خفية غير مرئية، فالجاني يستخدم برامجه وأدواته في التسلل خفية عبر الاسلاك، والشبكات، الممتدة حول العالم، ويصل الى الجهاز الضحية، ويقوم بالاستيلاء على المال المعلوماتي الموجود فيه بدون ان يراه احد[2].

وهذه الخفية هي التي تساعد الجاني على ان يبقى مجهولا، وبالتالي تشجع الكثير من المجرمين على ورود هذا المجال من الجرائم.

٤-صعوبة الاثبات:-جرائم الحاسوب هي جرائم ناعمة لا تترك اثار مادية ملموسة، بل تترك اثار رقمية غاية في الدقة والتعقيد، وسهلة المحو والازالة، ولذلك فان من الصعوبة بمكان اثباتها والتقاط الاثار الناجمة عنها، وحتى اذا تم اكتشاف هذه الاثار، فان الادلة المترتبة عليها تتعرض للمحو والازالة من قبل الجاني والذي يمكنه ان يستخدم برامج خاصة لتدمير الادلة والاثار الناتجة عن الجريمة[3].

وهذه الصعوبة في الاثبات هي نتيجة طبيعية ناجمة عن اختلاف وسائل الجرائم المعلوماتية عن الجرائم التقليدية، ففي حين يستخدم الجاني اساليب العنف مثل الكسر والسلاح في تنفيذه جريمة السرقة التقليدية، فان المجرم المعلوماتي يستخدم ادوات وبرامج رقمية في بيئة افتراضية لا تحتاج الى عنف.

---

[1] الجرائم الالكترونية ص١٩،٢٠، جرائم الكمبيوتر والإنترنت ص١١٩، ١٢٠.

[2] الجرائم الالكترونية ص١٩،٢٠، أمن المعلومات بلغة ميسرة ص١٢.

[3] الجرائم الالكترونية ص١٩، ٢٠، جرائم الكمبيوتر والإنترنت ص١٠٤، ١٠٥.

٥-انها لا تتطلب الازالةREMOBED: ذلك ان الجاني في الجريمة المعلوماتية لا يقوم بنقل اصل المعلومات المسروقة من مكانها والاستيلاء عليها، بل يقوم بنسخها فقط والاستيلاء على نسختها في حين يبقى الاصل لدى المالك، وهذا يساعد على جعل المجني عليه لا يشعر بارتكاب الجريمة، لأنه لا يفقد الاصل، وقد اثارت هذه المسالة خلاف عريض في الفقه حول مدى انطباق أحكام القانون الوضعي على السرقة المعلوماتية، باعتبار ان اصل المال المسروق لا ينتقل الى حيازة الجاني، بل يبقى في حيازة المجني عليه، وبالتالي لا تتحقق اركان الجريمة، وسنرى لاحقا كيف انتصر الفقه الاسلامي في معالجته لهذه المسالة في مقابل القانون الوضعي الذي بقي عاجزا امامها، ولا زال الى الان.

٦- توفر المعرفة التقنية عند مرتكب الجريمة:-

وتتميز جريمة السرقة المعلوماتية بان مرتكبها هو مجرم من نوع خاص تتوفر فيه معرفة تقنية عالية بالحاسب الالي، ونظام الاتصالات والشبكات، ومع ان جميع الجرائم المعلوماتية تتطلب معرفة تقنية في مرتكبها الا ان جريمة السرقة المعلوماتية بالذات تتطلب لارتكابها مهارات تقنية عالية اكثر عمقا مجالات الوصول عن بعد، واختراق لأنظمة الحاسوبية وانظمة الحماية الامن المعلوماتي.

٨_ فئات مرتكبي السرقة:-

في السنوات الاخيرة بدا يتبلور تصنيف رئيسي في مجتمع القراصنة وخبراء الامن، يرجع انواع المخترقين والقراصنة، الى نوعين هما:-

أ- Black hacker: هم المجرمون المحترفون الذين يرتكبون جريمة سرقة المعلومات من خلال التسلل الغير مشروع الى نظام الحاسب الالي، بغرض سرقة المعلومات والقيم المخزنة فيه.

ب-whit hacker: ويسمون ايضا بالقراصنة الاخلاقيين، وهم عبارة عن خبراء امن يقومون باختراق نظام الحاسوب باستخدام نفس تقنيات واساليب الهكر المجرمون اصحاب النوع الأول، ولكنهم يختلفون عنهم في الهدف، اذ ان هدف هذه الفئة هو اختبار نظام الامن من الحاسب الالي، ومعرفة نقاط الضعف فيه، وترقيعها واصلاحها قبل ان يستفيد منها النوع الاول من مجرمي المعلومات.

المبحث الثاني

مراحل السرقة الالكترونية[1]

على خلاف جرائم السرقة التقليدية، فان جريمة السرقة 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 السرقة المعلوماتية، او مراحل القرصنة بوجه عام، بحسب ما تواضع وتعارف عليه مجتمع القراصنة، من خمس مراحل:-

١- الإستطلاع reconnaissance

٢- مسح المنافذ scanning

٣- الدخول الى النظام gaining access

٤- الحفاظ على الدخول maintaining access

٥- التغطية أو تنظيف الاثار coбering track

---

[1] للاطلاع على شرح تفصيلي لهذه المراحل راجع كتاب مراحل السرقة الالكترونية للمؤلف (يصدر قريبا انشاء الله)، والمراجع المشار اليها فيه.

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[1].

وسوف نتناول فيما يلي المراحل اللازمة لارتكاب جريمة السرقة الالكترونية وهي الاستطلاع، والمسح، والدخول، ونسخ المعلومات.

المطلب الأول

مرحلة الاستطلاع او جمع المعلومات[2] 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

---

[1] the basic of hacking and penetration، p 11

[2] راجع في هذه المرحلة:

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

the basic of hacking and penetration،، p16-18

مداخله ومخارجه، ومواقع المال، واجهزة الرقابة والحراسة...الخ، ثم تقوم بارتكاب الجريمة، وهذا يتماثل مع ما يتم في مرحلة الاستطلاع.

والمعلومات التي يقوم المخترق أو 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.

ومن اهم المعلومات التي يجب ان يقوم الجاني 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

ومرحلة الإستطلاع 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.

ويتم جمع المعلومات في هذه المرحلة 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:-

١- الدخول على الموقع او البرنامج، وفي حالة الموقع يقوم الجاني بكتابة اسم الموقع على محرك البحث، او نسخ الرابط على المتصفح، ثم فتح صفحة الموقع، وفي حالة البرنامج يتم تنزيل او تركيب البرنامج اولا، ثم فتح صفحة البرنامج.

٢- كتابة اسم الشركة على نافذة البحث المختارة في صفحة الموقع اوالبرنامج، وضغط زر البحث.

٣- يقوم الموقع او البرنامج بالبحث وجلب جميع البيانات والمعلومات المتوفرة في الانترنت عن الشركة الهدف على شكل تقرير.

٤- يقوم الجاني بمراجعة تقرير المعلومات وتحليله ودراسته واستخلاص المعلومات المفيدة منه، مثل عناوينIP، ارقام الموظفين وارقام التلفونات، ونظام التشغيل وحسابات المستخدمين، خادم اسماء النطاق....الخ.

٥- يقوم الجاني بهذه الخطوات في عدة برامج ومواقع، وينتقل بين الادوات والمواقع المختلفة بحثا عن اكبر قدر من المعلومات.

٦- يقوم الجاني بحفظ هذه المعلومات اما الكترونيا في مجلد او ملف، او كتابتها وتسجيلها على الاوراق.

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:-

١- جمع المعلومات عن بيئة النظام المعلوماتي المستهدف، والبنية المعمارية التي يتكون منها.

٢- الكشف عن نقاط الضعف في النظام، وافضل الطرق لاستغلالها.

٣- 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.

انواع 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، وسواء 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:-

١- 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.

٢- 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.

٣- معلومات عن المنظمة:

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

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.

١- 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[١]:-

١- البرمجيات المستخدمة واصدارها.

٢- نظم التشغيل المستخدمة.

٣- معلومات الاتصال مثل اسماء وارقام الهاتف، وعناوين البريد الإلكتروني، وموقع المشرف.

٤- خوادم الويب المستخدمة واصدارها، ومنصة السكربت.

٥- الموقع الجغرافي للشركة او المنظمة الهدف.

٦- سياسات الامن او الخصوصية التي تشير الى انواع اليات الامن الموضوعة.

٧- الارتباطات الى خوادم اخرى والكينونات والشركات المرتبطة.

٨- 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

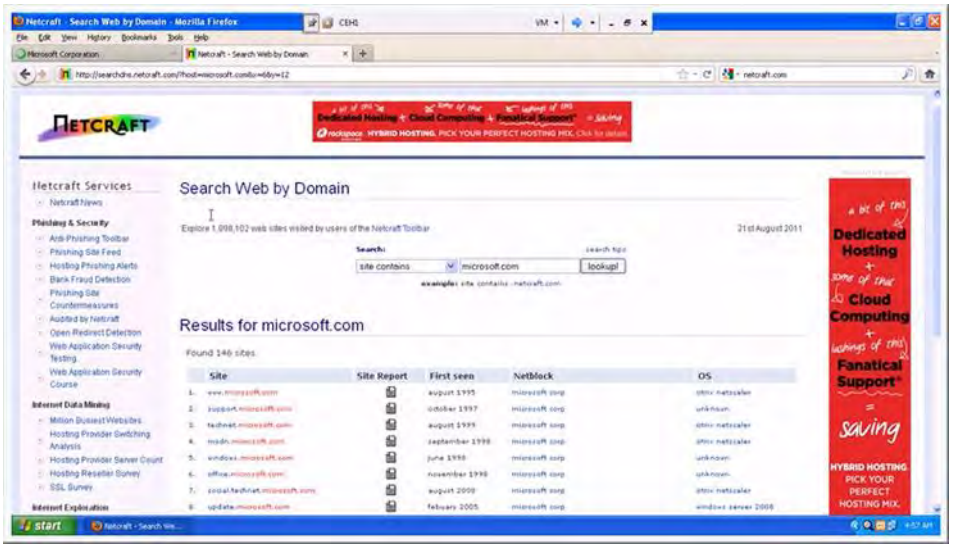
---

[١] الهكر الاخلاقي، ج٢ ص٤٥،٣٣، االقرصنة تحت الاضواء ص ٢٦، ٢٧.

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.

٢-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 serbes الخاص بالمنظمة، وتأخذ 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 [1].

٣_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 الاسم الخاص بها لتضمن ان شركة او منظمة واحدة فقط تستخدم هذا الاسم، وعندما تقوم اي شركة او منظمة بتسجيل اسمها، 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[2].

تقوم الية البحث في whois باستيراد هذه المعلومات وغيرها من سجلات التسجيل وجلبها الى من يطلبها، ويتم البحث داخل قواعد بيانات Whois من خلال الدخول الى موقعها على الانترنت، وعندما نقوم بفتح صفحة الموقع في الانترنت نكتب عنوان الشركة او المنظمة المستهدفة بالاختراق في خانة البحث،

---

[1] the basic of hacking and penetration،p31

كورس الهكر الاخلاقي، youtube، الحلقة الثالثة.

[2] CEH-Certified Ethical Hacker Study Guide،p،42

القرصنة تحت الاضواء ص٢٦

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[1]

- **البحث في خوادم DNS**:

الخادم او الملقم server:

تقوم الشركات والمؤسسات الكبيرة مثل البنوك بتخصيص 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 serber.

يتمتع الحاسوب الخادم / او الملقم serberبقدرات 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 serber، ويحصل على المعلومات المطلوبة منة.

تسمى هذه الطريقة في العمل داخل الشبكات بطريقة العميلclient-الخادمserber، وهي اساس العمل في الشركات الكبيرة، وبمقتضاها يخصص

---

[1] CEH-Certified Ethical Hacker Study Guide،p،42

كورس الهكر الاخلاقي، youtube، الحلقة الثالثة.

حاسوب بموصفات عالية كخادم للحواسيب الاخرى المرتبطة بالشبكة، ولا يقتصر عمل الحاسوب الخادم serber 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 الخادمserber، 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 للشبكة opreating system، لان النظام التشغيل هو الذي يوفر برمجيات طريقة الخادم العميل، ويتيح الحاسوب العمل كخادم serber [1]

خوادمDNS:

يخزن ملقم DNS معلومات تتضمن اسماء الحواسيب أوالخوادم التابعة للمنظمة أو الشركة، وارقام IP الخاصة بها، في سجلات تسمى سجلات موارد، وتعتبر ملقمات او خوادم الاسماء (DNS) هي المكان الرسمي الذي تخزن فيه المعلومات التي تتعلق بكل الأجهزة التابعة لشبكة المنظمة، وهي المصدر الرسمي

---

[1] تكنولوجيا الاتصالات وشبكات المعلومات ص١٤٥، ١٤٦، الشبكة المحلية للمعلومات، ص٢١ – ٢٣، الدليل الجديد لترابط الحواسيب ص ٤٦، وما بعدها.

للمعلومات عنها[1]، والتي من أهمها الاسم او العنوان الالكتروني لكل حاسب والذي يتكون من جزئين: اسم الحاسب هو اسم لكمبيوتر محدد "سيرفر "، واسم الشبكة الخاصة بشركة او منظمة ما، وكذلك رقم IP وهو رقم فريد يميز الحاسب الآلي ويعرف به داخل الشبكة.

وتشمل سجلات الموارد في خادم DNS عدة انواع رئيسية[2] من اهمهاسجل A host والذي يتضمن اسم أو عنوان الحاسب أو الخادم ورقم IP الخاص به، وفي حاله تلقيه طلب السؤال عن اسم معين فانه يعيد اليه رقم IP الخاص بهذا الاسم وسجل PTR والذي ويعالج طلبات لمعرفة الاسم أو العنوان الالكتروني الخاص برقم IP معين، حيث انه يرد باسم أو عنوان الحاسب أو الخادم المطابق لعنوان IP. أي انه يقوم بعملية تحويل من IP الى الاسم.

- **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 المقابلة لها، ومن خلال هذه العناوين يستطيع الجاني كسب الوصول الى أي جهاز في الشبكة واختراقه[3].

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

---

[1] طقم التدريب على الشهادة +Network، ٤١٠ -٤١٢.

[2] كورس الهكر الاخلاقي، youtube، الحلقة الثالثة، طقم التدريب على الشهادة +Network، ص٤١١، وما بعدها.

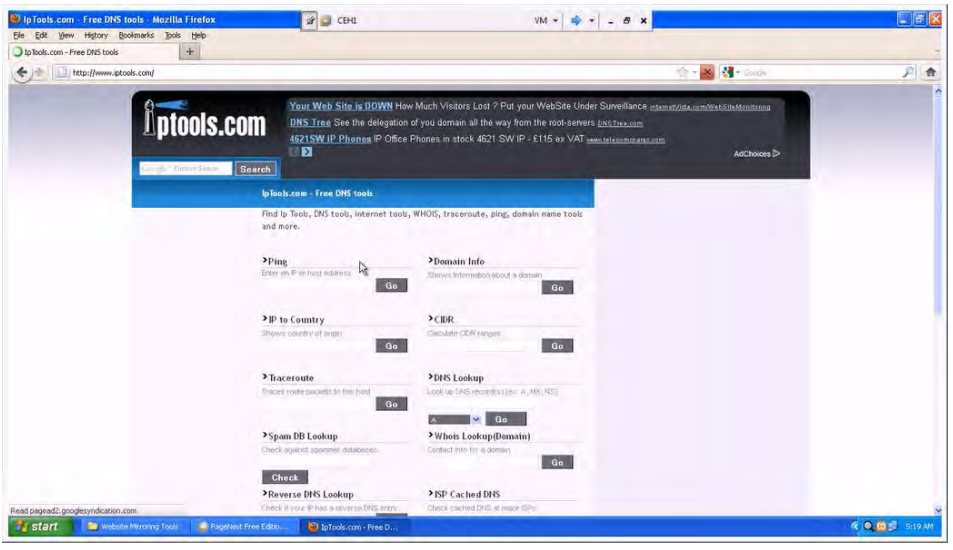
[3] the basic of hacking and penetration،p،32-34

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:

أ- البحث في المواقع[1]:-

هناك العديد من المواقع التي توفر امكانية البحث في خوادم DNS، مثل موقع IP TOOL -DNS stuff -DNS tools، 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 MD، ثم يضغط زر البحث وعندئذ يعيد الموقع كامل المعلومات عن المنظمة التي يتضمنها السجل المحدد.

الشكل التالي يبين صفحة هذا الموقع:



[1] كورس الهكر الاخلاقي، youtube، الحلقة الثالثة.

ب- عمليات نقل المنطقة[1]:-

لتخفيف الحمل عن الخادم الرئيسي DNS والحد من عمليات الاختناق في الشبكة، 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

---

[1] دورة احتراف الهكر الاخلاقي،، youtub، الحلقة الثالثة.

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، والاداة Nslood up[1].

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.

التكييف الشرعي لمرحلة الاستطلاع:

في هذه المرحلة لا يتم الاتصال المباشر بالهدف، فالادوات والطرق المستخدمة فيها لا تتصل الكترونيا بنظام الحاسب الالي المستهدف، بل يتم جمع المعلومات من خلال مصادر ومواقع عامة متوفرة في الانترنت، او من خلال اساليب التفاعل المباشر مع الموظفين، من دون المساس بالحاسب 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 تعتبر مرحلة تحضير للجريمة ولا تدخل في الفعل المادي المكون لها.

من الناحية الشرعية فإن افعال التحضير للجريمة لا يعاقب عليها إلا إذا كانت تشكل معصية في حد ذاتها، كما لوكان الجاني قد قام بإعداد الشراب المسكر وتحضيره للمجني عليه تمهيدا لسرقته، فرغم أن اعداد الشراب المسكر عمل

---

[1] دورة احتراف الهكر الاخلاقي، youtube، الحلقة الثالثة.

تحضيري إلا أن الجاني يعاقب عليه لأن حيازة المسكر معصية في حد ذاتها [1]، أما اذا كان العمل التحضيري لا يشكل معصية فإنه لا يعاقب عليه شرعا.

وبناء على ذلك فإنه يمكن القول أن اعمال الاستطلاع وجمع المعلومات هي أعمال تحضيرية لا يعاقب عليها شرعا لأنها لا تشكل معصية في حد ذاتها.

المطلب الثاني

مرحلة المسح scanning

تهدف مرحلة المسح scanning الى التعرف على الحواسيب المتصلة التي تعمل على الشبكة، والخدمات (التطبيقات والبرامج)التي تشغلها هذه الحواسيب والتي تعد منافذ يمكن الدخول من خلالها الى النظام، وهذه المرحلة ضرورية لأن الجاني مهما جمع من المعلومات فإنه لا يستطيع الوصول الى أي حاسب آلي بعيد واختراقه إلا إذا كان هذا الحاسب متصلا بالانترنت، أو بشبكة المؤسسة أو الشركة التي ينتمي اليها.

ويتم التعرف على الانظمة المتصلة والقابلة للوصول عبر الانترنت من خلال ارسال اشارة إتصال الى عنوان ip للحاسب الهدف، وفي حالة اذا استجاب الحاسب الهدف لهذه الرسالة، فإننا نعرف ان هذا الحاسب متصل وفعال.

---

[1] الأحكام العامة للنظام الجنائي في الشريعة الإسلامية، ص٢١٩.

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 (هذا يناظر رقم التلفون الذي يحتوي على رقم الجهاز ورقم المدينة)،

عناوين الحواسيب الآلية تسهيل الوصول الى اجهزة الكمبيوتر المتصلة بشبكة الانترنت، ومواقع 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"، وهو عبارة عن رقم يتكون من اربع مجموعات ارقام، تفصل بينها نقاط، ويشير الى عنون جهاز الكمبيوتر المحدد، مثل1 -16 -54 -128، وتماثل هذه الارقام ارقام الهاتف التي تتكون من عدد من الارقام تشير الى جهاز الهاتف المطلوب[1].

واذا اراد المستخدم الوصول الى موقع معين على شبكة الانترنت، كان عليه ان يحفظ الارقام التي تشير الى هذا الموقع، 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،

---

[1] زدني علما: انترنت، ص٢٣، الانترنت: استثمار المستقبل، ص٣٦.

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، والاسم 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.

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[1].

التعرف على الحواسيب المتصلة بالانترنت:

يستخدم البرنامج ping في معرفة ما اذا كان الحاسب الآلي متصلا بالانترنت ويعمل، وتقوم هذه الاداة بتوليد رسالة طلب إتصال وارسالها الى النظام الهدف، وتسال هذه الرسالة الحاسب الآلي الهدف ما اذا كان لازال متصلا؟، وفي حالة ما اذا كان الهدف فعالا ومتصلا بالأنترنت فانه يجيب برسالة: نعم انا فعال، اما في حالة ما اذا كان الحاسب غير فعال فانه يأخذ مهلة ولا يرد، وفي هذه الحالة اما يكون النظام الهدف في حالة ايقاف التشغيل، او في حالة عدم الاستجابة.

---

[1] لمزيد من التفاصيل، راجع:

- شبكات الحاسب، النظرية والتطبيق، ص٤٧٥ – ٤٩٠،
- طقم التدريب على الشهادة +Network، ص ٢٢٤، ٢٢٥.

الشكل التالي يبين هذه العملية:

مسح المنافذ:

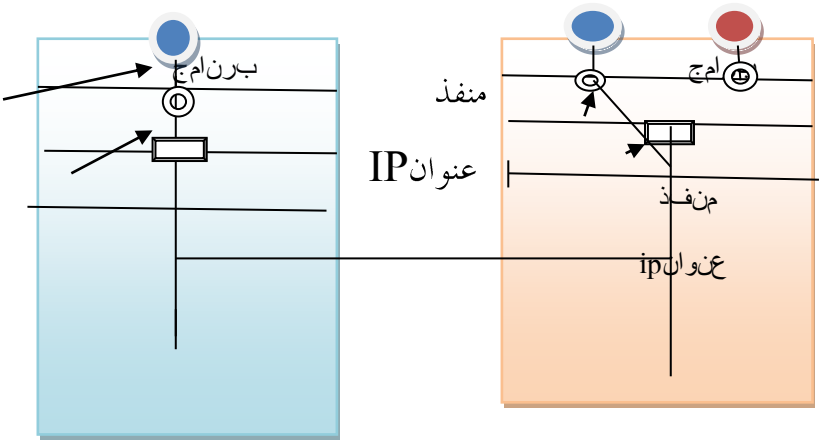
وبعد أن يتم التحقق من ان الحاسب الالي الهدف متصل بالانترنت، يقوم الجاني بعملية مسح المنافذ من أجل التعرف على الخدمات أوالبرامج العاملة في الحاسب الآلي الهدف مثل خدمة تلنت telnet، او خدمة ftb، او غير ذلك من الخدمات، ويمثل البرنامج أو الخدمة العاملة على النظام منفذ مفتوح للدخول اليه، ثم بعد اكتشاف المنافذ المفتوحة يقوم الجاني باستغلال أي منفذ مفتوح لاختراق النظام المستهدف.

مفهوم المنافذ:

عندما نرسل أي رسالة سواء كانت رسالة بريد الكتروني أو طلب اتصال من المتصفح بموقع ويب معين...الخ، فإنه توجد برامج داخل نظام التشغيل في حاسبنا الآلي هي التي تسجل عنوان الجهاز المرسل اليه على هذه الرسالة، ويتكون هذا العنوان من عنوان IP للجهاز المستقبل، وعنوان البرنامج داخل هذا الجهاز، وتصل الرسالة اولا الى عنوان IP للجهاز المتلقي، ثم تتوجه بعد ذلك الى عنوان

البرنامج او الخدمة المرسلة اليه، فاذا كانت عبارة عن رسالة بريد الالكتروني فإنها تتوجه أولا الى عنوان IP للجهاز المتلقي، ثم تواصل السير الى عنوان برنامج البريد الالكتروني الموجود داخل هذا الجهاز، واذا كانت عبارة عن طلب اتصال مع خدمة الويب فإنها تتوجه الى عنوان IP للحاسب الالي المتلقي ثم الى عنوان خدمة الويب. وهكذا... الخ، وتسمى عناوين البرامج والخدمات داخل الحاسب الآلي بالمنافذ، وتوجد في كل نظام منافذ متعددة بحسب عدد البرامج والخدمات المشغلة في هذا النظام.

يبين الشكل التالي اتصال من برنامج معين في حاسب الى برنامج في حاسب آخر:



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.

- **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 رقم٢١ وبرنامج تلنت يربط الى المنفذ رقم٢٣.

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 برنامج مخدم الملفاتFTP يتم دائما ربطة بالمنفذ رقم ٢١وبرنامج الويب يتم دائما ربطة بالمنفذ رقم ٨٠، 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/serbices على نظام und 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

برنامج وكيل يرتبط بهذه المنافذ ذات الخدمات النادرة، وعندما يتلقى البرنامج الوكيل اي طلب اتصال لبرنامج معين على عنوان الخدمة، فان البرنامج الوكيل يقوم بإنشاء اتصال بين العميل وبين البرنامج او الخدمة النادرة المطلوبة.

كيف يقوم الجاني بالاتصال 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:

رقم المنفذ (البرنامج) عنوانip

192-168-2-10 :21

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

رقم المنفذ اسم النظام

FTP-datum com :21

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

كيف يتم مسح المنافذ:

يستخدم الجاني برنامج مخصص لمسح المنافذ ويرسل هذا البرنامج الموجود في جهاز الجاني إشارة إتصال SYN الى المنفذ المحدد في جهاز المستقبل (جهاز لشركة أ، بنك..الخ) وينتظر تلقي الجواب او الرد من ذلك المنفذ، اذا كان المنفذ في حالة انصات أي جاهز للاتصال فانه يعيد جواب برسالة موافقة ACT/SYN، ومعنى هذه الرسالة ان البرنامج او الخدمة تعمل على المنفذ وجاهزة للاتصال، أو بعبارة اخرى ان المنفذ مفتوح للدخول، اما اذا رد جهاز المستقبل 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، الشكل التالي يبين هذه العملية:

الاداة NMUP:

الرنامج NMAPهي 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.

الخرج الذي تعيده NMAP يتضمن انواع عديدة من المعلومات ومن أهمها المنافذ المفتوحة والخدمات والبرامج العاملة عليها[1].

التكييف الشرعي لمرحلة المسح:

مرحلة المسح تتصل اتصالا مباشرا مع النظام الهدف، لأننا نقوم في هذه المرحلة بإرسال رسائل الى الجهاز الهدف لمعرفة ما اذا كان متصل بالانترنت أم لا، ثم بعد ان نتحقق من أنه متصل بالانترنت، نقوم بمسح المنافذ، أي ارسال طلبات الاتصال الى البرامج والخدمات داخل هذا الجهاز لمعرفة أي منها في حالة عمل، وهذا الاتصال النشط والمباشر يعتبر بدء في تنفيذ الجريمة، وبعض الكتاب يشبهونه بالطرق على الابواب والنوافذ، فاذا ضبط الجاني في هذه المرحلة، أي مرحلة

---

[1] للاطلاع على شرح لمرحلة المسح راجع كتاب مراحل السرقة الالكترونية للمؤلف والمراجع العربية والانجليزية المشار اليها فيه، وراجع أيضا في الفقرات السابقة التي شرحناها المراجع التالية:

CEH-Certified Ethical Hacker Study Guide،

the basic of hacking and penetration

االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات

الهكر الاخلاقي ج٤

كورس الهكر الاخلاقي، youtube، الحلقة الثالثة

، شبكات الحاسب، النظرية والتطبيق.

طقم التدريب على الشهادة +Network

المسح، فانه يكون في حالة شروع من منظور القانون الوضعي، وأما من الناحية الشرعية، فان القاعدة عند جمهور الفقهاء ان ضبط الجاني قبل أن يتم السرقة ينظر فيه الى الفعل، فإذا كان فعله يشكل معصية يعاقب بالتعزير، وإن كان لا يشكل معصية، فإنه لا يعاقب عليه[1]، ولكن يوجد من فقهاء المسلمين من يرى أن ضبط الجريمة قبل أن تتم يعتبر شروعا فيها ومعصية تستحق التعزير، ففي جريمة السرقة يعزر الجاني إذا ضبط ومعه آلة السرقة أو مترصدا للمال أو اذا تعرض للنقب أو لفتح الباب، أواذا دخل الحرز و لم يأخذ، والتعزير هنا على ان هذه الافعال شروع في الجريمة وليس معصية مستقلة كما يذهب اليه الجمهور، ويستنبط التعزير عند صاحب هذا الرأي من عقوبة الجريمة التي شرع فيها الا انه يكون اقل منها[2].

فعلى مذهب الجمهور يمكن القول أن الجاني لا يعاقب إذا ضبط في مرحلة المسح، وأما على الرأي الأخير فإنه يعاقب لأنه شرع في الفعل، وتكون عقوبته التعزير لأن الجريمة لم تتم.

---

[1] التشريع الجنائي الإسلامي ج٢ ص ٥٦٥، ٥٦٦.

[2] الأحكام السلطانية للماوردي ص٣١١، ٣١٢.

المطلب الثالث

مرحلة الدخول الى الحاسب الآلي

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.

(١)

الدخول عن طريق كسر كلمة المرور

من خلال المراحل السابقة، الاستطلاع، المسح، 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

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[1]، 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، 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.

---

[1] بروتكول IP/TCP الدليل الكامل، ص٢٣٥، طقم التدريب على الشهادة +Network، ص٤٩٨.

كسر كلمة المرور:

كما تقدم فإن الجاني بعد أن يتحقق من أن الحاسب الهدف متصل بالانترنت، يقوم بعملية مسح منافذ على النظام الهدف من اجل معرفة المنافذ المفتوحة في هذا النظام، واذا اكتشف الجاني ان خدمة (برنامج) ما من خدمات الاتصال عن بعد في حالة عمل، يقوم 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 البرامج التي تساعد الجاني في تخمين كلمة المرور بصورة مؤتمتة، ومن اشهر هذه البرامج، الاداة هيدراhydra، والاداة ميدوسا medusa، وتسمى هذه الادوات ادوات كسر كلمة المرور على الانترنت، وتعتمد هذه الأدوات 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 (البرنامج) المطلوب الاتصال بها، وعند ذلك ترسل الاداة تركيبة من اسم المستخدم وكلمة المرور الى الخدمة، واذا كانت هذه التركيبة خاطئة، او كان احد الامرين: اسم مستخدم او كلمة المرور غير صحيح، فان الاداة تعرض رسالة خطأ ويفشل الدخول، وتقوم 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[1].

---

[1] the basic of hacking and penetration،p،67

هجوم رفع الامتياز:

الغالب 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 ــ وحتى رؤيتها ــ على مدير النظام فقط او مستخدمين محددين ومعينين، وبوجه عام فان انظمة تشغيل الملقمات تعتمد على سياسة امان من عدة عناصر على النحو التالي[1]:

١- تحدد انظمة تشغيل الشبكات المستخدمين الذين يحق لهم الدخول الى نظام التشغيل، ويختار مدير النظام مستخدمين محددين 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.

---

[1] صيحة الحق، دروس مرئية عن الشبكات، ج١٣.

٢- 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، 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.

طرق رفع الامتياز:

- **الأدوات getadmin والاداة sechele**

التقنية المستخدمة: التقنية التي تستخدمها هذه الادوات هي الارتباط بعملية تمتلك امتيازات مدير النظام، ومن ثم ادراج شيفرة خبيثة (برنامج صغير) 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[1]، وهذه الثغرة يستطيع المستخدم استغلالها من اجل ادراج شيفرات (برامج) خبيثة داخل هذه العملية وتنفيذها بامتيازات المدير[2]، ومن اهم هذه الشيفرات

---

[1] احترف اوراكل خطوة بخطوة، ص ١٢٢٣.

[2] قراصنة قواعد البيانات بلا اقنعة، ص٢٠ – ٢٦.

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.

أ- 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 خدمةftp التي تأتي مع سماحيات افتراضية في الكتابة والتنفيذ، وهذا يتطلب وجود خطا في اعدادات تكوين نظام التشغيل بما يسمح بترك مثل هذه السماحيات الافتراضية[1].

---

[1] القرصنة تحت الاضواء، ص ١٨٨، ١٨٩.

ب- الاداة sechole:

تقوم الاداة sechole بوظيفة مماثلة للأداة getadmin فهي تضيف المستخدم الى مجموعة المدراء local administraters، وهى تستخدم نفس التقنية: الارتباط بعملية ذات امتياز ثم تشغيل شيفرة ضمن تلك العملية تقوم بإضافة المستخدم الحالي الى المجموعة adreinistraters [1]، 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 sechole الى احد دلائل IIS وتنفيذها بواسطته[2].

التكييف الشرعي للدخول بكسر كلمة المرور:

من وجهة نظر عدد من الكتاب المتخصصين فان كلمة المرور تعد بمثابة القفل الذي يوضع على الابواب والخزائن، وتمثل منافذ الكمبيوتر الابواب والنوافذ التي توضع عليها الاقفال، أما الملفات فهي بمثابة الخزائن التي تتضمن المعلومات، بالتالي يمكن القول ان الدخول الى اجهزة الكمبيوتر بطريقة كسر كلمة المرور يناظر

---

[1] القرصنة تحت الاضواء، ص١٩٠.

[2] المرجع السابق، ص١٩٠ – ١٩٢.

الدخول الى المنازل بطريقة الكسر للاقفال والاحراز، وكسر الملفات ككسر الصناديق والخزائن المقفلة، ومن الناحية الشرعية فان الدخول بطريقة الكسر يعد هتك للحرز بالقوة والكسر ويدخل الجريمة في عداد جرائم السرقة الحدية.

(٢)

الدخول عن طريق الثغرات البرمجية

– الثغرات البرمجية هي: عيوب او هفوات في تصميم البرنامج او في البيئة التي يعمل البرنامج ضمنها[١].

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[٢]، 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[٣]، وفي كل الاحوال يبحث المهاجم عن هذه الثغرات، وعندما يتمكن من العثور عليها وايجادها يقوم باستغلالها من خلال تمريب 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.

---

[١] القرصنة، الفنون ــ الاساليب ــ التدابير، ص١٤٣.

[٢] االقرصنة تحت الاضواء، ص٣٥٠.

[٣] القرصنة، الفنون ــ الاساليب ــ التدابير، ص١٤٥.

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 oberflow

- **مفهوم فيض الذاكرة المؤقتة:**

الذاكرة:-

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

١-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.

٢-ذاكرة الROM: وهى الذاكرة التي تخزن فيها البرامج الدائمة الخاصة بنظام الحاسب مثل برنامج الاقلاع وبرنامج الدخل والخرج.

٣-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 الفقرة 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[1]، بالنسبة للمبرمج او القارئ 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.

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[2]

---

[1] مكونات الحاسب وتجميعه، المملكة العربية السعودية، ص٢٣ -٢٦، اساسيات الحاسب الالي، ص ٣٠ -٣٣.

.

[2] كشف اسرار البيانات _ دليل التعلم الذاتي، ص١١.

المخزن المؤقت او الBuffer:

مجموعة محددة من المواقع المتجاورة في الذاكرة، 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[1]، والشكل التالي يمثل مصفوف داخل الذاكرة:-

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، فكل برنامج يعمل في الذاكرة يكون له مخزن مؤقت أو مصفوفة من خانات الذاكرة مخصصة لتخزين البيانات، 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 (مصفوفة خانات) في الذاكرة محدود بحجم

---

[1] راجع فيما تقدم: the shellcoder's Handbook، anley، chris، Wiley، 2007، p12.

وطول معين، مخصص لتخزين 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 الى الذاكرة الى تنفيذه وتمكين المهاجم من الدخول الى النظام والسيطرة عليه[1].

يرجع امكانية حدوث فيض الذاكرة المؤقتة Buffer oϐerflew الى عدم وجود آلية او وظيفة داخل لغة البرمجة 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

---

[1] راجع في كل ذلك:

االقرصنة تحت الاضواء، ص٣٤٩، القرصنة، الفنون _ الاساليب _ التدابير، ص١٤٨،

12،p، 2007، Wiley، chris، anley،s Handbook،the shellcoder

المخزن المؤقت الخاص ببرنامج ما[1]، فلغة c،c ++ تترك المسؤولية عن سلامة البيانات الى المبرمج، فاذا لم يكن المبرمج حذرا فانه يقع في هذا الخطأ اثناء تصميم البرنامج[2]، 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.

ومن أشهر البرامج التي تستعمل هذه الثغرة في الدخول الى الحاسب الآلي أداة الإختراق الشهيرة ميتاسبولايت.

التكييف الشرعي للدخول عبر الثغرات البرمجية:

من الممكن تشبيه الثغرات البرمجية بالثقوب والفتحات الصغيرة التي قد توجد في جدار المترل او السور المحيط به، ويستطيع المجرم في السرقة العادية ان يستغل هذه الثقوب والفتحات بطريق مختلفة مثل توسيعها ليتمكن من الدخول، او ادخال يده من الثقب وجلب المسروق اذا كان المسروق في متناول يده، او استخدام عصا او اداة طويلة معقوفة وتمريرها من الثقب اذا كان المسروق بعيدا، او غير ذلك من الصور التي لا حصر لها والتي تستخدم في استغلال مثل هذه الثقوب والفتحات الموجودة في تصميم المنازل.

من الممكن ايضا تشبيه الثغرات البرمجية بمناطق ضعف في جدار المترل، او في الابواب والنوافذ، ويمكن للجاني فتح ثغرة في هذه المناطق الضعيفة من خلال الهجوم عليها بأدوات واسلحة مختلفة، مثل اطلاق الرصاص عليها، او استخدام معول، او نحو ذلك من الادوات والاسلحة.

---

[1] 12،p، 2007، Wiley، chris، anley،s Handbook،the shellcoder

[2] القرصنة، الفنون _ الاساليب _ التدابير، ص١٤٨.

إن ترجيح اي من التشبيهين ينتج عنه آثار خطيرة من الناحية الشرعية، لأنه يترتب عليه القول بتوافر الحرز من عدمه، والذي يبدو من خلال الدراسة العميقة لهذا النوع من الدخول ان التكييف الثاني، أي أنها منطقة ضعف وليس فتحة، هو الارجح، وهو الذي يتفق مع حقيقة الثغرات البرمجية، لأن الدخول في هذا النوع يتم عن طريق ارسال مقذوف برمجي ملحق به برامج تحكم، ويقوم المقذوف البرمجي بإختراق منطقة ضعف في نظام التشغيل أو في البرامج والدخول الى الحاسب الآلي، ثم تنتشر داخل الحاسب برامج التحكم الملحقة بهذا المقذوف والتي تمكن الجاني من السيطرة على الحاسب، وهذه العملية تشكل هتكا للحرز بالقوة وفقا لأحكام الشريعة الإسلامية [1].

[1] للإطلاع على شرح تفصيلي لهذا النوع من الدخول والتقنيات والأدوات الخاصة به، راجع كتاب: مراحل السرقة الالكترونية للمؤلف (يصدر قريبا انشاء الله).

المبحث الرابع

مرحلة نسخ البيانات والمعلومات

نسخ البرامج والبيانات هو المرحلة النهائية في جريمة السرقة الالكترونية، وهو الهدف المقصود منها، وتتم عملية النسخ مع بقاء اصل المسروق لدى المجني عليه، فلا ينتقل هذا الاصل الى الجاني، وانما تنتقل اليه نسخته فقط، وهذا الامر يعد من اهم خصائص السرقة الالكترونية، وقد اثارت هذه الخصيصة مشاكل قانونية وعقبات كثيرة حالت دون تطبيق القانون الوضعي التقليدي على جرائم السرقة الالكترونية، وذلك لان اهم اركان السرقة في هذا القانون هو خروج المسروق نهائيا من حيازة المجني عليه، في حين انه في جريمة السرقة الالكترونية يبقى اصل المسروق لدى المجني عليه، وفي حيازته، ولا ينتقل الى الجاني.

سوف نتناول المشكلة القانونية بالتفصيل في الجزء الثاني من هذا الكتاب، اما في هذا المبحث فسنقتصر على بيان عملية النسخ التي تتم للبرامج والبيانات في جريمة السرقة الالكترونية، ونمهد لذلك بالإشارة الى اماكن التخزين في نظام الكمبيوتر، لأنها من الامور الضرورية لفهم الصورة الكاملة لجريمة نسخ للبيانات 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[1]: 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.

---

[1] دورة الهكر المتقدم، فيديوهات على موقع اليوتيوب، الحلقة الحادية عشرة.

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

Bideos\: 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[1]: 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:

---

[1] Linuɗ filsystem Hierarchy ،ɓerson 0.65 13inh Nguyen، p: 6 – .88

Root\:

\D6 : وهذا المجلد يتضمن كل الاجهزة المرتبطة بنظام التشغيل، مثل محركات الاقراص المرنة والصلبة والطابعات.. الخ، ويوجد ملف لكل جهاز من هذه الاجهزة داخل المجلد d6، 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.

\Home: يتضمن المجلدات الخاصة بالمستخدمين، فنظام يونيكس ينشئ لكل مستخدم مجلد يكون بمثابة المترل 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.

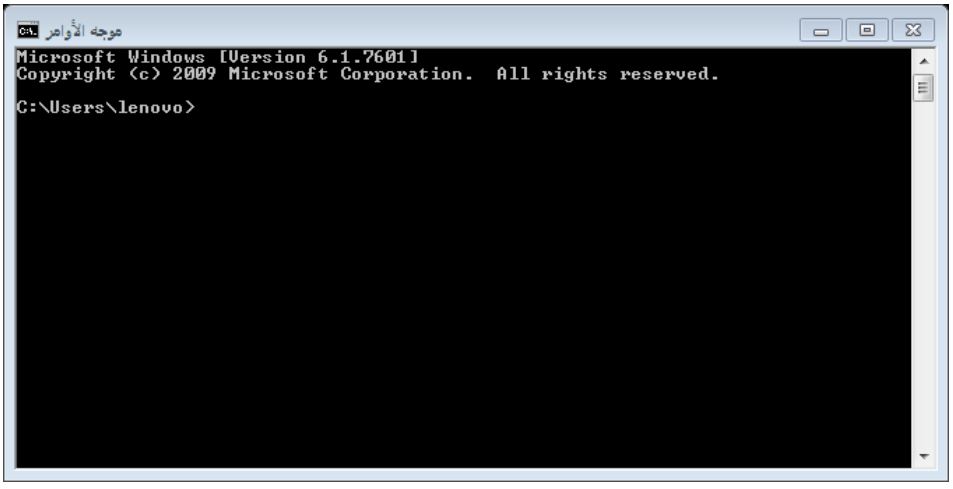
وعادة ما يتم ضبط انظمة التشغيل على مسح محتويات هذه الملفات المؤقتة التي تنشئها البرامج، عند كل اعادة تشغيل للنظام.

Bar\: 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.

لكن العلماء تمكنوا بعد ذلك من اختراع الواجهة الرسومية، والتي مثلت فيها الاوامر بأيقونات واشكال سهلة، مما ادى الى انتشار الكمبيوتر بحجم هائل في كل انحاء العالم

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

طريقة كتابة الاوامر[1]:

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:

---

[1] سطر اوامر لينكس، ص٢٦ – ٢٩.

```
Cp item1     item2
```

اي انسخ المجلد item1 الى المجلد item2.

واذا اراد نقل ملف يكتب الاتي:

```
M6  item1       item2
```

اي انقل المجلد

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.

البيانات المستهدفة للسرقة:

البيانات التي يستهدفها الجناة عادة من عملية اختراق نظام الضحية تشمل عدة انواع اهمها على الاطلاق هي البيانات المالية، سنشير هنا بايجاز الى بعض هذه الانواع، لكننا سنعود لمناقشتها تفصيلا في الفصل الثاني في مبحث مستقل بمناسبة بيان مدى انطباق احكام السرقة في الفقه الاسلامي عليها، ومن هذه الانواع:

١–البيانات المالية للهوية الشخصية مثل رقم بطاقة الائتمان، ورقم الحساب، ورقم الضمان الاجتماعي

٢– الودائع البنكية

٣– المعلومات مثل المقالات والابحاث والكتب والصوت والصور والفيديو

٤–البرامج مثل برامج الالعاب، وبرامج الاعمال التجارية.

الفصل الثاني

الأحكام الشرعية للسرقة الالكترونية

المبحث الاول

عدم ملائمة القانون الوضعي للسرقة الالكترونية

مقدمة:

باختراع الحاسب الالي وبزوغ ما يسمى بثورة الاتصالات والمعلومات، بدات تقنية المعلومات والانترنت تغزوا بالتدريج مناحي الحياة المختلفة في المجتمع الحديث، حتى اصبحت اليوم موجودة في جل الاعمال التجارية والحياتية للناس، واصبحت الاعمال والصفقات التجارية تتم من خلال الحاسب الالي وتقنية الاتصالات والانترنت، واصبح العالم كله قرية افتراضية، داخل هذه التقنية.

في موازاة هذا التطور الهائل في مناحي الحياة، ظهر نوع جديد من الجرائم اسفرت عنه تقنية المعلومات والانترنت، واستطاع المجرمون ان يستخدموا هذه التقنية في ارتكاب العديد من الجرائم، وكان من اهم هذه الجرائم جريمة السرقة الالكترونية، والتي نجم عنها خسائر بمليارات الدولارات.

وعندما بدات تعرض جرائم السرقات الالكترونية على القضاء ظهرت مشاكل وعقبات امام تطبيق قواعد القانون الجنائي الوضعي على هذا النوع من الجرائم المستحدثة، لكون قواعد السرقة في القانون الوضعي بنيت على المال العادي،

وغير ملائمة بالتالي للتطبيق على المال المعلوماتي، وكان من اثر ذلك ان انقسم الفقه والقضاء فريقين، الاول يريد تطويع وتحوير النصوص لتستوعب الجرائم الجديدة ولو ادى ذلك الى تشويه المبادئ التي قامت عليها هذه النصوص، واما الفريق الثاني فقد امتنع عن تطبيق نصوص القانون الوضعي التقليدي على هذه الجرائم، اما المشرع فقد ذهب في كثير من الدول الغربية الى سن قوانين جديدة لمواجهة جرائم المعلومات ضمن حقوق الملكية الفكرية والاسرار والعلامات التجارية، اعترافا منه بعدم ملائمة القانون الوضعي التقليدي للتطبيق عليها[1].

في هذا المبحث سوف نناقش اهم العقبات التي واجهت تطبيق القانون الجنائي الوضعي على جرائم السرقات الالكترونية.

عدم ملائمة اركان السرقة في القانون الوضعي[2]:

يجمع الشراح على ان اركان السرقة في القانون الوضعي هي ثلاثة.:

١. الاختلاس

٢. ان يكون محل السرقة مالا منقولا مملوكا للغير

٣. القصد الجنائي

وسوف نتناول فيما يلي اهم اركان السرقة في القانون الوضعي ومدى ملائمتها للتطبيق على جرائم السرقات الالكترونية.

---

[1] راجع فيما تقدم: لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الالية للمعلومات، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، الحماية الجنائية البيانات، بحث مقدم لمؤتمر الكمبيوتر والانترنت، عدم ملائمة القواعد التقليدية، بحث مقدم لمؤتمر الكمبيوتر والانترنت

[2] بحث لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الالية للمعلومات.

عدم ملائمة ركن الاختلاس:

يتحقق الاختلاس عندما يقوم الجاني بفعل مادي ينقل به الشيئ من حيازة المجني عليه الى حيازته هو، بما يقتضيه وذلك من حرمان المجني عليه نهائيا من المال المسروق، وانتقاله الى حيازة المتهم[1]، والاختلاس بهذا المعنى يقصد به ازالة العلاقة بين شيئ ما وبين صاحبه، بان يخرج الجاني هذا الشيئ من حيازة حائزه ويدخله في حيازته هو[2].

ولا يتحقق هذا المفهوم للاختلاس، في جريمة السرقة الالكترونية، وذلك لانه في السرقة الالكترونية لا ينتقل الشيئ المسروق من حيازة المجني عليه الى حيازة الجاني، وانما الذي تنتقل الى حيازة الجاني هو نسخة من هذا الشيئ فقط، واما اصل الشيئ فيبقى في حوزة المجني عليه ولايحرم منه المجني عليه على الاطلاق، مثال ذلك سرقة البرامج او المنشورات الالكترونية المكتوبة مثل المؤلفات والابحاث او الصوتيات والفيديوا والصور، ففي كل هذه الانواع ينتقل الى الجاني نسخة فقط من المادة عندما يقوم باختلاسها وتتريلها الى جهازه، واما اصل المادة فيبقى في مكانه في حوزة صاحبه يتصرف فيه كيف يشاء.

ويترتب على هذا ان الركن الاساسي لجريمة السرقة في القانون الوضعي وهو اخراج المال المسروق من حيازة المجني عليه وحرمانه منه لا يتحقق عملا ولا يمكن تطبيقه على جريمة السرقة الالكترونية، لان المال المسروق في هذه الجريمة يبقى في حوزة المجني عليه حتى بعد تمام عملية السرقة.

وقد ادى هذا افيما بعد لى اضطراب االفقه والقضاء، وافلات العديد من افعال السرقة للبرامج والمعلومات من العقاب،

---

[1] شرح قانون العقوبات، القسم الخاص، ص٤٤٦، الحماية الجنائية للتعاملات الالكترونية، ص٤٥

[2] قانون العقوبات، جرائم القسم الخاص، ص١١٠٥.

٢.مشكلة الطبيعة المعنوية للمعلومات:

وفقا لقواعد القانون الوضعي فان الاصل ان السرقة تقع على مال مادي قابل للحيازة والنقل.

واما الاموال المعنوية التي ليس لها كيان مادي مثل الافكار والاراء والابتكارات، فلا ترد عليها السرقة، لأنها غير قابلة للحيازة والنقل، وانما يتم حمايتها من خلال حق المؤلف.

وبما ان المعلومات والبرامج من الاشياء المعنوية وليس المادية، فان صفة المنقول لا تنطبق عليها، لانها ليس لها وجود مادي محسوس، فلا يمكن بالتالي ان ترد عليها جريمة السرقة وفقا لقواعد القانون الوضعي.

٣_عدم الاعتراف بصفة المالية للمعلومات:

هناك خلاف في الفقه والقضاء الوضعي حول توافر صفة المال للمعلومات، فهناك جانب منه ينفي عنها صفة المال، وهناك من يرى انها تعد من الاموال لانها اصبحت موضوعا للتجارة واصبح تباع ولها سوق خاص بها.

المبحث الثاني

مدى ملائمة احكام الاسلام للسرقة الالكترونية

- **تمهيد: مصادر أحكام السرقة في الاسلام:**

معظم الاحكام التي تناولت جريمة السرقة في االشريعة الاسلامية وردت في القرآن وفي السنة النبوية، وقد عمل الفقهاء على بسط هذه الاحكام بالشرح والتحليل في كتيهم حتى يتمكن القضاة والحكام من تطبيقها،فاستنبطوا الشروط اللازمة لتطبيق حد السرقة من النصوص الخاصة بهذه الجريمة، وذكروا كثيرا من الامثلة والتطبيقات المتنوعة لهذه الشروط والتي كانت موجودة في بيئاتهم وازمانهم، ومع ان تلك التطبيقات والامثلة كانت انعكاسا للزمن الذي عاشوا فيه، الا انها ترجع الى اصول عامة صالحة للتطبيق في كل زمان ومكان، وكان دور الفقهاء انهم طبقوا تلك الاصول على ما هو موجود في عصرهم من وقائع، وقد وجدوها مسايرة لازمانهم وعصورهم المختلفة، وافية بحاجاتهم، فلم تتخلف عنهم وقت حاجتهم اليها، وذلك لان شريعة الاسلام شريعة خالدة، احكامها صالحة لكل زمان ومكان

١ــ اية السرقة:

الاية التي تضمنت حكم السرقة في القرآن هي قوله تعالى (والسارق والسارقة فاقطعوا ايديهما جزاء بما كسبا نكالا من الله والله عزيز حكيم) المائدة: ٣٨.

وهذه الاية وردت بالفاظ العموم المعرفة بالالف واللام(السارق والسارقة)، ولذلك فهي تحمل على العموم عند الجمهور ويدخل فيها كل انواع السراق[1].

قال ابن عبد البر في الاستذكار: ((هذه الاية عامة في كل سرقة كيفما وجدت، وعلى اي حال جرت الا ما خصه الشرع،...))[2].

وعلى هذا يمكن القول ان اية السرقة هي ايه عامة تنطبق على كل انواع السرقة مما هو معروف ومما يجد عبر الزمن، طالما تحققت فيها تلك الشروط الخاصة التي ورد بها الشرع في السنة النبوية المطهرة، والتي من اهمها كما سنرى النصاب والحرز.

ولكن اذا وردت صورة نادرة للسرقة و لم توجد قرينة على ان الشارع قد قصدها بهذه الاية، كما انه لم توجد قرينة ايضا على ان الشارع لم يقصدها، فهل تدخل ضمن عموم هذه الاية وتطبق عليها، بناء على عموم لفظها، ام انها لا تدخل في عموم الاية بناء على ندرتها؟

يذهب جمهور الاصوليين الى ان الفرد النادر او الصورة النادرة تدخل في اللفظ العام، وذلك مراعاة لشمول اللفظ وعمومه[3].

وبناء على ذلك فان اي صورة نادرة من صور السرقة مما يجد على المسلمين، و لم توجد قرينة على انها مقصودة بالاية او انها غير مقصودة، فانها تدخل في عموم اية السرقة وتطبق عليها حكمها، وذلك مراعاة لشمول لفظ الاية وعمومه، ويمكن تطبيق ذلك في الوقت الحاضر على سرقة المعلومات والبرامج.

---

[1] احكام الفصول في احكام الاصول، ج١، ص٣٨٢.

[2] التمهيد والاستذكار، ج ٢٠، ٢٤٩..

[3] التمهيد في تخريج الفروع على الاصول، ص٤٣٦، الوجيز في اصول التشريع الاسلامي، ص١٦١، ١٦٢

٢.اركان شروط السرقة:

تضمنت السنة النبوية عدد من النصوص التي خصصت بعض اطلاق ايه السرقة وعمومها، مثل احاديث النصاب والحرز، وقد استنبط العلماء من هذه الاحاديث شروط تطبيق حد السرقة. ويمكن اجمال اهم الشروط والاركان التي استنبطها الفقهاء لتطبيق حد السرقة في الاتي:

١. ركن الاخذ

٢.ان يكون المسروق مالا يبلغ النصاب

٣. ان يكون المال محرزا.

٤.الخفية.

وسوف نبين في المباحث التالية مدى ملائمة هذه الاحكام والشروط للتطبيق على السرقة الالكترونية.

المطلب الأول

ركن الاخذ

الاخذ عند الفقهاء قد يكون خفية، او محاربة، او اختلاسا، او قهرا وغلبة، او مما اؤتمن عليه الشخص، فالاخذ خفية يسمى سرقة، والاخذ محاربة بقطع الطريق يسمى حرابة، وخطف المال خلسة من يد صاحبه يسمى اختلاسا، والاخذ عن طريق قهر الماخوذ منه وقسره بفضل قوة يسمى غصبا، والاخذ من الوديعة او مما اؤتمن عليه الشخص يسمى خيانة[1].

وعلى هذا فان الاخذ عند الفقهاء هو اصل عام يرجع اليه انواع مختلفة من السرقات، والاختلاف بين هذه الانواع انما يرجع الى زيادة بعض الشروط او تخلفها، واما معنى الاخذ وحقيقته فهو واحد، ولذلك قال الدسوقي في حاشيته[2]: ((فاخذ جنس يشمل الغصب وغيره))، اي ان الاخذ اصل عام يشمل انواع مختلفة من السرقة مثل الغصب وغيره.

والدليل على ان الاخذ اصل عام يشمل انواع مختلفة من السرقات هو قوله تعالى (وكان وراءهم ملك يأخذ كل سفينة غصبا) الكهف، الاية: ٧٩.

ووجه الاستدلال بالاية انها جعلت الغصب نوعا من انواع الاخذ[3]، فدل ذلك على ان الاخذ اصل عام يندرج فيه عدة انواع وصور من السرقة ومنها الغصب.

---

[1] المقدمات الممهدات، ج٢، ص٤٨٩، اختلاف الفقهاء، ص ١٧٠.

[2] حاشية الدسوقي على الشرح الكبير، ج٣، ص٤٤٢.

[3]: روح المعاني، ج١٦، ص ٤٦٧.

واذا كان الاخذ اصل عام لمختلف انواع السرقة، ومعناه فيها جميعها واحد، فهل من مقتضى معناه ولوازمه انهاء حيازة المجني عليه للشيئ المسروق، وازالة يده عنه، ام انه يكفي لتحقق ركن الاخذ في السرقة مجرد اثبات يد السارق على المال ولو بقيت يد المجني عليه قائمة وثابتة على المال المسروق، اي من دون ازالة يد المجني عليه عن المسروق؟

تطرق الفقهاء الى هذه المسالة عند كلامهم عن الغصب، والغصب عند الفقهاء هو اخذ المال بالقوة والقهر، وهو نوع من انواع الاخذ وصورة من صوره، وينطوي بالتالي على حقيقته ومعناه، ويتحقق الغصب عند الشافعية بمجرد اثبات اليد على مال الغير، فلا يشترط عندهم ازالة يد المجني عليه عنه، وهذا معناه ان الاخذ عندهم هو وضع اليد او ثبوت الحيازة على المال من قبل الجاني، ولو كانت يد المجني عليه لا زالت ثابتة عليه، فيتحقق الغصب عندهم بوجود الحيازتين معا للمال المسروق الى جانب بعضهما البعض، حيازة الجاني، وحيازة المجني عليه.

واما الغصب عند الحنفية فهو ازالة يد المالك عن ماله، ولا بد عندهم من ازالة يد المجني عليه من المال وانهاء حيازته له لتحقق الغصب، فوجود الحيازتين معا غير متصور عندهم[1].

وبما ان الغصب هو نوع من انواع الاخذ، وينطوي على جوهر الاخذ وحقيقته، فانه يمكن القول ان الاخذ عند فقهاء الشافعية بكل صوره يتحقق باثبات اليد فقط، وذلك خلافا للحنفية الذين يرون الاخذ ازالة يد واثبات يد، ازالة يد المالك، واثبات يد السارق.

---

[1] بدائع الصنائع، ج٧، ص٢١١، رد المحتار، ج٦، ص٢٥٩.

ويصور الامام الزنجاني من كبار ائمة الشافعية هذا الخلاف فيقول في كتابه تخريج الفروع على الاصول[1]:

((ذهب اصحاب الشافعي رضي الله عنه الى ان حد الغصب اثبات اليد العادية على مال الغير.

وذهب اصحاب ابي حنيفة رضي الله عنه الى ان حد الغصب اثبات اليد العادية وتفويت اليد المحقة او قصرها))

واما الامام الكاساني، وهو من كبار ائمة الفقه الحنفي، فهو يبين مترع الخلاف ويعرض حجة الشافعي في ان الغصب هو اثبات اليد فقط، فيقول: (اما حد الغصب فقد اختلف العلماء فيه، قال ابو حنيفة وابو يوسف رضي الله عنهما: هو ازالة يد المالك عن ماله المتقوم على سبيل المجاهرة والمغالبة بفعل في المال،....

وقال الشافعي هو اثبات اليد على مال الغير بغير اذنه والازالة ليست بشرط)

ثم يبين الامام الكاساني حجة الشافعي فيقول: –

(احتج – اي الشافعي – لتمهيد اصله بقوله سبحانه وتعالى: وكان وراءهم ملك ياخذ كل سفينة غصبا جعل الغصب مصدر الاخذ فدل على ان الغصب والاخذ واحد، والاخذ اثبات اليد، الا ان الاثبات اذا كان باذن المالك يسمى ايداعا واعارة وابضاعا في عرف الشرع، واذا كان بغير اذن المالك يسمى في متعارف الشرع غصبا) [2]

فالامام الكاساني يرى ان الاخذ هو فقط اثبات اليد على المال من غير ازالة يد مالكه عنه، وان الشافعي جعل الغصب نوع من انواع الاخذ، وبالتالي جعله بمعناه هو اثبات اليد فقط دون الازالة.

---

[1] تخريج الفروع على الاصول، ص١٩٥.

[2] بدائع الصنائع، ج٧، ص٢١١.

فهذين الامامين الجليلين قد صورا الخلاف بين الشافعية والحنفية في حقيقة الاخذ او الاستيلاء على المال في جريمة الغصب، والذي يفهم من كلامهما ان الاخذ او الاستيلاء عند الشافعية يتصور فيه وجود الحيازتين معا للجاني والمجني عليه على ذات المال المسروق، لان الاخذ عندهم يتم بوضع اليد دون شرط ازالة يد المجني عليه، ولا يوجد عندهم ما يمنع ان تثبت على المال يد الجاني الى جانب يد المجني عليه، وتكون هناك بالتالي حيازتين للمال المسروق، في نفس الوقت، حيازة الجاني وحيازة المجني عليه.

والامثلة التي اوردها الشافعية لهذا النوع من الاشتراك في الحيازة هي مثالين: مثال الجلوس على الفراش، ومثال ركوب الدابة، وسوف نبين هذين المثالين فيما يلي[1]:

المثال الاول: هو غصب الفراش عن طريق الجلوس فيه الى جانب المالك، فبهذا الجلوس يتحقق الغصب عندهم ولو لم ترفع يد المجني عليه عن الفراش، اي ولو بقي المجني عليه جالسا على الفراش الى جانب الغاصب، والملاحظ في هذا المثال انه وجدت الحيازتين معا الى جانب بعضهما البعض، وعدت حيازة الجاني غصبا، لان فعله هو غاية الاستيلاء في هذه الحالة.

المثال الثاني: هو مثال الدابة، وهو ان يسير الجاني الدابة اثناء ركوب صاحبها عليها او يركب عليها الى جواره، فيعد فعله غصبا مع ان يد المالك لا زالت ثابتة على الدابة، لان هذا الفعل هو غاية الاخذ والاستيلاء في هذه الصورة.

---

[1] راجع في هذين المثالين: مغني المحتاج، ج٢ ص٣٧٣، العزيز شرح الوجيز، ج٥، ص٤٠٦، روضة الطالبين، ج٥، ص٨، نهاية المحتاج، ج٥، ص٢١٥، ٢١٦.

ومع أن الشافعية أوردوا هذين المثالين فقط في جميع كتبهم، فانه يصح قياس اي امثلة اخرى من نوعها على ذات القاعدة، ولا فرق بين هذين المثالين وبين غيرهما مما يجد على حياة الناس كالاموال المعلوماتية ونحوها مما قد يجد مستقبلا، قال الشربيني في مغني المحتاج: (وكلام المصنف قد يفهم ان غير الدابة والفراش من المنقولات أنه لا بد فيها من النقل،.....

ثم قال: **والمعتمد انه لا فرق بينهما وبين غيرهما**)[1].

مفهوم الاخذ بين السرقة والغصب:

معنى الاخذ في السرقة عند الشافعية لا يختلف عن معناه في الغصب، فالاخذ عندهم واحد في كل صوره، وهو اثبات اليد على مال الغير، والاختلاف بين السرقة والغصب لا يرجع الى معنى ألاخذ في كل منهما، لأن معناه فيهما واحد، وإنما يرجع الى صفة هذا الأخذ، وذلك أن الاخذ في السرقة يكون خفية، وأما في الغصب فهو يتم جهرا وباالقهر والإكراه، ولذلك فإنه يمن القول أنه لا يشترط عند الشافعية في السرقة ازالة يد المجني عليه عن المسروق وانهاء حيازته له، بل قد يحدث الاخذ بازالة اليد او بدونه.

انطباق ركن الاخذ على نسخ المعلومات:

بحسب مذهب الشافعية الذي يعتبر ان الاخذ هو اثبات اليد على مال الغير من غير ازالة يد المالك، فان ركن الاخذ في السرقة يكون منطبقا على فعل النسخ الذي تتم به السرقة الالكترونية، وذلك ان مفهوم الشافعية للاخذ يتصور وجود يد المالك على المال الى جانب يد الجاني، وهو ما يتحقق عملا في السرقة

---

[1] مغني المحتاج، ج٢، ص٣٧٣.

الالكترونية، حيث يبقى اصل المال تحت يد المالك من غير نقص، وتذهب النسخة الى الجاني.

وعلى هذا ينطبق على السرقة الالكترونية اول ركن للسرقة الحدية في الشريعة الاسلامية، وهو ركن الاخذ.

حكم القراءة دون النسخ:

قد يتمكن الجاني من الدخول الى الحاسب الآلي للمجني عليه، ولكنه لا يقوم بنسخ البرامج أو المعلومات، وإنما يكتفي بالاطلاع عليها وقراءاتها فقط، فهل يعد فعله هذا جريمة شرعا، وهل تدخل هذه الجريمة ضمن جرائم السرقة الحدية؟

يتصل الحكم الشرعي لهذه الحالة بمسألة هي محل خلاف في الفقه الاسلامي، وهي مسألة مالية المنفعة، وما إذا كانت المنفعة تعد من الأموال ام لا، وقد ذهب الإمام أبو حنيفة الى أن المنافع ليست أموال، لأن المال عنده ما يمكن إحرازه وإدخاره لوقت الحاجة، والمنافع لا يمكن إدخارها وإحرازها.

ولكن جمهور الفقهاء على أن المنافع هي أموال، وقد أوردوا لذلك حجج كثيرة، من اهمها ان المال يدفع لتحصيل المنفعة كما في عقد الإجارة، وان المنفعة تجوز مهرا في الزواج، والمهر لا يكون إلا مالا.

والمنفعة التي هي مال عند الجمهور هي منافع كل ما له منفعة يستأجر عليها ويدفع العوض مقابلها، مثل منفعة البيت والكتاب والعطر، فما لا تصح إجارته كالنخل والشجر والنقود لا تعد منفعته مالا، وتضمن المنافع عند الشافعية، إما بالتفويت كأن يطالع في الكتاب أو يركب الدابة أو يشم المسك، أوبالفوات وهو

ضياع المنفعة من غير انتفاع كإغلاق الدار من دون السكن فيها أو مسك الكتاب مدة دون قراءته[1]، ويكون الضمان في الحالتين بأجرة المثل.

فعلى مذهب الجمهور يشكل الإطلاع على المعلومات وقراءتها جريمة لأنه إعتداء على منفعة متقومة، أي لها قيمة مالية.

وأما بالنسبة لتكييف هذه الجريمة وما إذا كانت تدخل في عداد جرائم السرقة أم لا، فإنه يمكن القول أنها تدخل في جرائم السرقة، لأن ركن السرقة هو الأخذ، والأخذ هو إثبات اليد على المال، وبما أن المنفعة مال فإنه يمكن اثبات اليد عليها.

وهذا الحكم يتفق مع ما يذهب اليه بعض فقهاء القانون الوضعي من أن الالتقاط للمعلومة عن طريق البصر وتخزينها في الذهن يعتبر مشكلا لجريمة سرقة[2].

---

[1] العزيز شرح الوجيز، ج٥، ص٤١٦، الحاوي الكبير، ج٧، ص١٦٢، مغني المحتاج، ج٢، ص٣٨٦، نهاية المحتاج، ج٥، ص٢٥١.

[2] قانون العقوبات ومخاطر تقنية المعلومات، ص٢٣٢.

المطلب الثاني

شروط السرقة: المالية والحرز

تمهيد: دور العرف في شروط السرقة

- **قاعدة يرجع في الالفاظ المطلقة الى العرف:**

قال الإمام ابن تيمية: (أن هذه الأسماء – أي الألفاظ المطلقة – جاءت في كتاب الله وسنة رسوله معلقا بها أحكام شرعية، وكل إسم فلا بد له من حد، فمنه ما يعلم حده باللغة، كالشمس والقمر والبر والبحر والسماء والأرض، ومنه ما يعلم بالشرع، كالمؤمن والكافر والمنافق، وكالصلاة والزكاة والصيام والحج، وما لم يكن له حد في اللغة ولا في الشرع فالمرجع فيه الى عرف الناس)[1].

ومعنى ذلك أن كل لفظ او اسم علق به الشرع احكاما شرعية، فانه لا بد له من حد يبين مضمونه ويعرف معناه،

والاسم الذي نص عليه الشرع، اما ان يعلم حده ومعناه من اللغة مثل الشمس والقمر والبر والبحر

واما ان يعلم معناه من الشرع كالمؤمن والكافر والصلاة والصيام...الخ.

فاذا لم يكن له ضابط لا في اللغة ولا في الشرع، فانه يرجع في تحديد معناه ومضمونه الى عرف الناس، مثل النفقة، والمالية، والحرز، والكفاءه في الزواج[2].

---

[1] القواعد الكلية لابن تيمية، ص٢١٠، ٢١١.

[2] راجع في هذه القاعدة أيضا: الأشباه والنظائر للسيوطي، ج١، ص٢٣٥، المنثور للزركشي، ج٢، ص٣٥٦.

والدليل على انه يرجع الى العرف في بيان هذه الالفاظ المطلقة ما يلي[1]:

١.قوله تعالى(فكفارته اطعام عشرة مساكين من اوسط ما تطعمون اهليكم) سورة المائدة: ٨٩.

فهذه الاية نصت على ان الاطعام الذي يجب في الكفارة هو الوسط المعتاد والمتعارف عليه في اطعام الاهل، اي انها احالت في بيان مقدار الطعام على العرف، وبما ان طعام الكفارة من الاحكام المطلقة التي لا يوجد لها حد او معنى في الشرع او اللغة، فقد دلت الاحالة على العرف في بيانه، على انه يرجع الى العرف في بيان الالفاظ والاسماء المطلقة.

٢.قوله تعالى (وعلى المولود له رزقهن وكسوتهن بالمعروف) البقرة: ٢٣٣.

فقد نصت الاية على انه يرجع في تحديد النفقة من وقت وملبس الى المعروف، والمقصود بالمعروف في الاية المتعارف عليه بين الناس، ولما كانت النفقة من الالفاظ والاحكام المطلقة والتي لم يضبطها الشرع بحد او معنى معين، فقد دلت الاحالة على العرف في بيانها انه يرجع في بيان الاحكام والالفاظ المطلقة الى العرف.

كيفية تطبيق القاعدة:

الالفاظ المطلقة التي يرجع فيها الى العرف هي احكام كلية ينتمي اليها مالاينحصر من الوقائع الجزئية، فالنفقة مثلا حكم كلي، والمالية والحرز ونحوها احكام كلية، فاذا وردت مسالة جزئية تنتمي الى هذه الكليات،مثل نفقة مرضع معينة سعاد او زينب مثلا، او وردت مسالة تنتمي الى المالية او الحرز كمسالة مالية المعلومات او

[1] العرف والعادة في راي الفقهاء، ص٨٩، ٩٠.

حرزها، فانه يتم تحكيم العرف والعمل بما يقضي به في هذه المسالة الجزئية، وهذا هو معنى العمل بهذه القاعدة[1].

انواع العرف المعتبر في تطبيق القاعدة:

ينقسم العرف الى عرف عام عند عامة المسلمين، والى عرف خاص باهل مهنة او صناعة او بلد او مدينة معينة.

وكلا النوعين من العرف حجة شرعية ومعتبر في الرجوع اليه في تطبيق الالفاظ المطلقة.

والآن بعد هذه التمهيد ننتقل الى دراسة تطبيق شروط السرقة على عناصر السرقة الالكترونية.

(١)

شرط المالية

يشترط في محل السرقة ان يكون مالا، والدليل على هذا الشرط هو احاديث النصاب، فهذه الاحاديث دلت على انه يجب ان يكون المسروق مالا، وان يكون هذا المال مقدارا معينا هو النصاب.

فمن ذلك الحديث الذي رواه الشيخان واصحاب السنن عن عائشة ام المؤمنين رضي الله عنها، ان رسول الله صلى الله عليه وسلم قال (لا تقطع اليد السارق الا في ربع دينار فصاعدا)، وما روي عن ابن عمر رضي الله عنهما: ان رسول الله صلى الله عليه وسلم قطع سارقا في مجن قيمته ثلاثة دراهم، وعن ابن عباس رضي الله عنه قال: قطع رسول الله صلى الله عليه وسلم في مجن قيمته دينار أو عشرة دراهم[2].

---

[1] العرف والعادة في راي الفقهاء، ص٨٩.

[2] التاج الجامع للأصول في أحاديث الرسول، ج٢، ص٢١.

والمالية من الالفاظ الكلية المطلقة التي لم يرد الشرع بتحديد معناها، وانما يرجع فيها الى العرف، فما يعتبر مالا في العرف، يجوز ان يكون محلا للسرقة، ويستوي في ذلك ان يكون العرف عاما او خاصا.

ويطلق المال في العرف على كل ماله قيمة اقتصادية، ويباع في السوق، وقد عرفه السيوطي في الاشباه والنظائر بانه: ((اسم لكل ماله قيمة، يباع بها، وتلزم متلفه))[1]، وهذا مذهب جمهور الفقهاء في تعريف المال، وينبني على هذا المذهب ان المعلومات والبرامج تعتبر من الاموال التي يجوز ان تكون محلا للسرقة، لان لها قيمة اقتصادية كبيرة في الوقت الحاضر، وقد اصبحت تباع في اسواق معروفة وخاصة بها.

والخلاف في اعتبار المعلومات من الاموال له جذور تاريخية في الفقه الاسلامي، وتتمثل في الخلاف حول جواز ان تقع السرقة على الكتب والمصاحف، فذهب الجمهور وابو يوسف من الحنفية الى جواز ان تكون محلا للسرقة، واحتجوا بانها من الاموال، وانها تباع وتشترى ولها اسواق خاصة بها، وقد بين هذه الحجج أحسن بيان الإمام الماوردي، فقال في كتاب الحاوي: (ودليلنا مع عموم الكتاب والسنة، انه نوع مال، فجاز القطع فيه كسائر الاموال فان منعوا ان يكون مالا، احتج عليهم بجواز بيعه واباحة ثمنه، وضمانه باليد، وغرم قيمته بالاتلاف، واختصاصه بسوق يباع فيها، كما يختص كل نوع من الاموال بسوق)[2].

كما ذكر بعض هذه الحجج الامام ابن قدامة في كتاب المغني فقال:

((فإنه – أي الامام احمد – سئل عمن سرق كتابا فيه علم لينظر فيه، فقال: كل ما بلغت قيمته ثلاثة دراهم فيه القطع، وهذا قول مالك والشافعي وابي ثور وابن

---

[1] الاشباه والنظائر، ج٢، ص٦٠٦، ٦٠٧.

[2] الحاوي الكبير، ج١٧، ص١٧٣.

المنذر لعموم الآية في كل سارق، ولأنه متقوم تبلغ قيمته نصابا، فوجب القطع بسرقته ككتب الفقه، ولا خلاف بين اصحابنا في وجوب القطع بسرقة كتب الفقه والحديث وسائر العلوم الشرعية))[1]

وأما الامام ابوحنيفة فقد ذهب الى ان الكتب لا تعد من الاموال لانها تدخر للقراءة وليس للتمول، وبالتالي لا تصلح محلا للسرقة الموجبة للحد.

ومع ذلك فإن الكتب والمعلومات يمكن ان تعد من الأموال عند الامام ابو حنيفة تخريجا على نظريته في دخول الصنعة على المال التافه والتي نبينها فيما يلي:

دخول الصنعة على المال التافه:

المال التافه هو المال الذي يوجد اصله مباحا في بلاد الاسلام مثل التراب والطين والنورة والجص والزرنيخ ونحوهما، وكذلك المال الذي يوجد نقص في حرزيته مثل الخشب او العاج، والمال الذي لا يبلغ النصاب، والاشياء التي لا يتمولها الناس في العادة، فكل هذه الاموال تافهة وحقيرة ولا يجوز ان تكون محلا للسرقة عند الامام ابو حنيفة لتفاهتها، ولما روي عن عائشة ام المؤمنين رضي الله عنها انها قالت: لم تكن اليد تقطع على عهد رسول الله صلى الله عليه وسلم في المال التافه[2].

ولكن هذا المال التافه اذا دخله العمل او دخلته الصنعة فانها تزيد من قيمته ويتحول الى مال له قيمة يجوز ان تقع عليه السرقة، وذلك مثل الخشب فانه مال تافه، لا تقوم به جريمة السرقة، ولكن اذا دخلته الصنعة، فان المال المصنوع منه

---

[1] المغني، ج١٢، ص٤٢٥.

[2] بدائع الصنائع للكاساني، ج٧، ص١٠٠.

يصبح من الاموال القيمة ويجوز ان تقع عليه السرقة، مثل الكراسي والدواليب والاسرة ونحوها من مصنوعات الخشب[1].

وباسقاط هذه النظرية على المال المعلوماتي فاننا نجد ان المعلومات والبيانات والبرامج هي كهرباء او نبضات كهربائية دخلتها الصنعة، فحولتها الى مال له قيمة يصلح ان يكون محلا للسرقة[2].

فالكهرباء ذاتها تعد من الاموال التافهة، اما لنقص حرزيتها قبل الصنعة، او لانها لا تبلغ النصاب، او لعدم تمولها لانها لا تدخر، ولكن عندما دخلتها الصنعة، وحولتها الى سلعه قيمة من برامج وبيانات ومعلومات، اصبحت مالا له قيمة يصلح ان تقوم به جريمة السرقة على مذهب الامام ابي حنيفة.

و يمكن القول بناء على ذلك ان السلع والاموال المعلوماتية تتوافر فيها صفة المال عند الامام ابو حنيفة تخريجا على نظريته في دخول الصنعة على المال التافه.

كما يمكن القول ايضا انه تتوافر فيها صفة المنقول، عند من يشترط ذلك، لان اصلها هي الكهرباء، وهي مصنوعة منها، والكهرباء تنتقل بين الاسلاك، وتخضع لجميع صنوف التحكم بها من القطع والوصل ونحوها، وقد اصبح من المتفق عليه فقها وقضاء انها من الاموال المنقولة[3].

---

[1] المبسوط للسرخسي، ج٩، ١٥٣، تبيين الحقائق للزيلعي، ج٢، ص٢١٥، المغني لابن قدامة، ج١٢، ص٤٢٣.

[2] راجع الملحق الخاص بلغة الحاسب نهاية الكتاب.

[3] دراسات في الفقه الجنائي الاسلامي، ص٦٥.

(٢)

الحرز

الحرز هو من الأسماء التي ليس لها ضابط أو حد معين في اللغة او في الشرع، ولذلك فانه يرجع في تطبيقه الى العرف، قال الامام الماوردي في الحاوي: (فاذا ثبت ان الحرز شرط في قطع السرقة، فالاحراز تختلف باختلاف المحروزات اعتبارا بالعرف، لانها لم تتقدر بشرع ولا لغة، فاعتبر فيها العرف)[١].

والحرز في العرف هو ما يحفظ به المال عادة، ويختلف حفظ المال باختلاف نوعه، فالمال النفيس مثل الجواهر والذهب والفضة يحفظ في العادة في البيوت في الغرف، والحيوانات مثل الماشية تحفظ في الحظائر، والبضائع تحفظ في المحلات داخل الاسواق، وهكذا، والمرجع في الحرز هو عرف الناس، وما يعدونه في عادتهم حرزا للمال. وهذا يختلف من مال الى اخر، ومن زمن الى زمن، ومن بلد الى اخر، وفي الليل اوالنهار، وجملة ذلك اعتبار شرطين: العرف، والصيانة وعدم التفريط[٢].

والاصل في اشتراط الحرز هو حديث النبي وصلى الله عليه وسلم(لا قطع في ثمر معلق ولا في حريسة الجبل، فاذا اواه المراح او الجرين، فالقطع فيما بلغ ثمن المجن)[٣].

ووجه الاستدلال ان الرسول صلى الله عليه وسلم شرط للقطع في سرقة الثمر ان يكون في الجرين، وفي حريسة الجبل التي هي الابل والماشية، ان تكون في المراح،

---

[١] الحاوي الكبير، ج١٧، ص١٤٠.

[٢] الحاوي الكبير، ج١٧، ص١٤١، ١٤٢.

[٣] بدائع الصنائع، ج٧، ص١٠٩.

والجرين حرز الثمر، والمراح حرز الابل والبقر والغنم، فدل ذلك على ان الحرز شرط في كل مال مسروق بحسبه وبحسب العرف.

هتك الحرز:

هتك الحرز هو ابطال عمله في حماية المال مما يسمح للجاني بالوصول الى سرقته، والهتك يختلف باختلاف الحرز، ولا يشترط فيه ان يكون بالقوة والكسر، بل قد يتم بالحيلة والخداع، كما لو استخدم مفاتيح او تسلل الى الدار او تسلق السور او نحو ذلك، كما لا يشترط فيه الدخول فيجوز ان يتم هتك الحرز ولو بدون دخول الجاني الى الحرز وهذا مذهب الجمهور، لان هتك الحرز عندهم يتم بالقدرة عليه وتجاوز مناعته والوصول الى الشيء المسروق، وهذا قد وجد من الجاني ولو لم يدخل، مثال ذلك ان يقف خارج الحرز ويتناول المسروق بمحجنة، او يجذبه بخشبة حتى يخرجه. وقد بين الامام الماوردي هذه المسألة في كتابه الحاوي فقال: (ودليلنا أن رسول الله صلى الله عليه وسلم أجرى على السارق بمحجنة حكم السرقة إسما ووعيدا، لأن شرطي القطع موجود في الحالين:

أما هتك الحرز فهو القدرة على ما بعد امتناعه، وهذا قد وجد منه وإن لم يدخله.....

وأما إخراج السرقة فهو أن يكون خروجها منه بفعله، وهذا موجود فيما إذا رماه من داخله أو جذبه من خارجه، لأنه قد صار مخرجا له بفعله، ولو سقط القطع عنه إلا أن يباشر حملها من حرزها، لصار ذلك ذريعة الى انتهاك الأموال بغير زاجر عنها، ولا مانع منها وهذا فساد)[1]

---

[1] الحاوي الكبير، ج١٧، ص ١٥٨، ١٥٩.

واما الإمام ابو حنيفة فقد اشترط الدخول الى الحرز، فلا يتم هتك الحرز عنده الا بالدخول.

اخراج المال من الحرز:

ويشترط في اخراج المال المسروق ان يتم بفعل الجاني، وقد يكون مباشرة بان يدخل الجاني الى الحرز ويحمل المال ويخرج به، او بالتسبب بان يستخدم الة او اداة ويلتقط بها المال من دون ان يدخل الى الحرز، مثل ان يستخدم عصا او محجن او طائر معلم، او ان يشير الى الماشية بالعلف فتخرج من الحرز، او ان يمشي بالام فيتبعها الفصيل او نحو ذلك من الوسائل في التقاط المال[1].

وهذا مذهب الجمهور واما الحنفية فانهم يشترطون للاخراج ان يدخل الجاني الى الحرز ويخرج المال، وسبب الخلاف يرجع الى ان مصطلح الاخراج فيه نوع خفاء في انطباقه على حالة جزئية، وهي حالة ان يتم اخراج المال باي وسيلة بدون الدخول في الحرز، فهل تندرج هذه الحالة ضمن مصطلح الاخراج، فيعد من يقوم بها مخرجا للمال من الحرز، ام لا؟ [2].

القاعدة في اصول الفقه بالنسبة للفظ الخفي انه يتم البحث في معنى المصطلح نفسه، فاذا كان هذا المعنى موجودا في الفرد او الحالة الجزئية او مع زيادة، فانه ينطبق عليه، اما اذا كان المعنى الموجود ينقص عن معنى المصطلح فانه لا ينطبق عليه[3].

---

[1] راجع في صور الاخراج بالمباشرة والتسبب: دراسات في الفقه الجنائي الاسلامي، ص١٧٥ – ١٧٨، وكتب الفقه العام للمذاهب في هذا الموضوع.

[2] بداية المجتهد،، ج٢، ص٨١٥.

[3] اصول الفقه الاسلامي لبدران، ص٤١١، ٤١٢.

وبما ان معنى الاخراج من الحرز هو ان يحصل الاخراج بفعل الجاني، والاخراج بالتسبب بدون الدخول الى الحرز يحصل بفعل الجاني ايضا، فانه يمكن القول بانطباق لفظ المخرج من الحرز على المخرج بالتسبب، لان الاخراج في الحالتين بالدخول او بالاداة حصل بفعل منه، ويؤيد ذلك ان الحنفية انفسهم لم يشترطوا الدخول الى الحرز فيما لا يتأتى فيه الدخول، مثل الصناديق ونحوها من الاحراز التي لايمكن الدخول فيها.

الحرز المعلوماتي:

الأصل ان الشيء يكون محرزا شرعا اذا كان يوجد مانع من جدار او سور او نحوه يمنع الغير من الوصول اليه، وأنه يرجع فيما يعد مانعا محققا للحرز وما لا يعد كذلك الى العرف، قال الامام ابن العربي المالكي في كتاب العارضة (اتفقت الأمة على أن من شروطها ــ أي السرقة ــ أن يكون المسروق محرزا بحرز مثله، ممنوعا عن الوصول اليه بمانع من العاة في حفظ باب الأموال)[1].

ففي البيوت يكون البيت محرزا بالجدار والباب[2]، لأن الجدار والباب هما مانع للغير من الدخول، وفي الحظائر يتحقق الحرز بالاسوار من الطين، أو الخشب او الحطب أو نحوه[3]، لأنها المانع للغير من الوصول الى ما يحفظ بداخلها، وهكذا.

وأما في مجال الحاسب الآلي فإن الحرز يتحقق بكل **ما يمنع الاشخاص الغير مصرح لهم من الوصول الى المعلومات المخزنة في الحاسب الآلي.**

---

[1] عارضة الأحوذي، ج٦، ص٢٢٨.

[2] الخلاصة للغزالي، ص٥٩٩، ٦٠٠.

[3] الحاوي الكبير للماوردي، ج١٧، ص١٤٦.

ولما كان مدار الحرز على العرف، فان الوسائل التي يتم بها حماية الحاسب الآلي من الغير ومنعه من الوصول الى المعلومات المخزنة فيه، يرجع فيها الى عرف الناس وعرف اهل الاختصاص.

ووسائل المنع من الوصول المتعارف عليها بين المختصين وعموم المستخدمين للحاسب الالي تشمل الاتي:

١.نظام التحقق من الدخول[١]: وهو البرنامج الذي يطلب منك قبل الدخول بيانات معينة مثل اسم المستخدم وكلمة المرور، فاذا لم تكن البيانات المدخلة صحيحة لا يسمح لك بالدخول، وهذا البرنامج يتطلب ان يكون للشخص حساب من اسم مستخدم وكلمة مرور لدى النظام.

٢.جدار النار، وهو عبارة عن اجهزة وكيلة، وموجهات، وحزمة من البرامج، تعمل جميعها على منع الدخول الى النظام او الخروج منه الا وفق معايير واذونات يحددها المسئولون عن النظام، وهو اشبه بالحارس على النظام، بل يطلق عليه هذا اللفظ في ادبيات القراصنة.

٣.التشفير، وهو تقنية تمنع قراءة المعلومات والبيانات الموجودة في النظام الا بمفاتيح معينة يملكها مدراء النظام او المأذون لهم من المستخدمين، فاذا نجح المهاجم في سرقة بيانات او معلومات من داخل النظام او من خارجه، فانه لن يستطيع قراءتها اذا كانت مشفرة الا بعد يقوم بكسر التشفير، ويعتبر التشفير عند المختصين بمثابة قفل يوضع على البيانات والمعلومات.

---

[١] راجع في كون هذا النظام من معايير امن الحاسوب:

CompTIA Security+ SY0-301 Authorized Cert Guide، second Edition ، Dabid l.،Prowse

٤.اغلاق المنافذ في النظام، لان المنافذ المفتوحة هي التي يستغلها المهاجم في الدخول الى النظام من خلالها، وبالنسبة للمنافذ التي تحتاج ان تكون مفتوحة بشكل دائم فإنها يجب ان تربط الى جدار النار، ويعتبر جدار النار في هذه الحالة بمثابة الحارس[١].

فهذه الوسائل اذا توافرت في نظام معلوماتي معين، فانه يعد حرزا لما وضع فيه من برامج وبيانات، وفقا لاحكام الشريعة الاسلامية.

هتك الحرز المعلوماتي:

هتك الحرز المعلوماتي يتم بالدخول الى النظام باي وسيلة من وسائل الدخول مثل الدخول عبر كسر كلمة المرور، او الدخول عبر فتح ثغرات برمجية في النظام الضحية، او التسلل عبر منافذ النظام المفتوحة[٢].

وكل هذه الانواع من الدخول تنشئ اتصال بين المهاجم ونظام الكمبيوتر الضحية، يسمح للمهاجم بالوصول اليه ونسخ اي بيانات او برامج منه الى جهازه.

ومع ان الاتصال الذي يتم من جهاز الجاني الى جهاز الضحية لا يعتبر من قبيل دخول الجاني كليا الى الحرز، الا انه يعد من أنواع هتك الحرز والدخول فيه، ذلك ان القاعدة في الدخول الى الحرز انه يتم بما يتناسب مع طبيعة الحرز نفسه، فاذا كان الحرز منزلا فان هتك الحرز يتم بالدخول الكامل اليه من الجاني، واذا

---

[١] راجع في هذه المعاييرالثلاثة: االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، لبنان، سكامبري،جويل، ستيوارت ماك كلور، جورج كيرتز، مركز الترجمة، الدار العربية للعلوم، الطبعة الثانية، ٢٠٠١.

[٢] راجع في أنواع الدخول الأخرى غير الدخول بكلمة المرور كتاب: مراحل السرقة الالكترونية للمؤلف.

كان الحرز كم اوجيب في ثوب المجني عليه فان الدخول الى الحرز وهتكه يتم بادخال اليد الى الكم او الجيب، وهكذا بالنسبة للصنادبق المغلقة ونحوها، ولذلك فان انشاء اتصال من جهاز الجاني الى نظام المعلومات الضحية يعتبر من قبيل الدخول وهتك الحرز، لان هذا النوع من الدخول هو الذي يتناسب مع طبيعة انظمة الكمبيوتر.

الاخراج من الحرز المعلوماتي:

الاخراج من الحرز المعلوماتي يقع على النسخة فقط، سواء كان المال المخرج بيانات او برامج، واما اصل المال فيبقى في النظام بحوزة المجني عليه وتحت يده، ولذلك فان المخرج يكون سارقا لنصف قيمة المال لا قيمته كله، لان النصف الاخر مازال في حوزة المجني عليه، ولذلك ايضا فان تقدير النصاب يتم على اساس نصف قيمة المال المخرج، فاذا بلغت نصف القيمة النصاب توافرت شروط الحد، اما اذا لم تبلغ نصف قيمة المال المخرج النصاب، فان الحد يسقط وننتقل الى التعزير.

وهذا الحكم هو قياس قول فقهاء الشافعية في غصب العقار إذا اجتمعت فيه يد المالك مع يد الغاصب، قال الخطيب الشربيني في المغني (وإن كان المالك فيها – أي في الدار – و لم يزعجه، فغاصب لنصف الدار لإستيلائه مع المالك عليها)[1]

[1] مغني المحتاج، ج٢، ص٣٧٤.

المطلب الثالث

الخفية

الخفية هي من طبيعة السرقة ذاتها، وهي التي تميزها عن الصور الاخرى لجرائم الاخذ، فبدون الخفية لا تكون الجريمة سرقة، بل جريمة اخرى من جرائم الاخذ، مثل الاختلاس، او الغصب والنهب، او الحرابة...الخ، قال الزيلعي في الكنز: (قوله في المتن خفية ؛ قال الاتقاني وقيد الخفية احترازا عن النهب والغصب والاختلاس)[1].

وقال ابن عابدين: (قوله: خفية ؛ خرج بها الاخذ مغالبة او نهبا، فلا يقطع به)[2].

ومعنى الخفية، الاستخفاء عن المجني عليه اثناء اخذ المال، ويعبر عنها الفقهاء بانها مسارقة عين المالك، اي اجتهاد الجاني ان لا يراه المالك اثناء السرقة، والمعتبر في الخفية عند فقهاء الحنفية هو الجاني، فاذا كان الجاني يجتهد في الاستخفاء اثناء عملية السرقة، فان شرط الخفية يكون متحققا، ولو كان المجني عليه، او اشخاص اخرين يعلمون بالسرقة، او حتى يرونه وهو يسرق المال، يقول الزيلعي في الكنز: (وشرطها_ اي السرقة_ ان تكون خفية على زعم السارق، حتى لو دخل دار انسان فسرق، واخرجه من الدار، وصاحب الدار يعلم ذلك، والسارق لا يعلم ذلك، قطع، ولو كان السارق يعلم بان صاحب الدار يعلم ذلك لا يقطع لانه جهر)[3].

---

[1] تبيين الحقائق شرح كنز الدقائق، ج٣، ص٢١١.

[2] رد المحتار، ج٦، ص١٤١

[3] تبيين الحقائق شرح كنز الدقائق، ج٣، ص٢١٢.

فهذا الكلام للامام الزيلعي يدل على ان العبرة في الخفية هي بنية الجاني وارادته، فاذا ارتكب الجاني السرقة، وهو ينوي الاستخفاء، و لم يكن يعلم ان مالك المال يراه، فان شرط الخفية يتحقق، ولو كان مالك المال، او اي شخص اخر، يراه فعلا وهو يرتكب السرقة، فالعبرة في وجود الخفية، او عدمها هي بظن السارق لا المجني عليه.

ولكن اذا كان الجاني قد علم بان المجني عليه يراه، ومع ذلك لم يبالي، وارتكب السرقة، فانه يكون قد جهر بالسرقة، وبالتالي لا نكون امام جريمة سرقة شرعا، وانما نهب او اختلاس او جريمة من جرائم الاخذ الاخرى غير السرقة.

وهذا المفهوم للخفية بديهي، لان الشرع قد اجاز ثبوت السرقة بالشهادة، والشهادة تقتضي ان يرى الشهود الجاني اثناء السرقة، او ان يراه المجني عليه ويذهب لاحضار الشهود، ففي هذه الاحوال تثبت السرقة الحدية باقوال الشهود، ولا يؤدي رؤيتهم للجاني هم والمجني عليه الى سقوط شرط الخفية، وهذا الامر متفق عليه بين المذاهب[1].

يمكن اذا القول، بان شرط الخفية يتحقق، اذا كان الجاني قد اراد الاستخفاء عن المجني عليه اثناء السرقة، وكان حريصا على ان لايراه احد، ولو كان المجني عليه او اي شخص اخر، يراه ويعلم به حقيقة،

علاقة الخفية بعدم الرضا:

يدخل بعض الفقهاء في العصر الحاضر شرط عدم الرضا في تعريف السرقة، فيعرفون السرقة بانها: اخذ مال الغير بغير علمه ورضاه، وبهذا لا تتوافر السرقة الحدية عندهم الا اذا تم اخذ المال بغير رضا المجني عليه.

---

[1] لمزيد من التفاصيل راجع: دراسات في الفقه الجنائي الاسلامي، ص٢٢٥.

ولكن المذاهب الاسلامية المختلفة لا تذكر هذا الشرط في تعريف السرقة، و لم يسبق ان ذكره اي فقيه من فقهاء المذاهب اثناء تعريفه للسرقة الموجبة للحد الشرعي، فشرط عدم رضا المجني عليه لا علاقة له بالسرقة الحدية عند فقهاء المذاهب، وليس شرطا لها، وانما هو من شروط السرقة التعزيرية، فالرضا يسقط الحرز، وينقل جريمة السرقة الى التعزير، واما عدم الرضا، فهو يجرد الجريمة من صفة السرقة، ويجعلها نهبا او محاربة، وبالتالي فان عدم الرضا هو من شروط السرقة التعزيرية، بانواعها المختلفة، وليس من شروط السرقة الموجبة للحد[1].

كما ان عدم رضا المجني عليه ليس عنصرا في الخفية عند فقهاء المسلمين، لان الخفية عندهم تتحقق كلما استتر الجاني، واجتهد في التخفي اثناء ارتكابه للسرقة، بصرف النظر عن موقف المجني عليه، وسواء كان المجني عليه راضيا، او ساخطا، فلا ترتبط الخفية عندهم بالرضا او عدم الرضا، و لم يقل احد من فقهاء المذاهب بذلك.

وخلاصة القول اذا ان شرط عدم رضا المجني عليه بالسرقة لا اصل له في الفقه الاسلامي، وليس مذكورا في تعريف السرقة الموجبة للحد عند علماء هذا الفقه، وانما اقحمه بعض فقهاء العصر الحديث في تعريف السرقة تقليدا للغرب لا اكثر ولا اقل.

---

[1] دراسات في الفقه الجنائي الإسلامي، ص٢٢٢، ٢٢٣.

مشكلة اساءة استخدام بطاقة الائتمان:

تثور هذه المشكلة عندما يقوم العميل باستخدام بطاقة الصراف الالي لسحب مبلغ منها زيادة عن رصيده، فهل يعتبر هذا الفعل سرقة، ام لا؟

اثار تكييف هذا الفعل بانه سرقة خلافا كبيرا في الفقه والقضاء الوضعي، ويرجع السبب في ذلك الى ان القانون الوضعي يشترط لتطبيق احكام السرقة عدم رضا المجني عليه بالسرقة، وهذا الشرط غير متحقق في حالة السحب الزائد عن الرصيد، لان البنك قد برمج الة الصرف وامرها بالاستجابة لطلب العميل، وبالتالي يعتبر راضيا عن عملية السحب الزائد التي تحدث من العميل، وهذا مما يؤدي الى عدم انطباق وصف السرقة على فعل السحب الزائد عن الرصيد، لتخلف شرط عدم الرضا اللازم لجريمة السرقة في هذا القانون.

وكان من نتيجة ذلك ان انقسم الفقه والقضاء الوضعي، فذهبت بعض احكام القضاء الى نفي وقوع جريمة السرقة في هذه الحالة، في حين ذهبت احكام اخرى الى انطباق وصف السرقة عليها.

موقف الفقه الاسلامي من المشكلة:

في الفقه الاسلامي لا تثور هذه المشكلة بالنسبة للسرقة الموجبة للحد، لان عدم رضا المجني عليه ليس من ماهية هذه السرقة ولا من شروطها، والسرقة الموجبة الحد تقوم في الفقه الاسلامي من دون اعتبار لحالة المجني عليه، وسواء كان راضيا، او ساخطا.

ولا يعد عدم الرضا ايضا عنصرا من عناصر الخفية اللازمة في السرقة الموجبة للحد، لان الخفية تتحقق باجتهاد الجاني في التخفي اثناء السرقة، ولا علاقة لرضا المجني عليه او عدم رضاه بتحقق الخفية، لان الخفية تتحقق باستخفاء الجاني، سواء كان المجني عليه راضيا، ام لا.

ولذلك فانه يمكن القول باطمئنان، ان وصف السرقة الحدية ينطبق على فعل السحب الزائد من الرصيد والذي يقوم به حامل البطاقة الائتمانية، ولا عبرة في الشريعة لرضا البنك، او حتى لعلمه بالسحب، وانما العبرة بنية الجاني، واجتهاده في اخفاء فعله عن البنك، فاذا كان الجاني حريصا على اخفاء فعل السحب عن البنك، فان جريمة السرقة الموجبة للحد تقوم في حقه، سواء كان البنك راضيا او غير راض، عالما بالسحب او غير عالم.

المبحث الثالث

تطبيقات السرقة الالكترونية

١_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، استتراف 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. وتعتبر البيانات الشخصية من الاموال في الشريعة الاسلامية، لان هذه البيانات اصبحت تباع في اسواق خاصة من ناحية، مثل رقم بطاقة الائتمان الذي يباع بمبلغ ٦٠ دولار، ولانها تعتبر بمثابة النقود، لانها تستخدم كاثمان للاشياء في الشراء عبر الانترنت، ولذلك تعتبر جريمة السرقة الحدية متحققة بمجرد الحصول على نسخة من البيانات الشخصية، ولو لم يستخدم الجاني هذه البيانات في ارتكاب سرقات أخرى.

٢-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، وبالتالي يعتبر اجرائها عملية سرقة لودائع مالية، كما لو قام الجاني باخذها ماديا سواء بسواء، والدخول الى نظام الكمبيوتر الخاص بالبنك يتم من خلال اساليب

الاختراق المختلفة[1]، وتتحقق السرقة بمجرد انه يتم نقل الوديعة واخراجها من حساب المجني عليه الى حساب آخر.

٣-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[2]. 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. ولا شك ان نسخ اي من هذه المعلومات بدون دفع ثمنها هو من قبيل السرقة، لانها سلع تباع في السوق، فهي من الاموال، واما الاخراج في هذا النوع من السرقات فإنه يقع على النسخة فقط، ويتم بمجرد النسخ.

٤-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

---

[1] راجع كتاب مراحل السرقة الالكترونية للمؤلف مبحث الدخول الى الحاسب.

[2] محاضرات في مبادئ قواعد البيانات، فهد آل قاسم، ص٣.

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، والبرنامج سواء كان نسخة او اصل، يمثل سلعة من السلع التي تباع وتشترى، بل يعتبر البرنامج من اهم السلع في السوق في الوقت الحاضر، ولذلك يمكن القول انه يعتبر من الاموال وفقا لاحكام الشريعة الاسلامية، ويعتبر نسخه محققا لشرط الاخراج من الحرز، وتتوافر به جريمة السرقة.

نتائج الدراسة

من خلال هذه الدراسة تم التوصل الى بعض النتائج والتوصيات التي نوردها فيما يلي:

١- جريمة السرقة الالكترونية من اخطر الجرائم في العصر الحديث بسبب فداحة الاضرار والخسائر الناجمة عنها التي تبلغ مليارات الدولارات في مقابل سهولة ارتكابها عن بعد.

٢- على الرغم من خطورة جريمة السرقة الالكترونية الا ان القوانين الجنائية التقليدية قد عجزت عن مواجهتها بسبب عدم ملائمة هذه القوانين للتطبيق على السرقة الالكترونية، وكان من اهم المشاكل التي برزت عند تطبيق هذه القوانين ان السرقة الالكترونية تقع دائما على نسخة من البرامج والبيانات، ويترتب عليها نقل نسخة منها الى الجاني وليس الاصل، وبالتالي يبقى الاصل في حوزة المجني عليه ولا تزول حيازته له، في حين ان القوانين الوضعية تشترط انهاء الحيازة لقيام جريمة السرقة.

٣- على عكس القوانين الوضعية التقليدية فان احكام السرقة في الشريعة الاسلامية قابلة للتطبيق على السرقة الالكترونية ويظهر ذلك جليا من خلال تتبع تطبيق اركان وشروط السرقة الحدية على وقائع وجوانب السرقة الالكترونية كما يلي:

- ركن الاخذ في السرقة الحدية ينطبق على عملية نسخ البيانات والبرامج في السرقة الالكترونية، وذلك لان مفهوم الاخذ عند الشافعية هو اثبات اليد على المال المسروق، ولا يشترط فيه ازالة يد المجني نهائيا عن المال المسروق، وهو ما

ينطبق على السرقة الالكترونية التي يبقى فيها اصل المسروق في يد المجني عليه وتذهب النسخة فقط الى الجاني.

- شرط المالية في السرقة الحدية ينطبق على المال المعلوماتي، وذلك لان المالية من الالفاظ المطلقة التي يرجع في تحديدها الى العرف، والمال في العرف هو الذي له قيمة اقتصادية ويباع ويشترى، وبما ان المعلومات لها قيمة اقتصادية وتباع وتشترى فانها تعد من الاموال شرعا.

- الحرز هو من الاحكام الكلية التي ليس لها ضابط في الشرع وبالتالي يرجع في تحديده الى العرف، والحرز في العرف هو ما يمنع الغير من الوصول الى الشيء عادة، وهو يختلف بحسب الشئ ذاته المراد حفظه، فحرز البيوت هو ما وضع لمنع الغير من دخولها بحسب العرف، مثل الجدار، والابواب،..الخ، وفي مجال الحاسب الآلي فان حرز الحاسب هو كل ما وضع لمنع الاشخاص الغير مصرح لهم من الدخول الى النظام المعلوماتي والوصول الى المعلومات المخزنة فيه، مثل برامج واجراءات الحماية المتعارف عليها في مجتمع امن المعلومات.

ثانيا: التوصيات:

في ضوء ما اثبتته الدراسة من انطباق شروط واحكام السرقة الحدية على السرقة الالكترونية يمكن اقتراح التوصيات التالية:

١ــ على الدول العربية والاسلامية ان تعمل على اعداد تشريع خاص بالسرقة الالكترونية مستمد من احكام الشريعة الاسلامية بالاسترشاد بما ورد في هذه الدراسة، وان تكف عن استيراد التشريعات الوضعية التي ثبت عجزها عن مواجهة هذه الجريمة.

٢ــ على الباحثين اعداد دراسات معمقة حول تطبيقات وانواع السرقة الالكترونية المختلفة لبيان حكم الشريعة الاسلامية في كل نوع من انواعها، وقد حالت ظروف الحرب في اليمن وشحة المراجع دون توسع الدراسة في تناول هذه الانواع رغم اهميتها.

٣ــ على مراكز البحوث والدراسات العربية والاسلامية اعداد وتشجيع الدراسات التي تبحث في حكم الشريعة الاسلامية في الظواهر الاجرامية المعلوماتية المختلفة غير السرقة الالكترونية، في ضوء ما ثبت من خلال هذه الدراسة من صلاحية الشريعة الاسلامية للتطبيق على السرقة الالكترونية وعلى كل جريمة قد تقع في المستقبل.

الملحقات

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 (١،٠). 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 ١، ولا نبضة تمثل برقم ٠، 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 (١)، او لا موصل (٠). 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 ١،٠، ويقوم بمعالجتها وفق هذه الشفرة، ثم يرسلها الى جهاز الاخراج في اللغة الطبيعية التي نتعامل بها(وصفي، ١٩٨٩، فكيرين، ١٩٩٣، بطرس ١٩٩٤).

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 (الرماحي ٨ ١٩٨):

يقوم النظام الثنائي على رمزين فقط هما ١،٠، وفي مقابل ذلك يتكون النظام العشري من عشرة رموز ٠-٩، ويتكون النظام الثماني من تسعة رموز ٠-٨.

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

- في النظام العشري توجد عشرة رموز ؛١،٠، ٢،٣،٤، ٥، ٦، ٧، ٨،٩

ونعبر عن الاشياء بهذه الارقام، فاذا كان لدينا شيئين، نعبر عنهما بالرقم ٢، 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 ٠، ١ للتعبير عن الكمية عشرة (١٠)، ونستخدم العددين ١، ٢ للتعبير عن الكمية اثناعشر (١٢)، وهكذا هلم جرا.

فاذا بعد العدد تسعة ٩، تكون الاعداد مركبة من الرموز العشرة مثل، ١٠، ١١، ١٢، ١٣، وهكذا.

-بالنسبة للنظام الثماني فهو يحتوى على ثمانية رموز ٠_٧، وهذا يعني ان النظام الثماني يتكون من ثمانية اعداد فقط ٠، ١، ٢، ٣، 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

١، ٠ (١٠)، واذا اردنا ان نعبر عن تسعة اشياء، فاننا نستخدم تركيبة من العددين ١، ١ (١١).

وهذا معناه ان تسلسل الاعداد في النظام الثماني هو كالتالي: ٠، ١، ٢، ٣، ٤، ٥، ٦، ٧، ١٠، ١١، ١٢، ١٣، ١٤، ١٥، ١٦، ١٧، ٢٠، ٢١، وهكذا

ويلاحظ على هذا التعداد ما يلي:

١. 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.

٢. ان الرقم ١٠ في النظام الثماني، يقابل العدد ٨ في النظام العشري، والرقم ٣٠ يقابل الرقم ٢٤ في النظام العشري، وهكذا، فنستطيع ان نقول ان العدد ٣٠ هو التمثيل العددي الثماني للعدد ٢٤ في النظام العشري، والعدد ١٠ 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 ١، واذا اردنا التعبير عن كمية اكبر من الواحد، نستخدم تركيبة من عددين من نفس النظام

فللتعبير عن شيء واحد في النظام الثنائي نستخدم العدد ١، 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 ١٠.

وهكذا بالنسبة للكميات الاخرى، على سبيل المثال، ١ في النظام الثنائي يقابل ١ في النظام العشري، و١٠ في النظام الثنائي تقابل ٢ في النظام العشري، و١١ في النظام الثنائي تعبر عن ٣ في النظام العشري

٠، ١، ١٠، ١١

٠، ١، ٢، ٣

ولكن نلاحظ اننا استنفدنا تركيبات اعداد النظام الثنائي عندما وصلنا الى الرقم ١١، والذي يعبر عن ثلاثة اشياء، او الرقم ٣ 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 ١٠٠ هو الذي يعبر عن الكمية ٤ في النظام العشري، وهكذا

وبناء على ذلك فان العدد ١٠ في النظام الثنائي هو التمثيل العددي الثنائي للرقم ٢ في النظام العشري، والعدد ١٠٠ في النظام الثنائي هو التمثيل العددي الثنائي للرقم ٤ في النظام العشري، وهكذا.

يتميز النظام الثنائي بانه لا يوجد فيه سوى الرقمين ٠، ١، ولذلك فان العد التصاعدي في النظام الثنائي، يتم بان نعد تصاعديا ابتداء من الصفر، مع اغفال

جميع الاعداد غير الصفر والواحد ٠، ١، ولذلك فاننا في حالة العد تصاعديا في النظام الثنائي، سنجد انفسنا نعد بالطريقة التالية:

٠، ١، ١٠، ١١، ١٠٠، ١٠١، ١١٠، ١١١.....الخ ١٢.

ويمكن اجمال التقابل بين الانظمة الثلاثة على النحو التالي:

العشري: ٠، ١، ٢، ٣، ٤، ٥، ٦، ٧، ٨،٩ ؛ ١٠، ١١، ١٢

الثماني: ٠، ١، ٢، ٣، ٤، ٥، ٦، ٧، ١٠، ١١، ١٢، ١٣، ١٤

الثنائي: ٠، ١، ١٠، ١١، ١٠٠، ١٠١، ١١٠، ١١١، ١٠٠٠، ١٠٠١، ١٠١٠، ١٠١١، ١١٠٠، ١١٠١، ١١١٠، ١١١١

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 ١ وهي ١، ويمثل الحرف B بالشفرة الثنائية للعدد ٢ وهي ١٠، والحرف C بالشفرة الخاصة بالعدد ٣ وهي ١١، 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، فكيرين (١٩٩٣):-

جدول دليل المنطقة للرموز

الرمز	دليل المنطقة	
0 _ 9	0	0
A _ I	1	1
J _ R	1	0
S _ Z	0	1

التمثيل العددي الثنائي للرموز ← | دليل المنطقة →

	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01
0 0	1	2	3	4	5	6	7	8	9
1	A	B	C	D	E	F	G	H	I

1									
1 0	J	K	L	M	N	O	P	Q	**R**
0 1		S	T	U	V	W	X	Y	**Z**

التمثيل الكهربائي للبيانات(بيرس، بدون تاريخ):

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

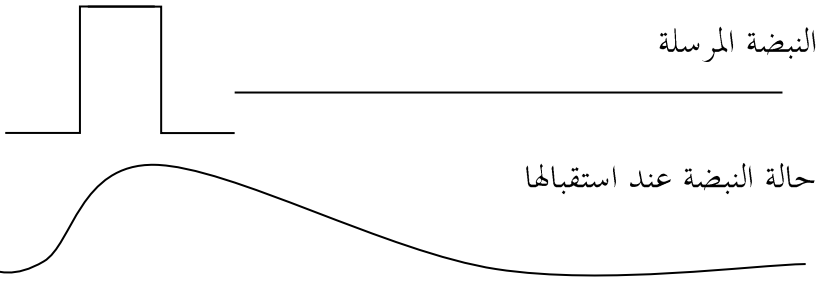
والسبب الذي يجعل الحاسب الالي لا يفهم إلا اللغة الثنائية، ولا يستطيع التعامل مع لغة البشر، هو ان الحاسب الالي جهاز او الة تعمل على الكهرباء، ومكون من دوائر الكترونية كهربائية، يسري فيها التيار الكهربائي، وكل مكونات الحاسب

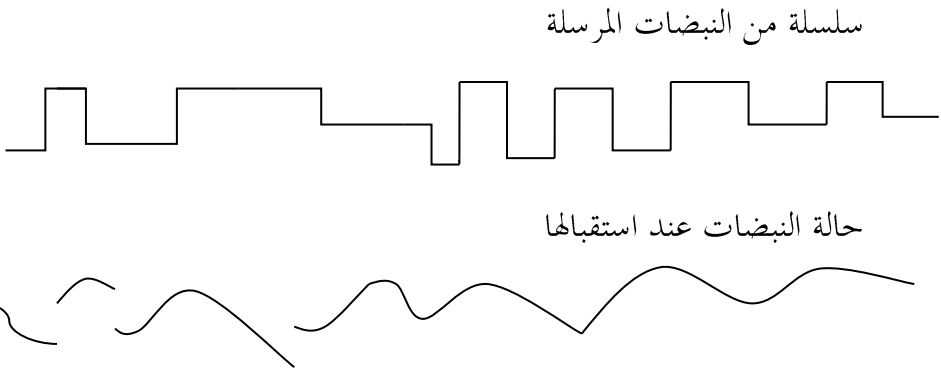
الالي من دوائر الكترونية، ومواصلات، واسلاك، تعمل على التيار الكهربائي، واذا اردنا ان نمثل الحروف كهربائيا داخل الحاسب، ونحولها كما هي الى اشارات كهربائية، فلن نستطيع ذلك، لان التيار الكهربائي عبارة عن سيل من الالكترونات، يمثل كل الكترون منه نبضة كهربائية، ولا يمكن ان يمثل اي شيء داخله الا على شكل نبضة ولا نبضة، قطع التيار ووصله، وانسب الانظمة العددية لتمثيل نبضات التيار الكهربائي، هو النظام العددي الثنائي، لان النبضة تمثل بالرقم ١، ولا نبضة او قطع التيار يمثل بالرقم ٠

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 ١٨٣٨ 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 كهربائية 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 ذلك١٥:





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 ١، ونعطي لحالة انقطاع التيار الرقم ٠، 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 ١، والصفر ٠، 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[1]:

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،

[1] مقدمة الى نظرية المعلومات، ص١٧٨، ١٧٩.

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[1].

[1] التكنولوجيا الرقمية، ص١٤١، ١٤٢.

اهم مراجع الكتاب

كتب التفسير والحديث:

١) روح المعاني في تفسير القرآن العظيم والسابع المثاني، ابي الفضل شهاب الدين محمود الالوسي، القاهرة، دار الحديث، ١٤٢٦ ه \ ٢٠٠٥ م

٢) التاج الجامع للاصول في احاديث الرسول، منصور علي ناصف، بيروت / لبنان، دار الفكر، ٢٠٠٠ م.

٣) عارضة الأحوذي بشرح صحيح الترمذي، ابن العربي المالكي، بيروت، دار الكتب العلمية، بدون تاريخ.

المراجع الاساسية للبحث:

_حرف الألف _

٤) الاشباه والنظائر، جلال الدين عبد الرحمن السيوطي، تحقيق محمد محمد تامر، حافظ عاشور حافظ، مصر، دار السلام، الطبعة الثالثة، ٢٠٠٦م

٥) الأحكام السلطانية والولايات الدينية، أبي الحسن علي بن محمد بن حبيب الماوردي، تحقيق د.أحمد بن مبارك البغدادي، الكويت، مكتبة دار إبن قتيبة، ط١، ١٩٨٩ م.

٦) اختلاف الفقهاء، ابي جعفر محمد بن جرير الطبري، لبنان، دار الكتب العلمية، ١٩٩٩ م

٧) اصول الفقه الاسلامي، بدران ابو العينين بدران، الاسكندرية، مؤسسة شباب الجامعة، بدون تاريخ

٨) الأحكام العامة للنظام الجنائي في الشريعة الإسلامية والقانون، عبد الفتاح مصطفى الصيفي، مصر، دار النهضة العربية، ٢٠٠٤ م.

٩) احترف اوراكل خطوة بخطوة، نجوى الخباز، سوريا، شعاع للنشر والعلوم، ط١، ٢٠٠٤

١٠) اساسيات الحاسب الالي، محمد احمد فكيرين، بيروت / لبنان، دار الراتب الجامعية، 1993م

١١) امن المعلومات بلغة ميسرة، خالد بن سليمان الغثبر، محمد بن عبدالله القحطاني، مركز التميز لامن المعلومات، ط١، ٢٠٠٩ م.

١٢) الانترنت والعولمة، بهاء شاهين، القاهرة، عالم الكتب، 1999م.

_حرف الباء _

١٣) بروتكول IP/TCP الدليل الكامل، احمد خالد المحمد، لبنان، شعاع للنشر والعلوم، الطبعة ١٩٩٩ م.

١٤) بداية المجتهد ونهاية المقتصد، ابي الوليد محمد بن احمد ابن رشد الحفيد، بيروت، دار ابن حزم، الطبعة الاولى ٢٠٠٣ م

١٥) بدائع الصنائع، علاء الدين ابي بكر بن مسعود الكاساني، بيروت، دار الفكر، ١٩٩٦ م.

_حرف التاء _

١٦) تبيين الحقائق شرح كتر الدقائق، فخر الدين عثمان بن علي الزيلعي، مصر، بولاق، ١٣١٤ ه

١٧) تخريج الفروع على الاصول، شهاب الدين محمود بن احمد الزنجاني، حققه الدكتور محمد اديب الصالح، المملكة العربية السعودية، مكتبة العبيكان، الطبعة الثانية ٢٠٠٦ م.

١٨) التمهيد والإستذكار، أبوعمر يوسف بن عبدالله بن عبد البر، تحقيق الدكتور عبدالله بن عبد المحسن التركي بالتعاون مع مركز البحوث والدراسات العربية والاسلامية، القاهرة، ٢٠٠٥ م.

١٩) التمهيد في تخريج الفروع على الاصول، جمال الدين ابي محمد عبد الرحيم بن الحسن الاسنوي، تحقيق محمد حسن اسماعيل، بيروت، دار الكتب العلمية، الطبعة الاولى ٢٠٠٤.

٢٠) التشريع الجنائي الاسلامي، عبدالقادر عودة، مصر، مكتبة دار التراث، ٢٠٠٥ م.

٢١) التكنولوجيا الرقمية، نيكولاس نيجروبونت، ترجمة سمير ابراهيم شاهين، مصر، مركز الاهرام للترجمة، ط١، ١٩٩٨م

٢٢) تكنولوجيا الاتصالات وشبكات المعلومات، محمد محمد الهادي، القاهرة، المكتبة الاكاديمية، 2001م

_حرف الجيم _

٢٣) الجرائم المعلوماتية، احمد خليفة الملط، الاسكندرية، دار الفكر الجامعي، الطبعة الثانية، ٢٠٠٦ م.

_حرف الحاء _

٢٤) حاشية البيجوري على شرح ابن القاسم، ابراهيم البيجوري، ضبط وتصحيح محمد عبد السلام شاهين، لبنان، دار الكتب العلمية، ط٢، ١٩٩٩ م

٢٥) حاشية الدسوقي على الشرح الكبير، محمد عرفة الدسوقي، دار احياء الكتب العربية، بدون تاريخ.

٢٦) الحاسب شرح تعليمي مبسط، سامي الرماحي،

٢٧) الحاوي الكبير، ابي الحسين علي بن محمد بن حبيب الماوردي، حققه محمود مطرجي واخرين، دار الفكر.

٢٨) الحماية الجنائية للتعاملات الالكترونية، شيماء عبد الغني محمد عطاالله، مصر، دار الجامعة الجديدة، ٢٠٠٧

_حرف الدال _

٢٩) دراسات في الفقه الجنائي الاسلامي،عوض محمد عوض،الاسكندرية، دار المطبوعات الجامعية، ١٩٧٧ م.

_حرف الراء _

٣٠) رد المحتار على الدر المختار شرح تنوير الابصار، محمد امين ابن عابدين، تحقيق عادل احمد عبد الموجود وعلي محمد معوض، الرياض، عالم الكتب، طبعة خاصة، ٢٠٠٣.

٣١) روضة الطالبين، النووي، بيروت، المكتب الاسلامي، ١٩٩١ م

_حرف الزين _

٣٢) زدني علما: انترنت، ارنود دوفور، ترجمة منى ملحيس، نبال إدلبي، بيروت، الدار العربية للعلوم، 1998م

_حرف السين _

٣٣) السياسة الجنائية في مواجهة جرائم الانترنت، حسين بن سعيد الغافري، القاهرة، دار النهضة العربية، ٢٠٠٩ م.

٣٤) سرقة المعلومات المخزنة في الحاسب الالي، عبدالله حسين علي محمود، القاهرة، دار النهضة العربية، الطبعة الرابعة، شرطة دبي.

_حرف الشين _

٣٥) شبكات الحاسب، النظرية والتطبيق، مصطفى محمد مشلح، لبنان، شعاع للنشر والعلوم، الطبعة الاولى ٢٠٠٨

٣٦) شبكات المعلومات والاتصالات، عامر ابراهيم قنديلجي، ايمان فاضل السامرائي، الاردن، دار المسيرة، ٢٠٠٩ م.

٣٧) شرح قانون العقوبات، القسم الخاص، محمود محمود مصطفى، شرح قانون العقوبات، القسم الخاص، مصر، مطبعة جامعة القاهرة، ط٨، ١٩٨٤ م.

_حرف الطاء _

٣٨) طقم التدريب على الشهادة Network+ الاصدار الثاني، محترفي تكنولوجيا المعلومات،، ترجمة مركز التعريب والبرمجة، لبنان، الدار العربية للعلوم ناشرون، ط١، ٢٠٠١.

_حرف العين _

٣٩) العزيز شرح الوجيز، ابي القاسم عبد الكريم بن محمد الرافعي، تحقيق الشيخ علي معوض، عادل احمد عبد الموجود، بيروت، دار الكتب العلمية، ١٩٩٧ م

٤٠) العرف والعادة في راي الفقهاء، احمد فهمي ابو سنة، مصر، دار البصائر، الطبعة الاولى، ٢٠٠٤ م

_حرف القاف _

٤١) القواعد الكلية، احمد بن عبدالحليم بن عبد السلام ابن تيمية، تحقيق محيسن بن عبد الرحمن المحيسن، السعودية، مكتبة التوبة، ط١، ٢٠٠٢ م

٤٢) قانون العقوبات ومخاطر تقنية، هشام محمد فريد رستم، المعلومات، اسيوط، مكتبة الالات الحديثة، ١٩٩٢ م

٤٣) االقرصنة تحت الاضواء، اسرار وحلول لحماية الشبكات، جويل سكامبري، ستيوارت ماك كلور، جورج كيرتز،، لبنان، مركز الترجمة، الدار العربية للعلوم، الطبعة الثانية، ٢٠٠١.

٤٤) القرصنة، الفنون _ الاساليب _ التدابير، نجوى مصطفى الخباز، لبنان، شعاع للنشر والعلوم، الطبعة الاولى ٢٠٠٩ م

٤٥) قراصنة قواعد البيانات بلا أقنعة، نجوى مصطفى الخباز، بيروت، شعاع للنشر والعلوم، ط١،٢٠٠٨ م.

٤٦) قانون العقوبات، جرائم القسم الخاص، رمسيس بهنام، مصر، منشأة المعارف، بدون تاريخ.

_حرف الكاف _

٤٧) كشف اسرار البيانات _ دليل التعلم الذاتي، جيم كيوغ، كين ديفيدسون،، لبنان، مركز التعريب والبرمجة، الدار العربية للعلوم، الطبعة الاولى، ٢٠٠٥ م

_حرف الميم _

٤٨) المغني، موفق الدين ابي محمد عبدالله ابن قدامة، تحقيق عبدالله بن عبد المحسن التركي، عبد الفتاح محمد الحلو،الرياض، دار عالم الكتب، الطبعة الثالثة، ١٩٩٧ م.

٤٩) المقدمات الممهدات، ابي الوليد محمد بن احمد ابن رشد الجد، تحقيق سعيد احمد اعراب، دار الغرب الاسلامي،١٩٨٨

٥٠) المبسوط،شمس الدين السرخسي، بيروت، دار المعرفة، بدون تاريخ

٥١) مغني المحتاج، شمس الدين محمد ابن الخطيب الشربيني، لبنان، دار الفكر، الطبعة الاولى، ٢٠٠٥ م

٥٢) مكونات الحاسب وتجميعه، المؤسسة العامة للتعليم الفني والتدريب المهني، المملكة العربية السعودية،،بدون تاريخ.

٥٣) موسوعة الكمبيوتر الميسرة، انطوان بطرس، لبنان، مكتبة لبنان، ١٩٩٤ م.

٥٤) مفاهيم الكمبيوتر الاساسية، وليام س ديفيز، ترجمة مؤسسة الابحاث اللغوية، 1987م.

٥٥) مقدمة الى نظرية المعلومات، الرموز، الاشارات، الضجيج، جون ر بيرس، ترجمة فايز فوق العادة، بدون تاريخ

_حرف النون _

٥٦) نهاية المحتاج،شمس الدين محمد بن شهاب الدين الرملي، القاهرة، ٢٠١٢ م.

_حرف الهاء _

٥٧) الهكر الاخلاقي، محمد طيبة، كتاب الكتروني متاح على موقع المهندسين العرب

ثانيا: البحوث:

- الجرائم الالكترونية، المفهوم والاسباب، ذياب البداينة، بحث مقدم الى الملتقى العلمي، الجرائم المستحدثة في ظل المتغيرات والمتحولات الدولية والدولية، كلية العلوم الاستراتيجية، عمان، ٢٠١٤ م.
- لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الالية للمعلومات، عمر الفاروق الحسيني، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد الاول، الطبعة الثالثة، ٢٠٠٤ م
- جرائم الكمبيوتر والانترنت، يونس عرب، ورقة عمل مقدمة الى مؤتمر الامن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، ٢٠٠٢ م.
- عدم ملائمة القواعد التقليدية، غنام محمد غنام،، بحث مقدم لمؤتمر الكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤ م.

- الحماية الجنائية البيانات، عبد القادر القهوجي، بحث مقدم لمؤتمر الكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤ م.

كورسات الفيديو:

- ، دورة الهكر المتقدم، محمد طيبة، فيديو، اليوتيوب، تم نشره في ٢٠١٥/٠٩/٢٩

- دورة الهكر الاخلاقي، محمد هاني، فيديو، اليوتيوب، تم تحميله في ٢٠١١/٠٨/٢٧.

١) دورة الهكر الاخلاقي، محمود عاطف، فيديو، على موقع اليوتيوب، **تم نشره في ٢٠١٤/٠٦/١٧**

- صيحة الحق، دروس مرئية عن الشبكات، فيديو. تم تحميله في ٢٠٠٨/١٠/١٧

- سنة اولى كمبيوتر، مقدمة عامة في اساسيات الكمبيوتر، ابراهيم عبد الحميد، تم نشره في ٢٠١٢/٣/٣.

المراجع الانجليزية:

١) CEH-Certified Ethical Hacker Study Guide

2010، WILEY،SYBEX،kimberly،Graves

٢) the basic of hacking and penetration،

2011، syngress،، patrick،Engebretson

٣) ethical hacking and penetration testing guide،

. crc 2015، Rafay،Baloch

٤) John ، chris، anley،s Handbook،the shellcoder

، Gerardo Richarte، Felix “FX” Linder،Heasman

2007،Wiley

٥) october 2013،aicpa،the top 5 cyber crimes

٦) Hacking and Securing ios Applications،

2012 ،REILLY، O، Jonathan،Zdziarski

٧) Handbook on Identity_ related crime،

2011، New York،UNODC

٨) Binh، Nguyen،Linux Filesystem Hierarchy ،

2003،Version 0.65

المحتويات

هذا الكتاب منشور في