**المهكرين**

هاكر أو قرصان أو مخترق (بالإنجليزية: Hacker) يوصف بأسود إن كان مخرب وأبيض إن كان يساعد على أمان الشبكة ورمادي إن كان مجهول الهوية، عموما كلمة توصف المختص المتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية. وأطلقت كلمة هاكر أساسا على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم. إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه. والقيام بهذا عملية اختيارية يمتحن فيها المبرمج قدراته دون أن يعرف باسمه الحقيقي أو أن يعلن عن نفسه. ولكن بعضهم استغلها بصورة إجرامية تخريبية لمسح المعلومات والبعض الآخر استغلها تجاريا لأغراض التجسس والبعض لسرقة الأموال.

هنا وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها ووجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز بمرتبات عالية مهمتهم محاولة اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبل للوقاية اللازمة من الأضرار التي يتسبب فيها قراصنة الحاسوب. في هذه الحالة بدأت صورة الهاكر في كسب الكثير من الإيجابيات. إلا أن المسمى الأساسي واحد. وقد أصبحت كلمة هاكر تعرف مبرمجا ذا قدرات خاصة يستخدمها في الصواب كما يمكن استخدامها في الخطأ.

**الخلاف حول تعريف الهاكر**

ينظر كثيرون للهاكر على أنه شخص مدمر وسلبي، ويقرن البعض كلمة هاكر مع قرصان الحاسوب. وذلك بتأثير من بعض ما ورد في الإعلام، حيث يرجع السبب لقلة فهمهم حقيقة الهاكر، وخلطهم لها بكلمة القرصنة (بالإنجليزية: Piracy) التعبير الذي يصف البيع غير المشروع لنسخ من أعمال إبداعية. وهي مستخدمة في انتهاك حقوق الملكية الفكرية وحقوق النشر خصوصا بالنسبة للأفلام والمسلسلات التلفزيونية والأغاني وبرامج الحاسوب. والتي أصبحت الشبكة العنكبوتية إحدى وسائل تسويقها.

أصل الخلاف أطلقه بعض الأكاديميون لعدم فهمم لطبيعة الهاكر وأسلوب عمله بالرغم من أنه أساسا مطور مبدع. ولكنهم رأو دوره سلبيا ومفسدا، متناسين أن الإنترنت يزدحم بمشاريع تم تطويرها من نشاط جماعي للهاكرز، من أمثلة تلك المشاريع: لينكس، ويكيبيديا، ومعظم المشاريع ذات المصدر المفتوح.

والكراكر Cracker مصطلح أطلق فيما بعد للتمييز بين الهاكر الصالح والهاكر المفسد، وبالرغم من تميز الإثنين بالذكاء وروح التحدي وعدم خوفهم من مواجهة المجهول. إلا أن الكراكر يقوم دائما بأعمال التخريب والاقتحام لأسباب غير ايجابية وهذا الشخص هو الذي يستحق تسمية قرصان الحاسوب. بينما الهاكر يبتكر الحلول للمشاكل ويحاول أن يبدع في عمله.

لقطة من فيلم ماتركس فيها ترينيتي تقتحم شبكة الكهرباء

ولكن سبل الإعلام تتكلم بصفة عامة على "الهاكر " وخلطت بين المصلح والمفسد، وبمرور الوقت اقترن اسم هاكر بالشخص المفسد.

**تصنيف الهاكر أخلاقيا**

* الهاكر ذو القبعة البيضاء | الهاكر الأخلاقي (White hat hacker)، ويطلق على الهاكر المصلح.
* الهاكر ذو القبعة السوداء (Black hat hacker)، يطلق على الهاكر المفسد، وهو يسمى بالإنجليزية Cracker.
* الهاكر ذو القبعة الرمادية (Grey hat hacker)، المترنح بين الإصلاح والعبث.

أما اصطلاح القبعات فأصله مرتبط بتاريخ السينما وخصوصا أفلام رعاة البقر حيث كان الرجل الطيب يرتدي دائما قبعة بيضاء بينما يرتدي الرجل الشرير قبعة سوداء والرمادية لمن يقع دوره بين هاتين الحالتين.

**دور الهاكر في عمران وتطوير الانترنت**

ساهم قراصنة الحاسوب أو الهاكرز في تصميم بنية وتقنيات الإنترنت، وما زالوا يقومون بالكثير من الجهود لتحسين بنية الشبكات وتطوير التقنيات المستخدمة في التشبيك. فهي فئة متميزة من مبرمجي الحاسوب وتعمل مهنيا في ذلك الحقل. من الممكن تفصيل بعض مهام قراصنة الحواسيب:

* الكشف على عيوب أمن المعلومات، وعرض الحلول لها وبذلك الحماية من المستخدم السلبي، القيام بإنجاز مشاريع مفتوحة المصدر، وعرضها مجاناً على الإنترنت مثل نظام تشغيل لينكس،
* القيام بتعديل السكريبتات الموجودة على مواقع الشبكات وتطويرها،
* تقديم استشارات أمنية لكبرى الشركات مثل مايكروسوفت، وشركات بناء الطائرات، والمؤسسات الصناعية الكبرى، وكذلك أرشيفات المعلومات الحكومية، لمنع سلب تصميمات الأجهزة والآلات من قبل منافسين على المستوي الوطني أو المستوى الدولي، ومنع دخول العابثين إلى شبكاتهم التي تحتوي على مسائل سرية أو حساسة ومنع التخريب.
* مساعدة السلطات الأمنية للدول في السيطرة على إساءة استغلال التقنية. كما تشكلت في بعض الدول الغربية وفي الولايات المتحدة وكندا جماعات متخصصة تابعة للسلطات الأمنية لمتابعة الناشرين في الإنترنت لصور مخلة بالآداب وشطب تلك المحتويات. ومن تلك الجماعات المتخصصة من يتحرى في الإنترنت ويقدم المعلومات التي تسهل العثور على هؤلاء الخارجين على القانون الذين يقومون بنشر تلك المنشورات والصور المخلة بالآداب للقبض عليهم وتقديمهم إلى المحاكم المختصة.

**أساليب الهاكر الهجومية**

* هجمات الحرمان من الخدمات (DoS):
* عملية خنق السيرفر وذلك باغراقه بالمواد والبيانات إلى أن يصبح بطيئاً أو حتى يتعطل وينفصل من مرور الشبكة كلياً.
* تجاوز سعة المخزن المؤقت (Buffer overflow):
* يتم الهجوم عن طريق إغراق ذاكرة الخادم فيصاب بالشلل.
* الثغرات الأمنية (Exploits):
* بعد أن يتعرف الهاكر على البرامج التي تدير السيرفر المستهدف يبحث عن ثغرات في تلك البرامج ليستغلها أو يفسدها.
* أحصنة طروادة (Trojan horse):
* يستقبل الجهاز المستهدف برنامج متنكر يفتح من خلاله ثغرة أمنية خفية ليتسلل من خلالها المهاجم.
* تطور استغلال أساليب الهاكر الهجومية إلى حد شدة التنافس بين الدول، وأصبحت طريقة لإلحاق أضرارا بالغة على بلد معادي، بدلا من شن حربا مسلحة علية بالدبابات والطائرات والذخيرة فتشن حربا معلوماتية عن طريق استغلال الثغرات الأمنية في شبكات العدو الحساسة وافسادها وإصابتها بالشلل. أصبح لتلك الظاهرة المتزايدة على المستوي العالمي تعبير "حرب الإنترنت" أو Cyberwar.
* في دول أوروبا وفي الولايات المتحدة الأمريكية بدأ التفكير في ابتكار أساليب لمقاومة هجوم الهاكر الذي يحاول افساد شبكة حساسة عامة، مثل شبكات توزيع الكهرباء أو شبكة تشغيل إشارات المرور. لأن انقطاع التيار ولو لمدة ساعة واحدة سيترتب عليه أضرارا بالغة للاقتصاد وحركة المرور وتعطل المؤسسات وتعطل المستشفيات. وكما اتت إلينا به وسائل الإعلام مؤخرا من نجاح الإسرائيليين الدخول إلى برنامج تشغيل المفاعل النووي الإيراني وإفساده، مما اضطر الخبراء الإيرانيون إلى تأجيل تشغيل المفاعل إلى حين فحص برمجة التشغيل بدقة وإصلاح ما تتسببه الهجوم الخارجي في برمجة التشغيل.

**أساليب جمع المعلومات**

* + - Sniffing تنصت :
* استشعار وأخذ البيانات من الشبكة عن طريق مايسمى ببرامج الشم التي تسجل كل ما يدور بين الكمبيوترات.
	+ - * Social Engineering الهندسة الاجتماعية :
* أسلوب انتحال شخصية تخدم الهاكر للحصول على معلومات مطلوبة للاقتحام حيث يتم اقناع الشخص المراد أخذ المعلومات منه أن الهاكر صديق أو ماشابه، أو أحد الأفراد الذين يحق لهم الحصول على المعلومات، لدفعه إلى كشف المعلومات التي لديه والتي يحتاجها الهاكر.
* War driving تقصي الشبكات اللاسلكية :
* عملية البحث مكانيا على وجود شبكات لاسلكية وعادة يتجول الهاكر بالسيارة بين المناطق باحثا عن شبكات الواي فاي أو الهوت سبوت حيث يتم استغلال وجود بيانات مشتركه بين المستخدمين لهذه الشبكات وثغرات في الأجهزة الموصوله بالشبكه تمكن الهاكر من اختراقها.
* "يكون الهاكر غالبا من المبرمجين أو مهندسين الشبكات أو من الافراد الملمين جدا بالتكنولوجيا والقيام بالقرصنه عن طريق استخدام اجهزه معينه هو في حالات قليله اما امكانيه القرصنه الحقيقية فتكون من مهاره الهاكر وذكائه الخارق بحيث يكشف الثغرات في مواقع الانترنت والبرامج و ليس من الدائم ان يكون هدف الهاكر هو التخريب فا في اغلب الأحيان يكون الهدف هو اثبات القوة والقدره علي هزم دفاعات الموقع مما يعني ان الهاكر استطاع هزيمه مصممين ومطورين الموقع.

**تقنيات وأدوات القرصنة**

**اختراق نظام المعلومات يتم في خمسة مراحل**

* الاستطلاع.
* المسح.
* الدخول إلى النظام.
* الحفاظ على إمكانية دخول النظام.
* تغطية المسارات.

**الاستطلاع واكتشاف البصمات**

هذه المرحلة هي مرحلة تحضيرية لاختراق النظام؛ حيث تتضمن جمع أكبر قدر ممكن من المعلومات عن الضحية بما في ذلك الشبكة المستخدمة، أنظمة التشغيل، المنصات، التطبيقات، الإصدار الخاص بخادم الويب ونقاط الضعف المتعلقة بالنظام.

 الاستطلاع من خلال محركات البحث: من الممكن أن يقوم محركات البحث بتوفير معلومات عن الضحية إلى حد لا يصدق. وباستطاعة محركات البحث ايضاً أن تقدم نسخ من المعلومات كانت مخزنة مؤقتاً وتم إزالتها من الشبكة العنكبوتية. إضافة إلى ما سبق، تقوم محركات البحث بتوفير معلومات تخص المواقع عن طريق Google earth مثلاً ومعلومات مالية باستخدام Google FinanceوYahoo Finance. أيضاٌ تتيح إمكانية رصد محتوى الضحية باستخدام التنبيهات باستخدام Google alerts وYahoo alerts.

 الاستطلاع من خلال مواقع الوظائف: إعلانات الوظائف الشاغرة تزود القرصان المهاجم بمعلومات وتفاصيل قيمة تخص البنية التحتية للضحية مثل متطلبات الوظيفة، معلومات عن الأجهزة والبرمجيات المستخدمة لوظائف حساسة مثل مسؤولي أمن الأنظمة. مثال على ذلك موقع www.jobs.ps.

 الاستطلاع من خلال المواقع الإلكترونية: استطلاع واستكشاف الموقع الإلكتروني الخاص بالضحية يوفر معلومات قيمة حول بنية الموقع وهذا يتم في عدة طرق مثل: دراسة شيفرة HTML والتي غالباً ما تضمن تعليقات، مخطوط، وهيكلية نظام الملفات. أو عن طريق التصوير المرآوي للموقع كاملاً باستخدام برامج مثل HTTrack website copier. أو عن طريق زيارة الموقع الإلكتروني www.archive.org والذي يحتوي على إصدارات مؤرشفة للمواقع مانحاً القدرة للقرصان المهاجم ليجمع معلومات عن الموقع الإلكتروني للضيحة منذ إنشائه.

 الاستطلاع من خلال البريد الإلكتروني: يتم استخدام برامج تتبع البريد الإلكتروني للتجسس على متلقي الرسائل الإلكترونية المستلمة والتي بدورها توفر معلومات كثيرة مفيدة[6] مثل الموقع الجغرافي للضحية، المدة التي استغرقها الضحية في قراءة الرسالة الإلكترونية، نوع الخادم، المستخدم، معلومات حول ما إذا تمت زيارة الروابط الإلكترونية المرفقة بلرسالة أو لا، نظام التشغيل المستخدم، وإذا ما تم توجيه الرسالة الإلكترونية إلى طرف آخر أو لا. من الأمثلة على هذه البرامج: TraceEmailوPoliteEmail.

 الاستطلاع من خلال مفهوم الذكاء التنافسي: حيث يقوم مفهوم الذكاء التنافسي على عملية جمع، تحديد، وتحليل المعلومات من مصادر متعددة مثل: المواقع، محركات البحث، المؤتمرات، الصحف، التقارير السنوية، الوكلاء، الموردين، وموظفي الهندسة الإجتماعية. العديد من الموقع تعمل على مبدأ الذكاء التنافسي مثل : Hoovers www.hoovers.com و LexisNexis www.lexisnexis.com.

 الاستطلاع من خلال محرك البحث Google: قرصنة جوجل تعني إنشاء استعلامات معقدة من خلال محرك البحث جوجل للحصول على معلومات قيمة عن الضحية. قاعدة بيانات جوجل للقرصنة تقدم عوناً كبيراً في مجال بناء الاستعلامات المناسبة اللازمة للوصول الى معلومات حساسة عن الضحية من خلال نتائج البحث في جوجل. للحصول على مزيد من المعلومات في هذا المجال يمكن قراءة دليل قرصنة جوجل لمختَبِري الإختراق. العديد من البرامج والتطبيقات يمكن استخدامها لهذا الهدف من بينها Metagoofil وGoogle Hacks.

 الاستطلاع من خلال بروتوكول WHOIS: يتم استخدام هذا البروتوكول للاستعلام من قواعد بيانات تحتوي على جدول بحث يتضطمن معلومات عن الشبكات، النطاقات، المضيفين، ومعلومات عن أصحاب النطاقات. يتم الإحتفاظ بقواعد البيانات هذه في سجلات الإنترنت الإقليمية. من الأمثلة على البرامج التي يتم استخدامها لهذا الهدف Whois وSmartWhois[4].

 الاستطلاع من خلال مزود اسم النطاق: وهو يشمل الحصول على معلومات عن بيانات المنطقة مثل اسم النطاق، اسم الحاسوب، عناوين بروتوكول الانترنت لشبكة معينة باستخدام برامج مثل DIG وDNSWatch. يتم استخدام المعلومات التي تم جمعها لأداء هجمات الهندسة الاجتماعية لجمع مزيد من التفاصيل.

 الاستطلاع من خلال الشبكة: في هذه التقنية يستطيع القرصان المهاجم الحصول على مجموعة من عناوين بروتوكول الانترنت وقناع الشبكة الفرعية التي يستخدمها الضحية. باستخدام برامج التتبع مثل Network Pinger يستطيع القرصان المهاجم بناء خريطة متكاملة لهيكلية الشبكة، أجهزة الموجه، وأماكن تواجد الجدار الناري في الشبكة. وأيضاً يتم استخدام برنامج Netcraft لتحديد نوع نظام التشغيل المستخدم على أجهزة الشبكة الخاصة بالضحية.

 الاستطلاع من خلال الهندسة الإجتماعية: تشير الهندسة الإجتماعية إلى أسلوب جمع المعلومات من الناس عن طريق التنصت، استراق الرؤية من وراء كتف الضحية، والتنقيب في مهملات الضحية.

 الاستطلاع من خلال مواقع التواصل الاجتماعي: حيث يقوم القرصان المهاجم هنا بجمع المعلومات عن الضحية من خلال مواقع التواصل الإجتماعي مثل: فيسبوك، تويتر، جوجل بلس، لينكد إن، ماي سبيس، وغيرها.

**كيف يخترق الهاكر المواقع**

**يتم ذلك مرورا بمرحلتين أساسيتين :**

 **جمع المعلومات :**

وأهم هذه المعلومات تكون عنوان الهدف على الشبكة (ip) ومعرفة نظام التشغيل الموجود على هذا الهدف والـسكربتات (Script) ليفحصها إذا كان فيها ثغرات برمجية (أخطاء يقع فيها مبرمج الـسكربت) وهذه الأخطاء أو الثغرات تسمح للهاكر بأن يفعل عدة أشياء ممنوعة .

 **الهجوم :**

هي مرحلة يتم فيها استغلال الثغرات والاستغلالات غالبا ما تكون على شكل روابط. فيقوم الهاكر بالدخول للوحة تحكم المدير أو تطبيق الأوامر على السيرفر أو رفع ملفات خبيثة كالشل (سكرايبت خبيث يستعمله الهاكرز) .

**المسح**

في هذه المرحلة يقوم الهاكر باستخدام المعلومات التي تم جمعها في مرحلة الاستطلاع من أجل جمع مزيد من التفاصيل المتعلقة بشبكة الضحية مثل الأجهزة المضيفة الفعالة على الشبكة، المنافذ المفتوحة، عناوين الآي بي، هيكلية النظام، الخدمات، والثغرات لجميع الأجزاء التي يتم مسحها. لمزيد من المعلومات حول هذه التقنية يمكن الرجوع إلى الأدوات مفتوحة المصدر لمختبري الإختراق ومبادئ حماية المعلومات.

 **التحقق من الأنظمة الفعالة**: عن طريق بينغ سكان والذي يتضمن ارسال طلب ICMP ECHO للضحية وفي حال كان المضيف فعالاً سيقوم بإرسال رد ICMP ECHO. بهذه الطريقة يستطيع القرصان المهاجم التعرف على جميع الأجهزة الفعالة على الشبكة المستهدفة وإذا ما كان هنالك أي جدار ناري أو لا. وللتحقق من الأنظمة الفعالة على محموعة من عناوين الآي بي يتم استخدام بينغ سويب بدلا من بينغ سكان. من أهم البرامج التي يتم استخدامها لهذه الغاية برنامج NMAP.

 **التحقق من المنافذ المفتوحة**: من خلال استكمال إقامة الاتصال الثلاثي عن طريق إرسال حزم البيانات إلى الجهاز المستهدف مع أحد الأعلام التالية: URG, ACK, RST, SYN, PSH, FIN يستطيع المهاجم كشف ما إذا كان هناك أي منافذ مفتوحة باستخدام برامج منها NetScan Tools Pro.

 **إجراء مسح إلى ما بعد نظام كشف التسلل**: يقوم المهاجمين عادة باستخدام تقنيات لتفادي أن يتم اكتشافهم من قبل نظام كشف التسلل مثل: استخدام حزم بيانات آي بي مقسمة، تقنية توجيه المصدر، تمويه عنوان الآي بي الخاص بهم أثناء اختراق شبكة الضحية، أو الإتصال بخوادم وكيلة وأجهزة مخترقة لبدء الهجوم.

 **معرفة نظام التشغيل المستخدم**: يتم استخدام هذه التقنية لمعرفة نظام التشغيل المستخدم على الجهاز المستهدف مما يساعد القرصان المهاجم على معرفة الثغرات المرتبطة بهذا النظام واستغلالها لاختراق نظام الضحية باستخدام برامج مثل ID Serve وNetcraft.

 **إجراء مسح لإيجاد الثغرات**: يتم إجراء مسح لاكتشاف الثغرات في النظام المستهدف وهذه الثغرات قد تكون متعلقة بالشبكة، بنظام التشغيل، او بالبرامج والخدمات باستخدام برامج مثل SAINT وNessus.

 **رسم مخططات الشبكة:** رسم مخططات الشبكة يوفر معلومات شاملة للمهاجم، عن طريق تحديد هيكلية الشبكة، بنية الشبكة، الجدران النارية، أنظمة كشف التسلل وآليات الحماية المستخدمة. برامج LANsurveyor و The Dude تستخدم لإنتاج مخططات الشبكات المسهدفة.

 **إعداد الأجهزة الوكيلة:** الوكيل هو جهاز كمبيوتر وسيط يستخدم للاتصال بأجهزة كمبيوتر أخرى. يقوم المهاجمون باستخدام خوادم وكيلة لإخفاء عناوين الآي بي الخاصة بهم وانتحال عنوان وهمي من الوكيل، أيضا قد يستخدم المهاجمون سلسلة من الخوادم الوكيلة لتجنب الكشف وبذلك يكون من الصعب على مسؤولي الأمن تتبع مصدر الهجوم. من أهم البرامج التي يتم استخدامها لهذه الغاية TOR وProxifier.

**التعداد**

يمكن اعتبار التعداد على أنه استطلاع فعال ونشط، بمعنى أنه يتطلب التفاعل بشكل مباشر مع النظام المستهدف من خلال إنشاء وصلات وتنفيذ استعلامات لجمع المزيد من المعلومات، ويتم إجراء التعداد في بيئة انترانت باستخدام التقنيات أدناه:

 **تعداد النت بيوس:** عنوان النت بيوس يتكون من 16 رمز أسكي، 15 رمز تمثل اسم الجهاز والرمز الأخير للخدمة أو نوع السجل. باستخدام تقنية تعداد النت بيوس يستطيع المهاجم الحصول على معلومات تتعلق بالأجهزة التي تنتمي إلى نطاق معين، الأسهم أو المشتركات على جهاز معين في الشبكة، إضافة إلى السياسات وكلمات السر المستخدمة.

 **تعداد بروتوكول إدارة الشبكة البسيط:** تتضمن هذه التقنية تعداد حسابات المستخدمين وأجهزة الكمبيوتر التي تستخدم بروتوكول إدارة الشبكة البسيط لجمع تفاصيل حول موارد الشبكة مثل الأجهزة والموجهات، وشبكة المعلومات مثل جداول التوجيه وجداول بروتوكول تحليل العناوين. ويتم ذلك باستخدام أدوات مثل OpUtils وٍSolar Wind’s IP Network Browser.

 **تعداد يونيكس/لينوكس:** في هذه التقنية تستخدم أوامر خاصة لتعداد موارد شبكة يونيكس[13] مثل: أمر finger لتعداد المستخدمين في المواقع البعيدة، أمر rpcinfo لتعداد بروتوكول استدعاء الإجراء عن بعد و الذي يسمح للتطبيقات التواصل عبر الشبكة، أمر rpcclient لتعداد أسماء المستخدمين على نظام لينوكس، وأمر showmount لإظهار كافة الدلائل المشتركة على النظام حتى للعملاء عن بعد المرتبطين على نظام الملفات. يتم استخدام أداة Enum4Linux لتعداد نظام لينوكس.

 **تعداد بروتوكول الوصول الخفيف إلى الدليل:** بروتوكول الوصول الخفيف إلى الدليل هو بروتوكول الإنترنت الذي يتم استخدامه للوصول إلى خدمات الدليل الموزعة. يتم استغلال خدمات هذا البروتوكول من قبل الدخلاء لجمع معلومات حساسة عن الستخدمين، عناوينهم، أسماء الخوادم وما إلى ذلك. يتم استخدام برنامج Softerra LDAP Administrator لهذا الغرض.

 **تعداد بروتوكول وقت الشبكة:** يستخدم بروتوكول وقت الشبكة لمزامنة الساعات بين أجهزة الكمبيوتر المتصلة بالشبكة. يقوم المهاجمون باستخدام أوامر خاصة موجهة إلى خادم بروتوكول وقت الشبكة لجمع معلومات حساسة عن الشبكةمثل الأجهزة المتصلة إلى الملقم، عناوين IP الخاصة بهم، أسماء النظام وأنظمة التشغيل. الأوامر الستخدمة هي: ntptrace, ntpdc وntpq.

 **تعداد بروتوكول نقل البريد البسيط:** يتم استخدام هذه التقنية لتعداد خوادم بروتوكول نقل البريد البسيط لتحديد المستخدمين الصالحين على الملقم إما باستخدام أوامر خاصة من خلال موجه تلنت أو باستخدام برامج خاصة مثل NetScan Tools Pro.

 **تعداد نظام اسم النطاق:** هذه التقنية تمكن الدخيل من جمع معلومات حساسة عن الشبكة مثل اسم خادم نظام اسم النطاق، اسم المضيف، عناوين IP، وأسماء المستخدمين. يتم ذلك عن طريق تظاهر الدخيل بأنه عميل لخادم نظام اسم النطاق من خلال إرسال طلب للخادم باستخدام Nslookup، وفي الرد يقوم الخادم بإرسال جزء من معلومات قاعدة البيانات الخاصة به والتي قد تحتوي على معلومات قيمة جداً.

**من مشاهير الهاكرز**

* إيهود تننباوم
* كيفن متنيك
* حمزة بن دلاج