الفصل الثامن :
مراحل الاختراق

سيركز هذا الفصل على جرائم الإنترنت التي تتطلب اختراقاً لجهاز أو مجموعة من الأجهزة، وبذلك تستثنى الجرائم التي لا علاقة لها بالاختراق، مثل جرائم الابتزاز أو جرائم الحقوق الفكرية. وسيقتصر هذا الفصل على الحديث عن المراحل التي تمر بها عملية الاختراق، ولكن قبل القيام بتفصيل هذه المراحل، ينبغي إلقاء الضوء على حجم هذا الجرم ومدى انتشاره، من خلال بعض الحقائق التي يقدمها موقع (zone-h) وهو من أهم المواقع المهتمة برصد جرائم الانترنت وخصوصا المتعلقة باختراق المواقع الإلكترونية وتغيير محتواها والتحكم بها.

فقد تلقى الموقع عام انطلاقه في ٢٠٠٢م، ما متوسطه ٢٥٠٠ حالة تشويه للمواقع المختلفة والمتباينة فيما بينها شهرياً، ثم ارتفعت هذه الحالات إلى حوالي ٦٠٠٠٠ حالة تشويه واختراق في ٢٠٠٩م، وارتفع العدد إلى ٩٥٠٠٠ حالة حتى شهر أبريل ٢٠١٠م.

ويبين الجدول ٨-١ والجدول ٨-٢ إحصاءات تشير إلى الزيادة المطّردة في حجم الاختراقات. وإحصاءات أخرى للاستفادة ومعرفة أسباب الاختراق وطرقه، ومقارنة نظم التشغيل المختلفة طبقا لمعدل اختراقها.

الاختراقات خلال الشهور	عام ٢٠٠٨	عام ٢٠٠٩	٢٠١٠ عام
يناير	١٨,٥٦٢	٣٧,٩٦٨	٥٣,٩٢١
فبراير	٥١,٩٢٥	٢,٩١٩	٥٧,٨٦٩
مارس	٤٨,١٣٨	٧	٧٣,٧١٥
إبريل	٤١,٤٩٢	٦٠,٤٧١	٩٥,٠٩٠
مايو	٢٩,٠١٧	٤٨,٠٨٧	
يونية	٣٨,٤٤٥	٤٣,٥٦٩	
يولية	٣٩,٥٤٩	٤٥,٤٨٠	
اغسطس	٧٤,١٢١	٨٣,٨٥٠	
سبتمبر	٤٢,٣٧٩	٧٤,٣٨٤	
أكتوبر	٥٤,٩٧١	٥٤,٤٦٢	
نوفمبر	٤٤,٤٨٦	٤٣,١٧٧	
ديسمبر	٣٤,٣٧٤	٥٠,٠٣٥	

جدول ٨-١ توزع الاختراقات حسب الأشهر

Operational System	Year 2008	Year 2009	Year 2010
Linux	352.468	378.744	256.648
Windows 2003	117.978	127.128	81.785
Windows 2000	21.929	12.529	2.805
FreeBSD	13.418	10.050	5.503
Unknown	4.642	3.933	1.815
Solaris $^{9}/_{10}$	3.002	7.699	364
SolarisSunOS	1.629	16	10
MacOSX	893	510	384
Win NT9x	440	225	132
Win 2008	364	2.977	3.165
Win XP	329	270	72
HP-UX	216	85	32
NetBSDOpenBSD	69	99	39
Solaris 8	35	41	5
BSDOS	10	14	2
AS/400	6	1	1
Com paq Tru64	6	16	2
NovellNetware	5	5	0
Unix	3	29	43
IRIX	3	12	5
OpenVMS	3	1	0
AIX	3	1	0
MacOS	3	0	2
OpenBSD	1	0	0
Win Vista	1	1	0
OpenServer	1	0	0
Win .NET	1	1	0
OS2	1	0	5
Dig i tal Unix	0	3	0
SCO Unix	0	19	2

جدول ٨-٢ توزع الاختراقات حسب نظم التشغيل

وإذا تبيّن مقدار انتشار هذا النوع من الجرائم الإلكترونية وخطورتها، فإن آلية عمليات الاختراق ومراحلها لا تتطابق في كل الحالات، حيث إن نوع العملية ومعطياتها يختلفان من مجرم إلى آخر، وبناءً على ذلك تختلف المراحل التي تمر بها تلك الجريمة. ومعرفة هذه المراحل ضرورية لمن يريد حماية نفسه منها. فدراسة الخصم ومعرفة خططه وطريقة عمله تساعد بشكل كبير على اتقاء شرّه.

ويمكن تقسيم المراحل التي تمر بها الجريمة في الإنترنت إلى ثلاثة مراحل رئيسة:

أولا: مرحلة جمع المعلومات

ثانيا: القيام بالاختراق

ثالثا: مسح الآثار

وقد يندرج تحت كل مرحلة بعض المراحل الفرعية التي سيأتي الحديث عنها بالتفصيل.

٨-١ مرحلة جمع المعلومات

ويشبه خبراء الحماية هذه المرحلة باللص الذي يقوم بالدوران حول المنزل، ويحاول بخفة أن يرى ما إذا كان أحد أبواب المنزل أو نوافذه مفتوحة ليستخدمه للدخول للمنزل وسرقته. وهذا فعلاً ما يقوم به المجرم في هذه المرحلة، حيث يقوم باستخدام بعض الأدوات التي ذكرناها في الفصل السابع لجمع أكبر قدر من المعلومات عن الشبكة، أو الجهاز أو الشخص المستهدف. وهذه المعلومات في الغالب تكون:

- قائمة بالأجهزة الموجودة في الشبكة، ومع كل جهاز يوجد أكبر قدر من المعلومات عنه، مثل نوعية نظام التشغيل، والمنافذ المفتوحة، والثغرات الموجودة في التطبيقات التي تعمل في الجهاز.

- محاولة معرفة تصميم الشبكة، وهناك برامج وتقنيات تساعد على ذلك. ونقصد بتصميم الشبكة هو معرفة مواقع جدران الحماية ومعرفة عدد الشبكات الفرعية (Subnets) وأرقام (IP) الخاصة بكل شبكة، ومعرفة أرقام (IP) الخاصة بالمحولات (Routers) الموجودة في كل قسم.
- معرفة عناوين التطبيقات التي يستخدمها الموظفون.
- معرفة ما اذا كانت المعلومات موجودة في مقر الشركة أو في مكان آخر.
- محاولة الحصول على أسماء المستخدمين وكلمات المرور واستخدامها للدخول للشبكة.
- معرفة البريد الإلكتروني للموظفين والمجموعات الإخبارية والمنتديات التي يشاركون فيها ومواقع التواصل الاجتماعي الخاص بهم.
- معرفة أرقام هاتف الشركة وأقسامها، وهذه مهمة في حالة استخدام المخترق لحيل الهندسة الاجتماعية للحصول على بعض المعلومات التي تساعده على الاختراق.

ولا يوجد حد للمعلومات التي يريد المخترق الحصول عليها، ولا يوجد حد لكيفية الحصول عليها. ومن الطريف ذكره أن بعضاً من أنجح عمليات الاختراق تم الحصول على معلومات مهمة، ساعدت على تنفيذها عن طريق التنقيب في (النفايات) الخاصة بالشركة لتي ترمي فيها بعض الشركات بمعلومات حساسة دون أن تعلم.

ويمكن تقسيم عملية جمع المعلومات إلى قسمين:

١. جمع المعلومات دون الاتصال المباشر بالجهة الضحية، وهذه المعلومات يمكن أن يحصل عليها المخترق بواسطة البحث في محركات البحث عن الجهة التي يريد اختراقها. فمثلا، خبر منشور عن شراء تلك الشركة لترخيص من شركة مايكروسوفت، يعني أنها ستقوم باستخدام مزود الويب (IIS)، وأنه ستوجد بعض المزودات التي تستخدم نظام التشغيل ويندوز.

٢. جمع المعلومات بالاتصال المباشر بالجهة الضحية. ويتم ذلك عن طريق استخدام البرامج المذكورة سابقاً التي تسمح بتحديد الأجهزة والمنافذ المفتوحة فيها، والبرامج والثغرات الموجودة في تلك الأجهزة.

وهذه المرحلة هي أهم مرحلة في عملية الاختراق، وهي تحدد ما إذا كانت العملية ستتم أم لا. فمن دون جمع معلومات كافية، لن يستطيع المجرم تنفيذ فعلته. وبعد الانتهاء من هذه المرحلة، ينتقل المجرم إلى المرحلة التالية، وهي مرحلة الاختراق الفعلي.

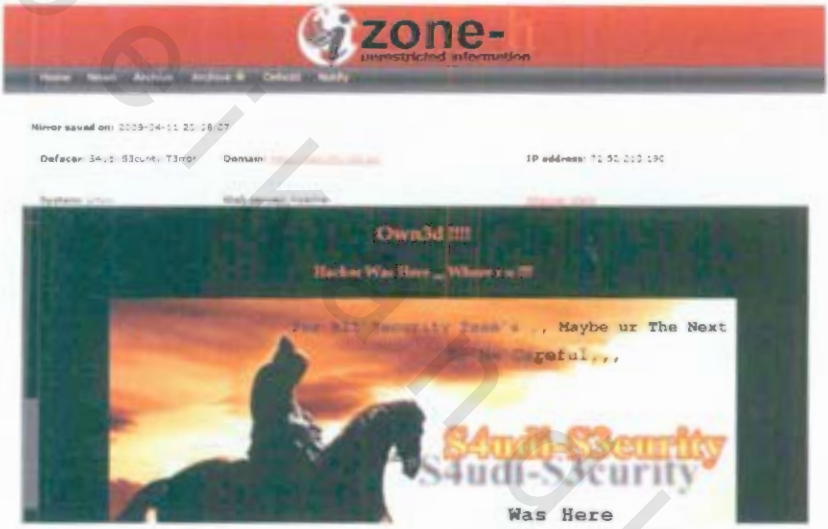
٨-٢ مرحلة الاختراق الفعلي

وفي هذه المرحلة، يقوم المخترق باستخدام المعلومات التي حصل عليها في المرحلة الأولى للقيام بعملية الاختراق. حيث يوجد لديه كل ما يريد لتنفيذ الهجمة، فهو يعرف الأجهزة التي يريد مهاجمتها، ويعرف كذلك الثغرات الموجودة فيها وكيفية استغلالها.

وعلى العكس من مرحلة عملية جمع المعلومات التي يستطيع المخترق فيها أن يأخذ كل الوقت الذي يريده، فإن مرحلة الاختراق الفعلي، لابد أن تتم مباشرة بعد عملية جمع المعلومات والتخطيط للهجمة، وذلك لضمان فعالية المعلومات وضمان عدم قيام المشرفين على الشبكة بإصلاح أو سد الثغرات الموجودة فيها.

وبناءً على نوعية الهجمة فإن عملية الاختراق قد تمر دون ملاحظة. فمثلا عند قيام المخترق بهجمة على شبكة لسرقة معلومات مهمة منها، فإنه في الغالب يرغب أن لا يلاحظ أصحاب تلك الجهة هجمته، لأن ذلك في بعض الأحيان قد يلغي فائدة المعلومات التي تمت سرقتها. فمثلاً، عندما يعلم أحد البنوك بأن أرقام البطاقات الائتمانية قد سرقت فإنه سيقوم بإيقاف هذه الأرقام، بحيث تصبح تلك الأرقام التي حصل عليها المخترق عديمة الفائدة.

ولكن هناك هجمات أخرى يقصد منها أن تلاحظ الضحية تأثيرها، مثل هجمات تعطيل الخدمة (DoS) وهجمات تغيير محتوى الموقع، فالمخترق في هذه الحالة يرغب أن يلاحظ أصحاب الشبكة، وغيرهم تأثير هجمته. وغالبا ما يكون هناك دافع سياسي أو عقائدي لتلك الاختراقات. ويوفر موقع (http://www.zone-h.org) معلومات غزيرة عن المواقع التي يتم اختراقها والعبث بمحتواها.



شكل ٨-١ يوضح اختراق إحدى مجموعات الهاكر لشركة أسترالية متخصصة في أمن المعلومات !!

يتضح من الشكل ٨-١ اسم المخترق، واسم الدومين الذي تم عليه الاختراق، ووقت وتاريخ الاختراق. وعنوان الـ (IP) الخاص بالضحية.

في أحيان كثيرة، فإن هذه المرحلة قد تحتوي على مرحلة فرعية، وهي مرحلة توفير وصول دائم للجهاز المخترق. حيث إن بعض المخترقين بعد اختراق جهاز أو شبكة معينة، فإنه قد يرغب في البقاء في الظل أكبر وقت ممكن من دون أن تتم ملاحظته، وهو بذلك يجني الفوائد الآتية:

عدم معرفة أصحاب الأجهزة بوجود الاختراق يجعلهم يحسون بالأمان، وهذا يعني حصول الشخص على قدر أكبر من المعلومات.

المعلومات التي يحصل عليها الشخص من الجهاز المُخترَق هي أكثر حساسية من المعلومات التي حصل عليها في أثناء المرحلة الأولى. حيث إن الجهاز المُخترَق ينتمي للشبكة الخاصة بالشركة مما يعني أنه داخل نطاق المنطقة الموثوقة التابعة للجهة، وهذا يسمح له بالحصول على قدر أكبر من المعلومات.

يمكن للمخترق استخدام هذا الجهاز لبدء هجمات أخرى على أجهزة وشبكات مختلفة، وهو بذلك يلغي هويته. حيث إن أي محاولة لتتبع أثر الهجمة سيقود إلى هذا الجهاز الوسيط الذي سيعمل المخترق على إزالة آثاره منه.

ومن الطريف أن بعض المخترقين عندما يتمكنون من الدخول إلى جهاز معين واختراقه، فإنهم يقومون بتحصين ذلك الجهاز بحيث لا يستطيع المخترقون الآخرون الدخول عليه. ويوجد العديد من الطرق والبرامج التي تسمح للمخترقين بعمل ذلك، ومن ضمنها ما يسمى بـ (Rootkit) التي تسمح للمخترق بالسيطرة على الجهاز على مستوى نظام التشغيل نفسه، وليس على مستوى التطبيقات فحسب.

٨-٣ مرحلة مسح الآثار

وفي هذه المرحلة فإن المخترق يقوم بمسح جميع الآثار التي تدل على عملية الاختراق، وذلك لخدمة أهداف عديدة، أهمها:

حماية نفسه، بحيث لا يستطيع أحد الوصول له، وهو بذلك يقطع الخط على من يريد تتبعه.

إشعار المشرفين على الجهاز المخترق بالأمان. حيث إنهم حتى لو قاموا بفحص الجهاز المخترق فلن يجدوا ما يثير المخاوف أو ما يشير إلى حدوث عملية الاختراق.

ويتمكن المخترق من مسح أثار الجريمة بطرق عديدة، أشهرها هو الآتي:

تعديل محتويات ملفات سجل العمليات الخاصة بالتطبيقات المختلفة، ومسح كل ما يتعلق به. حيث إن هذه الملفات في الغالب تعطي معلومات كافية للتعرف على المخترق.

تبديل بعض ملفات النظام بحيث لا تعرض أي معلومات خاصة بالمخترق، مثل برنامج (netstat) الذي يعرض أرقام الآيبي (IP) للأجهزة المتصلة بالجهاز حالياً. حيث يقوم المخترق بتبديل هذا البرنامج ببرنامج آخر يعرض جميع الاتصالات ماعدا جهاز المخترق.

وينبغي التوضيح بأن هذه المرحلة غير مطلوبة دائما. حيث يحتاجها المخترق عندما يقوم بالوصول المباشر للجهاز. فهي لا تنطبق على هجمات منع الخدمة مثلاً.

وينصح في نهاية هذا الفصل بعدم الانجراف خلف أي دعوات لتنظيم هجمات عدائية على مواقع المخالفين، وألا نكون صيداً رخيصا لأطراف تجهل ماهيتهم ونعلم أهدافهم. فقد ظهرت في فترة سابقة ما تسمى بحملات الجهاد الإلكتروني، وكان بعض الناس بنية طيبة يشارك في هذه الحملات بإنزال برامج على جهازه لشن الهجمات، وهذه البرامج تتجسس عليه ولا تحقق مراده. بل إن بعض البرامج التي انتشرت تلك الفترة كانت تشن هجمات (تعطيل) لمواقع عربية وإسلامية. لذا فالحماس والنية الطيبة لا تؤدي دائماً إلى خير، بل يجب التحقق من الأمور والوقائع وزيادة الوعي والتعامل مع القضايا والنوازل بحكمة وعقلانية.