BRUCE NIKKEL
Museumsführer im Museum ENTER

DIE HACKING GESCHICHTE

TEIL 4:
Internet Angriffe

Dies ist Teil vier einer vierteiligen Serie zur Geschichte des Computer-Hacking. In den ersten drei Artikeln haben wir uns mit dem frühen Hacken globaler Telefonvermittlungssysteme, dem Hacken mit DFÜ-Modems und der Entwicklung des Computervirus befasst. Dieser Artikel beschreibt die Geschichte internetbasierter Angriffe, einschliesslich Eindringlingen, Man-in-the-Middle-Angriffen und Denial-of-Service.

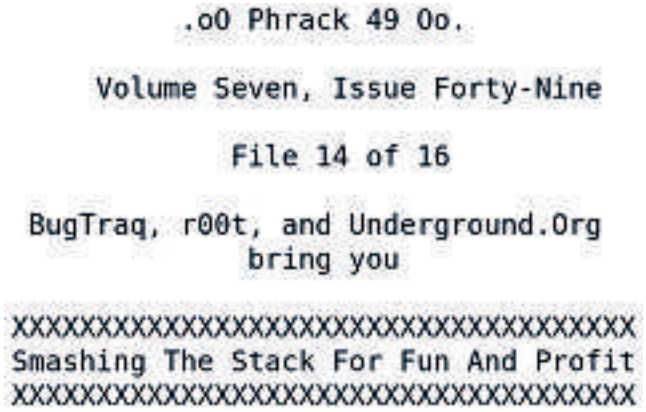
In den Anfangsjahren des Internets gab es keine Firewalls. Unternehmen verbanden ihre TCP/IP-Netzwerke direkt mit dem nächstgelegenen Internet Point-of-Presence (PoP) über dafür bestimmte Standleitungen, die von der Telefongesellschaft gemietet wurden, oder verwendeten Modems für die Einwahl bei Bedarf. Server wurden nicht aus Sicherheitsgründen erstellt («gehärtet»), und Internetdienste wurden so konfiguriert, dass sie maximale Funktionalität bieten (unsichere Standardeinstellungen). Das Internet der 1970er Jahre begann mit einzelnen miteinander verbundenen Systemen. Die 1980er Jahre waren ein Jahrzehnt des «Internetworking», in dem das Internet zu einem Netzwerk von Netzwerken wurde. Die 1990er Jahre waren das Jahrzehnt des World Wide Web und die Kommerzialisierung des Internets. Die erste kostenlose Implementierung des TCP/IP-Protokolls wurde mit BSD UNIX bereitgestellt, das bei Universitäten beliebt war. Diese offene Netzwerkumgebung und das schnelle Wachstum führten zu mehr Sicherheitsverletzungen, und es bildete sich eine Sicherheitsgemeinschaft (http://securitydigest.org/unix/).

«Beastie» BSD UNIX Mascot

Als das Internet wuchs, bestand eine der Herausforderungen beim Hacken darin, neue Maschinen im Internet zu identifizieren und herauszufinden, welche Dienste sie bereitstellten. Es wurden Scanner erstellt, um IP-Adressbereiche umfassend nach Live-Hosts zu durchsuchen und anschliessend die TCP- und UDP-Portnummern (1-65535) nach Diensten zu durchsuchen. Sobald ein Dienst gefunden wurde, wurde er auf Konfigurationsschwächen und Schwachstellen überprüft. Sowohl böswillige Hacker als auch Systemadministratoren verwendeten Scanner, um Sicherheitslücken in Netzwerken und Systemen zu finden (auszunutzen und zu reparieren). Der Satan-Scanner war ein beliebter Sicherheitsscanner, der 1993 von Dan Farmer und Wietse Venema (http://www.porcupine.org/satan/) entwickelt wurde.

Satan Scanning Instrument

Systemadministratoren begannen, Systeme mit defensiven Konfigurationen zu «härten», was es schwieriger machte, in sie einzudringen. Mit der Entdeckung der Code-Ausnutzung wurden die Hacking-Techniken weiterentwickelt. Die meisten Programme, die Dienste im Internet anbieten, wurden in der Programmiersprache C geschrieben. Programme, die Eingaben ohne ordnungsgemässe Überprüfung akzeptieren, können mit ausgeklügelten Speichermanipulations-Hacks (z.B. buffer overflow) ausgenutzt werden. Diese Code-Exploits können zur Ausführung von beliebigem Code auf einem System führen, sodass Angreifer unbefugten Zugriff erhalten. In einem berühmten Artikel, «Smashing The Stack For Fun and Profit», wurde diese Technik im Online-Hacking-Magazin Phrack (http://phrack.org/issues/49/14.html) beschrieben.



Phrack Hacker Online Magazine

Ethernet war eine beliebte Technologie zum Aufbau lokaler Netzwerke (LANs), die über einen Router mit dem Internet verbunden waren. Ethernet wurde als gemeinsam genutzte Bus Oberfläche konzipiert, und jeder in einem Netzwerksegment konnte die Kommunikation anderer Maschinen beobachten (dies waren die Zeiten dummer Ethernet-Hubs und Koaxialkabel). Tools, die als «Paket-Sniffer» bezeichnet werden, wurden entwickelt, um den Netzwerkverkehr abzuhören. Diese waren zur Fehlerbehebung gedacht, konnten aber auch verwendet werden, um Kennwörter aus unsicheren Protokollen (wie z.B. Telnet) zu stehlen. Verschlüsselte Protokolle wie Secure Shell (SSH) lösten dieses Problem, aber Hacker konnten weiterhin Kennwörter durch Erraten (Standardkennwörter des Herstellers) finden oder Brute-Force- und Wörterbuchangriffe ausführen, bei denen Tausende von Kennwörtern getestet werden. Mit der Popularität des Webs wurden Phishing-Sites verwendet, um Passwörter zu stehlen.

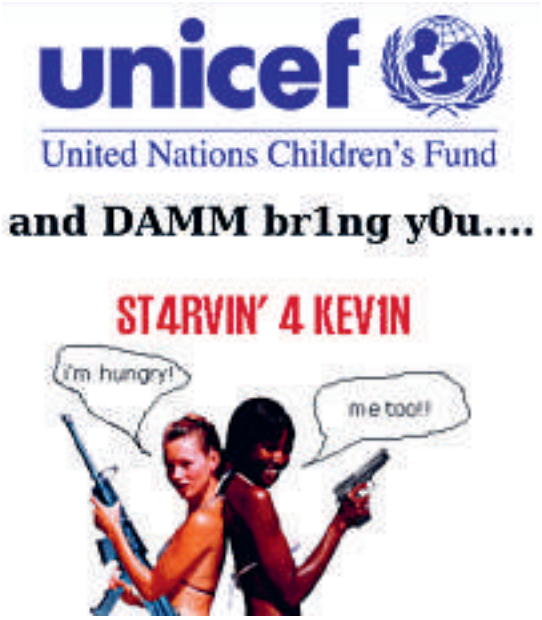
Ethernet Coaxial Kabel mit Verbindungsstück

Nicht alle Systeme benötigten Kennwörter für die Anmeldung. Wenn ein System (IP) und eine Person (Benutzer-ID) als vertrauenswürdig definiert wurden, erlaubten einige Dienste die automatische Anmeldung (z.B. BSD tools wie rshell and rlogin). Eine Technik namens «IP-Spoofing» wurde verwendet, um dieses Vertrauen auszunutzen. Gefälschte Pakete werden unter Verwendung einer imitierten Quell-IP-Adresse über ein Netzwerk gesendet, und der empfangende Host hat auf diese gefälschte Adresse geantwortet (wie das Senden eines Briefes per Post mit einer falschen Absenderadresse). Der berühmte Hacker Kevin Mitnick nutzte Spoofing, um auf den Computer des Sicherheitsforschers Tsutomu Shimomura zuzugreifen. Später wurde er verhaftet (http://wiki.cas.mcmaster.ca/index.php/The_Mitnick_attack).

Das Hacken von Webanwendungen wurde Ende der neunziger Jahre populär. Jedes Unternehmen beeilte sich, Internet-Websites zu erstellen, und viele hatten wenig oder gar keine Sicherheit. Die meisten Website-Hacks waren harmlose «Defacements», bei denen Angreifer die Startseite einer Website modifizierten, um die Organisation in Verlegenheit zu bringen. Wenn Hacker eine Website erfolgreich unkenntlich gemacht haben, können sie ihren erfolgreichen Hack auf www.attrition.org veröffentlichen, damit die Welt ihn sehen kann. Das Defacements-Archiv ist unter archive.org (https://web.archive.org/web/20010203115900/http://attrition.org:80/mirror/attrition/country.html) verfügbar.

2000 – hsr.ch

2000 – audi.de

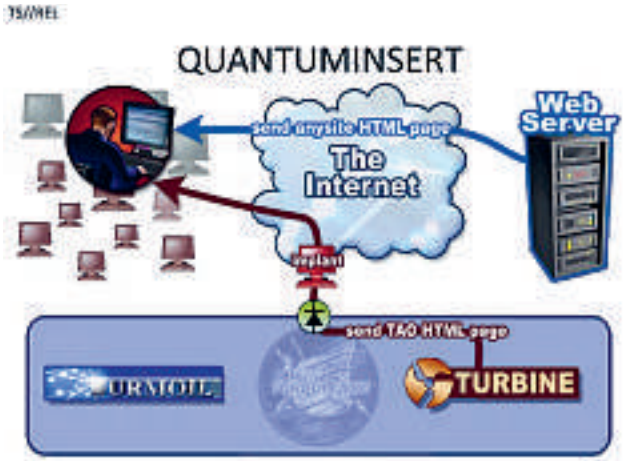


1998 – unicef.org

Einige Beispiele für gehackte Websites sind hier gezeigt. Die meisten Verunstaltungen waren humorvoll, einige protestierten gegen die Verhaftung von Kevin Mitnick, die um diese Zeit stattfand. Eine archivierte Liste gehackter Schweizer Websites finden Sie auch hier: https://web.archive.org/web/20010208130249/http://attrition.org/mirror/attrition/ch.html

Ein weiterer (heute noch häufiger) Internetangriff ist Denial of Service (DoS), bei dem die Infrastruktur (Website, Anwendung, Internetverbindung usw.) nicht verfügbar ist. Heutzutage werden DoS-Angriffe mithilfe von Botnetzen verteilt (Distributed DoS-DDoS), aber in den frühen Tagen des Internets haben andere Methoden funktioniert. Es konnten fehlerhafte IP-Pakete erstellt und gesendet werden, die den Zielhost zum Absturz brachten (z. B. «Ping of Death»). SYN-Flood-Angriffe sendeten Tausende von TCP-SYN-Paketen (möglicherweise gefälscht), um zu verhindern, dass ein Host neue Verbindungen akzeptiert. Andere Angriffe wie «Smurf» und «Fraggle» sendeten gefälschte IP-Pakete an Netzwerk-Broadcast-Adressen. Alle Computer im Netzwerk gingen auf den Broadcast ein und schickten der Opfermaschine gleichzeitig Antworten. Dies war eine frühe Form von DDoS.

Die Geheimdienste der Regierung haben immer versucht, elektronische Signale abzufangen. Das Echelon-Programm (https://en.wikipedia.org/wiki/ECHELON) ist ein frühes Beispiel für das Abfangen von Satellitenkommunikation. Nachdem das Internet populär wurde und wichtige Schlüsselorganisationen mit kritischer Infrastruktur verband, begannen sich Regierungen für Hacking zu interessieren. Die Snowden-Lecks zeigen das Ausmass der Hackerangriffe der westlichen Regierung nach den 9-11 Terroranschlägen in New York. Ein Beispiel für einen man-in-the-middle attack (mitm) wird beschrieben, bei dem ein unerwünschter HTML-Code in das normale Web eingefügt wurde. Das Ziel wird gezwungen, eine schädliche Website zu besuchen, wo es weiter ausgebeutet wird (ein erzwungener Drive-by-Angriff). Ein Archiv von Dokumenten aus bekannter staatlicher Überwachung, finden Sie hier:
https://archive.org/details/nsia-snowden-documents.



Vom Snowden Leak

Hacking entwickelte sich zu einem öffentlichen Spektakel. Hacker wollten berühmt sein, und die Presse wollte den Hype verkaufen. Social Media und Crowd Sourcing wurden zum Stil einer neuen Hacking-Generation. Diese Hacks basierten auf ideologischen Motiven und konzentrierten sich auf soziale Gerechtigkeit und wurden mit dem Begriff «Hacktivismus» beschrieben. Zwei berühmte Hacking-Gruppen waren Lulzsec (https://en.wikipedia.org/wiki/LulzSec) und Anonymous (https://en.wikipedia.org/wiki/Anonymous_(group)). Lulzsec war eine Gruppe von Personen, die zum Spass (für den «Lulz») hackten und über ihre Aktivitäten twitterten.

Lulzsec Branding

Lulzsec Tweet über die CIA Website Attacke

Anonymous war ein dezentrales Kollektiv von Personen ohne Struktur oder Organisation. Die Idee von Anonymous entstand in der 4chan-Online-Community und verwendete Guy-Fawkes-Masken, die im Film «V for Vendetta» populär gemacht wurden. Viele Hacking-Gruppen und Einzelpersonen verbinden sich noch heute mit Anonymous.

Guy Fawkes Maske

Anonymous Logo

Die meisten der in diesem Artikel beschriebenen Angriffe, Exploits und Hacks funktionieren nicht mit moderner Infrastruktur und sind aus historischer Sicht interessant. Hacking im Internet wird immer in irgendeiner Form existieren, aber die Sicherheit von Netzwerken, Betriebssystemen und Anwendungen wird immer besser. Heutzutage sind Menschen am stärksten gefährdet bei modernen Hackingangriffen. Kriminelle erkennen, dass technische Ausbeutung immer schwieriger und teurer wird, aber das Hacken von Menschen (auch als Social Engineering bekannt) ist billig und funktioniert immer noch.

Der Artikel wurde von Florence Kunz übersetzt.
Der englische Originalartikel befindet sich auf:
https://digitalforensics.ch/nikkel20e.pdf
Original English version can be found here:
https://digitalforensics.ch/nikkel20e.pdf