History of Hacking

Part 4: Internet Attacks

By Bruce Nikkel

Published in HISTEC Journal, a publication by the Swiss computer museum Enter (https://enter.ch).

This is part four of a four part series on the history of computer hacking. In the first three articles we covered the early hacking of global telephone switching systems, hacking with dial-up modems, and the evolution of the computer virus. This article describes the history of Internet based attacks, including intrusions, man-in-the-middle attacks, and denial of service.

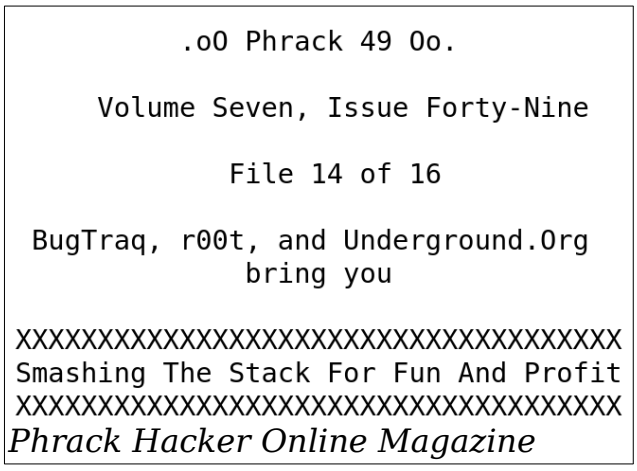
In the early years of the Internet there were no firewalls. Organizations connected their TCP/IP networks directly to the nearest Internet Point-of-Presence (PoP) with dedicated lines leased from the phone company, or using modems for dialup on demand. Servers were not built with security in mind ("hardened"), and Internet services were configured to provide maximal functionality (insecure default settings). The Internet of the 1970s began with individual systems connected to each other. The 1980s was a decade of "internetworking", where the Internet became a network of networks. The 1990s was the decade of the World Wide Web and the commercialization of the Internet. The first free implementation of the TCP/IP protocol was provided with BSD UNIX, which was popular among univerisities. This open networking environment and fast growth led to more security breaches, and a security community started to form (http://securitydigest.org/unix/).

"Beastie" BSD UNIX Mascot

As the Internet grew, one of the hacking challenges was to identify new machines on the Internet and find out what services they provided. Scanners were created to exhaustively search ranges of IP addresses for live hosts, and then scan the TCP and UDP port numbers (1-65535) for services. Once a service was found, it was scanned for configuration weaknesses and vulnerabilities. Both malicious hackers and system administrators used scanners to find security holes (to exploit, and to repair) in networks and systems . The Satan scanner was a popular security scanner created in 1993 by Dan Farmer and Wietse Venema (http://www.porcupine.org/satan/).

Satan scanning tool

System administrators started to “harden” systems with defensive configurations, making them more difficult to break into. Hacking techniques became more advanced with the discovery of code exploitation. Most programs providing services on the Internet were written in the C programming language. Programs accepting input without proper checking could be exploited with sophisticated memory manipulation hacks (buffer and stack overflows, for example). These code exploits could lead to the execution of arbitrary code on a system, allowing attackers to gain unauthorized access. A famous article, “Smashing The Stack For Fun And Profit” described this technique in the online hacking magazine Phrack (http://phrack.org/issues/49/14.html).



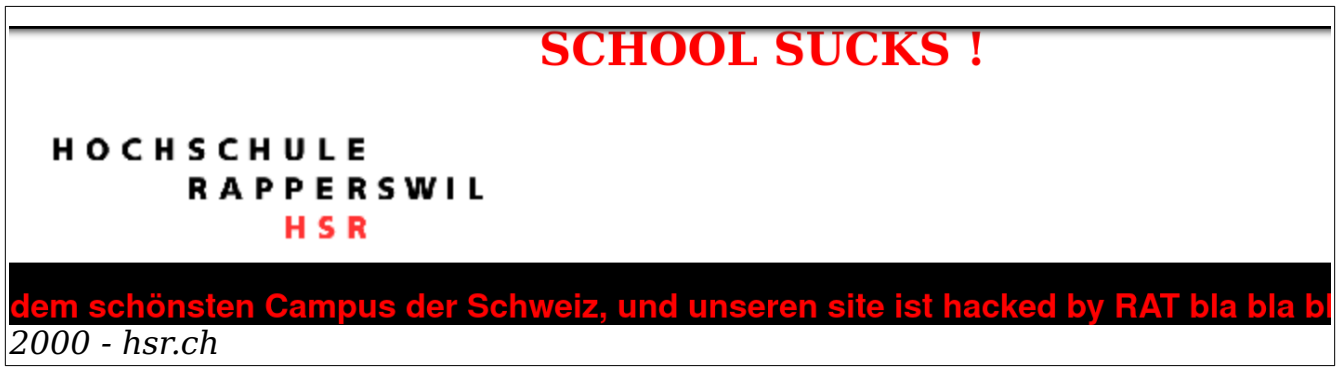
Phrack Hacker Online Magazine

Ethernet was a popular technology used to build Local Area Networks (LANs) which were connected to the Internet by router. Ethernet was designed as a shared bus topology and anybody on a network segment could observe the communication of other machines (these were the days of dumb ethernet hubs and coaxial cable). Tools called “packet sniffers” were developed for listening to network traffic. These were intended for troubleshooting, but could also be used to steal passwords from unsecure protocols (like telnet for example). Encrypted protocols like Secure Shell (SSH) solved this problem, but hackers could still find passwords by guessing (vendor default passwords), or perform brute force and dictionary attacks, where thousands of passwords are tested. With the popularity of the Web, phishing sites started to be used to steal passwords.

Ethernet Coaxial Cable with Connector

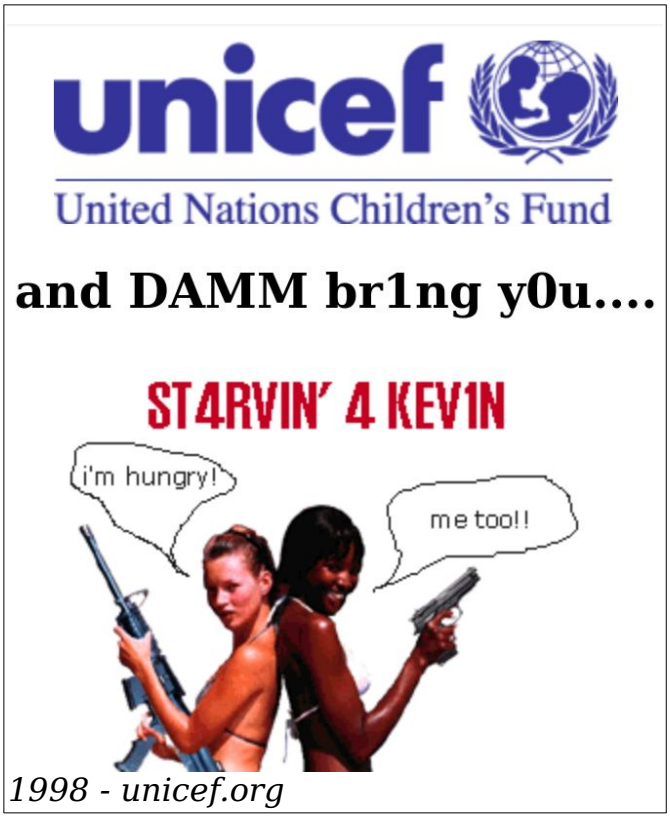
Not all systems required passwords for login. If a system (IP) and person (user-ID) were defined as trusted, some services allowed automatic login (BSD r-tools, like rshell, rlogin, and rcp). A technique called “IP spoofing” was used to exploit this trust. Spoofed packets are sent across a network using an impersonated source IP address, and the receiving host responded to that faked address (like sending a letter by post with a false return address). Famous hacker Kevin Mitnick used spoofing to access security researcher Tsutomu Shimomura's computer, before he (Mitnick) was arrested (http://wiki.cas.mcmaster.ca/index.php/The_Mitnick_attack).

Hacking web applications became popular in the late 1990s. Every company was rushing to create Internet websites, and many had little or no security. Most website hacks were harmless “defacements” where attackers modified the front page of a website to embarrass the organization. When hackers successfully defaced a website, they could publish their successful hack to www.attrition.org for the world to see. The defacements archive is available at archive.org (https://web.archive.org/web/20010203115900/http://attrition.org:80/mirror/attrition/country.html) and a few examples of hacked websites are shown here.



2000 - hsr.ch

2000 - audi.de



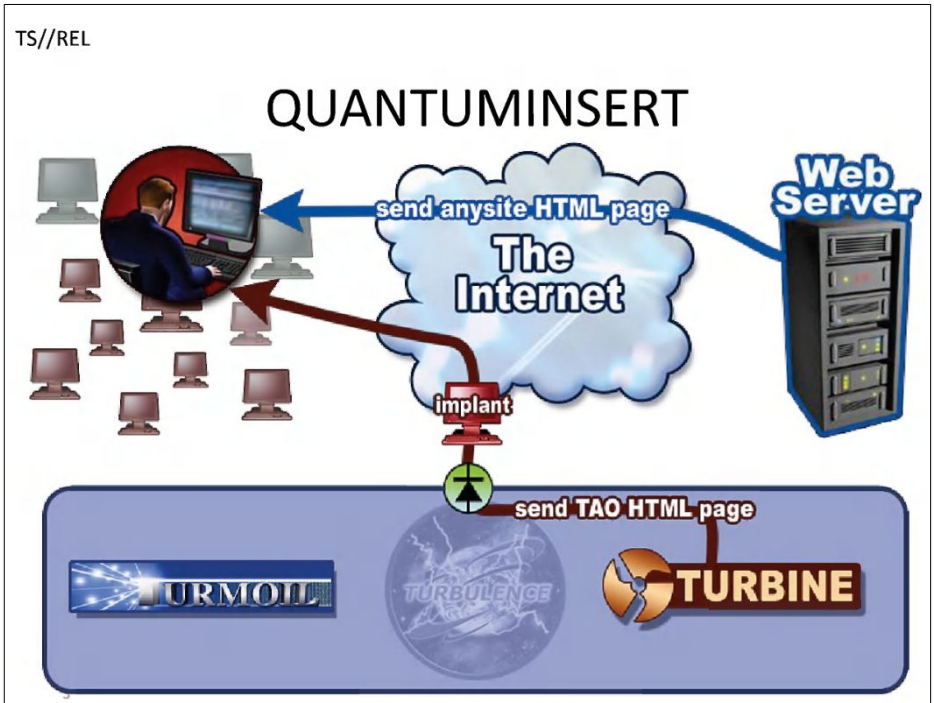
1998 - unicef.org

Most defacements were humorous, some were in protest of the arrest of Kevin Mitnick which happened around this time. An archived list of hacked Swiss websites is also listed here: https://web.archive.org/web/20010208130249/http://attrition.org/mirror/attrition/ch.html

Another Internet attack (still common today) is Denial of Service, or “DoS” which makes infrastructure (website, application, Internet connection, etc.) unavailable. Today DoS attacks are distributed (DDoS) using Botnets, but in the early days of the Internet other methods worked. Malformed IP packets could be created and sent which crashed the the destination host (“ping of death” for

example). SYN flood attacks would send thousands of TCP SYN packets (possibly spoofed), to prevent a host from accepting new connections. Other attacks like “smurf” and “fraggle” would send spoofed IP packets to network broadcast addresses. Every machine on the network would respond to the broadcast, and send replies to the victim machine that was spoofed, overwhelming it in the process. This was an early form of DDoS.

Government intelligence agencies have always tried to intercept electronic signals. The Echelon program (https://en.wikipedia.org/wiki/ECHELON) is an early example of satellite communications interception. After the Internet became popular and started connecting key organizations and critical infrastructure, governments became interested in hacking for intelligence and disruption. The Snowden leaks show the extent of western government hacking after the 911 terrorist attacks in New York. An example man-in-the-middle (mitm) attack is described where rogue html code was injected into normal web traffic, forcing the target (or victim) to visit a malicious website where further exploitation could be done (a forced drive-by attack). An archive of known documents related to known government surveillance is available here: https://archive.org/details/nsia-snowden-documents.



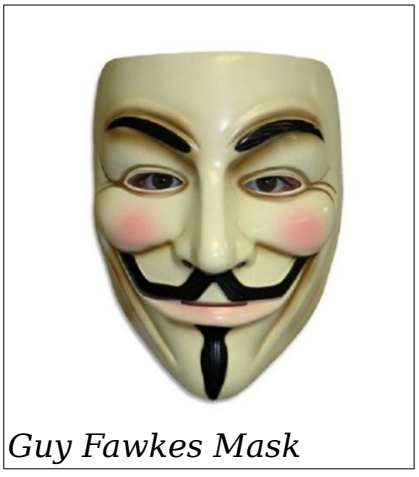
From the Snowden Leaks

Hacking started to evolve into a public spectacle. Hackers wanted to be famous, and the press wanted to sell the hype. Social media and crowd sourcing became the style of a new hacking generation. These hacks were based on ideological motives and focused on social justice, and described by the term “hacktivism”. Two famous hacking groups were Lulzsec (https://en.wikipedia.org/wiki/LulzSec) and Anonymous (https://en.wikipedia.org/wiki/Anonymous_(group)). Lulzsec was a skilled group of individuals who hacked for fun (for the “lulz”) and tweeted about their activity.

Lulzsec Branding

Lulzsec Tweet about CIA Website Attack

Anonymous was a decentralized collective of people, without a structure or organization. The idea of Anonymous originated in the 4chan online community, and used Guy Fawkes masks popularized by the movie “V for Vendetta”. Many hacking groups and individuals still associate themselves with Anonymous today.


Guy Fawkes Mask


Anonymous Logo

Most of the attacks, exploits, and hacks described in this article don’t work on modern infrastructure, and are interesting from an historic perspective. Hacking on the Internet will always exist in some form, but the security of networks, operating systems, and applications is always improving. Today people are the most vulnerable component in modern hacking and attacks. Criminals are realizing that technical exploitation is becoming more difficult and expensive, but hacking humans (also known as social engineering) is cheap and still works.

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