Introduction to Intelligent Security Systems

Alvin Lin

August 2018 - December 2018

Hackers: Activity and Prevention

- Hacking: showing computer expertise
- Cracking: breaching security on software or systems
- Phreaking: cracking telecom networks
- Spoofing: faking the originating IP address in a datagram
- Denial of Service (DoS): flooding a host with sufficient network traffic to overload it
- Port Scanning: searching for vulnerabilities

Hacker Attack Examples

- In April 2007, Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted.
- In June 2007, the US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks.
- In October 2007, China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas. In 2006, when the China Aerospace

Science and Industry Corporation intranet network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

- In the summer of 2008, the databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.
- In July 2011, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.
- Sony Hackers orchestrated multiple breaches of Sony's PlayStation network, knocking it offline for 24 days and costing the company an estimated $171 million.
- In February 2016, hackers angry about the US relations with Israel tried to call attention to their cause by breaching the US Department of Justice's database. CNN reported that the hackers released data on 10,000 Department of Homeland Security employees one day, and data on 20,000 FBI employees the next day. The information stolen included names, titles, phone numbers, and email addresses, but no sensitive information like SSNs were obtained.

Hacker threats include denial of service, defacing, graffiti, slander, reputation damage, loss of data, corporate espionage, or loss of financial assets.

Types of Hackers

- Script kiddies: mostly kids and students that use tools created by black hats.
- Underemployed adult hackers: former script kiddies usually.
- Ideological hackers: hack as a mechanism to promote some political or ideological purpose.
- Criminal hackers: real criminals who are in it for personal gain.
- Corporate spies: relatively rare.
- Disgruntled employees: usually the most dangerous to a company since they have insider access.

- Professional hackers: black hat hackers are malicious hackers to cause harm. White hat hackers are usually professional security experts and consultants who offer hacking/penetration testing as part of their services. Grey hats do not engage in malicious activity but may use hacking methods that are illegal or unethical.

Attack Purposes

- Reconnaisance attacks are an attempt to gather sensitive information about network services and systems (packet sniffers, ping sweep, port scans, queries regarding networking information).
- Denial of service attacks are network attacks devised to slow down or crash a system by flooding it with useless traffic (ping of death, teardrop attack).
- Access attacks are when attacks try to uncover exploits and vulnerabilities in order to gain access to a system's network (password attack, trust exploitation attack, man in the middle).

Gaining Access

- Front Door: password guessing, password stealing
- Back Door: often left by developers as debugging or diagnostic tools
- Trojan Horses: hidden inside of software downloaded from the internet, which usually will install a backdoor
- Software Vulnerability Explotation: allow for privilege escalation or arbitrary code execution

Once insider, hackers can modify logs to cover their tracks, steal files, modify files, install back doors, and attack other systems.

Spoofing

Attackers may use spoofing to alter their identity so that they appear as someone else.

- IP Spoofing: attackers use the IP address of another computer to acquire information or gain access. In a flying-blind attack, they send messages while impersonating another machine, but cannot receive messages addressed to that machine. In a source routing attack, an attack spoofs the address of a machine and inserts itself between the attacked machine and the spoofed machine to intercept replies.

- Email Spoofing: attackers can create accounts with similar addresses, modify mail clients, or telnet to port 25 of a mail server to send messages masquerading as someone else.

- Web Spoofing: attacks can register a web address matching another entity. With man in the middle attacks, the attacker acts as a proxy between the web server and the client. With URL rewriting attacks, the attacker redirects web traffic to another site that they control. With tracking state attacks, attackers can steal the authentication token of a legitimate user after authentication.

- Session Hijacking: after a legitimate user authenticates, the attacker takes the user offline by a denial of service and then impersonates the user.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech