Cyber Reference Aid

The purpose of this Cyber Reference Aid is to illustrate the various phases of an attack and to define some of the more common cyber threat terms.

Cyber Attack Cycle

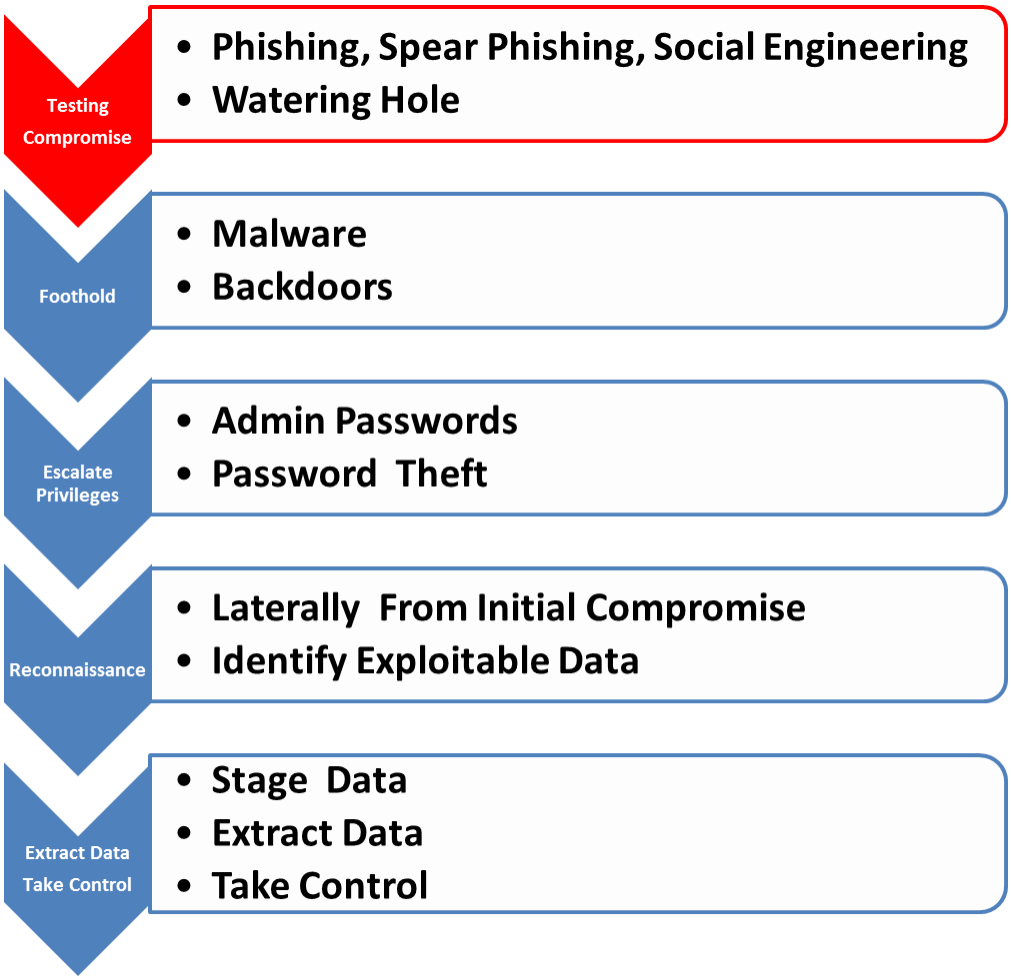
Testing and Compromise - Prior to the initial compromise, the cyber attack cycle may begin by testing key points of a network to determine weakness or vulnerabilities in protection methods. Testing may not always be utilized by the attacker, but may help facilitate the initial compromise. Some of the most common methods of compromise include phishing or spear phishing, watering holes, and SQL-injections. The vast majority occur from a user clicking on an unknown link or attachment that exploits vulnerabilities in the user's system, allowing a remote attacker access. One method is to send an attachment in an e-mail that appears to be legitimate. For example, an attacker may identify a professional organization a victim belongs to through social networking, such as LinkedIn. From there, the attacker may draft a well-crafted e-mail with an attachment, which when opened installs a back door into the user's operating system.

Foothold - Using the initial exploit, an attacker will navigate the system and install additional back doors and other malware to maintain access. The attacker may use the system to gain access to other systems or servers and install additional malware.

Escalate Privileges - The attacker needs to escalate privileges in order to gain access to different parts of the network. For example, an attacker may try different default administrative passwords and username combinations to exploit commonly shared administrative privileges. Once administrator access is gained, the attacker will begin reconnaissance.

Reconnaissance - An attacker will use this initial foothold and escalate privileges to navigate, relatively uninhibited, the network and identify data of value. The attacker may identify places where the data can be cached internally before extraction.

Extract Data/Take Control - Once the attacker has scouted the network to locate desired data, the attacker will extract the data. This is done by either moving data over to a cached location in or outside the network. The data can be encrypted to avoid being exposed by intrusion detection programs. The data can then be uploaded to a file share or extracted by other means. In addition to extracting data, the attacker may also choose to take control of critical infrastructure components.



Attacks and Threats Defined

Denial-of-Service Attacks

- **Denial-of-Service (DoS) -** The attacker prevents legitimate users from accessing information or services. DoS attacks most commonly occur when an attacker "floods" a network with requests, thus overwhelming the server, resulting in denial of service.[1]

- **Distributed Denial-of-Service (DDoS) -** The attacker gains access to another computer through a security loop-hole to facilitate the attack. The attacker may force the computer, now under their control, to send large amounts of data to a website or send spam to targeted e-mail addresses. [2]

- **Domain Name Server (DNS) Amplification Attack -** A popular form of DDos in which the attacker uses publically accessible open DNS servers to flood a target system with DNS response traffic. A misconfigured DNS server can be exploited to participate in a DDos attack.[3]

Social Engineering and Phishing Attacks

- **Phishing Attack -** The attacker uses e-mail or malicious websites to solicit personal information. Attackers often take advantage of current events and certain times of the year.[4]

- **SMiShing -** The attacker uses SMS text messages to "phish" for personally identifiable information and possibly steals funds from the victim. Victims are typically informed that their bank account has been temporarily deactivated, thus requiring them to reply with their credentials to reactivate their account.[5]

- **Social Engineering -** The attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may claim to be a new employee, repair person, or researcher and by asking questions under this persona, may gain enough information to infiltrate an organization's network.[6]

---

[1] US-Cert, Understanding Denial-of-Service Attacks, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST04-015
[2] US-Cert, Understanding Denial-of-Service Attacks, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST04-015
[3] US-Cert, Alerts and Tips, Last Revised July 22, 2013, https://www.us-cert.gov/ncas/alerts/TA13-088A
[4] US-Cert, Avoiding Social Engineering and Phishing Attacks, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST04-014
[5] National Cyber-Forensics & Training Alliance, Phishing Trends, Accessed October 2, 2013, http://www.ncfta.net/test-post.aspx
[6] US-Cert, Avoiding Social Engineering and Phishing Attacks, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST04-014

- **Spear-Phishing Attack -** The attacker uses a well-crafted e-mail to target select groups of people with something in common. E-mails are presumably sent from organizations or individuals the potential victims would normally get e-mail from, thus making them appear even more legitimate.[7]

Malware

- **Adware -** Adware is a type of malware that allows pop-up ads on computer systems, ultimately taking over a user's Internet browsing.[8]

- **Botnet -** A botnet is a network of private computers, each of which is called a "bot" (short for "robot") infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes. Infected computers are also referred to as "**zombies**."[9] Botnets are used to conduct a range of activities, to include distributing spam and viruses to conducting DoS attacks.[10]

- **Rootkit -** A rootkit is a type of malware that can be installed and hidden without knowledge. Rootkits are not necessarily malicious, but can hide malicious activities. An attacker may install the malicious software by taking advantage of vulnerabilities or facilitating the download through a social engineering attack. Attackers may obtain access to information, monitor actions, modify programs, or perform other functions without detection.[11]

- **Spyware -** Spyware is a type of malware that exploit infected computers for commercial gain. They can deliver unsolicited pop-up advertisements, steal personal information, monitor web-browsing activity for marketing purposes, or route HTTP requests to advertising sites.[12]

- **Trojan Horse -** A Trojan Horse is a type of malware disguised as legitimate software, often giving an attacker the ability to take remote control over a

---

[7] FBI, Spear Phishers, Last Revised February 4, 2009, http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

[8] National Cyber Security Alliance, StaySafeOnline- Glossary of Terms, Accessed October 2, 2013, http://staysafeonline.org/stay-safe-online/resources/glossary-of-terms

[9] National Cyber Security Alliance, StaySafeOnline- Glossary of Terms, Accessed October 2, 2013, http://staysafeonline.org/stay-safe-online/resources/glossary-of-terms

[10] US-Cert, Understanding Hidden Threats: Rootkits and Botnets, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST06-001

[11] US-Cert, Understanding Hidden Threats: Rootkits and Botnets, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST06-001

[12] McAfee, Glossary, Accessed October 2, 2013, http://home.mcafee.com/virusinfo/glossary#S

victim's computer. Unlike viruses and worms, Trojan Horses cannot replicate or propagate themselves.[13]

- **Virus -** A virus is a type of malware designed to spread from computer to computer on its own, potentially damaging the system software by corrupting or erasing data, using available memory, or by altering data. A virus cannot spread without a human action, such as running an infected program.[14]

- **Worm -** A worm is a type of malware that can replicate itself over and over within a computer and perform destructive tasks such as using up computer memory resources. Worms do not infect other files as viruses typically do, but instead continue to make copies, resulting in depletion of hard drive space or bandwidth.[15]

Other Hidden Threats

- **Back door -** A back door is a feature programmers often build into programs to allow special privileges normally denied to program users. If attackers learn about a back door, the feature may pose a security risk.[16]

- **Keylogger -** Keylogging is the action of tracking (or logging) the keys struck on a computer keyboard; usually hidden in the background so users are unaware their actions are being monitored.[17]

- **Pharming -** Pharming is when an attacker hijacks a website's domain name, or URL, redirecting users to an imposter website where fraudulent requests for information are made.[18]

- **SQL-Injection -** A SQL-injection is the insertion of programming code redirecting the logic of the program, giving control to the attacker.[19]

---

[13] US-Cert, Understanding Hidden Threats: Rootkits and Botnets, Last Revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST06-001

[14] Norton, Glossary, Accessed October 2, 3013, http://us.norton.com/security_response/glossary/define.jsp?letter=v&word=virus

[15] Norton, Glossary, Accessed October 2, 3013, http://us.norton.com/security_response/glossary/define.jsp?letter=w&word=worm

[16] McAfee, Glossary, Accessed October 2, 2013, http://home.mcafee.com/virusinfo/glossary?ctst=1#B

[17] National Cyber Security Alliance, StaySafeOnline- Glossary of Terms, Accessed October 2, 2013, http://staysafeonline.org/stay-safe-online/resources/glossary-of-terms

[18] Norton, Internet Security Glossary, Accessed October 1, 2013, http://us.norton.com/security-101/?inid=us_hho_topnav_security_101

[19] Microsoft, SQL Injection, Accessed September 27, 2013, http://technet.microsoft.com/en-us/library/ms161953(v=sql.105).aspx

- **Watering Hole -** A watering hole compromise is an unintended download of malicious code (software) that has been injected into legitimate websites the attacker believes will be visited by end users.[20]

Wireless Threats

Piggybacking – Internet users who fail to secure their wireless network provide opportunity for anyone with a wireless-enabled computer within range of the wireless access point a free ride (piggyback) on their wireless connection. The typical indoor broadcast range of an access point is 150-300 feet. Outdoors, this range may extend as far as 1,000 feet. Piggybacking could present a number of potential problems to include service violations, bandwidth shortages, and abuse by malicious actors.[21]

Wardriving – Wardriving is a specific kind of piggybacking whereby the locations of unsecured wireless networks are located by wardrivers and published online. The information is then available to malicious actors seeking an unsecured connection to mask their identity so they can perpetrate illegal online activity.[22]

Resources for Other Cyber Threat Related Terms

- [McAfee Glossary]
- [Symantec Glossary]

[20] Trend Micro, Watering Hole 101, Accessed September 27, 2013, http://about-threats.trendmicro.com/de/webattack/137/Watering+Hole+101

[21] US-Cert, Using Wireless Technology Securely, Updated 2008, http://www.us-cert.gov/sites/default/files/publications/Wireless-Security.pdf

[22] US-Cert, Using Wireless Technology Securely, Updated 2008, http://www.us-cert.gov/sites/default/files/publications/Wireless-Security.pdf