Chapter 2: Attacks, Concepts and Techniques

This chapter covers the ways that cybersecurity professionals analyze what has happened after a cyberattack. It explains security software and hardware vulnerabilities and the different categories of security vulnerabilities.

The different types of malicious software (known as malware) and the symptoms of malware are discussed. The different ways that attackers can infiltrate a system is covered, as well as denial of service attacks.

Most modern cyberattacks are considered to be blended attacks. Blended attacks use multiple techniques to infiltrate and attack a system. When an attack cannot be prevented, it is the job of a cybersecurity professional to reduce the impact of that attack.

Finding Security Vulnerabilities

Security vulnerabilities are any kind of software or hardware defect. After gaining knowledge of a vulnerability, malicious users attempt to exploit it. An *exploit* is the term used to describe a program written to take advantage of a known vulnerability. The act of using an exploit against a vulnerability is referred to as an attack. The goal of the attack is to gain access to a system, the data it hosts or to a specific resource.

Software vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code, despite all the effort companies put into finding and patching software vulnerabilities, it is common for new vulnerabilities to surface. Microsoft, Apple, and other operating system producers release patches and updates almost every day. Application updates are also common. Applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.

In 2015, a major vulnerability, called SYNful Knock, was discovered in Cisco IOS. This vulnerability allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco 1841, 2811, and 3825 routers. The attackers could then monitor all network communication and had the ability to infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed in the routers. To avoid this, always verify the integrity of the downloaded IOS image and limit the physical access of the equipment to authorized personnel only.

The goal of software updates is to stay current and avoid exploitation of vulnerabilities. While some companies have penetration testing teams dedicated to search, find and patch software vulnerabilities

before they can get exploited, third party security researchers also specialize in finding vulnerabilities in software.

Google's Project Zero is a great example of such practice. After discovering a number of vulnerabilities in various software used by end-users, Google formed a permanent team dedicated to finding software vulnerabilities. Google Security Research can be found here.

Hardware vulnerabilities

Hardware vulnerabilities are often introduced by hardware design flaws. RAM memory for example, is essentially capacitors installed very close to one another. It was discovered that, due to proximity, constant changes applied to one of these capacitors could influence neighbor capacitors. Based on that design flaw, an exploit called Rowhammer was created. By repeatedly rewriting memory in the same addresses, the Rowhammer exploit allows data to be retrieved from nearby address memory cells, even if the cells are protected.

Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and a physical security are sufficient protection for the everyday user.

Categorizing Security Vulnerabilities

Most software security vulnerabilities fall into one of the following categories:

Buffer overflow – This vulnerability occurs when data is written beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

Non-validated input – Programs often work with data input. This data coming into the program could have malicious content, designed to force the program to behave in an unintended way. Consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

Race conditions – This vulnerability is when the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or proper timing.

Weaknesses in security practices – Systems and sensitive data can be protected through techniques such as authentication, authorization, and encryption. Developers should not attempt to create their own

security algorithms because it will likely introduce vulnerabilities. It is strongly advised that developers use security libraries that have already created, tested, and verified.

Access-control problems – Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.

Nearly all access controls and security practices can be overcome if the attacker has physical access to target equipment. For example, no matter what you set a file's permissions to, the operating system cannot prevent someone from bypassing the operating system and reading the data directly off the disk. To protect the machine and the data it contains, physical access must be restricted and encryption techniques must be used to protect data from being stolen or corrupted.

Types of Malware

Short for Malicious Software, malware is any code that can be used to steal data, bypass access controls, or cause harm to, or compromise a system. Below are a few common types of malware:

Spyware – This malware is design to track and spy on the user. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses.

Adware – Advertising supported software is designed to automatically deliver advertisements. Adware is often installed with some versions of software. Some adware is designed to only deliver advertisements but it is also common for adware to come with spyware.

Bot – From the word robot, a bot is malware designed to automatically perform action, usually online. While most bots are harmless, one increasing use of malicious bots are botnets. Several computers are infected with bots which are programmed to quietly wait for commands provided by the attacker.

Ransomware – This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting data in the computer with a key unknown to the user. Some other versions of ransomware can take advantage of specific system vulnerabilities to lock down the system. Ransomware is spread by a downloaded file or some software vulnerability.

Scareware – This is a type of malware designed to persuade the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating the system is at risk or needs the execution of a specific program to return to normal operation. In reality, no problems were assessed or detected and if the user agrees and clears the mentioned program to execute, his or her system will be infected with malware.

Rootkit – This malware is designed to modify the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files. It is also common for rootkits to modify system forensics and monitoring tools, making them very hard to detect. Often, a computer infected by a rootkit must be wiped and reinstalled.

Virus - A virus is malicious executable code that is attached to other executable files, often legitimate programs. Most viruses require end-user activation and can activate at a specific time or date. Viruses can be harmless and simply display a picture or they can be destructive, such as those that modify or delete data. Viruses can also be programmed to mutate to avoid detection. Most viruses are now spread by USB drives, optical disks, network shares, or email.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation. This malicious code exploits the privileges of the user that runs it. Often, Trojans are found in image files, audio files or games. A Trojan horse differs from a virus because it binds itself to non-executable files.

Worms – Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network. Worms share similar patterns. They all have an enabling vulnerability, a way to propagate themselves, and they all contain a payload.

Worms are responsible for some of the most devastating attacks on the Internet. As shown in Figure 1, in 2001 the Code Red worm had infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers as shown in Figure 2.

Man-In-The-Middle (MitM) – MitM allows the attacker to take control over a device without the user's knowledge. With that level of access, the attacker can intercept and capture user information before relaying it to its intended destination. MitM attacks are widely used to steal financial information. Many malware and techniques exist to provide attackers with MitM capabilities.

Man-In-The-Mobile (MitMo) – A variation of man-in-middle, MitMo is a type of attack used to take control over a mobile device. When infected, the mobile device can be instructed to exfiltrate user-sensitive information and send it to the attackers. ZeuS, an example of an exploit with MitMo capabilities, allows attackers quietly to capture 2-step verification SMS messages sent to users.

Symptoms of Malware

Regardless of the type of malware a system has been infected with, these are common malware symptoms:

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.

Social Engineering

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. For example, an attacker could call an authorized employee with an urgent problem that requires immediate network access. The attacker could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

These are some types of social engineering attacks:

- **Pretexting -** This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
- **Tailgating -** This is when an attacker quickly follows an authorized person into a secure location.
- **Something for Something (Quid pro quo) -** This is when an attacker requests personal information from a party in exchange for something, like a free gift.

Wi-Fi Password Cracking

Wi-Fi password cracking is the process of discovering the password used to protect a wireless network. These are some techniques used in password cracking:

Social engineering – The attacker manipulates a person who knows the password into providing it.

Brute-force attacks – The attacker tries several possible passwords in an attempt to guess the password. If the password is a 4-digit number, for example, the attacker would have to try every one of the 10000 combinations. Brute-force attacks usually involve a word-list file. This is a text file containing a list of words taken from a dictionary. A program then tries each word and common combinations. Because brute-force attacks take time, complex passwords take much longer to guess. A few password brute-force tools include Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

Network sniffing – By listening and capturing packets sent on the network, an attacker may be able to discover the password if the password is being sent unencrypted (in plain text). If the password is encrypted, the attacker may still be able to reveal it by using a password cracking tool.

Phishing

Phishing is when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on their device, or into sharing personal or financial information. An example of phishing is an email forged to look like it was sent by a retail store asking the user to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing emails are customized to a specific person. The attacker researches the target's interests before sending the email. For example, an attacker learns the target is interested in cars, and has been looking to buy a specific model of car. The attacker joins the same car discussion forum where the target is a member, forges a car sale offering and sends email to the target. The email contains a link for pictures of the car. When the target clicks on the link, malware is installed on the target's computer.

Vulnerability Exploitation

Exploiting vulnerabilities is another common method of infiltration. Attackers will scan computers to gain information about them. Below is a common method for exploiting vulnerabilities:

Step 1. Gather information about the target system. This could be done in many different ways such as a port scanner or social engineering. The goal is to learn as much as possible about the target computer.

Step 2.One of the pieces of relevant information learned in step 1 might be the operating system, its version, and a list of services running on it.

Step 3. When the target's operating system and version is known, the attacker looks for any known vulnerabilities specific to that version of OS or other OS services.

Step 4. When a vulnerability is found, the attacker looks for a previously written exploit to use. If no exploits have been written, the attacker may consider writing an exploit.

Figure 1 portrays an attacker using **whois**, a public Internet database containing information about domain names and their registrants. Figure 2 portrays an attacker using the **nmap** tool, a popular port scanner. With a port scanner, an attacker can probe ports of a target computer to learn about which services are running on that computer.

Advanced Persistent Threats

One way in which infiltration is achieved is through advanced persistent threats (APTs). They consist of a multi-phase, long term, stealthy and advanced operation against a specific target. Due to its complexity and skill level required, an APT is usually well funded. An APT targets organizations or nations for business or political reasons.

Usually related to network-based espionage, APT's purpose is to deploy customized malware on one or multiple of the target's systems and remain undetected. With multiple phases of operation and several customized types of malware that affect different devices and perform specific functions, an individual attacker often lacks the skill-set, resources or persistence to carry out APTs.

DoS

Denial-of-Service (DoS) attacks are a type of network attack. A DoS attack results in some sort of interruption of network service to users, devices, or applications. There are two major types of DoS attacks:

Overwhelming Quantity of Traffic - This is when a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle. This causes a slowdown in transmission or response, or a crash of a device or service.

Maliciously Formatted Packets - This is when a maliciously formatted packet is sent to a host or application and the receiver is unable to handle it. For example, an attacker forwards packets containing errors that cannot be identified by the application, or forwards improperly formatted packets. This causes the receiving device to run very slowly or crash.

DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled

attacker.

DDoS

A Distributed DoS Attack (DDoS) is similar to a DoS attack but originates from multiple, coordinated sources. As an example, a DDoS attack could proceed as follows:

An attacker builds a network of infected hosts, called a botnet. The infected hosts are called zombies. The zombies are controlled by handler systems.

The zombie computers constantly scan and infect more hosts, creating more zombies. When ready, the hacker instructs handler systems to make the botnet of zombies carry out a DDoS attack.

Click Play in the figure to view the animations of a DDoS attack.

SEO Poisoning

Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, a malicious user could use SEO to make a malicious website appear higher in search results. This technique is called SEO poisoning.

The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or perform social engineering. To force a malicious site to rank higher in search results, attackers take advantage of popular search terms.

What is a Blended Attack?

Blended attacks are attacks that use multiple techniques to compromise a target. By using several different attack techniques at once, attackers have malware that are a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes. This trend of blended attacks is revealing more complex malware and placing user data at great risk.

The most common type of blended attack uses spam email messages, instant messages or legitimate websites to distribute links where malware or spyware is secretly downloaded to the computer. Another common blended attack uses DDoS combined with phishing emails. First, DDoS is used to take down a popular bank website and send emails to the bank's customers, apologizing for the inconvenience. The email also directs the users to a forged emergency site where their real login information can be stolen.

Many of the most damaging computer worms like Nimbda, CodeRed, BugBear, Klez and Slammer are better categorized as blended attacks, as shown below:

- Some Nimbda variants used email attachments; file downloads from a compromised web server; and Microsoft file sharing (e.g., anonymous shares) as propagation methods.
- Other Nimbda variants were able to modify the system's guest accounts to provide the attacker or malicious code with administrative privileges.

The recent Conficker and ZeuS/LICAT worms were also blended attacks. Conficker used all the traditional distribution methods.

What is Impact Reduction?

While the majority of successful companies today are aware of common security issues and put considerable effort towards preventing them, no set of security practices is 100% efficient. Because a breach is likely to happen if the prize is big, companies and organizations must also be prepared to contain the damage.

It is important to understand that the impact of a breach is not only related to the technical aspect of it, stolen data, damaged databases, or damage to intellectual property, the damage also extends to the company's reputation. Responding to a data breach is a very dynamic process.

Below are some important measures a company should take when a security breach is identified, according to many security experts:

- Communicate the issue. Internally employees should be informed of the problem and called to action. Externally, clients should be informed through direct communication and official announcements. Communication creates transparency, which is crucial in this type of situation.
- Be sincere and accountable in case the company is at fault.
- Provide details. Explain why the situation took place and what was compromised. It is also expected that the company take care of the costs of identity theft protection services for affected customers.
- Understand what caused and facilitated the breach. If necessary, hire forensics experts to research and learn the details.
- Apply what was learned from the forensics investigation to ensure similar breaches do not happen in the future.
- Ensure all systems are clean, no backdoors were installed, and nothing else has been compromised. Attackers will often attempt to leave a backdoor to facilitate future breaches. Make sure this does

not happen.

- Educate employees, partners, and customers on how to prevent future breaches.