2.1.1 Types of Malware

Cybercriminals use many different types of malicious software, or malware, to carry out their activities. Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system.

- Spyware : Track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details.

- Adware : Adware is often installed with software and is designed to deliver advertisements to a user, most often on a web browser.

- Backdoor : This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system. A backdoor works in the background and is difficult to detect.

- Ransomware : This malware locks down a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you can’t access it. Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down. Ransomware is often spread through phishing emails that encourage you to download a malicious attachment or through a software vulnerability.

- Scareware : This type of malware trick use into taking a specific action. Scareware mainly consists of normal windows that pop up to warn you that "system is at risk" and needs to run a specific program to fix the issue. If you agree to execute the specific program, your system will become infected with malware.

- Rootkit : This malware is designed to modify the operating system to create a backdoor, which attackers can then use to access your computer remotely. Most rootkits take advantage of software vulnerabilities to gain access (privilege escalation) and modify system files. Rootkits can also modify system forensics and monitoring tools, making them very hard to detect.

- Virus : A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code. Most viruses require end-user interaction to initiate activation and can be written to act on a specific date or time. Or they can be destructive, modify or delete data. Viruses can also be programmed to mutate in order to avoid detection. Most viruses are spread by USB drives, optical disks, network shares or email.

- Trojan Horse : This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous. Trojans exploit your user privileges and are most often found in image files, audio files or games. Unlike viruses, Trojans do not self-replicate but act as a decoy to sneak malicious software past unsuspecting users.

- Worms : This is a type of malware that replicates itself to spread from one computer to another. Unlike a virus, which requires a host program to run, worms can run by themselves. Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network. Worms share similar patterns: They exploit system vulnerabilities and they all contain malicious code (payload) to cause damage to computer systems or networks. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.

2.1.2 Symptoms of Malware

Regardless of the type of malware a system has been infected with, there are some common symptoms to look out for.

- an increase in central processing unit (CPU) usage, which slows down your device
- your computer freezing or crashing often
- a decrease in your web browsing speed
- unexplainable problems with your network connections
- modified or deleted files
- the presence of unknown files, programs or desktop icons
- unknown processes running
- programs turning off or reconfiguring themselves
- emails being sent without your knowledge or consent.

2.2.1 Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee’s vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

2.2.2 Denial-of-Service

Type of network attack, a DoS attack results in some sort of interruption of network service to users, devices or applications. DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money.

- Traffic Overload : When a network, or application is sent enormous amount of data, cannot handle and crashes.
- Maliciously Formatted Packets : data packet which is manipulated to crash a server.

2.2.3 Distributed DoS

A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems. The zombie computers will constantly scan and infect more hosts, creating more and more zombies. When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

2.2.4 Botnet

A bot computer is typically infected by visiting an unsafe website or opening an infected email attachment or infected media file. A botnet is a group of bots, connected through the Internet, that can be controlled by a malicious individual or group. It can have tens of thousands, or even hundreds of thousands, of bots that are typically controlled through a command and control server. These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute-force password attacks. Cybercriminals will often rent out botnets to third parties for nefarious purposes.

2.2.5 On-Path Attacks

Attackers intercept communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices. This type of attack is also referred to as a man-in-the-middle or man-in-the-mobile attack.

2.2.6 SEO Poisoning

Search Engine Optimization (SEO) which, in simple terms, is about improving an organization’s website so that it gains greater visibility in search engine results.

Search engines such as Google work by presenting a list of web pages to users based on their search query. These web pages are ranked according to the relevancy of their content. Attackers take advantage of popular search terms and use SEO to push malicious sites higher up the ranks of search results. This technique is called SEO poisoning.

2.2.7 Wi-Fi Password Cracking

Simple Social Engineering attack, attacks ask for WIFI password to connect to the private WIFI.

2.2.8 Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

- Password Spraying : This technique attempts to gain access to a system by ‘spraying’ a few commonly used passwords across a large number of accounts
- Dictionary Attacks : A hacker systematically tries a list of commonly used words as a password in an attempt to break into a password-protected account.
- Brute-Force Attacks : brute-force attacks, attacker using all possible combinations of letters, numbers and symbols in the password space until they get it right.
- Rainbow Attacks : Passwords in a computer system are not stored as plain text, but as hashed values. A rainbow table is a large dictionary of precomputed hashes and the passwords from which they were calculated. A rainbow attack compares the hash of a password with those stored in the rainbow table.
- Traffic Interception : Plain text or unencrypted passwords can be easily read by intercepting communications. If you store a password in clear, readable text, anyone who has access to your account or device, whether authorized or unauthorized, can read it.

2.2.9 Cracking Times

Passwords that include numbers, upper/lower case letters and symbols take longer to crack.

2.2.10 Advanced Persistent Threats

Attackers also achieve infiltration through advanced persistent threats (APTs) — a multi-phase, long term, stealthy and advanced operation against a specific target. For these reasons, an individual attacker often lacks the skill set, resources or persistence to perform APTs. Due to the complexity and the skill level required to carry out such an attack, an APT is usually well-funded and typically targets organizations or nations for business or political reasons. Its main purpose is to deploy customized malware on one or more of the target’s systems and remain there undetected.

Security vulnerabilities are any kind of software or hardware defect. A program written to take advantage of a known vulnerability is referred to as an exploit.

2.3.1 Hardware Vulnerabilities

Hardware vulnerabilities are most often the result of hardware design flaws. For example, the type of memory called RAM basically consists of lots of capacitors (holds electrical charge) installed very close to one another. However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbor capacitors. Based on this design flaw, an exploit called Rowhammer was created.

2.3.2 Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code. You should always verify the integrity of the downloaded IOS image and limit the physical access of such equipment to authorized personnel only.

2.3.3 Categorizing Software Vulnerabilities

Most software security vulnerabilities fall into several main categories:

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

- Non-Validated Input : Programs often require data input, but this incoming data could have malicious content, designed to force the program to behave in an unintended way. For example, 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.

- Weakness in Security Practices : Systems and sensitive data can be protected through techniques such as authentication, authorization and encryption. Developers should stick to using security techniques and libraries that have already been created, tested and verified and should not attempt to create their own security algorithms. These will only likely introduce new vulnerabilities.

- 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. Nearly all access controls and security practices can be overcome if an attacker has physical access to target equipment.

2.3.4 Software Updates

The goal of software updates is to stay current and avoid exploitation of vulnerabilities. Despite the fact that organizations put a lot of effort into finding and patching software vulnerabilities, new vulnerabilities are discovered regularly. That’s why some organizations use third party security researchers who specialize in finding vulnerabilities in software, or actually invest in their own penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited.

2.4.1 Cryptocurrency

Cryptocurrency is digital money that can be used to buy goods and services, using strong encryption techniques to secure online transactions.

Cryptocurrency owners keep their money in encrypted, virtual ‘wallets.’ When a transaction takes place between the owners of two digital wallets, the details are recorded in a decentralized, electronic ledger or blockchain system. This means it is carried out with a degree of anonymity and is self-managed, with no interference from third parties such as central banks or government entities.

Approximately every ten minutes, special computers collect data about the latest cryptocurrency transactions, turning them into mathematical puzzles to maintain confidentiality. These transactions are then verified through a technical and highly complex process known as ‘mining.’ This step typically involves an army of ‘miners’ working on high-end PCs to solve mathematical puzzles and authenticate transactions.

Once verified, the ledger is updated and electronically copied and disseminated worldwide to anyone belonging to the blockchain network, effectively completing a transaction.

2.4.2 Crypto Jacking

Crypto Jacking is an emerging threat that hides on a user’s computer, mobile phone, tablet, laptop or server, using that machine’s resources to 'mine’ cryptocurrencies without the user's consent or knowledge. Many victims of crypto jacking didn’t even know they’d been hacked until it was too late!

2.5 QUIZ

Scored 100% marks, 8/8 correct.