CertExams™
Net Sims | Exam Sims

Security+ Cram Notes

1. Threats, Attacks and Vulnerabilities

1.1 Given a scenario, analyze and determine the type of malware

Threats are potential sources of harm to a system or network. In the context of computer security, there are several types of threats that organizations and individuals must be aware of:

1. Malware: Malware refers to malicious software that is designed to harm or exploit a system or network. Types of malware include viruses, worms, Trojans, and spyware.

2. Hacking: Hacking refers to unauthorized access to a system or network. Hackers may attempt to steal sensitive information, disrupt operations, or use the compromised system for their own purposes.

3. Phishing: Phishing is a type of social engineering attack in which attackers send fake emails or messages that appear to be from a legitimate source, such as a bank or other financial institution, in an attempt to trick the recipient into revealing sensitive information.

4. Social Engineering: Social engineering attacks use psychological tactics to manipulate individuals into revealing sensitive information or performing actions that can harm the security of a system or network.

5. Denial-of-Service (DoS) Attacks: DoS attacks aim to make a system or network unavailable by overwhelming it with traffic or requests.

6. Ransomware: Ransomware is a type of malware that encrypts the data on a system or network and demands payment in exchange for the decryption key.

7. Advanced Persistent Threats (APT): APTs are a type of hacking attack that targets a specific organization or individual, often with the goal of stealing sensitive information or disrupting operations.

These are just a few examples of the types of threats that organizations and individuals must be aware of. Effective security requires a proactive approach, including implementing appropriate technical controls, educating employees, and regularly reviewing and updating security policies and procedures.

Viruses, worms, and Trojan horses are all harmful pieces of software. The way they differ is how they infect the computers, and spread across the systems and networks.

Virus: A computer virus attaches itself to a program or file so it can spread from one computer to another. Most of the viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. Note that, usually, a virus cannot be

CertExams.com

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

Copyright © 2000 - 2023 CertExams.com Version 2.0

spread without a human action, (such as running an infected program) to keep it going.

WORM: Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

Trojan Horse: The Trojan Horse, at first glance appears to be a useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening it because it appears to be receiving legitimate software or file from a legitimate source.

Rootkit: A rootkit is a collection of tools that enable administrator-level access to a computer. Typically, a hacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to gain root access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that monitor traffic, keystrokes, etc. using a "backdoor" into the system.

Potentially Unwanted Programs (PUPs): PUPs are a type of software that are typically installed along with other software and can be difficult to remove. They may contain adware, spyware, or other malicious code, and can slow down the victim's system and compromise privacy.

Fileless Virus: A fileless virus is a type of malware that runs entirely in memory and does not create any permanent files on the victim's system. This makes it difficult to detect and remove, as traditional antivirus software typically looks for malware on disk.

Command and Control: Command and control (C2) refers to the infrastructure used by attackers to control and manage a network of infected systems, known as a botnet. The C2 server typically sends commands to the bots, which carry out the attacker's commands.

Bots: Bots are software programs that run autonomously and carry out tasks on behalf of their operators. In the context of cybersecurity, bots are often used by attackers to build and manage botnets, launch attacks, and automate other malicious activities.

Cryptomalware: Cryptomalware is a type of malware that encrypts the victim's files and demands a ransom payment in exchange for the decryption key. This type of malware typically uses cryptography to encrypt the files, making it difficult to recover the data without paying the ransom.

CertExams.com

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

Copyright © 2000 - 2023 CertExams.com Version 2.0

Logic Bombs: A logic bomb is a type of malware that is designed to trigger when a certain condition is met. For example, a logic bomb may be programmed to delete all of the victim's files after a certain date.

Spyware: Spyware is a type of malware that is designed to collect sensitive information from the victim's system, such as passwords, financial information, and browsing history. This information is then typically sent back to the attacker for use in further attacks or for financial gain.

Keyloggers: A keylogger is a type of malware that records all of the keystrokes on the victim's system, including passwords, credit card numbers, and other sensitive information.

Remote Access Trojan (RAT): A RAT is a type of Trojan that provides remote access to the victim's system, allowing the attacker to control the system and steal sensitive information.

Backdoor: Back doors allow unauthorized access to a remote system through an entrance in the system of which the user is typically not aware. It allows an attacker to bypass access controls and gain unauthorized access and possible even take remote control of a system. Once the back door is installed the attacker can steal or damage information or implement other tools for further escalation of the attack. A backdoor attack can be used to bypass the security of a network. A back door is a program that allows access to the system without usual security checks. These are caused primarily due to poor programming practices.

The following are known back door programs:

1. **Back Orifice**: A remote administration program used to remotely control a computer system.

2. **NetBus**: This is also a remote administration program that controls a victim computer system over the Internet. Uses client - server architecture. Server resides on the victim's computer and client resides on the hackers computer. The hacker controls the victim's computer by using the client.

3. **Sub7**: **Sub7**, or **SubSeven** or **Sub7Server**, is the name of a popular backdoor program. This is similar to Back Orifice, and NetBus. Used to take control of victim's computer over the Internet. Its name was derived by spelling NetBus backwards ("suBteN") and swapping "ten" with "seven".

Ransomware: Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising not always truthfully - to restore access

CertExams.com

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

Copyright © 2000 - 2023 CertExams.com Version 2.0

to the data upon payment.

Crpto-malware: Type of ransomware that encrypts user's files, and demands ransom. Sophisticated crypto-malware uses advanced encryption methods so files could not be decrypted without unique key.

Adware: Software that automatically displays or downloads advertisements when it is used.

Bots: A set of computers that has been infected by a control program called a bot that enables attackers to exploit the computers to mount attacks.

Zombies: Zombies are malware that puts a computer under the control of a hacker. Hackers use zombies to launch DoS or DDoS attacks. The hacker infects several other computers through the zombie computer. Then the hacker sends commands to the zombie, which in turn sends the commands to slave computers. The zombie, along with slave computers start pushing enormous amount of useless data to target computer, making it unable to serve it legitimate purpose. This type of attack is known as DDoS attack.

Computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified botnets - not spam, viruses, or worms - as the biggest threat to Internet security.

Keylogger: A hardware device or software application that recognizes and records every keystroke made by a user

Logicbomb: A piece of code that sits dormant on a target computer until it is triggered by the occurrence of specific conditions, such as a specific date and time

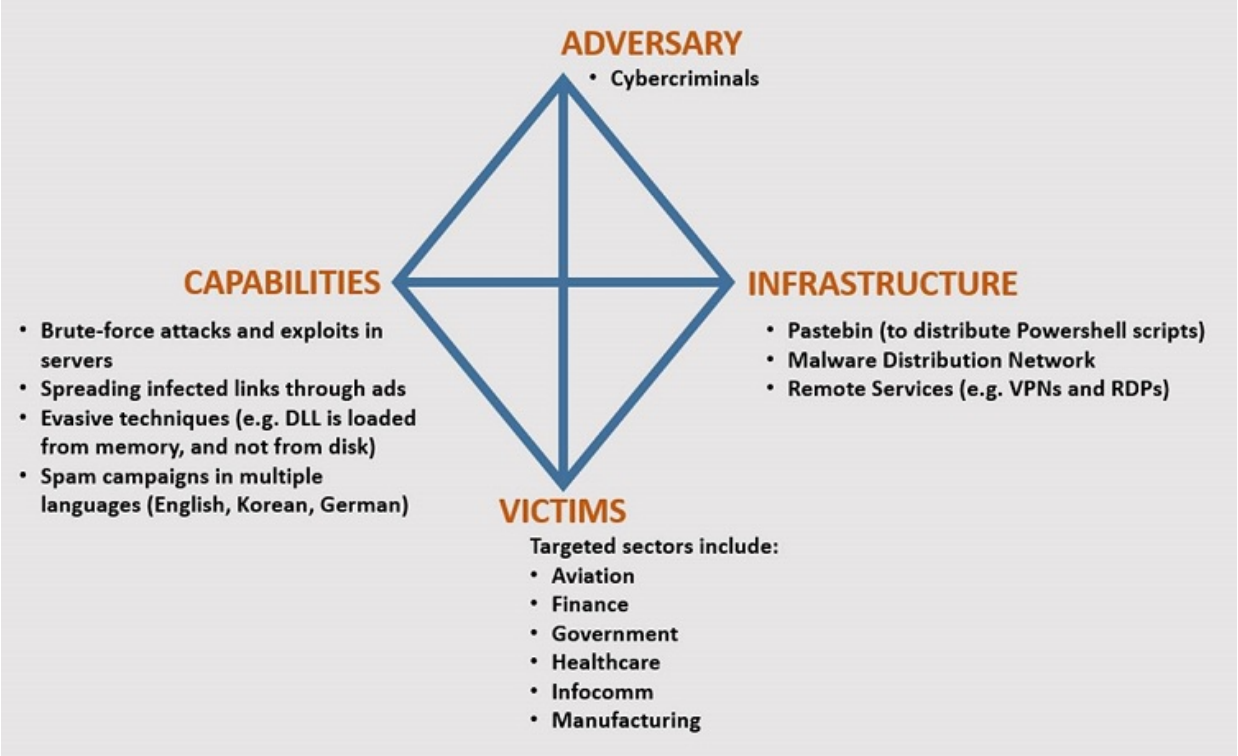
The Diamond Model of Intrusion Analysis is a cognitive model used by the threat intelligence community to describe a specific event. As an example, a completed diamond could take the following form:

CertExams.com

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

Copyright © 2000 - 2023 CertExams.com Version 2.0



Vulnerability is not a formal node of the Diamond Model for Intrusion Analysis.

CertExams.com

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

Copyright © 2000 - 2023 CertExams.com Version 2.0