27/10/2020

CS mid sem

18124011600I
Vishwas Achary

Q.1) (d) None of the above

Q.2) (c) Measure

Q.3) (c) ARP method

Q.4) (b) Routes or Gateway

Q.5) (c) Hacking

Q.6) (c) key stroke logging

Q.7) (c) HTTP Flood

Q.8) (c) Cyber Terrorism

Q.9) (b) phishing

Q.10) (b) A & B

Q. 11) Network Sniffer

→ The procedure of catching, decoding and analyzing network movement is called network sniffing.
→ It is a technique of observing each packet that crosses the network.
→ It is a tool that can enable you to find network issues by enabling you to catch and view packet level data on your network it likewise screens or sniffs out the data flowing over computer network links in real time.
→ A few sniffers work with TCP/IP packets yet more sophisticated tool can work with numerous other network protocols and at lower levels including Ethernet frames.

- Advantages:

→ It decrypts packets and makes it in plain text or readable format.
→ It captures packets and analyses packets and furthermore analyses the traffic of a network and makes a record.

- Disadvantages:

→ Intruding on the security of a network or to gain higher level authority.
→ A few sniffers can even change the targeted computer's data and harm the system.

- Tools of network sniffing :

1. Wireshark
2. Hping
3. kismet
4. Tcpdump
5. Windump

=> Let's explain wireshark in detail.

- It is a GUI based option to tcpdump it otherwise called Network/Packet protocol analyzer tool, it will attempt to catch network packets and tries to display that packet data as detailed as possible.
- It is one of the best open source packet analyzer tool available today for UNIX and Windows.

- Features:

- Opensource software which is available for Unix and Windows
- Import and export files of any other capture program
- Colorize packet display based on filters

- Some Intended Purpose:

- Network administrators use it to troubleshoot network problems.
- Network security engineer uses it to examine network problem

Q.12) Attack Vectors

→ An attack vector is a method or pathway used by a hacker to access or penetrate the target system.
→ Hackers steal information, data and money from people and organizations by investigating known attack vectors and attempting to exploit vulnerabilities to gain access to the desired system.
→ Once a hacker gains access to an organization's IT infrastructure, they can install a malicious code that allows them to remotely control IT infrastuse, spy on the organization or steal data or other resources.

∴ How do Hackers exploit Attack vectors?

→ There are many different types of attackers who commit cyber attacks
→ A disgruntled former employee may be aware of vulnerable attack vectors due to their role in the company.
→ An individual hacker may be trying to steal personalized information
→ A hacktivist might initate cyber attack again your organization to make a political statement
→ Buisness competitors may try to attack your IT infrastructure to gain a competitive edge.

* In all of these cases, the general methodology of exploiting attack vectors is the same:

1. Hackers identify a targeted system that they wish to penetrate or exploit
2. Hackers use data collection & observation tools such as sniffing, emails, malware or social engineering
3. Hackers use the information to identify the best attack vectors, then create tools to exploit it.
4. Hackers break the security system using the tools they created, then install malicious software applications
5. Hackers begin to monitor the network, stealing your personal and financial data or infecting your computers and other endpoint devices with malware bots.

Q.13) Cybes Crime

→ It is defined as a crime where a computes is the object of the crime or is used as a tool to commit an offense.

→ A cybescriminal may use a device to access a user's pessonal information, confidentional buisness information, government information, or disable a device.

→ It is also a cyber crime to sell or elicit the above information online.

• Categories of cybes crime

→ There are three major categories that cybescrime falls into:

- Individual
- property
- Covernment

→ The type of methods used and difficulty levels vary depending on the category.

∴ Individual

- This category of cybescrime involves one individual distributing malicious or illegal information online.
- This can include cyberstalking, distributing pornography and staffacking.

Property

- It is similar to real-life instance of a criminal illegaly possessing an individual's bank or credit card details.
- The hackers steal a person's bank detail to gain acces to funds, make purchase online or run phishing scams to get people to give away their information

Government

- This is the least common cybercrime, but is the most serious offense.
- A crime against the government is also known as cyber terrorism
- Government cybercrime includes hacking government websites, military websites or distributing propaganda
- These criminals are usualy terrorists or enemy government of other nations.

Q.14 Spyware

→ Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.

→ It is classified as a type of malware - malicious software designed to gain access to or damage your computer, often without your knowledge.

→ It gathers your personal information and relays it to advertisers, data firms, or external users

=> There are four main types of spyware.

- Adware : This type of spyware tracks your browser history and downloads, with the intent of predicting what products or services you're interested in.

- Trojan : This kind of malicious software disguises itself as legitimate software. For example :- Trojans may appear to be a Java or Flash player update upon download.

- Tracking cookies : These track the user's web activities, such as searches, history and downloads, for marketing purposes

- System monitors: This type of spyware can capture just about everything you do on your computer.
- System monitors can record all keystrokes, emails, chat-room dialogs, websites visited, and programs run.

Q.15) - Backdoor

→ It is a type of malware that is used to get unauthorized access to website by the cyber criminals.

→ The cybercriminal spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields.

- The malware is entered in the system through the backdoor and it makes its ways to the company's sensitive data including customers personally identifiable information

• How to prevent Backdoors

→ Business owners can use website scanners to defend themselves against backdoor attacks.

→ The website scanners mitigate malware, patch vulnerabilities and alert the admin against threats

• What to do if you suspect a backdoor attack

- Make sure the cybersecurity team reviews the site access logs for everything out of ordinary.

- Keep the plug-ins and themes on the websites updated and reinstall the core files to your CMS

- Audit your CMS and uninstall all the plug-ins from the file manager.