CYBER SECURITY
ASSIGNMENT - 1

Vishwas Acharya
18124011600I

IANT

Q.1) What is vulnerability scanning and types of vulnerability scanning?

Ans A vulnerability scanner is an application that identifies and creates an inventory of all the systems connected to a network.

- It is an inspection of the potential points of exploit on a computer or network to identify security holes.
- There are two types of vulnerability scanning on the basis of authenticity; Unauthenticated and authenticated scans.

• Authenticated scans :

- This scans allows for the scanners to directly access network based assets using remote administrative protocols such as secure shell (SSH) or remote desktop protocol (RDP) and authenticate using provided system credentials.

• Unauthenticated scans :

- This is a method that can result in a high number of false positives and is unable to provide detailed information about the assets operating system and installed software. This method is typically

used by threat actors & security analyst trying determine the security posture of externally accessible assets.

:- Types of vulnerability Scanner.

1) Network based scanners
↳ Port Scanners
↳ Network vulnerability scanners
↳ Web servers scanners.
↳ Web application vulnerability scanners.

2) Host-based Scanners
↳ It looks for system-level vulnerabilities such as insecure file permissions, application level bugs, backdoor and Trojan horse installation

3) Database Scanners
↳ This are a specialized tool used specifically to identify vulnerabilities in database pplications.

Q. 2) Discuss about the traffic probe in detail

Ans Probe is the ultimate network monitor

and protocol analyzer to monitor network traffic in real-time, and will help you find the sources of any network slow-downs in a matter of seconds.

1) High-Speed Traffic Processing
- LAN and MAN have evolved over a considerable time span (the last 30 years) and encompass wired and wireless physical links and speeds from 1Mb/s to 100Gb/s

2) Network Traffic Measurement
- Network traffic reports provide valuable insights into preventing such attacks. Traffic volume is a measure of the total work done by a resource or facility, normally over 24 hours, and is measured in units of erlang-hours. It is defined as the product of the average traffic intensity and the time period of the study.

3) Network Intrusion Detection
- A network-based intrusion detection system (NIDS) detects malicious traffic on a

network. NIDS usually require promiscuous network access in order to analyze all traffic, including all unicast traffic... The difference between a NIDS and a NIPS is that the NIPS alters the flow of network traffic.

Q.3] Write a short note on

(A) Metaspolite

- It is a framework and is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating system.

(B) Openvas.

- OpenVAS (Open Vulnerability Assessment System, originally known as GNessUs) is a software framework of several services and tools offering vulnerability scanning and vulnerability management

IANT
Date
Page

(c) SOCAT

- It is a command line based utility that establishes two bidirectional byte streams and transfers data between them.

(d) Datapipe

- Datapipe established partnerships with technology companies. It provides application management, hosting, professional services and security services for mid-to large-sized organization.
- It is the managed hosting & cloud services provides with the most complete set of services, global locations, and industry leading partners

(E) Fpipe.

- Fpipe by Foundstone, implements port redirection techniques natively in Windows. It also adds Uses Datagram Protocal (UDP) support, which datapipe lacks.
- Fpipe also adds more capability than datapipe in its ability to use a source port and bind to a specific interface

(F) Winselay

- It is a virus detection that infects other files in order to spread. Viruses are programs that copy themselves to spread from one system to another through Internet, Email, or carried in a removable medias such as a floppy disk, CD, DVD, or USB drive.

Q.4] What is network reconnaissance? and Discuss about Nmap?

Ans It is a term for testing potential vulnerabilites in a computer network. This may be a legitimate activity by the network owner/operator, seeking to protect it or to enforce its acceptable use policy.

- It also may be a precursor to external attacks on the network.

- Nmap is a short for Network Mapper, open-source tool for vulnerability scanning and network discovery.
- Network admin use Nmap to identify

what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

Q.5] What is network vulnerability scanning and discuss about service tools? (Datapipe, Fpipe and Winsebay)

Ans Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes.

- A vulnerability can detects and classifies system weakness in computers, network and communications equipment and predicts the effectiveness of countermeasures.

- **Datapipe** managed cloud, the company offers managed services for Amazon web services including Elastic compute cloud (EC2), CloudFront, S3, and Relational Database service (RDS).
- Datapipe provides application management, hosting, professional services and security services for mid- to large-sized organizations

- This services include monitoring, diagnostics, and problem resolution; enabling of software as a service to independent software vendors; custom application management, and remote infrastructure management.

- Fpipe provides following advantages to the service providers:
  - Future equipment availability.
  - Increasing bandwidth requirements.
  - OPEX costs
  - Additional Revenue Possibilities

- Winrelay provides following services:
  - It can be used as interchangeably with Fpipe on any windows platform.
  - Unexpected connection to the unsafe domains frequently.
  - virus removal tool.

Q6) Discuss about Netcat and Socat?

Ans - Netcat is also known as nc.
- It is a computer networking utility for reading from and writing to

network connections using TCP or UDP.
- It is quite simple to build a very basic client/server model using nc.
- On one console, start nc listening on a specific port for a connection.

- Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them.
- It is a network swiss army knife utility and it is very similar to Netcat.
- However, socat has many additional features that makes it a better alternative to Netcat.

Q.7] What is network sniffing what is it used for?. Advantage and disadvantages of network sniffing?

Ans 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.
- Network sniffing 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 tools can work with numerous other network protocols and at lower levels including ethernet frames.
- It is used for a network sniffer to analyze network traffic and bandwidth utilization so that underlying trouble in the network can be identified.
- It analyses network issue and identifies network abuse by inward and outside clients additionaly used to gain information for affecting network intrusion.

- Advantages

- It captures packets and analyses packets and furthermore analyses the traffic of a network and makes a record.
- It decrypts packets and makes it in

plain text or readable format
- It gathers relevant data like IP address, which protocol is used, hostname or servername and other sensitive data

- Disadvantages

- Getting special and private data of exchange, like username, passwords, account which is the main reason behind most unlawful uses of sniffing tools.
- A few sniffers can even change the targeted computer's data and harm the system. Recording email or text and resuming its content.
- Intruding on the security of a network or to gain higher level authority.

Q.8] What is packet sniffing?

Ans Packet sniffing is a method of checking each packet that crosses the network.
- A network sniffer is also called as a packet sniffer.

- It is a software application that uses a network connector card in promiscuous mode to catch all network packets.

Q.9] How does sniffer works?

Ans Sniffers also work differently depending on the type of network they are in.

- Shared ~~Network~~ Ethernet: In this environment all hosts are associated with a similar transport and compete with each other for bandwidth.

- Switch Ethernet: An Ethernet environment in which the host are connected to the switch rather than hub is called a switched Ethernet.

Q.10] How can we detect the sniffers?

Ans These are three methods to detect sniffers:

- Ping method: Most "packet sniffers" keep running on normal machines with a

normal TCP/IP stack. This implies that if you send a request to these machines, they will react. The trick is to send a request to IP address of the machine, however not to its Ethernet adapter.

- ARP method: In this technique, an attacker sends a fake ARP message to the local LAN. The objective of ARP spoofing is to hijack a system and an attacker wants to join his MAC address with the IP address of another host. The outcome is that any traffic implied for that IP address will be sent to the attacker.

- DNS method: Many sniffing programs do automatic reverse-DNS look ups on the IP addresses they see. Thusly, a promiscuous mode can be identified by looking for the DNS traffic that it produces. This method can distinguish double homed machines and can work remotely.

Q.11] Discuss packet sniffing mitigation?

Ans The following techniques and tools can be used to reduce severity against the sniffers:

- Authentication: Using strong authentication, such as one-time passwords or two-way authentication, is the first option for defense against packet sniffers.
- Anti-sniffer tools: Use these tools to employ software and hardware designed to detect the use of sniffers on a network.
- Switched infrastructure: Deploy a switched infrastructure to counter the use of packet sniffers in your environment.
- Cryptography: The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but renders them irrelevant.

Q.12] Write a short note on.

(A) Wireshark

=> 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.

(B) hping

=> It is a free packet generator and analyzer for the TCP/IP protocol distributed by Salvatore sanfilippo

- It is one type of tester for network security.

(C) KISMET

- It is open source software or free software which is mainly used for wireless LANs.
- It is a network identifier, packet sniffer and intrusion identification framework for 802.11 wireless LANs.
- It recognizes network by passively gathering packets and distinguishing

networks, which enables it to identify hidden networks and the presence of non-beaconing networks by means of data traffic.

(d) Tcpdump & windump

- Tcpdump : is free and open source software and it is under the BSD license. It is a common packet analyzer that keeps running under command line.
  - It enables the user to show TCP/IP and different packets being transmitted or received over a network to which the computer is attached.

- Windump: is free and it is released under a BSD-style license. It is used as a port of tcpdump for windows.
  - It can run under Windows 95, 98, ME, NT, 2000, XP, 2003 and Vista.
  - WinDump captures using the Winpcap library and drivers, which are freely downloadable from the WinPcap website.

Q.13] Discuss sql injection in detail.

Ans A sql injection tool is a tool that is used to execute SQL injection attacks.

- SQL injection is the attempt to issue SQL commands to a database via a website interface.
- SQL injection tools triggers attacks to exploit the security vulnerability available in an application's database layer.

• Injection Tools are:

- Havij SQL Injection
- Pangolin
- The Mole
- SQL Ninja

Q.14] Describe open port/service identification in detail?

Ans In security parlance, the term open port is used to mean a TCP and UDP port number that is configured to accept packets.

- Port are an integral part of the Internet's communication model. they are the channel through which applications on the client computer can reach the software on the server services, such as web pages or FTP, require their respective ports to be "open" on the server in order to be publicly reachable.
- Technically, a given port "open" is not enough for a communication channel to be established.
- There needs to be an application listening ~~to~~ on that port, accepting the incoming packets and processing them.

Q.15] Describe banner/version check in detail?

Ans Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.
- Administrators can use this to take inventory of the systems and services on their network. ~~However~~,

- However, an intruder can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.
- Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP) File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).