NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment Solution- Week 9

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Why do packet sniffers require the network interface card (NIC) to be put in promiscuous mode?

a. So that broadcast packets can be sent to the victim machine.
b. So that all packets crossing the NIC can be read.
c. So that headers of encrypted packets can be deciphered.
d. None of these.

Correct Answer: b

Detail Solution: In the promiscuous mode, a packet sniffer can read all traffic on the network segment to which the NIC is connected (irrespective of sender and receiver). The correct option is (b).

QUESTION 2:

Which of the following measures can prevent packet sniffing on a network segment?

a. Restrict physical access to the network by unauthorized persons.
b. Install the latest version of TCP protocol that does not contain vulnerabilities.
c. Use encryption to protect confidential information.
d. All of these.

Correct Answer: a, c

Detail Solution: To run the packet sniffer, the adversary has to first gain physical access to one of the machines in the network; restricting physical access can prevent this. Also, if the packet payload is encrypted, even after sniffing the contents cannot be decoded. Packet sniffing does not depend on the version of the TCP protocol that is being used. The correct options are (a) and (c).

QUESTION 3:

How can NMAP detect whether network sniffing is probably going on in a network?

a. By sending a NMAP ping request to all the machines on the network.
b. By conducting TCP stealth scan on all the machines in the network.
c. By using a script that checks whether any of the machines has the network card configured in the promiscuous mode.
d. None of these.

Correct Answer: c

Detail Solution: Using the following NMAP command, we can find out whether any of the network cards on the network is configured in the promiscuous mode. (It is done by broadcasting fake ARP packets)

```
      nmap –script=sniffer-detect <IP addresses to check>
```

The correct option is (c).

QUESTION 4:

Which of the following features are present in Ettercap?

a. IP-based and MAC-based filtering.
b. Character injection.
c. Packet filtering and dropping.
d. SQL injection.
e. All of these.

Correct Answer: a, b, c

Detail Solution: The Ettercap tool can carry out IP-based filtering, MAC-based filtering, character injection in a packet, packet filtering & dropping. However, it cannot be used to mount SQL injection attacks. The correct options are (a), (b) and (c).

QUESTION 5:

Which of the following can be used for computer-based social engineering attack?

a. Tailgating.
b. Sending out chain letter emails.
c. An illegitimate email falsely claiming to be from a legitimate site.
d. Reverse social engineering.

Correct Answer: b, c

Detail Solution: Tailgating and reverse social engineering are used for human-based social engineering attacks. Chain letter and phishing, as mentioned in (b) and (c), are example of computer-based social engineering attacks. The correct options are (b) and (c).

____

QUESTION 6:

Which of the following tools can be used to put the NIC in promiscuous mode?

a. macchanger
b. dnsenum
c. slowloris
d. arpspoof

Correct Answer: d

Detail Solution: macchanger tool is used for assigning random mac address, dnsenum is used for enumerating dns server, and Slowloris is used for mounting DoS attack. Using arpspoof we can poison the arp tables and it is used to put the NIC of the system in promiscuous mode.

The correct options is (d).

____

QUESTION 7:

Which of the following protocols are vulnerable to sniffing attack?

a. HTTP
b. FTP
c. HTTPS
d. SSL

Correct Answer: a, b

Detail Solution: HTTPS and SSL exchange data in secure channel, HTTP and FTP protocol exchanges data in plain text (unsecured form), thus it is vulnerable to sniffing attack.

The correct options are (a) and (b).

____

QUESTION 8:

How does Slowloris work?

a. It sends a single large packet to victim system.

b. It sends multiple HTTP requests to the victim system but never completes the request.
c. It mounts MAC attack on target system.
d. It turns on NIC of the system in promiscuous mode.

Correct Answer: b

Detail Solution: It sends multiple HTTP packets to connect with the victim system, but never completes resulting DoS for legitimate users.

The correct option is (b).

____

QUESTION 9:

Which of the following is/are example(s) of bandwidth flood?

a. ICMP flood
b. SYN flood
c. MAC Flood

Correct Answer: a, b, c

Detail Solution: In ICMP/MAC flood attack large number of ICMP/ARP packets are sent to victim. And once the ICMP/ARP tables are filled the system either act as unexpected nature (i.e. switch will start working as hub) or stops responding to legitimate user.

Similarly limited numbers of SYN requests can be handled by any system, and each SYN request must be open for 75 second so if an attacker tries sending large number of SYN packets then it causes DoS.

The correct options are (a), (b) and (c).

____

QUESTION 10:

For mounting DoS attack using hping3 tool what option can be used as an alternative of –i u10000?

a. --count
b. --fast
c. --faster
d. --flood

Correct Answer: b

Detail Solution: We use hping tool –I u10000 alias for sending 10 packets for a second, which is the same as using option –fast.

The correct option is (b).

____

**************END*******