EH ASSIGNMENT 5

Q.1 Explain MAC spoofing and Email spoofing

ANS. MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed.

Email spoofing is a threat that involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email.

Q.2 Perform practical of MITM tool and social engineering Tool.

ANS. Practical of MITM

Step 1: open terminal and type: macchanger

It is used to change the MAC address of our device

If your command is not running then you can find commands of

macchanger by typing: --help

Step 2: ifconfig eth0 down

It is used to bring down the network interface named "eth0". This

command disables the Ethernet interface, preventing it from sending or

receiving any network traffic.

Step3: macchanger –m (MAC address) eth0

It is used to change MAC address whatever you want by typing it after

“-m”

Step4: ifconfig eth0 up

After changing the MAC address, turn eth0 to up so then our device can

gain access to the network and then we can use our device to gain

access to other devices

Social Engineering Tool

We’re going to perform DNS spoofing, it’s one of the tools for social

engineering

Step 1: Host a Phishing page using se-toolkit: Website Attack Vectors ->

Credentials Harvestor -> Clone website/Use Web Template

Step 2: Now will use facebook’s template and SET hosted this on my IP:

192.168.29.169 at port 80

Step 3: Change the contents of the file etter.dns so the facebook.com

points to your own IP.

Step 4: Th load up “ettercap -g” and go to Plugins -> Manage the

Plugins -> double click DNS Spoof plugin. Make sure you see “*” next to

it

Step 5: Now ARP poison all the hosts in the network so that all the

traffic passes through your machine. Start sniffing

At the same time in SET windows, you’ll see “we got a hit” along with

some other info.

If the victims enter his/her credentials on your phishing page, you’ll see

details in the SET windows

Q.3 Explain Kali Linux tool SYN Flooding Attack using Metasploit

ANS. The SYN Flooding Attack is a type of Denial of Service (DoS) attack that exploits the way TCP connections are established between two devices. In a normal TCP handshake, the client sends a SYN packet to the server, the server responds with a SYN-ACK packet, and the client sends an ACK packet to complete the connection. However, in a SYN flooding attack, the attacker sends a large number of SYN packets to the target server without ever completing the handshake process. This causes the target server to allocate resources for each connection attempt, which eventually exhausts the server's resources, leading to denial of service for legitimate users.

Metasploit is a powerful tool that can be used to perform a SYN flooding attack on a target system. Here are the steps to perform a SYN flooding attack using Metasploit:

1.Open the Kali Linux terminal and start the Metasploit framework by typing "msfconsole" and hitting enter.

2.Once Metasploit is running, search for the "synflood" module by typing "search synflood" and hitting enter.

3.Load the "synflood" module by typing "use auxiliary/dos/tcp/synflood" and hitting enter.

4.Set the target IP address by typing "set RHOST <target_ip>" and hitting enter.

5.Set the target port number by typing "set RPORT <target_port>" and hitting enter.

6.Set the number of SYN packets to be sent per second by typing "set DELAY <packet_rate>" and hitting enter.

7.Type "exploit" and hit enter to start the SYN flooding attack.

This will start flooding the target system with SYN packets, eventually leading to a denial of service for legitimate users. It's important to note that performing a SYN flooding attack without the target's permission is illegal and can result in severe legal consequences.

Q.4Find online email encryption service

ANS. There are many online email encryption services available, here are a few options:

1.ProtonMail: This is a popular email encryption service that offers end-to-end encryption for all messages. It also has features like self-destructing messages, two-factor authentication, and more.

2.Tutanota: Tutanota is another secure email service that offers end-to-end encryption for all messages. It also has features like encrypted contacts and calendar, and the ability to send encrypted emails to non-Tutanota users.

3.Hushmail: Hushmail is a secure email service that offers end-to-end encryption, and also has features like two-factor authentication and the ability to send encrypted messages to non-Hushmail users.

4.Mailfence: Mailfence is an email service that offers end-to-end encryption for all messages, and also has features like digital signatures and two-factor authentication.

5.Virtru: Virtru is an email encryption service that can be used with popular email services like Gmail, Outlook, and Yahoo. It offers end-to-end encryption and also has features like revocation of sent messages and the ability to set expiration dates for messages.

Q.5 Types of Firewalls

ANS.

1. Packet Filtering Firewall
2. Stateful Inspection Firewall
3. Application Firewall
4. Proxy Firewall
5. Next-Generation Firewall (NGFW)
6. Cloud Firewall

Q.6 Explain Evading Firewalls.

ANS. Firewalls are security measures used to protect networks by controlling and filtering incoming and outgoing network traffic. They operate by monitoring network traffic and blocking any traffic that does not meet certain criteria, such as a particular port, protocol, or IP address.

Evading firewalls refers to the process of circumventing or bypassing these security measures in order to gain unauthorized access to a network or to carry out other malicious activities. This can be achieved through various methods, including:

1.Port Scanning: This involves scanning a target network for open ports and services that are not being monitored by the firewall. Once these ports and services are identified, attackers can use them to gain access to the network.

2.IP Spoofing: This is a technique that involves forging the source IP address of network packets in order to bypass firewall rules that are based on the source IP address. This can allow attackers to send malicious traffic to a target network without being detected.

3.Tunneling: This involves encapsulating one network protocol inside another, in order to bypass firewall filters that are designed to block specific protocols. For example, attackers can use HTTP tunneling to bypass firewalls that block outgoing connections to specific ports or protocols.

4.Application Layer Attacks: These attacks exploit vulnerabilities in application-layer protocols, such as HTTP, SMTP, and FTP, to bypass firewall filters and gain unauthorized access to a network.

To protect against evading firewalls, organizations can implement a range of security measures, including regularly updating firewall rules, using intrusion detection and prevention systems, and implementing multi-factor authentication for network access.