Module 5

Q.1 Explain MAC spoofing and Email spoofing.

Ans: MAC spoofing is technique used to change the Media Access Control address of a network device, such as a computer or smartphone, to impersonate another device on the same network.

The MAC address is a unique identifier assigned to every network interface, and MAC spoofing can be used to bypass network access controls or to launch man-in-the-middle attacks.

Email spoofing is a technique used to forge the sender's email address in an email message to make it appear as if it ws sent from a different source.

Email spoofing is often used in phishing attacks, where the attacker sends an email that appears to be from a trusted source, such as bank or a government agency, to trick the recipient into revealing information or downloading malware.

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: SYN Flooding is a type of DoS attack that exploits a vulnerability in the TCP/IP protocol stack.

The attack involves sending a large number of SYN packets to a victim’s server with spoofed source addresses that make it impossible for the server to complete TCP handshake process and establish a connection.

This results in resources exhaustion attack, where the server becomes overwhelmed and unable to respond to legitimate requests.

To launch a SYN flooding attack usin Metasploit, follow these steps:

1. Launch Terminal in Kali linux
2. Type “msfconsole” to start Metasploit Framework.
3. Type “use auxiliary/dos/tcp/synflood” to select the SYN flooding module.
4. Type “show options” to display the available options for the module.

5. Type “set RHOSTS <ip address of the target>” to specify the IP address of the victim server
6. Type “set THREADS <number of threads>” to specify the number of threads to use for the attack.
7. Type “exploit” to launch the attack.

Once the attack is launched, the victim server will be flooded with a larger number of SYN packets, causing it to become unresponsive and potentially crash.

Q.4 Find online email encryption service

Ans: There are several online email encryption services available that can help the privacy and security of your email communications.

The online email encryption services are:

1. ProtonMail
2. Tuanota
3. Mailfence
4. Virtru
5. StartMail

Q.5 Types of Firewalls.

Ans:

1. Packet filtering firewalls: They examine each packet of data that passes through the network and compare it against a set of predefined rules to determine whether to allow or block it.

2. Stateful inspection firewalls: It keeps track of the state of network connections and uses this information to make more intelligent decisions about which packets to allow or block.

3. Application-level gateways: They act as an intermediary between the client and the server, inspecting and filtering application specific traffic to ensure that only legitimate traffic is allowed through.

4. Next-generation firewalls: These firewalls combine the features of packet filtering, stateful inspection, and application-level gateways with additional security features like intrusion prevention and deep packet inspection.

5. Virtual private network firewall: These firewalls provide secure remote access to a private network by encrypting traffic between the client and the network.

Q.6 Explain Evading Firewalls

Ans: Evading firewalls refers to techniques used to bypass or circumvent network firewalls which are designed to monitor and control network traffic to prevent unauthorized access and protect against malicious attacks.

Attackers can use various methods to evade detection and bypass firewall rules, such as:

1. Encryption
2. Protocol tunneling
3. IP spoofing
4. Fragmentation
5. Evasion tools