MODULE - 3
Scanning and Enumeration

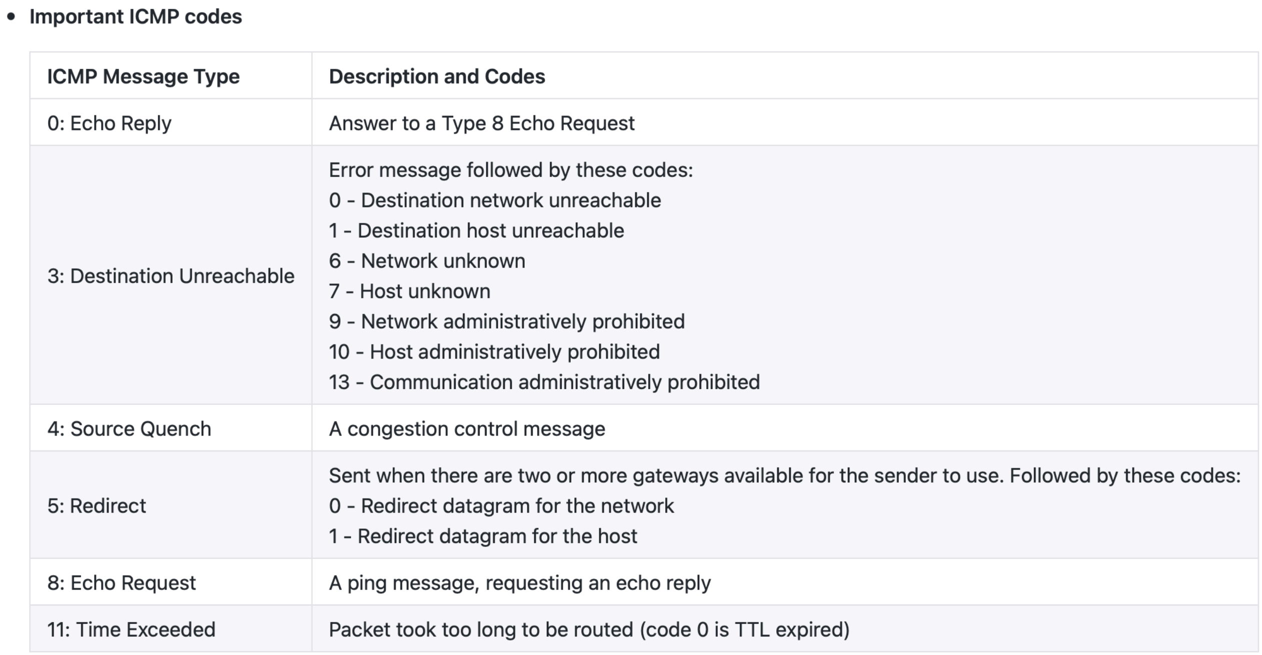
1. Connectionless Communication : UDP packets are sent without creating a connection. Examples are TFTP, DNS (lookups only) and DHCP .

2. Connection-oriented communication : TCP packets require a connection due to the size of the data being transmitted and to ensure deliverability.

3. Ping Scanning Tools :
    1. **Nmap** :
    2. **Hping3** :

```
hping -1 <ipaddress> —rand-dest -I eth0
```

    3. **Angry IP scanner**
    4. Solar-Winds Engineer toolkit
    5. Advanced IP scanner
    6. Pinkie
    7. Colasoft Ping , Visual Ping Tester, Ping Scanner Pro , **Nessus**



- **Important ICMP codes**

ICMP Message Type	Description and Codes
0: Echo Reply	Answer to a Type 8 Echo Request
3: Destination Unreachable	Error message followed by these codes: 0 - Destination network unreachable 1 - Destination host unreachable 6 - Network unknown 7 - Host unknown 9 - Network administratively prohibited 10 - Host administratively prohibited 13 - Communication administratively prohibited
4: Source Quench	A congestion control message
5: Redirect	Sent when there are two or more gateways available for the sender to use. Followed by these codes: 0 - Redirect datagram for the network 1 - Redirect datagram for the host
8: Echo Request	A ping message, requesting an echo reply
11: Time Exceeded	Packet took too long to be routed (code 0 is TTL expired)

4. **Nmap Scan Types** :
    1. Stealth Scan (-sS)
        - SYN , SYN/ACK , RST
        - Half-open scan or SYN scan - only SYN packets sent. Responses same as full.
        - Nmap -sS <target ip>
    2. Full Scan (-sT)
        - SYN, SYN/ACK, ACK, RST
        - Full connection and then tears down with RST
        - nmap -sT <target ip>
    3. TCP ACK scan / flag probe
        - TTL version - if TTL of RST packet < 64, port is open
        - Window version - if the Window on the RST packet is anything other than 0, port open
        - Can be used to check filtering. If ACK is sent and no response, stateful firewall present.
    4. NULL, FIN, XMAS Scan :
        : -sN : NULL scan
            Works only in Linux / Unix Systems,,,,, Not Applicable for Windows !!!!!
            1. No Flag, No Response : Open Port
            2. No Flag / RST/ACK : Closed Port.

: -sF : FIN scan

Works only in Linux / Unix Systems,,,,, Not Applicable for Windows !!!!!

: FIN / RST / ACK : Closed Port

: -sX : Xmas Scan (FIN,PSH,URG)

# **IDS Evasion Methods :**

5. IDLE Scan

: Uses TCP port scanning method BUT we spoof the "Source Address"

: Advantages :

Blame Someone Else

: Disadvantages :

Require a Zoombie

: Looks at the IPID to see if there is a response

: IPID increase of 1 indicates port closed

: IPID increase of 0 indicates port open

: IPID increase of anything greater indicates the third party was not idle

: nmap -sI <zombie host> <target ip>

# **SSDP Scan** :

Simple Service Discovery Protocol :

It basically a network protocol generally communicates with other machines

Closed Port : SYN , RST

UDP Scans :

1. Is port 31 is Open / No response : This means that the port is open
2. Is port 31 is Open / ICMP port Unreachable : This means that port is closed

6. Spoofing :

1. Decoy :

   nmap -Pn -D <spoofed IP> <tareget>
2. Source Address Spoofing :

   nmap -e <network Interface> -S <Source IP> <target>
3. MAC address Spoofing :

   nmap —spoof-mac <Mac|vendor> <target>

** Decoy will send Spoofed IP address along with your IP address

7. Firewall Evasion :

1. **Multiple Decoy IP addressess** : Nmap will send multiple packets with different Ip addresses, along with your attacker's IP address.
2. **IP fragmentation** :

   used to scan tiny fragment packets

   nmap -f <ip>
3. **Maximum transmission unit (MTU**) :

   nmap -mtu 8 <ip>

   8 Bytes

8. Time and Performance :

1. Paranoid (-T0)
2. Sneaky (-T1)
3. Polite (-T2)
4. Normal (-T3)
5. Aggresive (-T4)
6. Insane (-T5)

Some Important Switch :

1. -A : OS detection, Version Detection, Script scanning and traceroute
2. -T0 to -T2 : **Serial Scan**
3. -T3 to -T5 : **Parallel Scan**

9. Default Settings :

1. Nmap runs by default runs at level T3
2. Nmap runs by default TCP scans

5. **Service and Version Detection :**

1. -sV, —version-intensity (0 - 9), -sV —light-version (0) , -sV —version-all, -A

6. **OS Detection** :

-O , -O —Osscan-limit, -O —osscan-guess, -O —max-os-tries

7. **NSE Script :**

-sC == -script default = Default script
—script= [script Name]
—script-args = Nse script with arguments

8.**hping** :

9. **Evasion Concept** :

OS Fingerprinting :

1. Active : sending crafted packets to the targets
2. Passive : sniffing network traffic for things such as TTL windows, DF flags, ToS fields

# **Countermeasures** Part 1:

1. Misdirection / Fake Banner
2. IIS Lockdown : help lockdown a iis server especially in older environment
3. ServerMask : make the server look like it's something it is not like an older version of iis or apache
4. Turn off unused services
5. Change the ServerSignature (httpd.conf) file (mainly in linux)
6. Speaking of httpd.conf : mod headers

# **Countermeasures** Part 2 :

1. Firewalls configured to look for SYN scans
2. IDS should Detect Nmap/Snort
3. Open Only Required Port
4. Filter ICMP messages
5. Test Your Own Network
6. Keeps firewalls / IDS system updated / Patched

# **Vulnerability Scanner Tools** :

1. Nessus
2. MBSA (Microsoft Baseline Security Analyser)
3. Core Impact Pro
4. GFI Languard
5. Retina
6. Saint

# **Preparaing Proxies and Other Anonymizing Techniques** :

1. Placing the Blame on someone else
    1. What is Proxy ?
    2. Why use a Proxy ??
    3. How to use a Proxy ?
    4. HTTP Tunneling
    5. Anonymizers

1. **What is Proxy :**

    to hide their identities of their system behind the firewalls
    - Work on behalf of other systems
    - Filter Undesirable content
    - Anonymous ID on Website
    - NAT the IP address from the outside
    - Some Protection
    - Save Bandwidth : Caching of a Website !!

2. **Why to use a Proxy ?**

    - hide the attacker's IP address
    - Mask the actual source
    - Access internal Data

- Misdirection
- Help to create a proxy chains

3. **How to use a Proxy ?**

   There are several tools that can help you in proxying

   Proxy O'Plenty

   - Proxifier
   - SocksChain
   - Fiddler : HTTP debugging proxy server application
   - The Onion Routing (TOR)
   - Proxy Switcher
   - Proxy Workbench

4. **HTTP Tunneling** :

   Encapsulation of packets in HTTP and pass through the internet

   To detect this attack you have a only way to enumerate all the software and their uses

5. **Anonymizers :**

   This is the way of hiding ourselves (identity change)

   This helps in :

   1. Circumvent IDS & firewall rules
   2. Get to Restricted Content
   3. Protection from online attacks
   4. Privacy

Anonymous Tools :

1. **U-Surf** : Ultra Surf : Allows you to setup a proxy and route you through proxy to hide you identity
2. **G-Zapper** : this will stop the cookie so you can search anything without loggin in
3. **Mowser** : Portable Web Browser doesn't having any cookie
4. **WarpProxy** :
5. **Hide my IP**
6. **Hide you ass** : Similar to Hide my IP

# types of Scan :

1. Network Scan
2. Port Scan
3. Vulnerability Scan

TCP (20 Bytes)
UDP (8 Bytes)

# **Check for Live systems** :

1. **ICMP Sweep** :
2. **Port Scan**
3. **Firewalking** : **Firewalk** is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. **Firewalk** works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway.

Like Traceroute, but determines whether or not a particular packet can pass from the attacker's system to the target via a packet filtering device.

What is Firewalking ?

1. Define a Firewall's ACL (What's allowed)
2. It uses TTL
3. What happens to the packet
   1. Forwarded = Open
   2. Dropped = Closed
4. Traceroute
   1. traceroute <ipaddress>
   2. traceroute -p53 <ipaddress>

      Try Different Ports see if you can penertrate through it

Tool for Firewalking :

1. traceroute : Manual Way
2. Firewalk : Automatically changes port

command :

```
firewalk -s20-100 -i eth0 -n -pTCP [ Gateway_IP_adderss That is Blocking ] [ Destination_IP_Adderss ]
        -n for no DNS lookup
        -p : Protocol
```

# **More anti-virus evasion technique** :

1. Spoof you ip and sniff the response
2. Use a proxy or pwned machine
3. Fragmented IP Packets
   some IDS ignore small packets and they allow them to traverse through IDS
4. Source Routing : Technique use to specifiy the specific route that a packet should take through the network

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