***Attacks and Logs :-***

1. ***Nmap Scanning :***

Nmap Scanning is a method used by attackers to scan a network to discover different hosts, ports and services that is used by a computer network. Attackers use this to gather information about the network’s open ports, services, and operating system. This phase of reconnaissance is often a precursor, a standby step to a more targeted attack. Any network-connected device, like web servers are the common target for such Nmap scans. Nmap is a standard tool used in penetration testing and network security assessments.

Attackers generally follow the following steps: -

1. These commands have to be run on a terminal; hence a terminal is opened.
2. Attacker uses the Nmap tool, inputs commands like,

“ nmap -F [url of the website] ”.

1. Nmap runs the command and displays all the ports and servers present in the web server.

These operations are generally performed on a Linux-based operating system, because they support mainframe accessibility. Nmap scanning exploits the inherent nature of the network protocols.

To proceed with the Nmap Scanning, the attacker can use a series of commands to achieve said task. Some of those commands are mentioned below: -

1. nmap -F [url of the website]
2. nmap -F [IP\_address]
3. nmap -F [IP\_address.*0/24*]
4. nmap -F [IP\_address.*m-n*]
5. nmap -iL [address of the text file where the IP\_addresses are stored]
6. nmap --open [url of a website] >> [name of the text file]
7. nmap -p [name of the ports to be scanned] [url of the website]
8. nmap -p [name of the ports to be scanned] [url of the website] -v
9. nmap -p [name of the ports to be scanned] [IP\_address]
10. nmap -oN [name of the text file] -v -F [url of the website]

Although Nmap Scanning isn’t a specific attack and might not trigger suspicion right away, log entries help in a premonition of said attacks, since Nmap at least has to access the targeted web server which can provide us with various types of log entries:-

1. Firewall logs:

[timestamp] SRC= IP\_address DST=honeypot\_IP PROTO=TCP DPT=22 SYN

[timestamp] SRC= IP\_address DST=honeypot\_IP PROTO=TCP DPT=80 SYN

[timestamp] SRC= IP\_address DST=honeypot\_IP PROTO=UDP DPT=161

1. Web server access logs (for port 80/443 scans):

[timestamp] IP\_address - - "GET / HTTP/1.1" 400 "-" "Nmap..."

These log entries provide with details of when and by whom was the web server accessed by which port, etc. Some specific steps would be :-

* Look for a high frequency of connection attempts from a single IP address.
* Identify connection attempts to unusual ports.

To prevent such scanning attempts, certain tools can be used, namely:-

* Intrusion detection systems (IDS).
* SIEM systems.
* iptables, firewalls.
* Honeypots

***References:***

* <https://www.youtube.com/watch?v=7SPzUFKzTPs&list=PLgC1p8gIeVMtMyNPiGPtPwWe4fKJR-IbC&index=1>
* <https://nmap.org/>

1. ***Metasploit:***

Metasploit is a penetration testing framework that provides tools for developing and executing exploit code against a remote target machine. Attackers use it to exploit known vulnerabilities in the web services or applications. This tool is efficient nd commonly used to penetrate Web servers, application servers, operating systems, etc, to perform several web penetration attacks, which includes remote code execution, data breaches, and system compromise. Metasploit is widely used by corporate sector for penetration testing and red teaming exercises.

Attackers generally follow the following steps: -

1. Attacker performs reconnaissance (e.g., using Nmap) to identify vulnerabilities.
2. Attacker selects an appropriate Metasploit exploit module.
3. Attacker configures the exploit module with the web server’s IP address and port.
4. Attacker executes the exploit.
5. If successful, the attacker gains a shell or other form of access to the web server.

Like every other penetration attack, the evidence of the attack can be captured from various types of log entries: -

1. Web server access logs:

[timestamp] attacker\_IP - - "GET /vulnerable\_endpoint HTTP/1.1" 200 ...

1. System logs:

[timestamp] process\_name: suspicious\_process started by attacker\_IP

These log entries provide with details of the attack. Some specific indicators would be: -

* Look for unusual requests or commands in web server and application logs.
* Identify suspicious processes or network connections in system logs.
* Analyze firewall logs for unexpected traffic.
* Look for exploit-specific signatures in honeypot logs.

To prevent such exploits, certain security tools can be used, namely: -

1. IDS/IPS (Snort, Suricata)
2. SIEM systems
3. WAFs

Along with tools and logs to detect and counter such attacks, certain prevention methods should also be taken. Some of them are jotted down below: -

1. Keep software and systems updated
2. Implement strong access controls
3. Use an IDS/IPS
4. Honeypot deployment

***References:***

* <https://www.youtube.com/watch?v=PbxI5GQkqdA&t=163s>
* <https://www.youtube.com/watch?v=5m4KF9XbkzU>