CLINT AND SI THE HACKERS

Nmap

Nmap (Network Mapper) is a free and open-source tool used for network discovery and security auditing. It allows administrators to identify what devices are running on their networks, discover available hosts and services, and detect security vulnerabilities.

Common Commands

Basic Scan of a Single Host:

```
nmap <target_ip>
```

Scan a Range of IP Addresses:

```
nmap <starting_ip>-<ending_ip>
```

Aggressive Scan with OS and Service Detection:

```
nmap -A <target_ip>
```

Scan Specific Ports:

```
nmap -p 80,443 <target_ip>
```

Perform a Stealth SYN Scan:

```
nmap -sS <target_ip>
```

Hashcat

Hashcat is a powerful password recovery tool that uses GPU acceleration to crack hashed passwords. It's widely used for testing password strength and recovering lost passwords.

Common Commands

Basic Hash Cracking:

```
hashcat -m 0 -a 0 hash.txt wordlist.txt
```

Brute-Force Attack:

```
hashcat -m 1000 -a 3 hash.txt ?a?a?a?a
```

Hybrid Attack:

```
hashcat -m 0 -a 6 hash.txt wordlist.txt ?d?d
```

Using Rules for Mutation:

```
hashcat -m 0 -a 0 hash.txt wordlist.txt -r rules/best64.rule
```

Resuming a Session:

```
hashcat --session=mySession --restore
```

Wireshark

Wireshark is a widely-used network protocol analyser that lets you capture and interactively browse the traffic running on a computer network. It's essential for network troubleshooting, analysis, and protocol development.

Common Commands (using TShark for CLI)

List Available Network Interfaces:

```
tshark -D
```

Capture Packets on an Interface:

```
tshark -i eth0
```

Capture with a Filter:

```
tshark -i eth0 -f "tcp port 80"
```

Save Captured Packets to a File:

```
tshark -i eth0 -w capture.pcap
```

Read and Display from a Capture File:

```
tshark -r capture.pcap
```

Aircrack-ng

Aircrack-ng is a suite of tools designed for assessing Wi-Fi network security. It focuses on monitoring, attacking, testing, and cracking Wi-Fi networks.

Common Commands

Monitor Mode Activation:

```
airmon-ng start wlan0
```

Capture Packets:

```
airodump-ng wlan0mon
```

Capture Specific Access Point:

```
airodump-ng --bssid <AP_MAC> --channel <channel> --write capture wlan0mon
```

Deauthenticate a Client:

```
aireplay-ng --deauth 0 -a <AP_MAC> wlan0mon
```

Crack a Captured WPA Handshake:

```
aircrack-ng -w wordlist.txt -b <AP_MAC> capture.cap
```

Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. It includes tools like a proxy server, scanner, intruder, and repeater to find and exploit vulnerabilities.

Common Commands/Features

Start Burp Suite from Command Line:

```
java -jar burpsuite_community_v2023.10.jar
```

Configure Browser Proxy:

- Set your browser to use proxy 127.0.0.1:8080.
- Allows Burp Suite to intercept browser traffic.

Intercept and Modify HTTP Requests:

- Use the "Proxy" tab to intercept requests.
- Modify headers, parameters, or cookies before forwarding.

Use the Intruder Tool:

- Select a request and send it to "Intruder".
- Configure payload positions and types for automated testing.

Repeater for Manual Testing:

- Send requests to "Repeater" to manually modify and resend them.
- Useful for testing how different inputs affect the response.

NetExec

NetExec is a tool used to execute commands on remote systems over a network. It facilitates remote administration and automated task execution.

Common Commands

Execute a Command on a Remote Host:

```
netexec -H <host_ip> -C "<command>"
```

Execute Commands on Multiple Hosts:

```
netexec -H hosts.txt -C "<command>"
```

Run a Script Remotely:

```
netexec -H <host_ip> -S script.sh
```

Use Specific Credentials:

```
netexec -H <host_ip> -U <username> -P <password> -C "<command>"
```

Copy a File to a Remote Host:

```
netexec -H <host_ip> -U <username> -P <password> -F localfile remotepath
```