

# Tools

## Network and Traffic Analysis

Wireshark –

- Used when analyzing live or captured packets.
- Why? To see exactly what packets were sent or received, to detect anomalies, attacks, or misconfigurations.

Tool	Command / Filter	Flags / Syntax	What it does
Wireshark	wireshark	—	Launches Wireshark GUI
Wireshark	wireshark <file>.pcap	<file> capture file	Opens a capture file
Wireshark	ip.addr == <ip_address>	Display filter	Shows traffic to/from IP
Wireshark	tcp.port == <port>	Display filter	Shows traffic on TCP port
Wireshark	http	Display filter	Shows HTTP traffic
Wireshark	dns	Display filter	Shows DNS traffic

Netcat/Ncat –

- Network debugging or exploitation.
- Creates listeners, transfers files, or test connectivity.

Tool	Command	Flags / Syntax	What it does
Netcat	nc -lvpn <port>	-l listen, -v verbose, -n no DNS, -p port	Opens a listener
Netcat	nc <ip_address> <port>	<ip_address> <port>	Connects to a host
Netcat	nc -lvpn <port> > <file>	> redirect output	Receives a file
Netcat	nc <ip_address> <port> <<file>	< input redirect	Sends a file

### curl –

- Testing web requests
- Send custom http/https requests and inspect the response.

Tool	Command	Flags / Syntax	What it does
curl	curl http://<domain>	—	Sends GET request
curl	curl -I http://<domain>	-I headers only	Shows HTTP headers
curl	curl -X POST -d "user=<u>&pass=<p>" http://<domain>/<path>	-X method, -d data	Sends POST request

### wget –

- Download files from the web.
- Retrieve files without interaction from servers.

Tool	Command	Flags / Syntax	What it does
wget	wget http://<domain>/<file>	—	Downloads file
wget	wget -r http://<domain>	-r recursive	Downloads site

### Nmap –

- Network reconnaissance and enumeration.
- Used to discover hosts, open ports, services, OS details and more, using NSE scripts.

Tool	Command	Flags / Syntax	What it does
Nmap	nmap <ip_address>	—	Basic scan
Nmap	nmap -sV <ip_address>	-sV service version	Detects versions
Nmap	nmap -O <ip_address>	-O OS detection	Detects OS
Nmap	nmap --script <script> <ip_address>	--script NSE	Runs scripts

### Masscan –

- Large scale or fast port scanning
- Quickly identify open ports across large networks. Sometimes less accurate than Nmap due to the high speed.

Tool	Command	Flags / Syntax	What it does
Masscan	masscan <network_range> -p<ports> --rate=<rate>	-p ports, --rate speed	Fast large-scale scan

## **Infrastructure, Firewalls and Logging**

### pfSense –

- Acting as a firewall/router in a network or lab
- Used to control traffic, firewall rules and integrate IPS (intrusion prevention system) and IDS (intrusion detection system)

Tool	Command	Flags / Syntax	What it does
pfSense	https://<pfSense_ip>	Web GUI	Manage firewall/router

### Sysmon –

- Monitors Windows system activity
- Gains detailed visibility into processes, network, and file changes.

Tool	Command	Flags / Syntax	What it does
Sysmon	sysmon -i <config>.xml	-i install	Installs Sysmon
Sysmon	sysmon -c	—	Shows configuration

### Event viewer –

- Windows incident investigation
- Analyze security, system, and applications logs.

Tool	Command	Flags / Syntax	What it does
Event Viewer	eventvwr.msc	Windows tool	Opens event logs

## **SIEM and Threat Analysis**

### ELK –

- A centralized log collection and analysis
- Used to store, search, analyze and visualize large volumes of logs in real time.

### Splunk –

- SIEM operations and security monitoring
- Used to detect threats, investigate incidents, and correlate events across systems.

### MITRE ATT&CK –

- Threat modeling and attack analysis
- Maps attacker techniques and helps understand adversary behavior.

## **Enumeration, Exploitation and Credential Attacks**

### NetExec –

- Active directory and network exploitation
- Used to enumerate users, shares, credentials and execute actions across systems.

Tool	Command	Flags / Syntax	What it does
NetExec	nxc smb <network_range>	SMB module	Enumerates hosts
NetExec	nxc smb <ip_address> -u <u> -p <p>	-u user, -p pass	Authenticates

### CrackMapExec (CME) –

- Credential testing
- Validates credentials and assess domain security.

Tool	Command	Flags / Syntax	What it does
CME	cme smb <ip_address> -u <u> -p <p>	SMB module	Tests credentials

### Impacket –

- Advanced Windows domain attacks
- Exploits Kerberos, dumps credentials, performs remote execution.

Tool	Command	Flags / Syntax	What it does
Impacket	impacket-secretsdump <u>:<p>@<ip_address>	—	Dumps credentials
Impacket	impacket-psexec <u>@<ip_address>	—	Remote execution

### Hydra –

- Online password attack
- Used for online brute force or credentials spraying against network services.

### Medusa –

- Parallel login brute force attacks
- Efficiently test large credential list against services

Tool	Command	Flags / Syntax	What it does
Medusa	medusa -h <ip_address> -u <u> -P <list> -M <service>	-M module	Parallel brute force

## HYDRA Vs. MEDUSA

- Hydra – flexible, wide protocol support, great for single target or small-scale attacks
- Medusa – handles large credentials lists, smaller protocols support, designed for massive parallelism.

Feature	Hydra	Medusa
Ease of use	high	medium
Protocol support	wide	limited
Parallel performance	medium	high
Password spraying	yes	yes
Large scale attacks	limited	best
Best use case	Single target / quick tests	Large user and pass lists
• Parallel performance - the ability to run many tasks at the same time to complete work faster and more efficiently		

## cupp –

- Targeted password attacks
- Creates a password list according to given information.

## Crunch –

- Targeted password attacks
- Creates a password list based on chosen characters and numbers.

Tool	Command	Flags / Syntax	What it does
cupp	cupp -i	Interactive	Generates wordlist
Crunch	crunch <min> <max> <charset> -o <file>	-o output	Generates wordlist

## John –

- Offline password cracking
- Recovers passwords from hashes.

## Hashcat –

- High performance password cracking
- Crack passwords efficiently using CPU/GPU acceleration.

Tool	Command	Flags / Syntax	What it does
John	john <hash_file>	—	Cracks hashes
John	john --show <hash_file>	--show	Shows results
Hashcat	hashcat -m <type> -a <mode> <hash_file> <wordlist>	-m hash, -a mode	GPU cracking

### smbclient -

- Access SMB shares
- List, download or upload files to windows file shares.

### PsExec -

- Remote command execution
- Used to execute commands on remote Windows systems.

Tool	Command	Flags / Syntax	What it does
smbclient	smbclient //<ip>/<share> -U <u>	-U user	Access SMB
PsExec	psexec \\<ip_address> cmd	Windows tool	Remote command

### msfconsole -

- Exploitation and post-exploitation
- Used to exploit vulnerabilities, gain shells, escalate privileges, and perform post-exploitation actions in a controlled environment

### msfvenom -

- Payload generation and encoding
- Used to create custom payloads, shells, and executables with specific formats and encoders for exploitation.

### BeEF (Browser Exploitation Framework) -

- Client-side browser exploitation
- Used to hook browsers via JavaScript and exploit browser-based weaknesses after a user visits a malicious page.

### Burp Suite -

- Web application security testing
- Used to intercept, inspect, and modify HTTP/HTTPS traffic to identify vulnerabilities like XSS, SQLi, and authentication issues.

### Searchsploit

- Exploit database search
- Used to find known exploits matching discovered software or services.

Tool	Command	Flags / Syntax	What it does
msfconsole	msfconsole	—	Launch Metasploit
msfvenom	msfvenom -p <payload> LHOST=<ip> LPORT=<port> -f <fmt> > <file>	payload options	Generate payload
BeEF	beef-xss	—	Start BeEF

Tool	Command	Flags / Syntax	What it does
BeEF	http://<ip>:<port>/hook.js	Hook	Browser hook
Burp	burpsuite	—	Launch Burp
Searchsploit	searchsploit <keyword>	—	Search exploits
Searchsploit	searchsploit -m <id>	-m copy	Copy exploit

## **Digital Forensics**

### Autopsy –

- Digital forensic investigations
- Analyze disks, timelines, deleted files and artifacts.

### Volatility –

- Memory forensics
- Analyze RAM for processes, malware, and injected code.

### Bulk\_extractor –

- Large scale forensic analysis
- Extracts artifacts like emails, URLs, pcap files and more without file systems

### Foremost –

- File carving from raw data.
- Recovers files based on headers and footers (start and end signature)

### Scalpel –

- Precise file carving
- Recovers specific file types with more control (via scalpel.conf)

### HxD –

- Manually inspecting or editing raw binary data
- View, analyze and modify files at the hexadecimal level.

Tool	Command	Flags / Syntax	What it does
Volatility	volatility -f <mem> windows.pslist	-f memory	List processes
Volatility	volatility -f <mem> windows.netscan	—	Network scan
Bulk_extractor	bulk_extractor <image> -o <dir>	-o output	Extract artifacts
Foremost	foremost <image>	—	File carving
Scalpel	scalpel <image> -o <dir>	-o output	Controlled carving