EH-7 Quick Revision Sheet

1. Exploits & Metasploit

- Purpose: Prove real vulnerabilities, deeper access.
- Tools: Exploit-DB, searchsploit, Metasploit.
- Example:
  msfconsole > search openssh
  use exploit/module
  set RHOST/LHOST, exploit

2. Post-Exploitation

- Tool: Meterpreter
  > sysinfo, hashdump, load mimikatz
- Use: Collect data, escalate privileges.

3. Password Cracking

- Tools: John the Ripper, Hashcat
- Types: Brute-force, dictionary, rainbow tables.
- Commands:
  john --format=nt hashfile.txt
  hashcat -m 1000 -a 0 hashes.txt rockyou.txt

4. Living Off the Land (LotL)

- Use built-in tools: PowerShell, certutil, wmic.
- Avoid detection, blend with system processes.

5. Persistence & Privilege Escalation

- Persistence: registry keys, reverse shell, metsvc.
- Escalation Tools: LinPEAS, Exploit-Suggester.
- Exploits: Dirty COW, sudo misconfig, SUID bins.

6. Fuzzing, Evasion & Timestomping

- Fuzzing: Peach, sfuzz -> find crashes.
- Evasion: Obfuscate payloads (Invoke-Obfuscation).
- Timestomping: match legit file timestamps.

Summary Table (Recall)

Exploit   -> Metasploit, searchsploit
Passwords-> Meterpreter, hashdump, mimikatz
Cracking -> John, Hashcat
LotL   -> PowerShell, Empire

EH-7 Quick Revision Sheet

Privilege -> LinPEAS, DirtyCOW
Persistence -> metsvc, registry, services