Tools for CEH practical exam

Here's a comprehensive list of tools commonly used for the CEH practical exam:

1. **Nmap**
2. **Wireshark**
3. **Metasploit**
4. **Burp Suite**
5. **Aircrack-ng**
6. **SQLMap**
7. **Hydra**
8. **John the Ripper**
9. **Nikto**
10. **Maltego**
11. **OWASP ZAP**
12. **Netcat**
13. **Snort**
14. **Ettercap**
15. **Recon-ng**
16. **Social-Engineer Toolkit (SET)**
17. **Cobalt Strike**
18. **Empire**
19. **Malware Analysis Tools (e.g., Cuckoo Sandbox)**
20. **Nessus**
21. **OpenVAS**
22. **Shodan**
23. **Beef (Browser Exploitation Framework)**
24. **Fuzzbunch**
25. **Hashcat**
26. **Arachni**
27. **Radare2**

28. Goby

29. PowerSploit

30. Powershell Empire

Feel free to ask if you need more information or assistance!

Here's a list of key commands for the CEH tools mentioned, along with one-line descriptions of their purposes:

1. Nmap

- `nmap -sS [target]`

  Conduct a SYN scan to identify open ports.

- `nmap -sP [target]`

  Perform a ping scan to discover active hosts.

2. **Wireshark**

- *Capture packets in real-time for analysis.*

  Usage: Open Wireshark and start capturing on the desired interface.

3. **Metasploit**

- `msfconsole`

  Launch the Metasploit console for penetration testing.

- `use exploit/windows/smb/ms17_010_eternalblue`

  Load the EternalBlue exploit module.

4. **Burp Suite**

- *Intercept and analyze HTTP requests.*

  Usage: Set your browser to use Burp as a proxy.

5. **Aircrack-ng**

- `airmon-ng`

  Enable monitor mode on a wireless interface.

- `aircrack-ng [file]`

  Crack WPA/WPA2 keys using captured packets.

6. **SQLMap**

- `sqlmap -u "[URL]" --dbs`

  Retrieve database names from a vulnerable web application.

7. hy**dra**

- `hydra -l [username] -P [passwordlist] [protocol]://[target]`

  Perform a brute-force attack on specified protocol.

8. **John the Ripper**

- `john [password-file]`

  Start cracking passwords from a file.

9. **Nikto**

- `nikto -h [target]`

  Scan a web server for vulnerabilities.

10. **Maltego**

- *Visual link analysis for OSINT.*

  Usage: Create a new graph and run transformations.

11. **OWASP ZAP**

- *Start ZAP for web application security testing.*

  Usage: Launch ZAP and set the proxy in your browser.

12. **Netcat**
    - `nc -l -p [port]`

      Listen on a specified port for incoming connections.

13. **Snort**
    - `snort -A console -c /etc/snort/snort.conf -i [interface]`

      Run Snort in IDS mode to monitor traffic.

14. **Ettercap**
    - `ettercap -G`

      Launch the graphical interface for man-in-the-middle attacks.

15. **Recon-ng**
    - `recon-ng`

      Start the reconnaissance framework.

16. **Social-Engineer Toolkit (SET)**
    - `setoolkit`

      Launch the Social-Engineer Toolkit for social engineering attacks.

17. **Cobalt Strike**
    - *Use for advanced threat emulation.*

      Usage: Launch the application and set up your environment.

18. **Empire**
    - `./empire`

      Start the Empire framework for post-exploitation.

19. **Cuckoo Sandbox**
   - *Run malware samples in a controlled environment.*
     Usage: Set up and submit files to the Cuckoo interface.

20. **Nessus**
   - *Scan networks for vulnerabilities.*
     Usage: Access the web interface and configure scans.

21. **OpenVAS**
   - *Start a vulnerability scan using OpenVAS.*
     Usage: Configure and launch scans via the web interface.

22**. Shodan***
   - `shodan search [query]`
     Search for devices based on a specific query.

23. **Beef**
   - *Start the Beef framework for browser exploitation.*
     Usage: Launch Beef and access the web interface.

24. **Fuzzbunch**
   - *Utilize fuzzing tools for exploitation.*
     Usage: Follow specific commands for your attack scenarios.

25**. Hashcat**
   - `hashcat -m [hash-type] -a [attack-mode] [hash-file] [wordlist]`
     Crack hashes using specified modes and wordlists.

26. **Arachni**
   - `arachni [URL]`
     Scan a web application for vulnerabilities.

27**. Radare2**

- `r2 [binary]`

  Analyze binary files for vulnerabilities.

28. **Goby**

- *Use Goby for asset discovery and vulnerability scanning.*

  Usage: Follow the GUI to configure scans.

29. **PowerSploit**

- `Import-Module PowerSploit`

  Import PowerSploit functions for PowerShell exploitation.

30. **Powershell Empire**

- `./empire`

  Start the PowerShell Empire for post-exploitation tasks.

Feel free to reach out if you need more information on any specific command or tool!