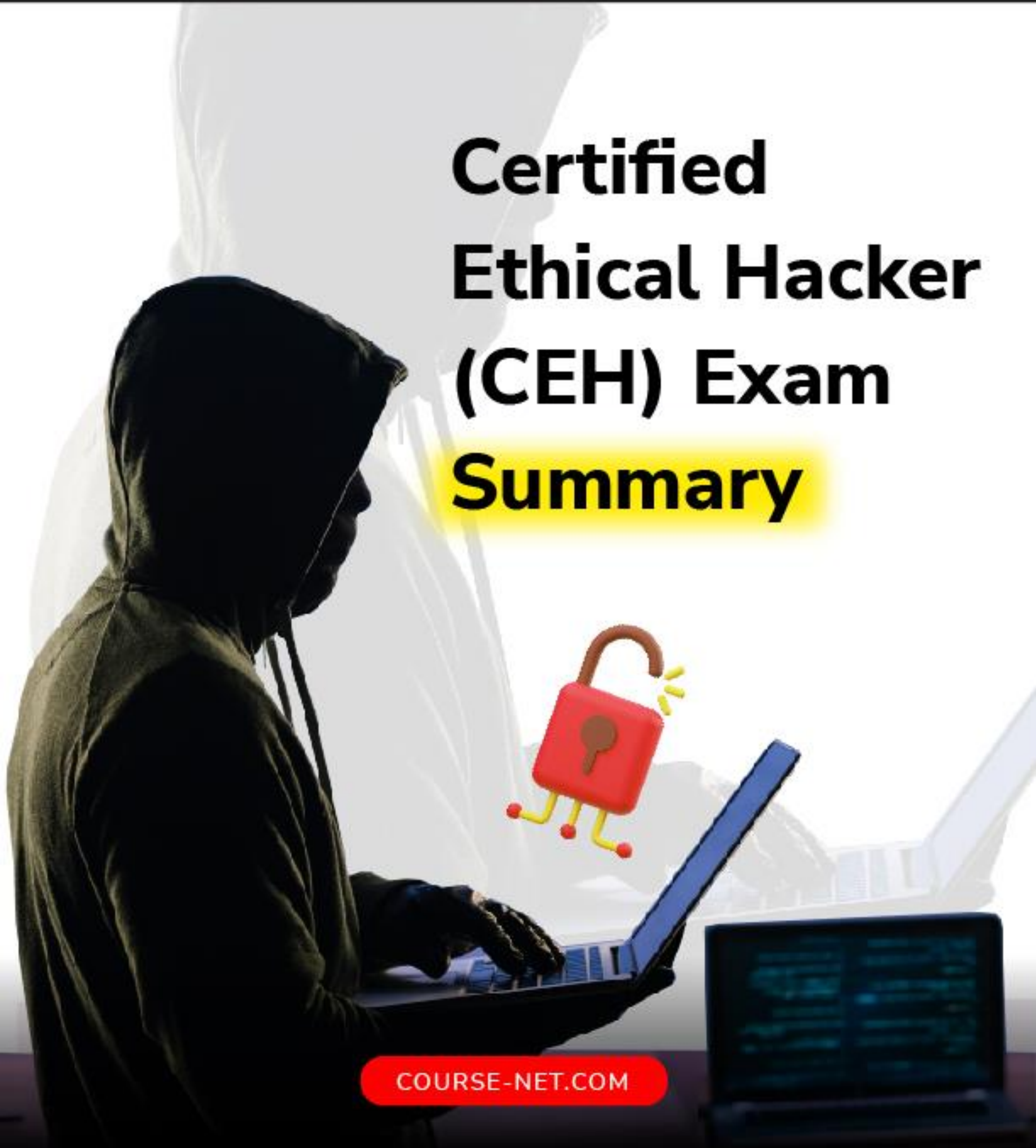
Empowering IT People

Certified Ethical Hacker (CEH) Exam Summary



COURSE-NET.COM

Certified Ethical Hacker (CEH) Exam Summary

5 phases to a penetration test

1. Reconnaissance
2. Scanning & Enumeration
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

Useful Reconnaissance Phase

In Google Hacking database:

- **Operator:** searching additional search items
- **`site:`** Search only within a domain
- **`ext:`** Specific file extension
- **`loc:`** Specific maps location
- **`intitle:`** keywords in title tag of page
- **`allintitle:`** any keywords can be in title
- **`inurl:`** keywords anywhere in URL
- **`allinurl:`** any of the keywords can be in URL
- **incache:** search Google cache only

In DNS record types

- **Service (SRV):** Hostname and port numbers of server
- **Start of Authority (SOA):** Primary name server
- **Pointer (PTR):** IP to Hostname; for reverse DNS
- **Name Server (NS):** NameServers with namespace
- **Mail Exchange (MX):** E-mail servers
- **CNAME:** Aliases in zone. List multi services in DNS
- **Address (A):** IP to Hostname; for DNS lookup
- **DNS footprinting:** whois, nslookup, dig

In TCP Header Flags

- **SYN:** Initial communication, has sequence #
- **ACK:** Acknowledge to, and answering SYN
- **PSH:** Forces delivery without concern for buffering
- **URG:** Indicates data being sent out of band
- **RST:** Forces termination (both directions)
- **FIN:** Ordered close to communications

Useful in Scanning & Enumeration

ICMP Message Types

- **0:** Echo Reply: Answer to type 8 Echo Request
- **3:** Destination Unreachable: No host/network. Additional codes:
  - 0 - Destination network unreachable
  - 1 - Destination host unreachable
  - 6 - Network unknown
  - 7 - Host unknown
  - 9 - Network administratively prohibited
  - 10 - Host administratively prohibited
  - 13 - Communication administratively prohibited
- **4:** Source Quench: Congestion control message
- **5:** Redirect: 2+ gateways for sender to use or the best route not the configured default gateway. Additional Codes:
  - **0 -** redirect datagram for the network
  - **1 -** redirect datagram for the host
- **8:** Echo Request: Ping message requesting echo
- **11:** Time Exceeded: Packet too long be routed

Important CIDR Notation & Netmask Ends

/30 = 4	*.225.252
/28 = 16	*.255.240
/26 = 64	*.255.192
/24 = 256	*.255.0
/22 = 1024	*.248.0
/20 = 4096	*.240.0

Important Port Range

0 — 1023: Well-known
1024 — 49151: Registered
49152 — 65535: Dynamic

Important Port Numbers

FTP: 20, 21
SSH: 22
Telnet: 23
SMTP: 25
WINS: 42

DNS: 53
HTTP: 80, 8080
Kerbers: 88
POP3: 110
Portmapper: 111

NNTP: 119
NTP: 123
RPC-DCOM: 135
NetBIOS/SMB: 137, 138, 139
IMAP: 143
SNMP: 161, 162
LDAP: 389
HTTPS: 443
CIFS: 445
RADIUS: 1812
RDP: 3389
IRC: 6667
Printer: 515, 631, or 9100

HTTP Error Codes

`2xx` - OK
`4xx` - Could not provide request
`5xx` - Could not process request

`nmap` *`<scan options> <target>`*

-sA: ACK scan
-sS:SYN
-sI: IDLS scan
-sN: NULL
-sR: RPC scan
-sW: Windos
-PI: ICMP ping
-PT: TCP ping
-oX: XML output
-T<0-4>: Slow to Fast
-sF: FIN scan
-sT: TCP scan
-sn: PING sweep
-sS: Stealth Scan
-Po: No ping
-sX: XMAS tree scan
-PS: SYN ping
-oN: Normal output
-A OS/Vers/Script

Useful During Sniffing and Evasion

About MAC Address: First half = 3 bytes/24 bits is manufacturer UID. Second half = unique number

Stateful Inspection: Concerned with the connections. Doesn’t sniff packets, it just verifies if it’s a known connection, then passes along.

HTTP Tunnelling: Crafting of wrapped segments through a port rarely filtered by the Firewall (e.g., 80) to carry payloads that may otherwise be blocked.

IDS Evasion Tactics: Slow down OR flood the network (and sneak through in the mix) OR fragmentation

Useful During Gaining Access

C|EH rules for passwords: Must not contain user's name. Min 8 chars. 3 of 4 complexity components e.g., special, number, uppercase, lowercase
Sidejacking: Steal cookies exchanged between systems and use to perform a replay-style attack.

Authentication Types

- Type 1: *Something you know*
- Type 2: *Something you have*
- Type 3: *Something you are*

Attack target type

- **OS:** Attacks targeting default OS settings
- **App level:** Application code attacks
- **Shrink Wrap:** off-the-shelf scripts and code
- **Misconfiguration:** not configured well

Attack method type

- **Passive Online:** Sniffing wire, intercept cleartext password/replay/MITM
- **Active Online:** Password guessing.
- **Offline:** Steal copy of password i.e., SAM file (typically in `C:\Windows\system32\config`). Cracking efforts on a separate system
- **Non-electronic:** Social Engineering

Session Hijacking

Refers to the active attempt to steal an entire established session from a target

- Sniff traffic between client and server
- Monitor traffic and predict sequence
- Desynchronise session with client
- Predict session token and take over session
- Inject packets to the target server

Legal Bodies

18 U.S.C 1029 & 1030
RFC 1918 - Private IP Standard
RFC 3227 - Collecting and storing data
ISO 27002 - InfoSec Guidelines
CAN-SPAM - email marketing
SPY-Act - License Enforcement
DMCA - Intellectual Property
SOX - Corporate Finance Processes
GLBA - Personal Finance Data
FERPA - Education Records
FISMA - Gov Networks Security Std
CVSS - Common Vuln Scoring System
CVE - Common Vulns and Exposure

About Cryptography

Symmetric Algorithms

DES: 56 bit key (8 bit parity); fixed block
3DES: 168 bit key; keys = 3
AES: 128, 192, or 256 bit
IDEA: 128 bit
Twofish: Block cipher key size = 256 bit
Blowfish: 64 bit block
RC6: 128 bit block

Asymmetric Algorithms

Diffie-Hellman: key Exchange, used in SSL or IPSec
ECC: Elliptical Curve. Low process power or mobile platform
RSA: 2 x Prime 4,096 bit. Modern standard

Hash Algorithms

MD5: 128 bit hash (as 32bit hex)
SHA1: 160 bit hash
SHA2: 224, 256, 384 or 512 bit hash

Cryptography Attacks

Known Plain-text: Search plaintext for repeatable sequences.
Ciphertext-only: Obtain several messages with same algorithm. Analyze to reveal repeating code.
Replay: Performed in MITM. Repeat exchange to fool system in setting up a communication channel.

About Social Engineering

Human based attacks

- Dumpster diving
- Impersonation
- Technical Support
- Should Surfing
- Tailgating/Piggybacking

Computer based attacks

- Phishing - Email SCAM
- Whaling - Targeting CEO's
- Pharming - Evil Twin Website

Web-based Hacking

CSRF: Cross Site Request Forgery
Dot-dot-slash Attack: Variant of Unicode or un-validated input attack

Buffer Overflow: A condition that occurs when more data is written to a buffer than it has space to store and results in data corruption. Caused by insufficient bounds checking, a bug, or poor configuration in the program code.

SQL Injection attack types

Union Query: Use the UNION command to return the union of target DB with a crafted data
Tautology: Term used to describe behavior of a DB when deciding if a statement is true.
Blind SQL Injection: Trial and Error with no responses or prompts.
Error based SQL Injection: Enumeration technique. Inject poorly constructed commands to have DB respond with table names and other information

About Wireless Network Hacking

Wireless sniffing

Compatible wireless adapter with promiscuous mode is required; pretty much the same as sniffing wired.

802.11 Specifications

- **WEP:** RC4 with 24bit vector. Keys are 40 or 104bit
- **WAP:** RC4 supports longer keys; 48bit IV
- **WPA/TKIP:** Changes IV each frame and key mixing
- **WPA2:** AES + TKIP features; 48bit IV

Bluetooth Attacks

- **Bluesmacking:** DoS against a device
- **Bluejacking:** Sending messages to/from devices
- **Bluesniffing:** Sniffs for Bluetooth
- **Bluesnarfing:** actual theft of data from a device

Kind of Virus

- **Boot:** Moves boot sector to another location. Almost impossible to remove.
- **Camo:** Disguise as legit files.
- **Cavity:** Hides in empty areas in exe.
- **Macro:** Written in MS Office Macro Language
- **Multipartite:** Attempts to infect files and boot sector at same time.
- **Metamorphic virus:** Rewrites itself when it infects a new file.
- **Network:** Spreads via network shares.
- **Polymorphic Code virus:** Encrypts itself using built-in polymorphic engine. Constantly changing signature makes it hard to detect.
- **Shell virus:** Like boot sector but wrapped around application code, and run during application start.
- **Stealth:** Hides in files, copies itself to deliver payload.

Denial of Service Types

- **SYN Attack:** Send thousands of SYN packets with a false IP address. Target will attempt SYN/ACK response. All machine resources will be engaged.
- **SYN Flood:** Send thousands of SYN Packets but never respond to any of the returned SYN/ACK packets. Target will run out of available connections.
- **ICMP Flood:** Send ICMP Echo packets with a fake source address. Target attempts to respond but reaches a limit of packets sent per second.
- **Application level:** Send “legitimate” traffic to a web application than it can handle.
- **Smurf:** Send large number of pings to the broadcast address of the subnet with source IP spoofed to target. Subnet will send ping responses to target.
- **Fraggle Attack:** Similar to Smurf but uses UDP.
- **Ping of Death:** Attacker fragments ICMP message to send to target. When the fragments are reassembled, the resultant ICMP packet is larger than max size and crashes the system

Linux Specials

Linux File System

`/`	-Root
`/var`	-Variable Data / Log Files
`/bin`	-Biniaries / User Commands
`/sbin`	-Sys Binaries / Admin Commands
`/root`	-Home dir for root user
`/boot`	-Store kernel
`/proc`	-Direct access to kernel
`/dev`	-Hardware storage devices
`/mnt`	-Mount devices

Identifying Users and Processes

0	- Root UID
1	- INIT process
1-999	- Accounts of Services
>= 1000	- All other users

Windows Specials

Windows Registry

Two elements make a registry setting: a key (location pointer), and value (define the key setting). Root level keys are as follows:

- `HKEY_LOCAL_MACHINE` - Info on Hard/software
- `HKEY_CLASSES_ROOT` – Info on file associations and Object Linking and Embedding (OLE) classes
- `HKEY_CURRENT_USER` – Profile info on current user
- `HKEY_USERS` – User config info for all active users
- `HKEY_CURRENT-CONFIG` – pointer to hardware profiles

EC-Council
Hackers are here. Where are you?