

# Certified Ethical Hacker (CEH) Exam Cheat Sheet

## Basics

### 5 phases to a penetration test

Reconnaissance  
Scanning & Enumeration  
Gaining Access  
Maintaining Access  
Covering Tracks

### Attack Types

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

## Legal

### 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

### Regional Registry Coverage Map



## Cryptography

### Symmetric Encryption

Key pairs required =

#### Symmetric Algorithms

**DES**: 56bit key (8bit parity); fixed block

**3DES**: 168bit key; keys ≤ 3

**AES**: 128, 192, or 256; replaced DES

**IDEA**: 128bit key

**Twofish**: Block cipher key size ≤ 256bit

**Blowfish**: Rep. by AES; 64bit block

**RC**: incl. RC2 → RC6. 2,040key, RC6 (128bit block)

#### Asymmetric Encryption

Public key = Encrypt, Private Key = Decrypt

#### Asymmetric Algorithms

**Diffie-Hellman: key Exchange**, used in SSL/IPSec

**ECC**: Elliptical Curve. Low process power/Mobile

**El Gamal**: !=Primes, log problem to encrypt/sign

**RSA**: 2 x Prime 4,096bit. Modern std.

#### Hash Algorithms

**MD5**: 128bit hash, expres as 32bit hex

**SHA1**: 160bit hash, rq 4 use in US apps

**SHA2**: 4 sep hash 224,256,384,512

#### Trust Models

**Web of trust**: Entities sign certs for each other

**Single Authority**: CA at top. Trust based on CA itself

**Hierarchical**: CA at top. RA's Under to manage certs

**XMKS** - XML PKI System

### Cryptography Attacks

**Known Plain-text**: Search plaintext for repeatable sequences. Compare to t versions.

**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 comms channel.

### Digital Certificate

Used to verify user identity = nonrepudiation

Version: Identifies format. Common = V1

**Serial**: Uniquely identify the certificate

**Subject**: Whoever/whatever being identified by cert

**Algorithm ID**: Algorithm used

**Issuer**: Entity that verifies authenticity of certificate

**Valid from/to**: Certificate good through dates

**Key usage**: Shows for what purpose cert was made

**Subject's public key**: self-explanatory

**Optional fields**: e.g., Issuer ID, Subject Alt Name...

## Reconnaissance

### Definition

Gathering information on targets, whereas foot-printing is mapping out at a high level. These are interchangeable in C|EH.

### Google Hacking:

Operator: keyword additional search items

site: Search only within domain

ext: File Extension

loc: 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

### DNS

port 53 nslookup (UDP), Zone xfer (TCP)

### DNS record types

**Service (SRV)**: hostname & port # of servers

**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

### TCP Header Flags

**URG**: Indicates data being sent out of band

**ACK**: Ack to, and after SYN

**PSH**: Forces delivery without concern for buffering

**RST**: Forces comms termination in both directions

**SYN**: Initial comms. Parameters and sequence #'s

**FIN**: ordered close to communications

### DHCP

Client — Discover—> Server

Client<—Offers— Server

Client —Request—> Server

Client<—ACK— Server

IP is removed from pool

## Scanning & Enumeration

### ICMP Message Types

**0**: Echo Reply: Answer to type 8 Echo Request

**3**: Destination Unreachable: No host/ network 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

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

### CIDR

Method of the representing IP Addresses **IPv4**

### Notation

/30=4 .225.252

/28=16 .255.240

/26=64 .255.192

/24=256 .255.0

/22=1024 .248.0

/20=4096 .240.0

TCP/IP model	Protocols and services	OSI model
Application	HTTP, FTP, Telnet, NTP, DHCP, PING	Application
Transport	TCP, UDP	Presentation
Network	IP, ARP, ICMP, IGMP	Session
Network Interface	Ethernet	Transport
		Network
		Data Link
		Physical

### Port Numbers

0 — 1023: Well-known

1024 — 49151: Registered

49152 — 65535: Dynamic

### Important Port Numbers

FTP: 20/21

SSH: 22

Telnet: 23

SMTP: 25

WINS: 42

TACACS: 49  
 DNS: 53  
 HTTP: 80 / 8080  
 Kerbers: 88  
 POP3: 110  
 Portmapper (Linux): 111  
 NNTP: 119  
 NTP: 123  
 RPC-DCOM: 135  
 NetBIOS/SMB: 137-139  
 IMAP: 143  
 SNMP: 161/162  
 LDAP: 389  
 HTTPS: 443  
 CIFS: 445  
 RADIUS: 1812  
 RDP: 3389  
 IRC: 6667  
 Printer: 515,631,9100

Tini: 7777  
 NetBus: 12345  
 Back Orifice: 27374  
 Sub7: 31337

### **HTTP Error Codes**

200 Series - OK  
 400 Series - Could not provide req  
 500 Series - Could not process req

### **Nmap**

Nmap is the de-facto tool for this pen-test phase

### **Nmap <scan options> <target>**

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

### **Scan Types**

TCP: 3 way handshake on all ports.  
 Open = SYN/ACK, Closed = RST/ACK  
 SYN: SYN packets to ports (incomplete handshake).

Open = SYN/ ACK, Closed = RST/ ACK  
 FIN: Packet with FIN flag set  
 Open = no response, Closed = RST  
 XMAS: Multiple flags set (fin, URG, and PSH)

### **Binary Header: 00101001**

Open = no response, Closed = RST  
 ACK: Used for Linux/Unix systems  
 Open = RST, Closed = no response  
 IDLE: Spoofed IP, SYN flag, designed for stealth.

Open = SYN/ACK, Closed= RST/ACK

NULL: No flags set. Responses vary by OS.  
 NULL scans are designed for Linux/ Unix machines.

### **NetBIOS**

#### **nbstat**

nbstat -a COMPUTER 190  
 nbstat -A 192.168.10.12 remote table  
 nbstat -n local name table  
 nbstat -c local name cache

nbstat -r -purge name cache  
 nbstat -S 10 -display ses stats every 10 sec  
**1B** == master browser for the subnet  
**1C** == domain controller  
**1D** == domain master browser

### **SNMP**

Uses a community string for PW  
 SNMPv3 encrypts the community strings

### **Sniffing and Evasion**

IPv4 and IPv6

IPv4 == unicast, multicast, and broadcast  
 IPv6 == unicast, multicast, and anycast.  
 IPv6 unicast and multicast scope includes link local, site local and global.

### **MAC Address**

First half = 3 bytes (24bits) = Org UID  
 Second half = unique number

### **NAT (Network Address Translation)**

Basic NAT is a one-to-one mapping where each internal IP== a unique public IP.  
 Nat overload (PAT) == port address translation. Typically used as is the cheaper option.

### **Stateful Inspection**

Concerned with the connections. Doesn't sniff ever packet, 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.

### **Snort IDS**

It has 3 modes:  
 Sniffer/Packet logger/ Network IDS.  
 Config file: /etc/snort, or c:\snort\etc  
 #~alert tcp!HOME\_NET any ->\$HOME\_NET 31337 (msg: "BACKDOOR AT-TEMPT-Back-orifice.")  
 Any packet from any address !=home network. Using any source port, intended for an address in home network on port 31337, send msg.

**Span port:** port mirroring

**False Negative:** IDS incorrectly reports stream clean

### **IDS Evasion Tactics**

Slow down OR flood the network (and sneak through in the mix) OR fragmentation

### **TCPdump syntax**

#~tcpdump flag(s) interface

### **Attacking a System**

#### **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

#### **LM Hashing**

7 spaces hashed: AAD3B435B51404EE

#### **Attack types**

**Passive Online:** Sniffing wire, intercept cleartext password / replay / MITM

**Active Online:** Password guessing. **Offline:** Steal copy of password i.e., SAM

file. Cracking efforts on a separate system

**Non-electronic:** Social Engineering

### **Sidejacking**

Steal cookies exchanged between systems and use tp perform a replay-style attack.

### **Authentication Types**

Type 1: Something you know

Type 2: Something you have

Type 3: Something you are

### **Session Hijacking**

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

1. Sniff traffic between client and server
2. Monitor traffic and predict sequence
3. Desynchronise session with client
4. Predict session token and take over session
5. Inject packets to the target server

### **Kerberos**

Kerberos makes use of symmetric and asymmetric encryption technologies and involves:

**KDC:** Key Distribution Centre

**AS:** Authentication Service

**TGS:** Ticket Granting Service

**TGT:** Ticket Granting Ticket

### **Process**

1. Client asks KDC (who has AS and TGS) for ticket to authenticate throughout the network. this request is in clear text.
2. Server responds with secret key. hashed by the password copy kept on AD server (TGT).
3. TGT sent back to server requesting TGS if user decrypts.
4. Server responds with ticket, and client can log on and access network resources.

### **SAM file**

C:\Windows\system32\config

### **Registry**

2 elements make a registry setting: a key (location pointer), and valu (define the key setting).

Rot 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

HEKY\_CURRENT-CONFIG—pointer to\hardware Profiles\.

**HEKY\_LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion**

\RunServicesOnce

\RunServices

\Run Once

\Run

### **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

## Types of Social Engineers

**Insider Associates:** Limited Authorized Access

**Insider Affiliates:** Insiders by virtue of Affiliation that spoof the identity of the Insider

**Outsider Affiliates:** Non-trusted outsider that use an access point that was left open

## Physical Security

### 3 major categories of Physical Security measures

**Physical measures:** Things you taste, touch, smell

**Technical measures:** smart cards, biometrics

**Operational measures:** policies and procedures

## Web-based Hacking

**CSRF** - Cross Site Request Forgery

### Dot-dot-slash Attack

Variant of Unicode or un-validated input attack

### SQL Injection attack types

**Union Query:** Use the UNION command to return the union of target Db with a crafted Db

**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

### 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.

**Stack:** Premise is all program calls are kept in a stack and performed in order. Try to change a function pointer or variable to allow code exe

**Heap:** Takes advantage of memory "on top of" the application (dynamically allocated). Use program to overwrite function pointers

**NOP Sled:** Takes advantage of instruction called "no-op". Sends a large # of NOP instructions into buffer. Most IDS protect from this attack.

### Dangerous SQL functions

The following do not check size of destination buffers:

gets() strcpy() stract() printf()

## Wireless Network Hacking

### Wireless sniffing

Compatible wireless adapter with promiscuous mode is required, but otherwise 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

Spec	Dist	Speed	Freq
802.11a	30m	54 Mbps	5GHz
802.11b	100m	11 Mbps	2.4 GHz
802.11g	100m	54 Mbps	2.4 GHz
802.11n	125m	100 Mbps+	2.4/5GHz

### 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

## Trojans and Other Attacks

### Virus Types

**Boot:** Moves boot sector to another location. Almost impossible to remove.

**Camo:** Disguise as legit files.

**Cavity:** Hides in empty areas in exe. **Marco:** 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 on application start.

**Stealth:** Hides in files, copies itself to deliver payload.

### DOS 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

### Viruses

#### Heartbleed: CVE-2014-0160

Founded by Neel Mehta, Heartbleed is a vulnerability with heartbeat in OpenSSL software Library. Allowed for MITM to steal information protected under normal conditions by SSL/TLS encryption.

#### POODLE: CVE-2014-3566

MITM exploit which took advantage of inter-

net and software client fallback to SSL 3.0.

#### Shellshock: CVE-2014-6271

Exploit a vuln that executes codes inside the ' ' where the text should not be exe.

**ILOVEYOU:** A worm originating in the Philippines. Started in May 5, 2000, and was built on a VBS macro in Microsoft word/excel/templates.

**MELISSA:** Email virus based on MS word macro. Created in 1999 by David L. Smith.

## Linux Commands

### Linux File System

/	-Root
/var	-Variable Data / Log Files
/bin	-Binaries / 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

INIT process ID	1
Root UID, GID	0
Accounts of Services	1-999
All other users	Above 1000

### Permissions

4 - Read  
2 - Write  
1 - Execute  
User/Group/Others  
764 - User>RWX, Grp>RW, Other>R

### Snort

action protocol address port -> address port  
(option:value;option:value)  
alert tcp 10.0.0.1 25 -> 10.0.0.2 25  
(msg:"Sample Alert"; sid:1000;)

## Command Line Tools

### NMap

nmap -sT -T5 -n -p 1-100 10.0.0.1

### Netcat

nc -v -z -w 2 10.0.0.1

### TCPdump

tcpdump -i eth0 -v -X ip proto 1

### Snort

snort -vde -c my.rules 1

### hping

hping3 -I -eth0 -c 10 -a 2.2.2.2 -t 100 10.0.0.1

### iptables

iptables -A FORWARD -j ACCEPT -p tcp -dport 80

## Tools of the Trade

### Vulnerability Research

National Vuln Db

Eccouncil.org

Exploit-db

### Foot-printing

### Website Research Tools

Netcraft

Webmaster

Archive

### DNS and Whois Tools

Nslookup

Sam Spade

ARIN

WhereisIP

DNSstuff

DNS-Digger

## **Website Mirroring**

Wget  
Archive  
GoogleCache

## **Scanning and Enumeration**

### **Ping Sweep**

Angry IP Scanner  
MegaPing

### **Scanning Tools**

SuperScan  
NMap (Zenmap)  
NetScan Tools Pro

Hping  
Netcat

### **War Dialing**

THC-Scan  
TeleSweep  
ToneLoc  
WarVox

### **Banner Grabbing**

Telnet  
ID Serve  
Netcraft  
Xprobe

### **Vulnerability Scanning**

Nessus  
SAINT  
Retina  
Core Impact  
Nikto

### **Network Mapping**

NetMapper  
LANState  
IPSonar

### **Proxy, Anonymizer, and Tunneling**

Tor  
ProxySwitcher  
ProxyChains  
SoftCab  
HTTP Tunnel  
Anonymouse

### **Enumeration**

SuperScan  
User2Sid/Sid2User  
LDAP Admin  
Xprobe  
Hyena

### **SNMP Enumeration**

SolarWinds  
SNMPUtil  
SNMPScanner

### **System Hacking Tools**

#### **Password Hacking**

Cain  
John the Ripper  
LCP  
THC-Hydra  
ElcomSoft  
Aircrack  
Rainbow Crack  
Brutus

KerbCrack

#### **Sniffing**

Wireshark  
Ace  
KerbSniff  
Ettercap

#### **Keyloggers and Screen Capture**

KeyProwler  
Ultimate Keylogger  
All in one Keylogger

Actual Spy  
Ghost  
Hiddern Recorder  
Desktop Spy  
USB Grabber

### **Privilege Escalation**

Password Recovery Boot Disk  
Password Reset  
Password Recovery  
System Recovery

### **Executing Applications**

PDQ Deploy  
RemoteExec  
Dameware

### **Spyware**

Remote Desktop Spy  
Activity Monitor  
OSMomitor  
SSPro  
Spector Pro

### **Covering Tracks**

ELsave  
Cleaner  
EraserPro  
Evidence Eliminator

### **Packet Craftin/Spoofing**

Komodia  
Hping2  
PackEth  
Packet Generator  
Netscan  
Scapy

Nemesis

### **Session Hijacking**

Paros Proxy  
Burp Suite  
Firesheep  
Hamster/Ferret  
Ettecap  
Hunt

### **Cryptography and Encryption**

#### **Encryption**

TureCrypt  
BitLocker  
DriveCrypt

#### **Hash Tools**

MD5 Hash  
Hash Calc

#### **Steganography**

XPTools  
ImageHide  
Merge Streams  
StegParty  
gifShuffle  
QuickStego  
InvisibleSecrets  
EZStego  
OmniHidePro

#### **Cryptanalysis**

Cryptanalysis  
Cryptobench

#### **Sniffing**

#### **Packet Capture**

Wireshark  
CACE  
tcpdump  
Capsa  
OmniPeek  
Windump  
dnsstuff  
EtherApe

## **Wireless**

Kismet  
Netstumbler  
**MAC Flooding/Spoofing**  
Macof  
SMAC

### **ARP Poisoning**

Cain  
UfaSoft  
WinARP Attacker

### **Wireless**

#### **Discovery**

Kismet  
NetStumbler  
insider  
NetSurveyor

#### **Packet Sniffing**

Cascade Pilot  
Omnipeek  
Comm View  
Capsa

#### **WEP/WPA Cracking**

Aircrack  
KisMac  
Wireless Security Auditor  
WepAttack  
WepCrack  
coWPatty

#### **Bluetooth**

BTBrowser  
BH Bluejack  
BTScanner  
Bluesnarfer

#### **Mobile Device Tracking**

Wheres My Droid  
Find My Phone  
GadgetTrack  
iHound

### **Trojans and Malware**

#### **Wrappers**

Elite Wrap

#### **Monitoring Tools**

HiJackThis  
CurrPorts  
Fport

#### **Attack Tools**

Netcat  
Nemesis

#### **IDS**

Snort

#### **Evasion Tools**

ADMutate  
NIDSBench  
IDSInformer  
Inundator

### **Web Attacks**

Wfetch  
Httprecon  
ID Serve  
WebSleuth  
Black Widow  
CookieDigger  
Nstalker  
NetBrute

#### **SQL Injection**

BSQL Hacker  
Marathon  
SQL Injection Brute  
SQL Brute  
SQLNinja  
SQLGET