

Certified Ethical Hacker (CEH) Exam Cheat Sheet

CERTIFIED ETHICAL HACKER EXAM CHEAT SHEET



STATIONX
THE CYBER SECURITY COMPANY

Basics

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

5 phases to a penetration

Reconnaissance

Scanning & Enumeration

Gaining Access

Maintaining Access

Covering Tracks

Legal

18 U.S.C 1029 & 1030

RFC 1918 - Private IP Standard

RFC 3227 - Collecting and storing data

ISO 27002 - InfoSec Guideline

CAN-SPAM - email marketing

SPY-Act - License Enforcement

DMCA - Intellectual Property

SOX - Corporate Finance Processes

GLBA - Personal Finance Data

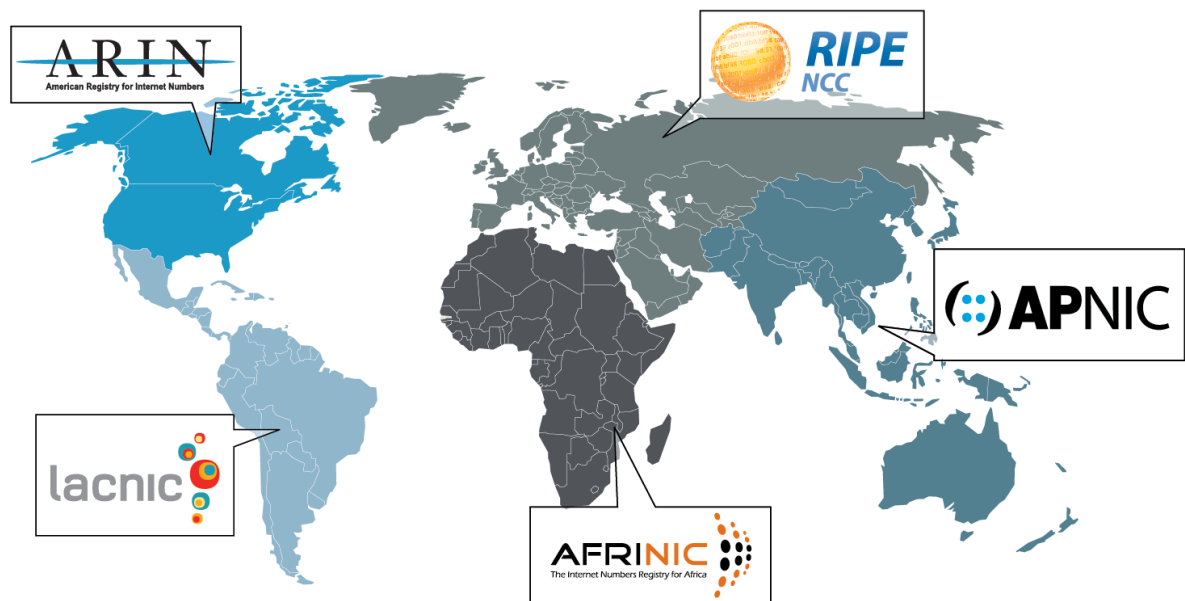
FERPA - Education Records

FISMA - Gov Networks Security Std

CVSS - Common Vuln Scoring System

CVE - Common Vulns and Exposure

Regional Registry Coverage Map



Cryptography

SYMMETRIC ENCRYPTION

Only one key used to encrypt and decrypt

ASYMMETRIC ENCRYPTION

Public key = Encrypt,
Private Key = Decrypt

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 ≤ 256 bit

Blowfish: Rep. by AES; 64bit block

RC: incl. RC2 \rightarrow RC6.
2,040key, RC6 (128bit block)

ASYMMETRIC ALGORITHMS

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

ECC: Elliptical Curve. Low process power/Mobile

EI 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

DNS RECORD TYPES

Service (SRV): hostname & port # of servers

Start of Authority (SOA): Primary name server

Pointer (PTR): IP to Hostname; for reverse DNS

allintitle: any keywords can be in title	Name Server (NS): NameServers with namespace
inurl: keywords anywhere in url	Mail Exchange (MX): E-mail servers
allinurl: any of the keywords can be in url	CNAME: Aliases in zone. list multi services in DNS
incache: search Google cache only	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

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

DHCP
Client – Discover-> Server
Client<--Offers-- Server
Client –Request-> Server
Client<--ACK-- Server
IP is removed from pool

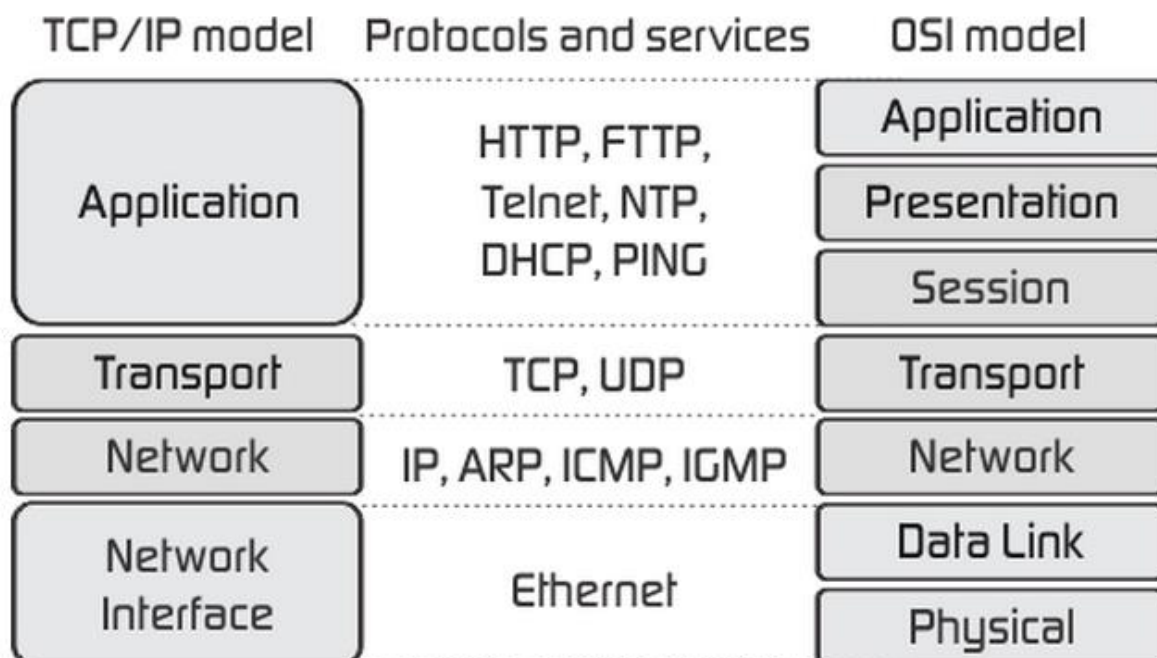
Scanning & Enumeration

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

CIDR

Method of the representing IP Addresses.

IPV4 NOTATION	
/30=4	.255.252
/28=16	.255.240
/26=64	.255.192
/24=256	. 255.0
/22=1024	.248.0
/20=4096	.240.0



PORT NUMBERS	HTTP Error Codes
0 – 1023: Well-known	200 Series – OK
1024 – 49151: Registered	400 Series – Could not provide req
49152 – 65535: Dynamic	500 Series – Could not process req

IMPORTANT PORT NUMBERS			
FTP:	20/21	NetBIOS/SMB:	137-139
SSH:	22	IMAP:	143
Telnet:	23	SNMP:	161/162
SMTP:	25	LDAP:	389
WINS:	42	HTTPS:	443
TACACS:	49	CIFS:	445
DNS:	53	RADIUS:	1812
HTTP:	80 / 8080	RDP:	3389
Kerbers:	88	IRC:	6667
POP3:	110	Printer:	515, 631, 9100
Portmapper (Linux):	111	Tini:	7777
NNTP:	119	NetBus:	12345
NTP:	123	Back Orifice:	27374
RPC-DCOM:	135	Sub7:	31337

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

NMAP 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.

SNMP

Uses a community string for PW
SNMPv3 encrypts the community strings

NETBIOS

nbstat	
nbtstat -a COMPUTER 190	nbtstat -S 10 -display ses stats every 10 sec
nbtstat -A 192.168.10.12 remote table	1B ==master browser for the subnet
nbtstat -n local name table	1C == domain controller
nbtstat -c local name cache	1D == domain master browser
nbtstat -r -purge name cache	

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.

IDS EVASION TACTICS

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

TCPDUMP SYNTAX

#~tcpdump flag(s) interface

SNORT IDS

It has 3 modes:

Config file: /etc/snort, or
c:snortetc #~alert tcp!HOME_NET
any ->\$HOME_NET 31337 (msg :
"BACKDOOR ATTEMPT-Back-
orifice.")

Span port: port mirroring

Sniffer/Packet logger/ Network IDS.

Any packet from any address !=home network. Using any source port, intended for an address in home network on port 31337, send msg.

False Negative: IDS incorrectly reports stream clean

LM HASHING

7 spaces hashed:
AAD3B435B51404EE

SAM FILE

C:Windowssystem32config

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

ATTACK TYPES

Passive Online: Sniffing wire, intercept clean text 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 to 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.

REGISTRY

2 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.

HKEY_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

CSRF - CROSS SITE REQUEST FORGERY

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() strcat() 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 virus:	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

Linux Commands

LINUX FILE SYSTEM		IDENTIFYING USERS AND PROCESSES
/	-Root	INIT process ID 1
/var	-Variable Data / Log Files	Root UID, GID 0
/bin	-Binaries / User Commands	Accounts of Services 1-999
/sbin	-Sys Binaries / Admin Commands	All other users Above 1000
/root	-Home dir for root user	
/boot	-Store kernel	PERMISSIONS
/proc	-Direct access to kernel	4 - Read
/dev	-Hardware storage devices	2 - Write
/mnt	-Mount devices	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

CEH Tools

VULNERABILITY RESEARCH	SCANNING AND ENUMERATION
National Vuln Db	Ping Sweep
Eccouncil.org	Angry IP Scanner
Exploit Database	MegaPing
	Scanning Tools
	SuperScan
	NMap (Zenmap)
	NetScan Tools Pro
	Hping
	Netcat
	War Dialing
	THC-Scan
	TeleSweep
FOOT-PRINTING	
Website Research Tools	
Netcraft	
Webmaster	
Archive	
DNS and Whois Tools	
Nslookup	

Sam Spacde	ToneLoc
ARIN	WarVox
WhereisIP	Banner Grabbing
DNSstuff	Telnet
DNS-Digger	ID Serve
Website Mirroring	Netcraft
Wget	Xprobe
Archive	Vulnerability Scanning
GoogleCache	Nessus
	SAINT
	Retina
	Core Impact
	Nikto
SYSTEM HACKING TOOLS	Network Mapping
Password Hacking	NetMapper
Cain	LANState
John the Ripper	IPSonar
LCP	Proxy, Anonymizer, and Tunneling
THC-Hydra	Tor
ElcomSoft	ProxySwitcher
Aircrack	ProxyChains
Rainbow Crack	SoftCab
Brutus	HTTP Tunnel
KerbCrack	Anonymouse
Sniffing	Enumeration
Wireshark	SuperScan
Ace	User2Sid/Sid2User
KerbSniff	LDAP Admin
Ettercap	Xprobe
Keyloggers and Screen Capture	Hyena
KeyProwler	SNMP Enumeration
Ultimate Keylogger	SolarWinds
All in one Keylogger	SNMPUtil
Actual Spy	SNMPScanner
Ghost	
Hiddern Recorder	
Desktop Spy	
USB Grabber	
Privilege Escalation	CRYPTOGRAPHY AND ENCRYPTION
Password Recovery Boot Disk	Encryption
Password Reset	TureCrypt
Password Recovery	BitLocker
System Recovery	DriveCrpyt
Executing Applications	Hash Tools
PDQ Deploy	MD5 Hash
RemoteExec	Hash Calc
Dameware	Steganography
Spyware	XPTools
Remote Desktop Spy	ImageHide
Activity Monitor	Merge Streams
OSMomitor	StegParty
SSPro	gifShuffle
Spector Pro	QuickStego
Covering Tracks	InvisibleSecrets

ELsave	EZStego
Cleaner	OmniHidePro
EraserPro	Cryptanalysis
Evidence Eliminator	Cryptobench
Packet Craftin/Spoofing	
Komodora	
Hping2	WIRELESS
PackEth	Discovery
Packet Generator	Kismet
Netscan	NetStumbler
Scapy	insider
Nemesis	NetSurveyor
Session Hijacking	Packet Sniffing
Paros Proxy	Cascade Pilot
Burp Suite	Omnipeek
Firesheep	Comm View
Hamster/Ferret	Capsa
Ettecap	WEP/WPA Cracking
Hunt	Aircrack
	KisMac
	Wireless Security Auditor
SNIFFING	WepAttack
Packet Capture	WepCrack
Wireshark	coWPatty
CACE	Bluetooth
tcpdump	BTBrowser
Capsa	BH Bluejack
Omnipeek	BTScanner
Windump	Bluesnarfer
dnsstuff	Mobile Device Tracking
EtherApe	Wheres My Droid
Wireless	Find My Phone
Kismet	GadgetTrack
Netstumbler	iHound
MAC Flooding/Spoofing	
Macof	TROJANS AND MALWARE
SMAC	Wrappers
ARP Poisoning	Elite Wrap
Cain	Monitoring Tools
UfaSoft	HiJackThis
WinARP Attacker	CurrPorts
	Fport
WEB ATTACKS	Attack Tools
Wfetch	Netcat
Httprecon	Nemesis
ID Serve	IDS
WebSleuth	Snort
Black Widow	Evasion Tools
CookieDigger	
Nstalker	
NetBrute	
SQL Injection	

BSQL Hacker	ADMutate
Marathon	NIDSBench
SQL Injection Brute	IDSInformer
SQL Brute	Inundator
SQLNinja	
SQLGET	

The information in this cheat sheet is not only useful for passing the Certified Ethical Hacker Exam, but can act as a useful reference for penetration testers and those pursuing other security certifications.

However you choose to use it, we hope you've found it a helpful resource to keep around.