CEH V9 NOTES

https://dadsmancave.wordpress.com/2016/07/10/ceh-v9-notes/

This is the small (and I hope) useful cheat sheet for the CEH V9 certification.

1. Introduction to Ethical Hacking

Basics

There are three main phases to a pen test:

preparation

assessment

conclusion

What is the hacking methodology?

Reconnaissance

Footprinting

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

Black box testing, the ethical hacker has absolutely no knowledge of the TOE. It's designed to simulate an outside, unknown attacker, takes the most amount of time to complete.

White box testing, pen testers have full knowledge of the network, system, and infrastructure they're targeting.

Gray box testing, is also known as partial knowledge testing. What makes this different from black box testing is the assumed level of elevated privileges the tester has. Whereas black box testing is generally done from the network administration level, gray box testing assumes only that the attacker is an insider.

Attack Types

EC Council broadly defines four attack types categories:

Operating system attacks Generally speaking, these attacks target the common mistake many people make when installing operating systems— accepting and leaving all the defaults. Things like administrator accounts with no passwords, all ports left open, and guest accounts (the list could go on forever) are examples of settings the installer may forget about.
Application-level attacks These are attacks on the actual programming codes of an application. Although most people are very cognizant of securing their OS and network, it's amazing how often they discount the applications running on their OS and network. Many applications on a network aren't tested for vulnerabilities as part of their creation and, as such, have many vulnerabilities built into them. Applications on a network are a goldmine for most hackers.
Shrink-wrap code attacks These attacks take advantage of the built-in code and scripts most off-the-shelf applications come with. These scripts and code pieces are designed to make installation and administration easier, but can lead to vulnerabilities if not managed appropriately.
Misconfiguration attacks These attacks take advantage of systems that are, on purpose or by accident, not configured appropriately for security.
An asset is an item of economic value owned by an organization or an individual. Identification of assets within the risk analysis world is the first and most important step.

A threat is any agent, circumstance, or situation that could cause harm or loss to an IT asset.

A vulnerability is any weakness, such as a software flaw or logic design, that could be exploited by a threat to cause damage to an asset.

18 U.S.C § 1029

Basically, the law gives the U.S. government the authority to prosecute criminals who traffic in, or use, counterfeit access devices. In short, the section criminalizes the misuse of any number of credentials, including pass- words, PIN numbers, token cards, credit card numbers, and the like.

18 U.S.C § 1030

This law prosecutes criminals that use computers to access or misrepresent themselves as someone else. This is the all encompassing committing a crime using a computer or performing hacking activities without prior approval.

Ports and Protocols

The port numbers range from 0 to 65,535 and are split into three different groups:

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

Some of the more important well-known port numbers to remember are:

FTP (20/21)
Telnet (23)
SMTP (25)
DNS (53/TCP – Zone Transfers 53/UDP – Queries)

Kerberos – 88
POP3 (110)
NetBIOS (137–139)
SNMP (161 – Management /162 – Traps)

LDAP – 389

CIFS/SMB Shares – 445

RADIUS/Diameter – 1812/1813

ISO/OSI layers

Application – data
Presentation – data
Session – data
Transport – segment
Network – packet
Data -frames
Physical – bytes

All Peoples Seems To Need Data Processing – mnemonic phrase to remember the layers.

Passwords

EC-Council rules for the passwords:

The password must not contain any part of the user's name. For example, a password of "KevinR0ck$!" wouldn't work for the CEH exam, because you can clearly see my name there.
The password must have a minimum of eight characters. Eight is okay. Nine is better. Seven? Not so good.
The password must contain characters from at least three of the four major components of complexity—that is, special symbols (such as @&*#$), uppercase letters, lowercase letters, and numbers. U$e8Ch@rs contains all four, whereas use8chars uses only two.
LM Hashing – 7 spaces hashed = AAD3B435B51404EE

Attack Types

Four main attack types are defined within CEH.

passive online attack basically amounts to sniffing a wire in the hopes of either intercepting a password in clear text or attempting a replay or man-in- the-middle (MITM) attack.
active online, occurs when the attacker begins simply trying passwords—guessing them, for lack of a better word
offline attacks occur when the hacker steals a copy of the password file (remember our discussion on the SAM file earlier?) and works the cracking efforts on a separate system.
non-electronic = the social engineering.
sidejacking. The idea is to steal the cookies exchanged between two systems and ferret out which one to use as a replay-style attack

Physical Security

Human-Based Attacks

Dumpster diving
Impersonation
Technical support
Shoulder surfing
Tailgating and piggybacking

Computer-Based Attacks
phishing.

Three major categories of physical security measures:

Physical measures include all the things you can touch, taste, smell, or get shocked by. For example, lighting, locks, fences, and guards with Tasers are all physical measures. Technical measures are a little more com- plicated. These are measures taken with technology in mind, to protect explicitly at the physical level. For example, authentication and permissions may not come across as phys- ical measures, but if you think about them within the context of smart cards and bio- metrics, it's easy to see how they should become technical measures for physical security.
Operational measures are the policies and procedures you set up to enforce a security-minded operation.

2. Footprinting and Reconnaissance

FOR ECCouncil Vulnerability Research is part of the reconnaissance.

Difference in definition between reconnaissance and footprinting:

For many, recon is more of an overall, over-arching term for gathering information on targets, whereas footprint- ing is more of an effort to map out, at a high level, what the landscape looks like. They are interchangeable terms in CEH parlance, but if you just remember that footprinting is part of reconnaissance.

DNS is using port 53; Name lookups generally use UDP, whereas zone transfers use TCP.

DNS record types:

SRV– Service Defines the host name and port number of servers providing specific services, such as a Directory Services server.
SOA – Start Of Authority This record identifies the primary name server for the zone.The SOA record contains the host name of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.
PTR – Pointer Maps an IP address to a host name (providing for reverse DNS lookups).You don't absolutely need a PTR record for every entry in your DNS namespace, but these are usually associated with e-mail server records.
NS – Name Server This record defines the name servers within your namespace.These servers are the ones that respond to your clients' requests for name resolution.
MX -Mail Exchange This record identifies your e-mail servers within your domain.
CNAME – Canonical Name This record provides for domain name aliases within your zone. For example, you may have an FTP service and a web service running on the same IP address. CNAME records could be used to list both within DNS for you.
A – Address This record maps an IP address to a host name, and is used most often for DNS lookups.
DNS Footprinting tools: whois, nslookup, dig

3. Scanning Networks

Seven generic scan types for port scanning:

TCP Connect Runs through a full connection (three-way handshake) on all ports. Easiest to detect, but possibly the most reliable. Open ports will respond with a SYN/ACK, closed ports with a RST/ACK.
SYN Known as a "half-open scan." Only SYN packets are sent to ports (no completion of the three-way handshake ever takes place). Open ports will respond with a SYN/ACK, closed ports with a RST/ACK.
FIN scans run the communications setup in reverse, sending a packet with the FIN flag set. Closed ports will respond with RST, whereas open ports won't respond at all.
XMAS A Christmas scan is so named because the packet is sent with multiple flags (FIN, URG, and PSH) set. Closed ports will respond with RST, whereas open ports won't respond at all
ACK Used mainly for Unix/Linux-based systems. Open ports will send RST, closed ports, no answer
IDLE Uses a spoofed IP address to elicit port responses during a scan. Designed for stealth, this scan uses a SYN flag and monitors responses as with a SYN scan.
NULL Almost the opposite of the XMAS scan. The NULL scan sends packets with no flags set. Responses will vary, depending on the OS and version, but NULL scans are designed for Unix/Linux machines.
War dialing is a process by which an attacker dials a set of phone numbers specifi- cally looking for an open modem.

The MAC address that is burned onto a NIC is actually made of two sections.The first half of the address, 3 bytes (24 bits), is known as the Organizational Unique Identifier, and is used to identify the card manufacturer.The second half is a unique number burned in at manufacturing, to ensure no two cards on any given subnet will have the same address.

MAC Spoofing Set the MAC address of a NIC to the same value as another

MAC Flooding Overwhelm the CAM (content addressable memory) table of the switch so it coverts to hub mode

ARP Poisoning Inject incorrect information into the ARP caches of two or more endpoints.

INTERNET CONTROL MESSAGE PROTOCOL

ICMP is a transport protocol that creates message datagrams that can be exchanged by network hosts for troubleshooting, error reporting, and information.

ICMP HEADER EXAMPLE:

Type	Code	Description
0	0	Echo Reply
3		Destination Unreachable
3	13	Administratively Prohibited
8	0	Echo Request
5	0	Redirect
11	0	Time Exceeded

Don’t forget!!

Type 3 Code 13 means administratively prohibited

The TCP header flags are:

URG (Urgent) When this flag is set, it indicates the data inside is being sent out of band.
ACK (Acknowledgment) This flag is set as an acknowledgment to SYN flags. This flag is set on all segments after the initial SYN flag.
PSH (Push) This flag forces delivery of data without concern for any buffering.
RST (Reset) This flag forces a termination of communications (in both directions).
SYN (Synchronize) This flag is set during initial communication establishment. It indicates negotiation of parameters and sequence numbers.
FIN (Finish) This flag signifies an ordered close to communications.

Response type:

FIN Scan – No Response = Open Port RST/ACK = Closed Port

XMAS Scan – No Response = Open Port RST/ACK = Closed Port

NULL Scan – No Response = Open Port RST/ACK = Close Port

NMAP

Nmap is the de-facto tool for footprinting networks. It is capable of finding live hosts, access points, fingerprinting

operating systems, and verifying services. It also has important IDS evasion capabilities.

nmap <scan options> <target>

Scan Types	
`-sP`	Probe only (host discovery, not port scan)
`-sS`	SYN Scan
`-sT`	TCP Connect Scan
`-sU`	UDP Scan
`-sV`	Version Scan
`-O`	OS Detection
`--scanflags`	Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

Aggregate Timing Options	
`-T0`	*Paranoid:* Very slow, used for IDS evasion
`-T1`	*Sneaky:* Quite slow, used for IDS evasion
`-T2`	*Polite:* Slows down to consume less bandwidth, runs ~10 times slower than default
`-T3`	*Normal:* Default, a dynamic timing model based on target responsiveness
`-T4`	*Aggressive:* Assumes a fast and reliable network and may overwhelm targets
`-T5`	*Insane:* Very aggressive; will likely overwhelm targets or miss open ports

Probing Options	
`-Pn`	Don't probe (assume all hosts are up)
`-PB`	Default probe (TCP 80, 445 & ICMP)
`-PS<portlist>`	Check whether targets are up by probing TCP ports
`-PE`	Use ICMP Echo Request
`-PP`	Use ICMP Timestamp Request
`-PM`	Use ICMP Netmask Request

Wireshark display filters

Display filters work basically like: proto.field operator value

Analyse the following examples:

tcp.flags == 0x29
ip.addr != 192.168.1.1
tcp.port eq 25 or icmp
ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16
http.request.uri matches “login.html”

Tcpdump syntax:

tcmdump flag(s) interface

4. Enumeration

SNMP

Simple Network Management Protocol was designed to manage IP-enabled devices across a network. As a result, if it is in use on the subnet, you can find out loads of information with properly formatted SNMP requests. Later versions of SNMP make this a little more difficult, but plenty of systems out there are still using the protocol in version 1.

5. System Hacking

6. Malware Threats

Trojans and Other Attacks

Windows will automatically run everything located in Run, RunServices, RunOnce, and RunServicesOnce

Virus types:

Boot sector virus Also known as a system virus, this virus type actually moves the boot sector to another location on the hard drive, forcing the virus code to be executed first. They’re almost

impossible to get rid of once you get infected. You can re-create the boot record—old-school fdisk or mbr could do the trick for you—but it's not necessarily a walk in the park.

RootKit A rootkit is a type of program often used to hide utilities on a compromised system. Typically runs at the Kernel or Library level. Requires reimage from known good media to remove.
Shell virus Working just like the boot sector virus, this virus type wraps itself around an application's code, inserting its own code before the application's. Every time the application is run, the virus code is run first.
Multipartite virus Attempts to infect both files and the boot sector at the same time. This generally refers to a virus with multiple infection vectors. .
Macro virus Usually written with VBA (Visual Basic for Applications), this virus type infects template files created by Microsoft Office—normally Word and Excel. The Melissa virus was a prime example of this.
Polymorphic code virus This virus mutates its code using a built-in polymorphic engine. These viruses are very difficult to find and remove because their signatures constantly change.
Metamorphic virus This virus type rewrites itself every time it infects a new file.

DOS attack types:

SYN attack The hacker will send thousands upon thousands of SYN packets to the machine with a false source IP address. The machine will attempt to respond with a SYN/ACK but will be unsuccessful (because the address is false). Eventually, all the machine's resources are engaged and it becomes a giant paperweight.
SYN flood In this attack, the hacker sends thousands of SYN packets to the target, but never responds to any of the return SYN/ACK packets. Because there is a certain amount of time the target must wait to receive an answer to the SYN/ACK, it will eventually bog down and run out of available connections.
ICMP flood Here, the attacker sends ICMP Echo packets to the target with a spoofed (fake) source address. The target continues to respond to an address that doesn't exist and eventually reaches a limit of packets per second sent.
Application level A simple attack whereby the hacker simply sends more "legitimate" traffic to a web application than it can handle, causing the system to crash.
Smurf The attacker sends a large number of pings to the broadcast address of the subnet, with the source IP spoofed to that of the target. The entire subnet will then begin sending ping responses to the target, exhausting the resources there. A **fraggle** attack is similar, but uses UDP for the same purpose.
Ping of death In the ping of death, an attacker fragments an ICMP message to send to a target. When the fragments are reassembled, the resultant ICMP packet is larger than the maximum size and crashes the system.

7. Sniffing

8. Social Engineering

Types of Social Engineers

Insider Associates Have limited authorized access, and escalate privileges from there.
Insider Affiliates Are insiders by virtue of an affiliation, they spoof the identity of the insider.
Outsider Affiliates Are nonTtrusted outsiders that use an access point that was left open.
Physical Security

9. Denial-of-service

10. Session Hijacking

11. Hacking Web Servers

Web-Based Hacking

This dot-dot-slash attack (directory traversal) is also known as a variant of “Unicode” or unvalidated input attack.

12. Hacking Web Applications

13. SQL Injection

SQL injection attacks types:

Union query The thought here is to make use of the UNION command to return the union of your target database with one you’ve crafted to steal data from it.
Tautology An overly complex term used to describe the behavior of a database system when deciding whether or not a statement is true. Because user IDs and passwords are often compared, and the “true” measure allows access, if you trick the database by providing something that is already true (1 does, indeed, equal 1), then you can sneak by.
Blind SQL injection This occurs when the attacker knows the database is susceptible to injection, but the error messages and screen returns don’t come back to the attacker. Because there’s a lot of guesswork and trial and error, this attack takes a long while to pull off.
Error-based SQL injection This isn’t necessarily an attack so much as an enumeration technique. The objective is to purposely enter poorly constructed statements in an effort to get the database to respond with table names and other information in its error messages.

The buffer overflow attack categories are as follows:

Stack This idea comes from the basic premise that all program calls are kept in a stack and executed in order. If you affect the stack with a buffer overflow, you can perhaps change a function pointer or variable to allow code execution.
Heap Also referred to as heap overflow, this attack takes advantage of the memory "on top of" the application, which is allocated dynamically at runtime. Because this memory usually contains program data, you can cause the application to overwrite function pointers.
NOP Sled A NOP sled makes use of a machine instruction called "no-op." In the attack, a hacker sends a large number of NOP instructions into the buffer, appending command code instruction at the end. Because this attack is so common, most IDSs protect against it.

Dangerous Functions for buffer overflows

The following functions are dangerous because they do not check the size of the destination buffers:

gets()
strcpy()
strcat()
printf()

14. Hacking Wireless Networks

Wireless Network hacking

802.11 Specifications

Spec Distance Speed Freq

802.11a 30M 54Mbps 5Ghz
802.11b 100M 11Mbps 2.4Ghz
802.11g 100M 54Mbps 2.4Ghz
802.11n 125M 100Mbps+ 2.4Ghz, 5Ghz

WEP Uses RC4 for the stream cipher with a 24b initialization vector

Key sizes are 40b or 104b

WPA Uses RC4 for the stream cipher but supports longer keys; 48 bits IV
WPA/TKIP Changes the IV with each frame and includes key mixing
WPA2 Uses AES as the stream cipher and includes all the features of TKIP; 48 bits IV.

Rogue APs (evil twins) may also be referenced as a “mis- association” attack.

15. Hacking Mobile Platforms

Bluetooth attacks :

Bluesmacking is simply a denial-of-service attack against a device.
Bluejacking consists of sending unsolicited messages to, and from, mobile devices.
Bluesniffing is exactly what it sounds like, and, finally.
Bluescarfing is the actual theft of data from a mobile device.

War driving used to refer to, quite literally, driving around in a car, 35mph or less, looking for open access points. In the ethical hacking realm, it still indicates a search for open WAP

16. Evading IDS, Firewalls and Honeypots

Snort rule:

alert tcp !HOME_NET any -> $HOME_NET 31337 (msg :”BACKDOOR ATTEMPT-Backorifice”)

If you happen to come across a packet from any address that is not my home network, using any source port, intended for an address within my home network on port 31337, alert me with the message ‘BACKDOOR ATTEMPT-Back- orifice.’”

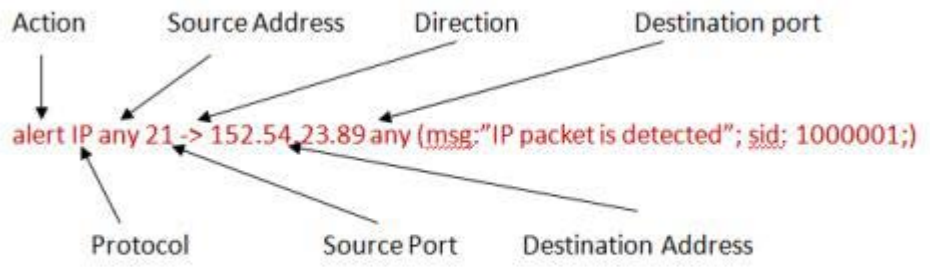

Figure 5. A Snort rule example.

Span port = port mirroring

False negative – when an IDS reports a particular stream as clean but it’s not

17. Cloud Computing

NIST Cloud Computing Reference

Cloud Consumer – Person or Organization that uses cloud computing services

Cloud Provider – Person or Organization that providing services to interested parties

Cloud Carrier – Intermediary for providing connectivity and transport services between cloud consumers and providers

Cloud Auditor – A party for making independent assessments of cloud service controls and taking an opinion thereon

Cloud Broker – An entity to manage cloud services in terms of use, performance, and delivery who also maintains a relationship between cloud providers and consumers.

18. Cryptography

Symmetric Encryption – The formula for calculating how many key pairs you will need is N (N – 1) / 2 where N is the number of nodes in the network

Symmetric algorithms:

DES A block cipher that uses a 56-bit key (with 8 bits reserved for parity); fixed blocked size.
3DES A block cipher that uses a 168-bit key. 3DES (called triple DES) can use up to three keys in a multiple-encryption method.
AES (Advanced Encryption Standard) A block cipher that uses a key length of 128, 192, or 256 bits, and effectively replaces DES.
IDEA (International Data Encryption Algorithm) A block cipher that uses a 128-bit key.
Twofish A block cipher that uses a key size up to 256 bits.
Blowfish A fast block cipher, largely replaced by AES, using a 64-bit block size and a key from 32 to 448 bits.
RC (Rivest Cipher) Encompasses several versions from RC2 through RC6. A block cipher that uses a variable key length up to 2,040 bits. RC6, the latest version, uses 128-bit blocks, whereas RC5 uses variable block sizes (32, 64, or 128).

Asymmetric Encryption

Generally: public key = encrypt, private key = decrypt.

Asymmetric algorithms:

Diffie-Hellman Developed for use as a key exchange protocol, Diffie- Hellman is used in Secure Sockets Layer (SSL) and IPSec encryption.
Elliptic Curve Cryptosystem (ECC) Uses points on an elliptical curve, in conjunction with logarithmic problems, for encryption and signatures. Uses less processing power than other methods, making it a good choice for mobile devices.
El Gamal Not based on prime number factoring, this method uses the solving of discrete logarithm problems for encryption and digital signatures.
RSA An algorithm that achieves strong encryption through the use of two large prime numbers. Factoring these numbers creates key sizes up to 4,096 bits. RSA can be used for encryption and digital signatures and is the modern de facto standard.

Hash algorithms:

MD5 (Message Digest algorithm) Produces a 128-bit hash value output, expressed as a 32-digit hexadecimal.
SHA-1 Developed by the NSA (National Security Agency), SHA-1 produces a 160-bit value output, and was required by law for use in U.S. government applications.
SHA-2 Developed by the NSA, actually holds four separate hash functions that produce outputs of 224, 256, 384, and 512 bits.

Trust Models

web of trust, multiple entities sign certificates for one another.
single authority system has a CA at the top that creates and issues certs. Users trust each other based on the CA itself.
hierarchical trust system also has a CA at the top (which is known as the root CA), but makes use of one or more intermediate CAs underneath it— known as registration authorities (RAs)— to issue and manage certificates.

Cryptography Attacks:

Known plaintext attack In this attack, the hacker has both plaintext and corresponding ciphertext messages—the more, the better. The plaintext copies are scanned for repeatable sequences, which are then compared to the ciphertext versions. Over time, and with effort, this can be used to decipher the key.
Ciphertext-only attack In this attack, the hacker gains copies of several messages encrypted in the same way (with the same algorithm). Statistical analysis can then be used to reveal, eventually, repeating code, which can be used to decode messages later on.
Replay attack Most often performed within the context of a man-in-the- middle attack. The hacker repeats a portion of a cryptographic exchange in hopes of fooling the system into setting up a communications channel. The attacker doesn't really have to know the actual data (such as the password) being exchanged, he just has to get the timing right in copying and then

replaying the bit stream. Session tokens can be used in the communications process to combat this attack.

A digital certificate is an electronic file that is used to verify a user's identity, providing non-repudiation throughout the system.

Version This identifies the certificate format.. The most common version in use is 1.
Serial Number Fairly self-explanatory, the serial number is used to uniquely identify the certificate itself.
Subject Whoever or whatever is being identified by the certificate.
Algorithm ID (or Signature Algorithm) Shows the algorithm that was used to create the digital signature.
Issuer Shows the entity that verifies the authenticity of the certificate. The issuer is the one who creates the certificates.
Valid From and Valid To These fields show the dates the certificate is good through.
Key Usage Shows for what purpose the certificate was created.
Subject's Public Key A copy of the subject's public key is included in the digital certificate.
Optional fields These fields include Issuer Unique Identifier, Subject Alternative Name, and Extensions.