Introduction To Ethical Hacking

Created by : Chris Taylor

Synopsis:

This course will teach you everything from the prerequisites of ethical hacking to skills you need. You will learn the difference in tactics between Red Teamers and Penetration Testers. Learn how to perform both passive and active reconnaissance, networking, exploitation, and a whole lot more.

$WHOAMI

Name: Chris Taylor [Blue Cosmo]

Occupation:

- CEO of CosmodiumCS
- Security Educator for Artem NexGen
- Malware Developer
- Youtuber and Hacker

Socials:

- Website
- YouTube
- GitHub

Foundations: [REQUIREMENTS]

- Introduction to CyberSecurity Course
- Linux Fundamentals
- Security Linux Operating System
  - Kali Linux
  - Parrot OS

STAGE-00 // INTRODUCTORY CONCEPTS

What Is Ethical Hacking?

The use of hacking to find vulnerabilities in client systems before black hat hackers do. This way, clients can fix those vulnerabilities and become more secure.

The scheduled event where a ethical hacker finds these vulnerabilities is called an engagement.

Types Of Ethical Hackers:

Red Teamer:

- Lower level clientele is unaware of engagement. Permission for the engagement was permitted by higher level authorities.

Penetration Tester:

- Lower level clientele is aware of engagement. Permission for the engagement was permitted by the client in general.

Engagements:

1. Physical
    a. Physically testing the security of a client. Showing up to a location and acting as how a black hat would act. “Breaking in” and finding vulnerabilities and information on the client.
2. Digital
    a. Remotely testing the security of a client. Testing the security of websites and servers and attempting to discover any vulnerabilities.
3. Institutional
    a. Testing the vulnerabilities within the client organization itself. How easy is it to enter the building, plug malicious USB’s in, etc.

The Five Stages Of A Hack:

1. Reconnaissance
    a. Gaining information on a target
2. Scanning and Enumeration
    a. Obtaining a brief blueprint about the network on a target
3. Gaining Access
    a. Getting access into a target
4. Maintaining Access
    a. Being able to keep your access to a target
5. Covering Tracks
    a. Removing all traces of your presence

Legal:

To keep engagements legal, clients can create a “scope” or “rules of engagement”. It is a limitation on what an ethical hacker can and can not target.

We must also understand that we are hacking with ethical intentions. So we need keep things like legal documents in mind.

De-Escalation Policy:

This document ensures your safety as an Ethical Hacker in the event of you getting caught during an engagement. It ensures the clientele that you are authorized to be performing the engagement, and that you are not a malicious threat.

Non Disclosure Agreement: [NDA]

This contract states that you can’t share any sensitive information related to the engagement with any person or entity.

Sharing any information related to the engagement will have severe consequences for you, your client, and the company you work for.

Reporting:

After an Ethical Hacker performs an engagement, they need to write up a report on the vulnerabilities discovered and how they were discovered.

Reports include:

- Security flaws and vulnerabilities
- What the client did well
- The output of scans showing how we discovered vulnerabilities

We can examine this example report created by The Cyber Mentor

STAGE-01 // PASSIVE RECONNAISSANCE

Passive Reconnaissance:

Passive reconnaissance is the process of getting as much information as possible on a client without directly engaging with them.

- Takes more time
- Provides better vision of target
- Necessary for successful engagement

Open Source Intelligence: [OSINT]

A passive reconnaissance method of using the internet to discover information on a client.

- Searching information on client
- Client website
- Social media
- Google dorking
- Google maps

Google Dorking:

Google is the best search engine we can use for passive reconnaissance. With Google, we can add certain syntax to our searches to filter search results. This process is called Dorking.

SYNTAX	DESCRIPTION
site:	Specify website
intitle:	Specify content in html title
inurl:	Specify URL path contents
ext:	Specify file extensions results

Google Maps:

Before we conduct active reconnaissance [for a physical engagement], we can use Google Maps to analyze the client location.

Things to look for:

- Cameras
- Entry points
- Building layout

Other Passive Reconnaissance Tactics:

- Keep track of information, employees, vectors, etc. that you find
- Use HaveIBeenPwned to see if client emails have been compromised.
- Wappalyzer
- Sherlock

STAGE-02 // NETWORKING BASICS

Internet Protocol [IP] Address:

- The “address” of a computer
- Two types:
    1. Public
        a. Available for others on the network to see
    2. Private
        a. A globally identifiable address

IPV4 - X.X.X.X

IPV6 - XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

IPV4:

- Each octet ranges from 0–255
- 192.168.1.0 & 172.22.0.1 are default network addresses
- Your public address will likely share the first 3 octets of one of the aforementioned addresses
- We can shortcut multiple addresses that share octets into a subnet

Port:

- The area allocated on a device to host a process across the network
- Represented by a number
- Specified with a colon
- There are 65,353 ports on a machine
    - Some may be open, some may be closed

192.168.1.22:443

Networking Basics:

Networking

- how interconnected computers operate

Protocol

- A set of rules that govern how systems communicate

Stack

- A collection of protocols that work together

Protocols	Standing	Description	Port
HTTP	Hypertext Transfer Protocol	Allows computers to access the web	80
HTTPS	Secure Hypertext Transfer Protocol	A more secure version of HTTP	443
FTP	File Transfer Protocol	Transfer files between computers	21
SSH	Secure Shell	Remotely access a computer	22
TCP	Transmission Control Protocol	Allows computers to connect	
UDP	User Datagram Protocol	Connectionless protocol	
IP	Internet Protocol [v4/v6]	Main networking protocol	
SMTP	Simple Mail Transfer Protocol	Sends emails	24,456,587
ARP	Address Resolution Protocol	Connect an IP address to a Media Access Control [MAC] address	

3 Way Handshake:

SYN

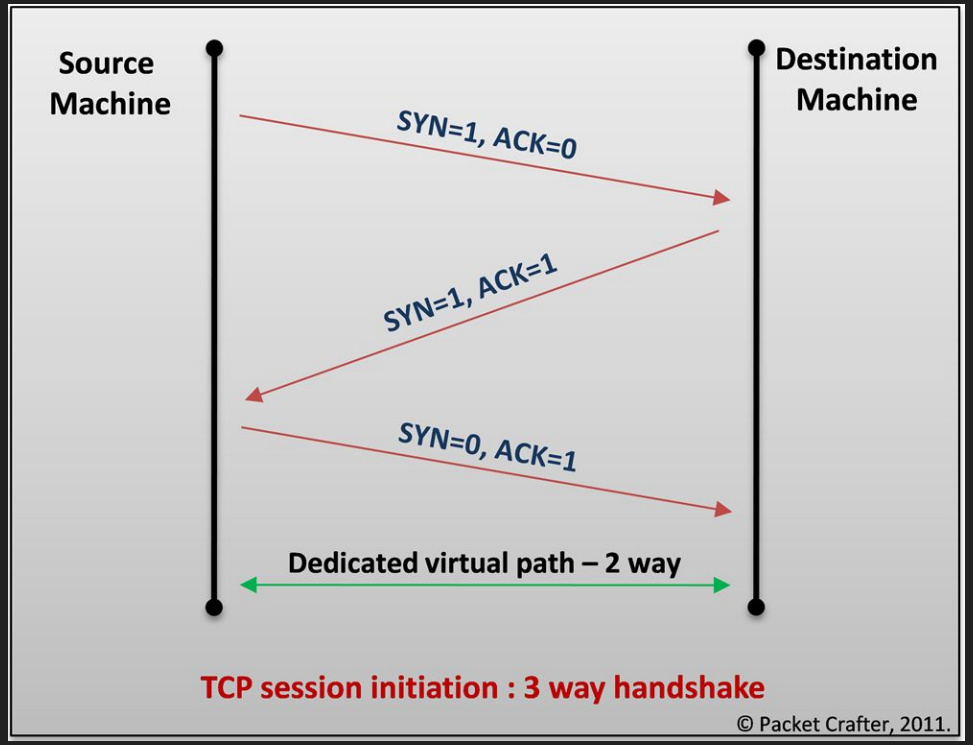
- Synchronize

ACK

- Acknowledge

ISN

- Initial Sequence Number



TCP v UDP:

TCP

- Uses 3 way handshake
- Standard connections
- Example protocols: http, ftp, ssh

User Datagram Protocol

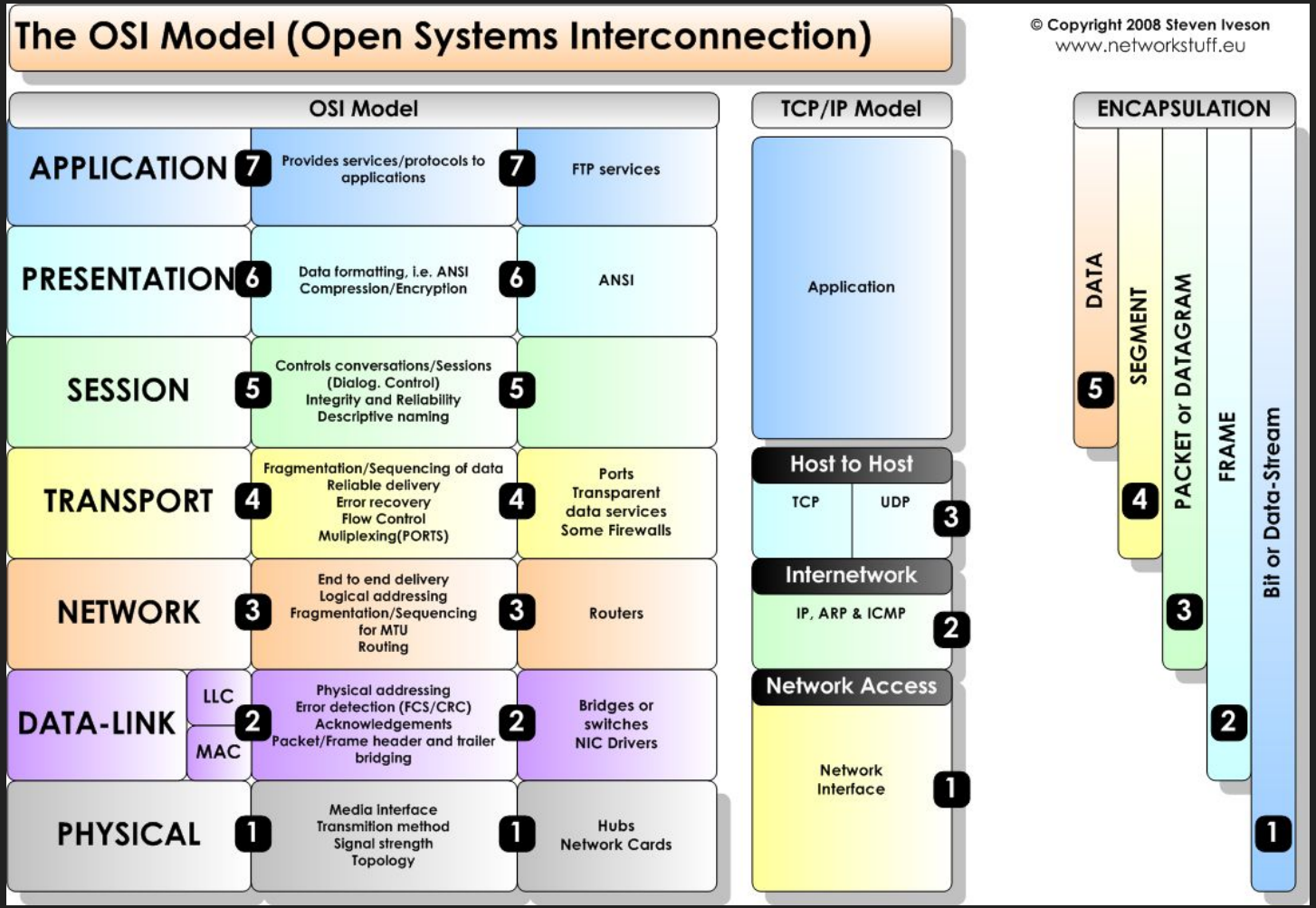
- Doesn’t use handshake
- Fast connections
- Example protocols: dns, snmp, dhcp

Models:

- The approach used in networking is to create a suite in the form of layered protocol stacks.
- Each layer performs a specific operation

Models:

- TCP/IP [4 layer model]
  - Transmission Control Protocol / Internet Protocol
- OSI Model [7 Layer model]
  - Open Systems Interconnection



STAGE-03 // ACTIVE RECONNAISSANCE

Active Reconnaissance:

The process of gaining as much information off of a client as possible by directly engaging with them.

One of the tactics we can use is called scanning. Scanning is the process of analyzing network infrastructure, getting information on the layout, devices, servicer versions, ports, and other network related information.

Netdiscover:

A scanning tool that performs Address Resolution Protocol [ARP] reconnaissance.

ARP is a mapping protocol that attaches the IP address of a physical machine to a MAC address.

NMAP Basics:

NMAP [Network Mapper] is a tool we can use to scan and get a layout of the network. We can use this to discover devices, service versions, and ports on a client's network.

Stage Scanning:

Stage scanning is a concept where we perform a scan in stages. Scanning can take a very long time, so by breaking our scan into steps, we can more easily perform larger scans.

We must first scan all the ports on the network, simply to see what ports are open. From there we can aggressively scan the open ports to gain as much information as possible. You may also use this script to automate the process.

Social Engineering:

Social engineering is the art hacking people. An attacker can get confidential information by using their social skills and manipulating a victim. This requires an understanding of sociology, psychology, and honestly… being a good liar

STAGE-04 // ENUMERATION

Enumeration:

Enumeration is essentially the process of discovering vulnerabilities on a clients system. This stage of the ethical hack is often the longest yet most important step.

Nikto

Nikto is a vulnerability scanner for websites. This great for our enumeration stage so we can discover possible vulnerabilities we can exploit.

```
nikto -h https://example.com
```

STAGE-05 // GAINING ACCESS

Gaining Access: [Exploitation]

Gaining unauthorized access to a system is the literal definition of hacking. Meaning this stage is where the actual hack occurs.

We can obtain access in one of two ways, locally and remotely.

Obtaining Local Access:

- need to be on the same network as client
- need to have physical access to the network
- can serve difficult when attempting to avoid difficulties
  - security guards
  - cameras
  - firewalls
  - anti-virus [AV]
- tactics like social engineering and hardware hacking tools may serve useful

Obtaining Remote Access:

- Obtained remotely over the internet
- More anonymized
- Easier **if** vulnerability is found
- Works through the use of shells

Hak5:

Hak5 is a penetration testing hardware company that sells tools that penetration testing, red teaming, system administrators, and other security professionals use alike.

Let’s explore some of their tools

USB Rubber Ducky:

A USB device that acts like a keyboard. It can inject keystrokes at a super fast speed and its known as a Human Interface Device [HID] device.

LAN Turtle:

This piece of tech is a device used to plug into a network and get a shell the second you do, it's a covert system administration and penetration testing tool.

Bash Bunny:

This device can emulate plenty of other USB devices. Things like keyboards, ethernet, serial, and other devices.

SharkJack:

This tool that you plug into an ethernet port and can have it perform network related tasks. It can scan networks, become a hardware backdoor, and so much more!

Wi-Fi Pineapple:

The Wi-Fi Pineapple is a Wi-Fi auditing tool. It can create rogue access points that clients can connect to so we can monitor network traffic. We can also use it to gain access to the network by cracking WPA2 passwords.

Shells:

A shell is a remote terminal. We can obtain shells in two ways:

1. Bind Shell
    a. Attacker computer connects to client computer
2. Reverse Shell
    a. Client computer connects to attacker computer

In order to get our shell, we need to set up a listener. A listener will listen on a certain port and wait for our connecting computer to make a connection.

NetCat:

NetCat is a tool we can use to set up a listener for our shell. In bind shells the listener is set up on the client computer. In reverse shells in the listener is set up on the attacker computer. We can then connect to the listener on an opposing computer.

Bind Shell	nc -lnvp PORT -e /bin bash
Reverse Shell	nc -lnvp PORT
Connecting	Nc HOST PORT

STAGE-06 // MAINTAINING ACCESS

Shell Stabilization:

When we get our shells, we may need to stabilize them in order for them to become more ideal for use. We can use the following syntax:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'

export TERM=xterm

“ctrl” + “z”

stty raw -echo; fg
```

Backups:

- Make backups of important files we may manipulate
- Since this is ethical, we may need to restore certain files

Persistence

Since this is an Ethical Hacking course, we will not be teaching you how to perform persistence. However, persistence is our ability to maintain access, so the hacker can connect back to the client at any time.

Privilege Escalation: [PrivEsc]

More often than not, we don’t have root permissions when we first gain access. In order to get higher access, we need to perform PrivEsc. This is the process of getting more privileges.

PEASS

PEASS is a tool we can use to escalate our privileges. There are two versions, LinPEASS [Linux clients] and WinPEASS [Windows clients]. We can remotely upload these files to find vulnerabilities in our target system.

STAGE-07 // POST ENGAGEMENT AND RESOLUTION

Post Engagement:

Once we finish the engagement, we need to clean up the client network. If we leave our malware, scripts, admin accounts on the network… it leaves it vulnerable to black hat hackers

Things to clean up:

- Remove malware and scripts
- Delete any accounts we may have made
- Remove backdoors and remote access vectors
- Basically, revert it back to how it originally was

Conclusion:

All in all, this course should have taught you the basics of ethical hacking. You know can be prepared to have the basic skill sets needed to practice ethical hacking professionally. But these are just the basics. Keep learning, keep growing, and as always,

Happy Hacking!

Thank You!

SUBSCRIBE