Study Guide

Penetration Testing and Ethical Hacking

Created By: Alec Mather-Shapiro, Teaching Assistant

Module 1: Introduction

Lesson 1.0: Introduction EH

Skills Learned From This Lesson: Course preparation, Course Outline

- Instructor Ken Underhill CEH, CHFI
- Modules are listed
- Course Structure
  - Pre-assessment, Post-assessment

Lesson 1.1: CIA Black White Grey Hats EH

Skills Learned From This Lesson: Methodology, CIA Triad, The Hats. IAM, Red/Blue

- Prerequisites: Basic networking, understanding of operating systems, security, understanding of mobile
- Methodology
  - Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks
- The Hats
  - Black - Criminal Hackers
  - White - Pen Testers, Good Guys
  - Grey - Somewhere in the middle. May be helping but unauthorized
- The Boxes:
  - Black Box Testing: Completely blind testing. Simulates a true attacker situation
  - White Box Testing: Simulates insider threat level.
  - Grey Box Testing:User level. Some access but no knowledge
- Identity And Access Management - “Giving the right people the right access at the right time”
- Red/Blue

  - Blue is the defense
  - Red is the offense
- CIA Triad
  - Confidentiality - Only the people who need access have it
  - Integrity - The data is valid and not altered
  - Availability - The information is available when we need it
- Authentication: Something you are, something you have, something you know
- Nonrepudiation: I can prove you did it

Lesson 1.2: Laws EH

Skills Learned From This Lesson: High level view of laws, Application of each type

- HIPPA - Protects private medical information
- PCI-DSS - Process and store cardholder data. Great for securing other industries
- SOX - Protects investors- Auditing for financial reporting
- DMCA - Copyright act. Protects content like Cybrary
- FISMA - Requires Information Security Programs in the federal systems
- IOC/IEC 27001: 2013 - Management needs to examine InfoSec risk. Design/Implement the risk mitigation strategy.

Lesson 1.3: Bonus VB and Kali EH

Skills Learned From This Lesson: Download VBox, Download Kali, Setting up a new NAT Network

- Use the Cybrary Pro Labs! They're used for this course
- Virtual Box Installer: https://www.virtualbox.org/wiki/Downloads
  - Get the extension pack as well (for Windows)
  - Might have missing NAT network
    - File - Preferences - Network - +sign "create NAT network"
    - Assign the network to the VM
- Kali Download: https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

Lesson 1.4: Password Crack Lab EH

Skills Learned From This Lesson: Create MD5 Hash, Using John the Ripper to Crack Hashes

- Creating an MD5 Hash
  - https://www.md5hashgenerator.com
- John the ripper syntax
  - john --format=raw-md5 /usr/share/wordlists/rockyou.txt.gz /root/Desktop/passw.txt
  - John *format-selection filePathForWordList LocationOfFileWithHashes*

Module 2: Footprinting

Lesson 2.0: Intro Pre-Assessment EH

Skills Learned From This Lesson: Active Footprinting, Passive Footprinting

- Use the Cybrary labs!
- Multiple types of Footprinting (Active, Passive)
- Active is interaction. Passive is no interaction
- Filetype:[string] for finding file type

Lesson 2.1: Footprinting EH

Skills Learned From This Lesson: Active/Passive Footprinting, Open Source Intelligence (OSINT), Shodan.io

- Active = interaction
  - Direct contact, Port Scan
- Passive = publicly available
  - Open Source Intelligence (OSINT)
- Benefits: Know Security Posture, Reduce focus area, vulnerability identification, network mapping
- Lots of ways to gather freely available information (OSINT)
  - Google, shodan, whois, social media, job boards …
- Google hacking to find freely available information
- Shodan is the “search engine for hackers”
- Set up alerts on companies (Visual ping)
- Tools: Maltego (intelligence gathering), Recon-ng, OSRFramework

Lesson 2.2: Lab Intro EH

Skills Learned From This Lesson: Google Hacking lab, Nikto Lab, Shodan lab, Harvester Lab

- Google Hacking lab:
  - Filetype: *type* - to find a specific filetype
- Shodan lab
- Nikto lab - Gather information from websites
- Harvester Lab - Gather company information

Lesson 2.3: Footprinting NIKTO EH

Skills Learned From This Lesson: Nikto Help, Nikto Scanning Websites, Basic nikto switches

- Lab document found in course supplemental materials
- Used to find vulnerabilities in websites
- Nikto -h for nikto help (truncated)
  - Nikto -H (everything)
- Nikto -e 1 -h webscantest.com
  - **-e** is an evasion switch
  - **1** is random encoding
  - **-h** defines hostname or IP address
- XSS - Cross Site Scripting

Lesson 2.4: Footprinting Harvester EH

Skills Learned From This Lesson: theharvester help file, theharvester switches,

- Lab document found in course supplemental materials
- Theharvester -h for help file
- theharvester -d microsoft.com -l 50 -b google.com -h myresults.html
  - **-d** is the domain or company
  - **-l** is the result limiter
  - **-b** defines the data source
  - **-h** allows us to use shodan database
- Used to find IP address, email address, and other information

Lesson 2.5: Footprinting Shodan EH

Skills Learned From This Lesson: Using shodan.io, shodan account registration, shodan filters

- Lab document found in course supplemental materials
- Allows you to find potentially vulnerable devices on the internet
- Needs a shodan account to access
- Basic search
  - “Cisco router” in the search box. Shows IP addresses from all over the world
  - Select a country to filter on
  - Select a city to filer on
  - Can shows usernames and passwords

Lesson 2.6: Footprinting Google Hacking EH

Skills Learned From This Lesson: Location of Google Hacking Database, GHDB Searching, GHDB searches

- Lab document found in course supplemental materials
- Google Hacking Database
- Use it to search for specific commands to use in Google
- **filetype: type** -searches for only files of a specific type.
    - Example: filetype: doc would return Microsoft Word documents
- **intitle: string** -searches for pages that contain the string in the title.
    - Example: intitle: login would return results with the word login in the title
- **inurl: string** -displays pages with the string in the URL.
    - Example: inurl:passwd would show all pages with the word passwd in the URL.
- **site: domain** -displays pages for a specific website or domain. Can be combined with other search terms.
    - Example: site:microsoft.com passwds would show all pages with the text passwds in the website.

Module 3: Scanning and Enumeration

Lesson 3.0: Scan Enumeration EH

Skills Learned From This Lesson: Scanning Methodology, TCPThree-way handshake, TCP Header Flags

- Scanning Methodology
- TCP Three-way handshake: SYN - SYN/ACK - ACK
- TCP Header Flags
  - Synchronize (SYN, Acknowledgement (ACK), Reset (RST), Finished (FIN)

Lesson 3.1: TCP Handshake EH

Skills Learned From This Lesson: SYN, SYN/ACK, ACK

- **Host A** sends SYN (with sequence number ie.100)
- **Host B** send SYN (unique sequence number ie. 300) /ACK (sequence number +1. Ie 101)
- **Host A** send ACK (unique sequence number +1 ie. 301)
- Then the session is established

Lesson 3.2: Banner Grab EH

Skills Learned From This Lesson: Fragmentation, ICMP Messages, Banner Grabbing, Vulnerability Scanners

- Use fragmentation to break up packets to get past Intrusion Detection Systems
- ICMP Messages: 0: Echo Reply, 3: Destination Unreachable, 8: Echo Request
- Various port scans
  - Full-open = TCP scan. Easy to detect
  - Half-open = Syn scan. Stealthy
  - Inverse TCP = no response if port is open
- Nmap is the network mapper
- Banner grabbing
  - We want to see what OS or services are in use
- DNS Zone Transfer can be used to get various pieces of information
- Source Routing the attacker forces the routing path
- Enumeration is discover of hosts, devices and/or services
- Common Vulnerability Scoring System (CVSS)
- Discover, Prioritize, Assess, Report, Remediate, Verify

Lesson 3.3: Live Systems Lab Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Using VNC Viewer

- Log into Cybrary Labs
- Select Ethical Hacker labs
- Use VNC viewer to connect to Kali

Lesson 3.4: Live Systems Lab Part 2 EH

Skills Learned From This Lesson: Opening Kali Terminal, Using ifconfig

- Click on root terminal to open the command line interface (CLI)
- Type ifconfig to view network information
- Ethernet interfaces = eth
- Loopback interface = lo
- IP Address is the IPv4 address besides inet under the eth interface

Lesson 3.5: Live Systems Lab Part 3 EH

Skills Learned From This Lesson: Using nmap help file, nmap -sn scanning,nmap resource document

- To open nmap help pages use: *nmap -h*
- Download the resource document that has the common nmap commands!
- nmap -sn 192.168.0.1/24
    - -sn is sending ping requests
    - 192.168.0.1/24 is the IP address range
- nmap is great for scanning for Pen Tests

Lesson 3.6: Live Systems Lab Part 4 EH

Skills Learned From This Lesson:Using the hping3 help file, Using the hping3, Clearing the Command line

- To open the hping3 help file use: *hping3 -h*
- Using *clear* on the command line will remove all previous input
- hping3 -1 192.168.0.1
    - -1 uses ping scans

Lesson 3.7: Port Check Lab 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Using VNC Viewer, Opening Kali Root Terminal

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Select *Performing a Scan for Open ports*
- Connect with VNC Viewer to Kali Machine

Lesson 3.8: Port Check Lab 2 EH

Skills Learned From This Lesson: Basic nmap scan, Reading nmap output

- nmap 192.168.0.1
  - Default Syn Scan on the machine with the IP of 192.168.0.1
  - Scans the top 1000 most common ports

Lesson 3.9 Port Check Lab 3 EH

Skills Learned From This Lesson: Basic hping3 Scan, hping3 Flags Reading hping3 Output

- hping3 -8 0-5000 192.168.0.1
  - -8 enables SCAN mode
  - 0-5000 sets range of ports
  - -S sets SYN flag
- hping3 ACK responses

Lesson 3.10: Scanning Techniques Lab Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Using XAMPP Console, Using ipconfig

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Select *Implementing Scanning Techniques* lab
- Open the XAMPP console to enable Apache Web Services on port 80
- To find IP address inWindows: Open a command prompt (cmd.exe) and type *ipconfig*

Lesson 3.11: Scanning Techniques Lab Part 2 EH

Skills Learned From This Lesson: Using VNC Viewer, Opening Kali Root Terminal, nmap TCP SYN scan

- nmap -sS 192.168.0.1
    - -sT is TCP SYN Port scan
- Does a TCP SYN scan on the top 1000 ports
- Doesn't show 1000 results. Just the ports that are open

Lesson 3.12: Scanning Techniques Lab Part 3 EH

Skills Learned From This Lesson: nmap TCP Connect scan, Top 1000 ports

- nmap -sT 192.168.0.1
    - -sT is a TCP connect port scan
- Does a TCP Connect scan on the top 1000 ports

Lesson 3.13: Scanning Techniques Lab Part 4 EH

Skills Learned From This Lesson: Downloading zenmap. Installing zenmap

- Download zenmap from https://nmap.org/dist/nmap-7.70-setup.exe
- Follow the installation steps to get zenmap installed on the lab machine

Lesson 3.14: Scanning Techniques Lab Part 5 EH

Skills Learned From This Lesson: Using zenmap GUI, nmap XMAS Scan Switch, nmap reason Switch

- Open zenmap (GUI version of nmap) by clicking on the zenmap icon
- nmap -sX 192.168.0.3
    - -sX is the christmas tree scan switch
- XMAS scan is very noisy
- Ports are marked open is there is no response
- Use it against Linux machines, not Windows machines
- nmap -sX -reason 192.168.0.3
    - -reason shows the reason why it's open

Lesson 3.15: Scanning Techniques Lab Part 6 EH

Skills Learned From This Lesson: nmap ACK switch, nmap Specific Port Scanning, Filtered/Unfiltered Ports

- nmap -sA -p 80 192.168.0.1
  - -sA - is the ACK switch
  - -p {port number} - specifies a specific port to be scanned
- This scan shows port state (filtered/unfiltered)
  - Port 80 shows as ***Unfiltered***

Lesson 3.16: Scanning Techniques Lab Part 7 EH

Skills Learned From This Lesson: Using Run to Open Windows Firewall, Configurings Windows Firewall to Block Incoming Connections,

- Start Menu - Run
- Type **firewall.cpl** and hit enter
- Click *Turn Windows Firewall On or Off*
- Under *Private Network Settings* select *Block all incoming connections, including those in the list of allowed apps*
- Repeat for *Public Network Settings*
- nmap -sA -p 80 192.168.0.1 on the machine again
  - Port 80 now shows as ***filtered***

Lesson 3.17: Scanning Techniques Lab Part 8 EH

Skills Learned From This Lesson: hping3 SYN Scanning, hping3 Specifying Port

- hping3 -8 0-5000 -S 192.168.0.1
  - -8 enables scan mode
  - 0-5000 is the port range
  - -S is the SYN scan

Lesson 3.18: Scanning Techniques Lab Part 9 EH

Skills Learned From This Lesson: hping3 ACK Scan, hping3 Scan Flags

- hping3 -c 1 -V -p 80 -s 5555 -A 192.168.0.1
    - -c is packet count
    - -V is verbose
    - -p specifies a specific port to scan
    - -s is the port where the packets are sent from
    - -A is the ACK flag

Lesson 3.19: Scanning Techniques Lab Part 10 EH

Skills Learned From This Lesson: Turning on Windows Firewall from the Control Panel, hping3 ACK Scan, hping3 Scan Flags

- Select Start Menu -> Control Panel
- System and Security -> Windows Firewall
- Click *Turn Windows Firewall On or Off*
- Under *Private Network Settings* select *Block all incoming connections, including those in the list of allowed apps*
- Repeat for *Public Network Settings*
- hping3 -c 1 -V -p 80 -s 5555 -A 192.168.0.1
    - This is the same as the first scan

Lesson 3.20: Scanning Techniques Lab Part 11 EH

Skills Learned From This Lesson: hping3 XMAS Scan, hping3 XMAS Scan Flags

- hping3 -c 1 -V -p 80 -s 5555 -M 0 -UPF 192.168.0.1
    - -c is packet count
    - -V is verbose
    - -p specifies a specific port to scan
    - -s is the port where the packets are sent from
    - -A is the ACK flag
    - -M sets TCP sequence number
    - -UPF sets the URG, Push and Fin flags
- Windows machines is not going to respond from port 80 even if the port is open

Lesson 3.21: OS Fingerprinting Lab Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, nmap SYN Scan, nmap OS Detection

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Select the *OS Fingerprinting* Lab
- Open Kali VNC Viewer
- nmap -sS -O 192.168.0.1 192.168.0.4
  - -sS is a TCP SYN Scan
  - -O enables OS detection

Lesson 3.22: OS Fingerprinting Lab Part 2 EH

Skills Learned From This Lesson: DVWA, Using p0f, p0f for Passive Operating System Fingerprinting,

- Use XAMPP to enable apache Web Services
  - Apache is running DVWA (Damn Vulnerable Web Application)
- p0f -p -i eth0
  - -p = promiscuous mode
  - -i = the interface to listen on
- Open 192.168.0.1 in the web browser on the Kali machine
- OS scanning allows you to better identify possible vulnerabilities and exploits

Lesson 3.23: Mapping Networks Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Installing zenmap

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Open the *Mapping Networks lab*
- In Internet Explorer -> Select zenmap from the intranet page
- Tools -> zenmap
- Click executable - Select Run
- Map networks to show clients what their network looks like
- Helps to identify potential vulnerabilities

Lesson 3.24: Mapping Networks Part 2 EH

Skills Learned From This Lesson: Using zenmap, zenmap Network Diagram, Disabling Port Scanning with nmap

- Open zenamp
- nmap -sn 192.168.0.1/24
  - -sn disables port scanning
- Zenmap creates a network diagram for us in the **Topology Tab**

Lesson 3.25: Mapping Networks Part 3 EH

Skills Learned From This Lesson: Installing Manage Engine Op Manager

- In Internet Explorer -> Installation Files -> Select Op Managers from the intranet page
- Select the **Free Edition**
- In the Port Selection Panel change **Webserver = 8443**
- Skip Technical Support Registration
- Select POSTGRESSQl

Lesson 3.26: Mapping Networks Part 4 EH

Skills Learned From This Lesson: Configuring Op Manager, Running a Network Scan with Op Manager

- http://localhost:8443 to access the Web Login Page
- Username: admin | Password: admin
- Enumeration is mapping out the network
- Under **Discovery Input**
  - Start IP: 192.168.0.1
  - End IP: 192.168.0.255
- Add Credentials
  - Windows/WMI - Windows Credentials
  - PRACTICELABS.COM/Administrator | Passw0rd
- Discovery-Credentials: **Public**
- Discovery-Rules: **MYSQL**
- Save and Execute to scan the network
- Dashboard shows information from the scan

Lesson 3.27: Banner Grabbing Lab Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Starting Apache Web Services

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Open the *Banner Grabbing lab*
- Open XAMPP to start Apache Web Services
- http://192.168.0.1/dvwa/login.php
  - Web page for Damn Vulnerable Web Application

Lesson 3.28: Banner Grabbing Lab Part 2 EH

Skills Learned From This Lesson: Using telnet to Grab Banners, HTTP GET Request

- Use telnet to grab the DVWA banner
- telnet 192.168.0.1 80
- GET /dvwa/HTTP/1.1
  - GET is an HTTP GET request to get data from the server
  - HTTP is the connection protocol
- Host: 1928.168.0.1

Lesson 3.29: Banner Grabbing Lab Part 3 EH

Skills Learned From This Lesson: Using nc to Grab Banners, HTTP GET Request

- nc 192.168.0.1 80
- GET /dvwa/HTTP/1.1
  - GET is an HTTP GET request to get data from the server
  - HTTP is the connection protocol
- Host: 1928.168.0.1

Lesson 3.30: Banner Grabbing Lab Part 4 EH

Skills Learned From This Lesson: Using nmap to Grab Banners, HTTP GET Request

- nmap -sS -p 80 -A 192.168.0.1
  - -sS is SYN scan
  - -p specifies one specific port
  - -A is aggressive mode

Lesson 3.31: Enumeration Tools Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Using nslookup, DNS Zone Transfers

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Open the *Using Enumeration Tools* lab
- nslookup is used to pull DNS records
- Open command prompt (cmd.exe)
- nslookup
    - >server 192.168.0.1
    - >set type-any
        - Retrieves all records from the server
    - ls -d practise-labs.com

Lesson 3.32: Enumeration Tools Part 2 EH

Skills Learned From This Lesson: Using dig, DNS Zone Transfers

- dig (Domain Information Groper)
- dig axf practise-labs.com 192.168.0.1
    - axfr provides a complete listing of the domain records

Lesson 3.33: Enumeration Tools Part 3 EH

Skills Learned From This Lesson: Using psinfo, DNS Zone Transfers

- Double click PSTools folder
- Copy psinfo.exe to the desktop
- Open command prompt
- Change directory to desktop (cd Desktop)
- Psinfo.exe 192.168.0.1 -h -d
    - -h displays hotfixes
    - -d displays disk info

Lesson 3.34: Enumeration Tools Part 4 EH

Skills Learned From This Lesson: Using finger

- Open the terminal
- finger -s root (displays information about users on the system)

Module 4: System Hacking

Lesson 4.0: System Hacking EH

Skills Learned From This Lesson: Password Attacks, Password Cracking Tools, Steganography Tools

- SAM Files (Security Accounts Manager
  - Stores password hashes on Windows systems
  - SYSKEY allows you to partially encrypt the hash
- Types of password attacks
  - Dictionary - uses a series of strings (essentially like a dictionary list of possible passwords)
  - Brute-force - tries all possible combinations to crack a password
  - Rule-Based - Leveraging the rules of an organization (minimum complexity requirements)
  - Rainbow Tables - Precomputed tables containing pre-cracked hashes
- Salting
  - Adding random characters into the hash for added security
- Aircrack is used to crack wireless passwords
- Cain and Abel - password recovery tool for Windows
- John the Ripper -
- Hydra is used often for cracking Web Based auth
- Hashcat is used to crack hashes
- Spectre and Meltdown - exploiting flaws in protected memory being stored in CPU cache
- Rootkits - provide continued access to a machine
  - Horse Pill - infects initial ramdisk in Linux. Controls early boot process
  - Gray Fish - Attributed to the Equation Group (NSA)
- Steganography Tools
  - QuickStego, OpenStego, MP3Stego, StegoShare
- Covering BASH Tracks
  - Disable history: **export HISTSIZE=0** (HISTSIZE = number of stored commands)
  - history -c

Lesson 4.1: Lab Intro EH

Skills Learned From This Lesson: TFTO, Backdoor Trojans

- TFTP - Trivial File Transfer Protocol
  - Allows a client to get/push a file to a remote host
  - RFC 1350
  - Doesn't do user authentication
  - Doesn't allow listing of directories
- Backdoors allow attackers to open command-line shells on your machine
  - Maintain access
  - Collect information
  - Terminate tasks and process
  - Download/upload additional files
  - Perform Denial of Service
  - Change computer settings
  - Restart or shutdown the computer

Lesson 4.2: Backdoor System Hacking EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Setting Up Tftpd64.exe

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Select *Planting a Backdoor* lab
- Download TFTP exe from the intranet page (found in the web browser)
- Launch Tftpd64.exe
- When the Windows Firewall window pops up, select **Public, Private, Domain and the Allow Access**
- Click Browse to select tftpd server directory - Select **C:\Program Files(x86)\Nmap**
- Click Server Interface drop down list - Select **192.168.0.5**

Lesson 4.3: System Hacking Plant Backdoor EH

Skills Learned From This Lesson: Using PSExec to Create a Backdoor, Connecting to a backdoor with TFTP Client

- Open PSTools
- Copy PSExec.exe to the desktop
- Command Prompt (cmd.exe)
  - Cd Desktop
- PSExec.exe \\PLABWIN10 cmd
  - Opens command shell availability on the target machine
- Use TFTP to connect to PLABWIN10
  - dism /online /Enable-Feature /FeatureName:TFTP
  - tftp 192.168.0.5 GET ncat.exe
    - Transfers the backdoor to the target machine
- Backdoors allow us to maintain access on the target machine

Module 5: Malware

Lesson 5.0: Malware Viruses EH

Skills Learned From This Lesson: Malware, Virus Life Cycle, Virus Varieties

- Malware is any malicious program or code
    - Symptoms: Computer slowness, Ad pop-ups, High System Resource use, Disabled anti-virus
- Get them from: hacked websites, game demos, hidden in various file sharing sites, malicious emails
- Virus is a self-replicating malicious program. Needs to have a host program to propagate
- Virus Life Cycle
    - Design, Replication, Launch, Detection, Incorporation, Elimination
- Lots of varieties of computer viruses
    - **Boot Sector Virus**- Moves Boot Sector to a new location allowing the virus code to be executed first
    - **Ransomware** - locks your computer and demands some sort of payment
    - **Shell Virus** - wraps around an application allowing its code to be executed before the application's
    - **Cluster Virus -** modifies discovery table entries so that system and user process point to the virus code
    - **Multipartite Virus** - attempts to infect the boot sector and files simultaneously
    - **Macro Virus** - Infected virus transmitted through Microsoft Products VBA scripting
    - **Polymorphic Code Virus** - mutates the code so the signature is always changing
    - **Encryption Virus** - uses encryption to avoid detection
    - **Metamorphic Virus -** rewrites itself
    - **Stealth Virus** - attempts to avoid AB by intercepting AV requests to the OS
    - **Cavity Virus** - overwrites null content sections of host files
    - **Spare Layer Virus -** Only infects occasionally
    - **File Extension Virus -** Changes file extensions to take advantage of user who aren't working with file extension view off

Lesson 5.1: Malware Worms Trojans EH

Skills Learned From This Lesson: Skill, Skill, Skill

- Worms are self-replicating and self-propagating program
  - **Code Red** - Exploit IIS in 2001 via buffer overflow
  - **SQL Slammer -** DoS worms that used a buffer overflow exploit in Microsoft SQL
  - **Nimda -** Spread through open network shares, websites, email. Used backdoor left behind by Code Red
- Tojans - Appear to perform desired functions but performs actions without the users knowledge. Think of the *Trojan Horse*
  - **Covert Channel -** used to transmit information in a way that is unintended. Violates security policy on a system
  - **Overt Channel -** Performs actions and send data in legitimate ways
- Indicators of a Trojan Infection
  - CD Drawer randomly open/closes
  - Computer screen flips
  - Documents randomly print
  - Browser redirection
  - Mouse pointer disappears

Lesson 5.2: Malware Lab Intro EH

Skills Learned From This Lesson: Definition of Ports, Various Malware Troubleshooting Tools

- Port is a connection interface between devices
- Stinger - a McAfee tools for detection and removal of malware
  - https://www.mcafee.com/enterprise/en-ca/downloads/free-tools/stinger.html
- Currports - Monitors TCP and UDP port connections
- TCPView - Shows all TCP/UDP connections
- What's Running - Shows all running processes
- HashCalc - Generates hashes for file intergrity

Lesson 5.3: Malware Stinger EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Setting Up McAfee Stinger, McAfee Stinger Scans and Settings

- Log into the Cybrary labs!
- Select *Ethical Hacker Practice Labs*
- Select the *Trojan Protection* Lab
- Open Internet Explorer - Tools - Hacking Tools
- Select stinger30-epo file
- Download and save the stinger file
- In the navigation bar, highlight and type **cmd** to open a command prompt at that location
- Run Stinger.bat
- Click the Stinger File - Agree to the UAC - Update Stinger
- Open Stinger - Click **Scan**
- Select View Logs
- Log Settings - Can include all scans and pick log save location
- Advanced - Settings - Select **Remove** from “On Threat Detection”
    - Automatically removes infected files

Lesson 5.4: Malware Currports EH

Skills Learned From This Lesson: Starting Currports, Sorting Data in Currports

- DVD Drive - CEH Tools - Currports - Currports application files
- Use the column headers to sort by the various settings in the application
- Currports gives us visibility into what’s running on the ports

Lesson 5.5: Malware TCP View EH

Skills Learned From This Lesson: Starting TCPView, Sorting Data in TCPView

- DVD Drive - CEH Tools - TCPView - TCPView application
- Use the column headers to sort by the various settings in the application

Lesson 5.6: Malware What’s Running EH

Skills Learned From This Lesson: Installing What’s Running, Examining Process with What’s Running, Creating a What’s Running Snapshot

- Open Internet Explorer - Tools - Hacking Tools
- Run whatsRunning3_0_Setup.exe
- Install What’s Running
- Right click on What’s Running - **Run as Administrator**
- Process Tab shows all running process
- Open OneDrive.exe to view the process information
- Right click on a process to open a context menu
- Selecting *Show Process in Tree* show a hierarchical view
- The Services menu show all running services\
- IP menu shows IP options
- Drivers menu shows running drivers
- Startup menu allows configuration of startup processes
- Open Snapshot menu to save a snapshot of What’s Running

Lesson 5.7: Malware Hash Calc EH

Skills Learned From This Lesson: Installing Hash Calc, Creating Hashes, Adding Data to Various Hash Types

- DVD Drive - CEH Tools - HashCalc - HashCalc Setup File
- Install Hash Calc with the default settings
- Unselect *View the Read Me File*
- Open Hash Calc
- Use the three dots to select a file to hash
- Leave default hash type selections
- Select calculate
- Data Format - Text String
    - Type “Welcome to device PLABWIN10”
- HMAC Hash Type - Adding a Key Value - **TidyMind**
- Data Format - Hex String
    - Unselect HMAC
    - Data 0000ff

Module 6: Sniffing

Lesson 6.0: Sniffing EH

Skills Learned From This Lesson: Active/Passive Sniffing, Wireshark, MAC Flooding

- Capturing network traffic
    - **Active** - Monitor and alert
    - **Passive** - Listening only
- Non -encrypted traffic is easy to sniff
    - Telnet, HTTP, SMTP, POP, FTP, IMAP
- Wireshark is the most popular network sniffing tool
- There are various command line tools to memorize for the exam!
- **MAC Flooding -** Attacker wants a switch to fail open and act like a hub
- **ARP Poison -** Poison the network with incorrect MAC Address/IP bindings for the purpose of traffic redirection
- **Switched Port Analyzer (SPAN) Port -** Send a copy of every network packet on one switchport to another port for monitoring
- Defense against sniffing
    - Encrypted the data in transit
    - Hardware-swtiched networks to isolate sensitive network segments
    - Cisco switches has IP DHCP Snooping that prevents ARP poisoning
    - Policies preventing promiscuous mode on network adapters

Lesson 6.1: Sniffing Lab Intro EH

Skills Learned From This Lesson: Benefits of Wireshark, Sniffing, MAC Spoofing

- Wireshark: Captures Packets, Identifies and analyzes protocols, displays contents of packets
- MAC spoofing can help avoid attribution
- Sniffing logs network traffic
- Wireshark is dog that sniffs and identifies packets
- Download the Wireshark Display Filters from the course material!

Lesson 6.2: Sniffing Wireshark EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Installing Wireshark, High Level Wireshark Usage

- Log into the Cybrary labs!
- Select *Ethical Hacker Sniffer Labs*
- Internet Explorer - Intranet - Tools - Hacking Tools - Wireshark Installer
- Install Wireshark - Add a Desktop Icon
- Select Capture - Interfaces - Local Area Connection
- Click Stop to stop the capture
- Edit - Find Packet - Filter (This allows us to select the filters we want to sort with)
- Capture shows:
  - Number
  - Time
  - Source
  - Destination
  - Protocol
  - Additional Info
- To save the packet capture (pcap) file - Select Save As

Lesson 6.3: Sniffing MAC Spoof EH

Skills Learned From This Lesson: Installing SMAC, Generating Random MAC, Updating the MAC Address

- MAC Spoofing makes it difficult for people to trace our activity back to our IP or MAC address
- Internet Explorer - Intranet - Tools - Hacking Tools - SMAC installer
- Install SMAC
- Proceed past the registration tool
- Select the NIC that you want to modify the MAC address of
- After you select the NIC, select the **Random** button to generate a random MAC address
- Select **Update MAC** to update the MAC address of the NIC
- This will restart the NIC with the new MAC
- There are lots of ways to spoof a MAC address
  - Kali has options
  - There are CLI options

Module 7: Social Engineering

Lesson 7.0: Social Engineering EH

Skills Learned From This Lesson: Definition of Social Engineering, Phases of Social Engineering Attack, Insider Threats

- Deception used to manipulate people to divulge personal information
- Four Phases:
  - Research a target company
  - Select a victim
  - Develop relationship - Creates a deeper understanding of an organization
  - Exploit relationship
- Human-based Social Engineering
  - **Impersonation** - pretending to be someone else
  - **Vishing -** using a telephone (voice phishing)
  - **Eavesdropping -** listening in on conversations
  - **Shoulder Surfing** - reading over someone's shoulder
  - **Dumpster Diving -** exactly what it sounds like
  - **Piggybacking -** attacker asks someone to let them in
  - **Tailgating -** uses a fake badge
  - **Reverse Social Engineering -** Tech support scams. Browser redirect, poisoning cookies
  - **Phishing -** emails sent to get people to disclose information
  - **Smishing -** phishing sent to your phone
- Insider Threats - These are threats coming from within the organization
  - Employees, former employee, contractor
  - Non-responders (constant negligence), Inadvertent Insiders (comply with policy), insider collusion, persistent malicious insiders, disgruntled employees
  - "The call is coming from inside the house!"
- Social Engineering Countermeasures
  - Research, Reject requests for help, don't post personal info, don't post sensitive data, follow policies
- Insider Threat Countermeasures
  - Deterrence, know the weakest+ links, identify valuable information, monitor ingress and egress points

Lesson 7.1: Social Engineering Lab Intro EH

Skills Learned From This Lesson: Common Social Engineering Attacks, Signs of Phishing Email, EC- Council Definition

- Common Social Engineering Attacks
    - **Phishing** - signs to look for
        - Strange sender address
        - Generic greeting
        - Link for you to click on (hover on it to see where the link is going to)
        - Strange date range on the email
    - **Pretexting** - building trust with the victim or contacting someone to get them to confirm their identity
    - **Baiting -** similar to phishing but with the promise of something good.
    - **Quid pro quo -** Similar to baiting but the difference is a promise of a service
    - **Tailgating -** use of a fake badge and follows an authorized person in
    - **Piggybacking -** No badge but asks someone to let them in

Lesson 7.2: Social Engineering Lab Recon EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Basic Social Engineering, Open Source Intelligence (OSINT)

- Log into the Cybrary labs!
- Select *Social Engineering Reconnaissance Labs*
- Open Source Intelligence (OSINT) on yourself or the person named by the lab document
- You can use posts to check someone's activity
- Photos can reveal location and interests
- Posts can reveal lots about people. "Practice Safe Posting!"
- Filling out a bio can allow people to create a profile on you (password cracking, security questions)

Module 8: Denial of Service

Lesson 8.0: Denial of Service EH

Skills Learned From This Lesson: DoS, DDos, Types of DoS/DDoS Attacks

- The goal is to prevent a user or organization from accessing a resources
- Affects the Availability of the machine
- Denial of Service (DoS) - leverages a single machine to perform a Denial of Service
- Distributed Denial of Service (DDoS) - leverages multiple machines to perform a Denial of Service
- Types of Attacks
    - ○ UDP Flood - large number of UDP packets to random ports
        - ■ Tools: LOIS, UDP Unicorn
    - ○ ICMP Floop - send a flood of ping packets.
    - ○ Ping of Death - send malformed packets with the goal of causing a buffer overflow
    - ○ Smurf - spoofs a victim's IP and sends large amounts of ICMP packets
    - ○ SYN Flood - sends SYN packets
    - ○ Slowloris - opens connections but never completes request. The goal is to have a server block other connections
    - ○ Distributed Reflection Denial-of-Service (DRDoS) - user UDP packets
- Botnets are “zombie” computers or devices used with Command & Control servers to perform attacks
- Countermeasures:
    - ○ Recognize the signs, contact your ISP, incident response plan, load balancers, Anti-DDoS solutions

Module 9: Sessions Hijacking

Lesson 9.0: Hijacking EH

Skills Learned From This Lesson: Spoofing vs Hijacking, Steps of Hijacking, Preventing Sessions Hijacking, IPSec

- Attacker is trying to take control of an active sessions between a client and a server
- Intent of spoofing is to sniff traffic
- Intent of hijacking is to take over the entire sessions
- **Steps for Hijacking**
  - Sniff - sniff traffic between client and server
  - Monitor - monitor sniffed traffic
  - Desynchronize - using TCP RST or FIN flags to knock off the victim machine
  - Predict - predict sessions tokens
  - Inject - inject packets and pretend to be the client
- Tools for sessions hijacking
  - Ettercap, Ferret, Burp Suite
- Preventing Sessions Hijacking
  - Unpredictable sessions IDs
  - Limiting incoming connections
  - Reduce remote access
  - Regenerate sessions keys after authentication
  - IPSec
    - Transport mode - IP Header is not encrypted and can be used with (Network Address Translation) NAT
    - Tunnel mode - entre packet is encrypted
    - Authentication Header - guarantees integrity and authentication of the IP packet sender
    - Encapsulating Security Payload (ESP) - a Protocol that provides integrity, authenticity, and confidentiality of the entire packet in tunnel mode
    - Internet Key Exchange (IKE) - Produces encryption keys
    - Oakley - Uses Diffie-Hellman to create keys

<u>Lesson 9.1</u>: Session Hijacking Lab Intro EH

Skills Learned From This Lesson: Address Resolution Protocol (ARP), Man-in-the-Middle (MitM) Attacks

- Address Resolution Protocol (ARP)
- ARP is used to resolve IP addresses to MAC addresses
- ARP is a broadcast protocol
- Man-in-the-Middle (MitM) Attack - attacker is secretly monitoring traffic between two machines

<u>Lesson 9.2</u>: Sessions Hijacking Lab Part 1 EH

Skills Learned From This Lesson: Using the Cybrary Live Lab, Using Ettercap for Sniffing Traffic, Ettercap ARP Poisoning

- Log into the Cybrary labs!
- Select *Implementing Network-level Session Hijacking Labs*
- Open the XAMPP console - start Filezilla if there is an error message
- Open Kali through VNC Viewer
- Start - Sniffing and Spoofing - Ettercap-Graphical
- Sniff - Unified Sniffing - eth0 *(starts ettercap on eth0)*
- Host - Scan for hosts *(scans for hosts)*
- Host - Host list *(shows list of hosts)*
- Click on desired hosts - Add to Target *X*
- Select MitM - ARP poisoning
- Sniff Remote Connections
  - This will poison the ARP caches of your selected machines

<u>Lesson 9.3</u>: Sessions Hijacking Lab Part 2 EH

Skills Learned From This Lesson: Using Ettercap for Sniffing Traffic, Using Ettercap to See Plaintext Credentials

- Start - Start Sniffing
- Open http://192.168.0.1/dvwa
- Login to dvwa (username: admin | password: password)
- Ettercap will see the plaintext traffic containing the user credentials

Module 10: Web Server and Apps

Lesson 10.0: Web Server EH

Skills Learned From This Lesson: Web Server Definition, HTTP Request Methods, Directory Traversal Attacks

- Web servers “serves” content to the World Wide Web
- Responds to client requests on port 80 (HTTP) or 443 (HTTPS)
- HTTP Request Methods
  - GET - requests data. Possible to send data but it is tagged in URL
  - HEAD - server does not return a message body in the response
  - POST - used to request that the origin server accept the entity in the request. Safer that GET when not stored in browser history
  - PUT - requests that stored entity be stored under the supplied Request-URI
  - DELETE - request that server delete the resource identified by the Request-URI
  - TRACE - invoked a remote, application layer loopback
  - CONNECT - reserved for use with a proxy
- Directory Traversal
  - Attackers tries to get to root or other directories
  - Dot-dot-slash attack
    - http://www.test.com/../../../../../../../
- Website Mirroring is used to grab a copy of the entire website: HTTTrack

Lesson 10.1: Web Application EH

Skills Learned From This Lesson: OWASP Top 10

- A1:2017-Injection
  - Can result in data loss or corruption
  - **Prevention:** Use a dafe APIT, Whitelist server side input validation, Use SQL controls to stop SQL injection attacks
- A2:2017-Broken Authentication
  - Can result in identity theft and fraud
  - **Prevention:** Multi Factor authentication, No default credentials, Check for weak passwords,limit login attempts

- A3:2017-Sensitive Data Exposure
    - Can lead to identity theft
    - **Prevention:** Classify data, apply appropriate controls, encrypt all data (rest/in-transit)
- A4:2017-XML External Entities (XXE)
    - Can lead to data extraction, DoS, Internal System Scans
    - **Prevention:** Use less complex data formats, patch all XML processors and libraries, disable XML external entity processing
- A5:2017-Broken Access Control
    - Can cause admin privileges for attackers and users
    - **Prevention:** Deny by default, disable web server directory listing, log access control failures
- A6:2017-Security Misconfiguration
    - Can lead to unauthorized access or complete compromise
    - **Prevention:** Hardening, segmented application architecture
- A7:2017-Cross Site Scripting (XSS)
    - Can lead to remote code execution, stealing of credentials and delivery of malware
    - **Prevention:** Separating untrusted data from active browser content, escaping untrusted HTTP requests, enabling Content Security Policy (CSP)
- A8:2017-Insecure Deserialization
    - Can lead to remote code execution
    - **Prevention:** Implement integrity checks, code isolation
- A9:2019-Using Components with Known Vulnerabilities
    - Can lead to massive data breaches
    - **Prevention:** patching,obtain from official sources,
- A10:2017-Insufficient Logging and Monitoring
    - Can lead to successful exploitation
    - **Prevention:** log all access control failures with sufficient context, effectively monitor logs and alerts

Lesson 10.2: Web Server Lab Intro EH

Skills Learned From This Lesson: Burp Suite, Proxies, Burp Suite Benefits

- Burp Suite is a web hacking tool
- Proxies are gateway between local network and the internet
- Burp Suite does not have PPTP
- Burp has a free and Pro version
- Burp has: Proxy, Scanner, Intruder, Spider, Repeater, Decoder, Comparer, Extender, Sequencer
- OWASP Top 10 was updated in 2017
- Exploit Pack is a tool pack for more advanced penetration testing

Lesson 10.3: Web Tool Burp Suite Lab Intro EH

Skills Learned From This Lesson: Using Burp Suite, Configure Burp Suite

- Open Burp Suite in a Kali Linux Machine
- Skip the update prompt
- Temporary Project - Default - Start Burp Suite
- Open the Proxy Tab
    - Options
        - Interface is set to 127.0.0.1:8080
- Open Firefox Settings - Preferences - Advanced - Network - Settings
    - Manual Proxy Configuration - 127.0.0.1 Port 8080
    - Use this proxy server for all protocols
- Click on Proxy - Intercept tab in Burp Suite
    - Burp Suite Proxy intercepts the web traffic
    - Select forward to forward the packets
- Features
    - Scanner is only the paid version
    - Intruder is used for various attacks
    - Proxy - HTTP History can be used to highlight and identify important requests

Module 11: SQL Injection

Lesson 11.0: SQL Injection EH

Skills Learned From This Lesson: SQL Definition, SQL Commands,

- Structured Query Language (SQL) is used to sort, manipulate and retrieve data stored in a database
- SQL Commands
  - remember to end with a **;**
  - SELECT - allows us to select from a table in a database
  - DELETE - used to delete records in a table
  - UPDATE - used to update existing records in the table
  - INSERT INTO - inserts a new record into a table
- SQL Injection is a code injection technique that exploits vulnerability in application software
- Can be used to spoof identities, void transactions, data dumps, etc…
- Types
  - Union-based - use the UNION statement to join SELECT queries
  - Error-based - goal is to get an error that discloses information about the database
  - Blind - no error message received
    - Boolean-based - slow attack. HTTP response may change
    - Time-based- forces a databased to wait a period of time before responding
- Tools: SQLMap, Whitewidow, BBQSQL, Blisqy

Module 12: Hacking Wifi and Bluetooth

Lesson 12.0: Wifi Bluetooth EH

Skills Learned From This Lesson: WEP-WPA-WPA2, Wireless Hacking, Hacking Bluetooth

- Wireless network data connection
- Check up on the frequencies of the wireless network standards
- SSID does not provide security
- Wireless Authentication
  - Open System Authentication
    - Makes networks available to a variety of client
  - Shared Key Authentication
    - Each client knows ahead of time
- WEP
  - Very vulnerable
  - Initialization vector for integrity and confidentiality
  - 32-bit ICV
  - Flaws
    - Easy packet modification, Susceptible to known plaintext attack, Susceptible to DoS attack
- WPA (Wi-Fi Protected Access)
  - Temporal Key Integrity Protocol
  - Key changes after every frame
  - Keys are transferred during EAP
  - Flaws
    - Weak Keys, Packet spoofing
- WPA2
  - Uses AES
  - Compliant with FIPS 140-2
  - Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity
  - WPA2-Enterprise uses a server key
  - Flaws
    - Deauthentication attack

- Wireless Hacking
  - Rogue Access Point
    - Attacker installs a new access point behind the company's firewall
    - Allows access to the network
  - MAC Spoofing
    - Attacker spoofs MAC address of an approved client
  - Ad hoc
    - Relies on using a Wi-fi adapter to connect to another system
  - Misconfiguration
  - Client Misassociation
    - Clients attaches to an AP that is not part of their network
  - Jamming Attacks
    - DoS attack
  - Honeyspot
    - Attacker sets up rogue AP with improved signal
- Tools
  - Aircrack-ng, Kismet, Cain & Abel, Wifite
- Bluetooth Threats
  - Bluejacking - sending anonymous messages to a victim
  - Bluesnarfing - extracts information from a distance
  - Bluetooth Honeypots - Bluepot can be used to draw malware and bluetooth devices

Module 13: Mobile Hacking and Security

Lesson 13.0: Mobile Android EH

Skills Learned From This Lesson: OWASP Mobile Top 10. Smishing

- OWASP Top 10 Mobile
    - Improper Platform Usage
        - Misuse of TouchID
        - Keychain IP
    - Insecure Data Storage
        - Insecure storage
    - Insecure Communication
        - Incorrect SSL version, weak negotiation, cleartext communication
    - Insecure Authentication
        - Failing to identify end users, weak sessions management
    - Insufficient Cryptography
        - Poorly done, or absent cryptography
    - Insecure Authorization
        - Failed authorization decision on the client side
    - Client Code Quality
        - Insecure code, buffer overflows
    - Code Tampering
        - Attacker modifies pieces of the code
    - Reverse Engineering
        - Attacker analyzer the core binaries to find vulnerabilities
    - Extraneous Functionality
        - Hidden backdoors, disable two-factor authentication

Lesson 13.1: Mobile Android Part 2 EH

Skills Learned From This Lesson: Android Hacking Tools, Android Rooting Tools, Android Vulnerability Scanners

- Android Hacking Tools
  - **AndroidRAT**
    - Takes control of Android OS
    - Run as a service. Activated with an SMS or call
    - Collect logs, location, messaging, etc...
  - **Hackode-** 3 categories: Recon, Security Feed, Scanning
  - **Csploit-** Catalogs local hosts, install backdoors, grabs wifi password
  - **FaceNiff-** Sniffer for twitter, facebook
  - **Shark for Root-** Wireshark for Android
  - **Droidsheep** - Operates as a router to gain access to active sessions
  - **Droidbox-** Checks hashed for APK packages
  - **APKInspectoy** -Reverse Engineer app code
- Android Rooting
  - Oneclickroot, ResuceRoot, KingRoot
- Vulnerability Scanners
  - Ostorlab, Appvigil, AdroTotal, Akana, SanDroid

Lesson 13.2: IOS Arch Jailbreak EH

Skills Learned From This Lesson: iOS Jailbreaking Tools, iOS Malware, Securing iOS

- iOS Jailbreaking Tools
  - Electra
  - Cydia - 3rd party app store
  - PP Assistant -
  - Pangu - popular in pen testing world
  - Redsn0w - might be on exam
- iOS Malware
  - AppBuyer - simulated apples protocols to buy apps in victims name
  - KayRaider - steal user credentials by intercepting iTunes traffic on jailbroken devices
  - XCodeGhost - target Chinese Developers. Found in unofficial distributions of XCode

- Securing iOS devices
    - Update software, active location features, long passcode, auto-wipe, remove app permissions, turn off siri

Lesson 13.3: IOS Mobile Device Management EH

Skills Learned From This Lesson: Mobile Device Management (MDM), BYOD,

- Mobile Device Management (MDM)
    - Data segregation
    - Email security
    - Securing corporate documents
    - Enforcing policy
    - On-prem or cloud
    - All types of mobile devices
    - Reduces support costs and risk
- MDM Solutions
    - ManageEngine Mobile Device Manager Plus, VMWAre AirWatch, IBM MaaS360
- Bring Your Own Device (BYOD)
    - Increased productivity, reduced costs, improved mobility, end user appeal
    - Who pays for the device and data?
    - What industry regulations are there?
    - How do you secure the devices?
        - Password protection, Control wireless network connectivity, control application access, update software, backup data, remote wipe, location tracking, antivirus, control app downloads
    - Where is the data stored?
    - Support? Privacy?

Module 14: IDS, Firewalls, Honeypots

Lesson 14.0: IDS EH

Skills Learned From This Lesson: IDS vs IPS, Detection Methods, Snort

- Intrusion Detection System
    - Monitors a network ro system for malicious activity or policy violations
    - Two flavours: Host-based Intrusion Detection Systems (HIDS), Network-based Intrusion Detection System (NIDS)
    - Detects intrusion by monitoring traffic and matching it to library of known attacks
    - Can check for abnormal behaviours
    - Alerts administrator
- Intrusion Prevention System
    - Combined with IDS
    - Prevents malicious activity (drops packets, resets connection, blocks traffic from an IP address)
- Detection Methods
    - **Signature-based:** packets are compared against known attacks
    - **Anomaly-based**: compares traffic against a known baseline
    - **Stateful protocol analysis**: deviation of protocol states by comparison of observed events
- Alert Types:
    - **True positive** - Bad traffic. Alert
    - **False positive** - Good traffic. Alert
    - **False negative (worst)** - Bad traffic. No Alert
    - **True negative -** Good traffic. No Alert
- Snort is most test IDS tool for the CEH exam
- Snort Rule Actions
    - **Pass -** ignores the packet
    - **Log** - logs a packet
    - **Alert** - sends alert message when rule conditions are met
    - **Activate** - create an alert and then activate another rule for more conditions
    - **Dynamic rules** - invoked by other rules using activate activation
    - **User defined -** sends message to Syslog. Take multiple actions on a packet

- Snort Direction Operator
    - **<>** bi-directional traffic flow
    - **->** single direction traffic flow
    - any can be used to define IP address
    - **: (colon)** is the range indicator for port ranges
    - Numeric IP addresses must be used with CIDR netmask
- Evading IDS
    - **Insertion attack** - IDS doesn't flag as malicious. Host machine
    - **DoS** - overwhelm IDS. Overwhelm the machine or the network admin
    - **Obfuscation** - unique attack patterns (polymorphic shellcode)
    - **Unicode -** changes signature
    - **Fragmentation -** splits a payload into smaller packets
- Evasion tools
    - Ssl proxy, nmap (T0 or T1 switch), whisker, Stick and Snot
- Countermeasure for IDS Evasion
    - snort -z switch, traffic re-assembly, closely monitor fragmented traffic

Lesson 14.1: Firewalls EH

Skills Learned From This Lesson: Firewall Definition, Firewall Technologies, Firewall Limitations

- Devices that filters traffic based off rules
- Permissive rules first. Denial rules after
- Firewall Technologies
    - **Packet Filtering (static) -** Filters based on source, destination and port.
    - **Circuit-level gateway -** Outside sender doesn't know end user IP
    - **Stateful Inspection -** monitors the state and characteristics of the connection
    - **Application Proxy -** functions as a proxy between systems. Resource heavy
    - **Network Address Translation -** firewall assigns an outside IP address for the computer in the private network
- Limitation
    - Not effective against social engineering, cannot enforce password policies, doesn't help against security awareness issue
    - First line of defense
- Evasion
    - IP Address Spoofing, fragmentation,ICMP tunneling, HTTP tunneling,

Lesson 14.2: Honeypots EH

Skills Learned From This Lesson: Types of Honeypots, Honeynet Project

Intrusion Detection System

- Two Types
  - **Low interaction:** Services frequently requested by attackers
  - **High interaction:** mimics a real system
- You want to entice attackers to attack the honeypot
- Low interaction tools
  - Dionea, Thug, Conpot
- High Interaction tools
  - Capture-HPC, Dockpot
- Honeynet project is a resource for learning all about honeypots. They collect information on various attack patterns
- Detecting Honeypot
  - No outbound traffic
  - Random machine outside the DMZ
  - Too Insecure
  - Use Send-Safe to detect Honeypots

Module 15: IoT

Lesson 15.0: IoT Basics EH

Skills Learned From This Lesson: IoT Architecture, IoT Protocols, IoT Challenges

- Network of devices (smart devices, vehicles, airplanes,etc…)
- Collects and exchange data
- 4 Stages IoT Architecture
    - Sensors,Actuators
    - Internet Gateways, Data Acquisition Systems
    - Edge IT
    - Data Center, Cloud
- Smart homes are the most used device
- Wearables are the second
- Various protocols
    - Infrastructure: IPv4/6,6LowPAN,RPL
    - Identification: URIs, EPC, uCode
    - Communications: Wifi, Bluetooth
    - Discovery: mDNS, DNS-SD
    - Data: MQTT, CoWP, AMQP, Websocket
    - Device Management: TR-069, OMA-DM
    - Sematic: JSON-LD, Web Thing Model
    - Multi-Layer Frameworks: Weave, Homekit, IoTivity
- Communication Models
    - Device-to-Device, Device-to-Cloud, Device-to-Gateway, Back-en Data Sharing
- Challenges
    - Security, Connectivity, Compatibility and Longevity, Standards, Intelligent Analysis & Actions

Lesson 15.1: IoT OWASP EH

Skills Learned From This Lesson: IoT OWASP Top 10 , IoT OWASP Countermeasures

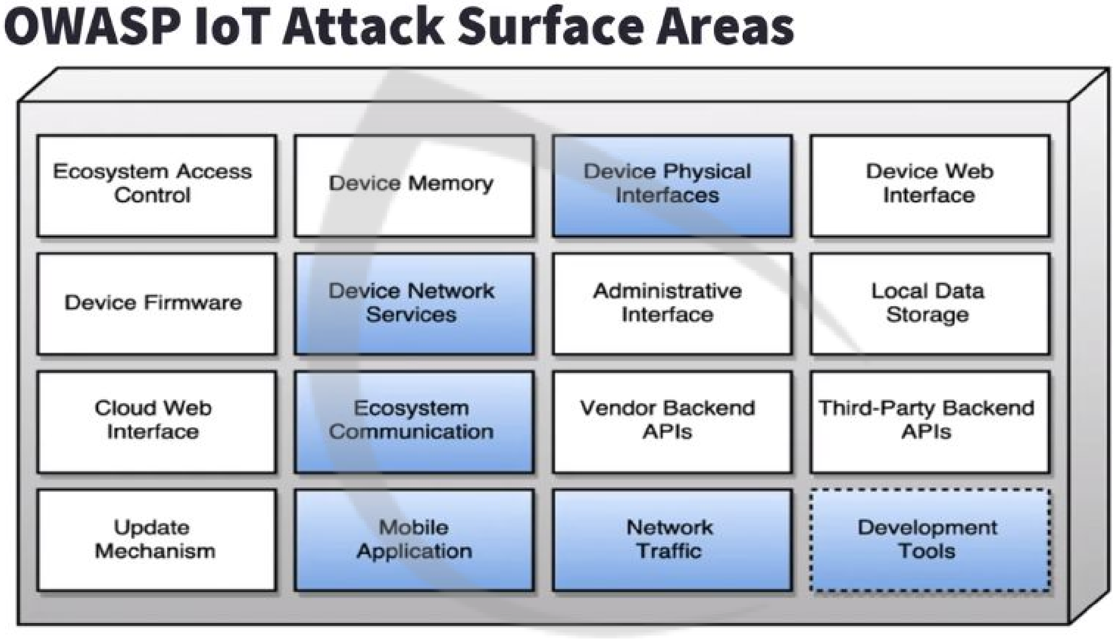
- OWASP Top 10 (2014)
    - Insecure Web Interface
        - Change default credentials, ensure robust password recovery methods, ensure interface is not susceptible to XSS CSRF, nothing sent in plaintext

- Insufficient Authentication/Authorization
  - Strong passwords, granular access control, multi-factor authentication, secure password recovery
- Insecure Network Services
  - Only open necessary ports, ensure service are not vulnerable to buffer overflows or DoS
- Lack of Transport Encryption
  - Ensure data is encrypted with proper protocols (like TLS), only use accepted encryption standards
- Privacy Concerns
  - Ensure only data critical to the functionality is collected, encrypt data, only authorized individuals have access to the information
- Insecure Cloud Interface
  - Change default credentials, ensure robust password recovery methods, ensure interface is not susceptible to XSS CSRF, nothing sent in plaintext
- Insecure Mobile Interface
  - Change default credentials, ensure robust password recovery methods, ensure interface is not susceptible to XSS CSRF, nothing sent in plaintext
- Insufficient Security Configurability
  - Keep admin users separate, encrypt data at rest/in-transit, strong password policy, log security events
- Insecure Software/Firmware
  - Updates, encrypt update file, no sensitive data in update file, signature/verification of update file, secure the update server
- Poor Physical Security
  - Ensure data storage can't be easily removed, encrypt data at rest, eliminate the use of USB, ensure devire can't be disassembled easily, limit admin capabilities

Lesson 15.2: IoT Surface Area Tools EH

Skills Learned From This Lesson: IoT Methodology, IoT Attack Surface Area

- IoT follows the same general PenTesting methodologies



OWASP IoT Attack Surface Areas

Ecosystem Access Control	Device Memory	Device Physical Interfaces	Device Web Interface
Device Firmware	Device Network Services	Administrative Interface	Local Data Storage
Cloud Web Interface	Ecosystem Communication	Vendor Backend APIs	Third-Party Backend APIs
Update Mechanism	Mobile Application	Network Traffic	Development Tools

- IoT Hacking Tools
  - Wireshark Burp, Binary Ninja, IDA PRO, Ubertooh One

Module 16: Cloud

Lesson 16.0: Cloud EH

Skills Learned From This Lesson: Types of Cloud Services, Cloud Deployment Models, Benefits of Cloud Computing

- Cloud is just someone else's computer
- AWS, GCP, Azure
- Types of Cloud Services
  - Infrastructure as a Service - build everything. Essentially a data centre
    - Responsible for: Applications, Data, Runtime, Middleware, OS
  - Platform as a Service
    - Responsible for: Applications, Data
  - Software as a Service
    - `On demand model.
- Deployment Models
  - Private - Just for your organization
  - Community - Shared by multiple organizations
  - Hybrid - Composite of two or more clouds
  - Public - Available for general use
- Benefits of Cloud Computing
  - Faster Software, reduced infrastructure costs, elasticity, reliability, mobility, DRP/BCP
- Virtualization allows you to use one piece of hardware to run multiple simulated environment
- Cloud Threats
  - Data breach/loss, insider threats, account hijacking, DoS/DDoS, insecure APIs

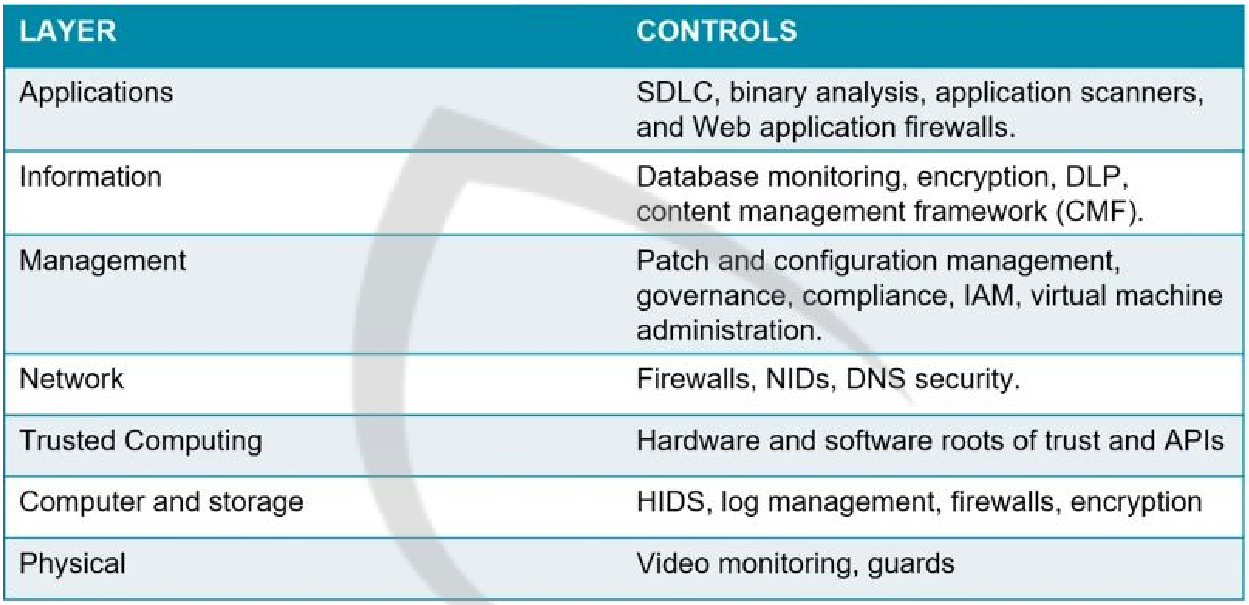
Lesson 16.1: Cloud Attacks EH

Skills Learned From This Lesson: Cloud Attacks

- Side channel attacks need a VM on the same physical host as a target
- Kinds of attacks
  - Side Channel, SQL injection, Wrapping, Man-in-the-cloud, service hijacking by sniffing, session hijacking by XSS, DNS amplification attack

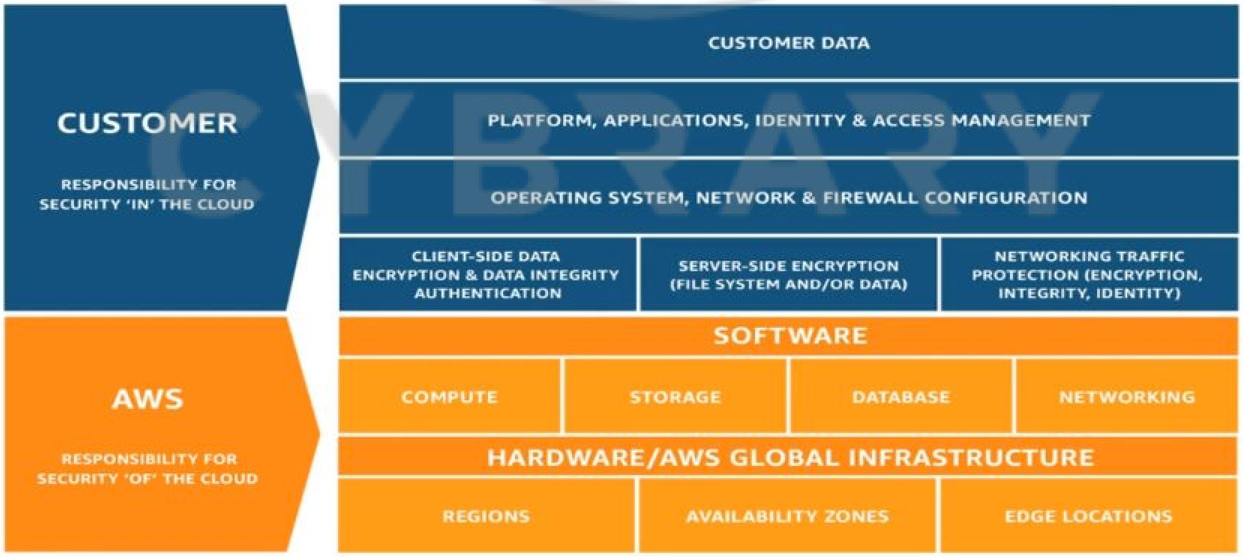
Lesson 16.2:Cloud Final EH

Skills Learned From This Lesson: Cloud Security Considerations, Cloud Security Controls, Cloud Security Best Practices



LAYER	CONTROLS
Applications	SDLC, binary analysis, application scanners, and Web application firewalls.
Information	Database monitoring, encryption, DLP, content management framework (CMF).
Management	Patch and configuration management, governance, compliance, IAM, virtual machine administration.
Network	Firewalls, NIDs, DNS security.
Trusted Computing	Hardware and software roots of trust and APIs
Computer and storage	HIDS, log management, firewalls, encryption
Physical	Video monitoring, guards

- Shared Responsibilities


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

- Security Considerations
    - Is the data critical?
    - Can I move the data?
    - Availability? BCP/DRP?
    - Backups? Encryption?
    - Ownership?
    - Vendor?
- Cloud Security Controls
    - Encryption
    - Change management (track changes)
    - Strong IAM controls
- Cloud Security Best Practices
    - End-to-end encryption
    - Encryption at rest
    - Vulnerability and incident response
    - Data retention policy
    - RNAC
    - VPC
    - Compliance certifications

Module 17: Sessions Hijacking

Lesson 17.0: Algorithm Cryptography CEH

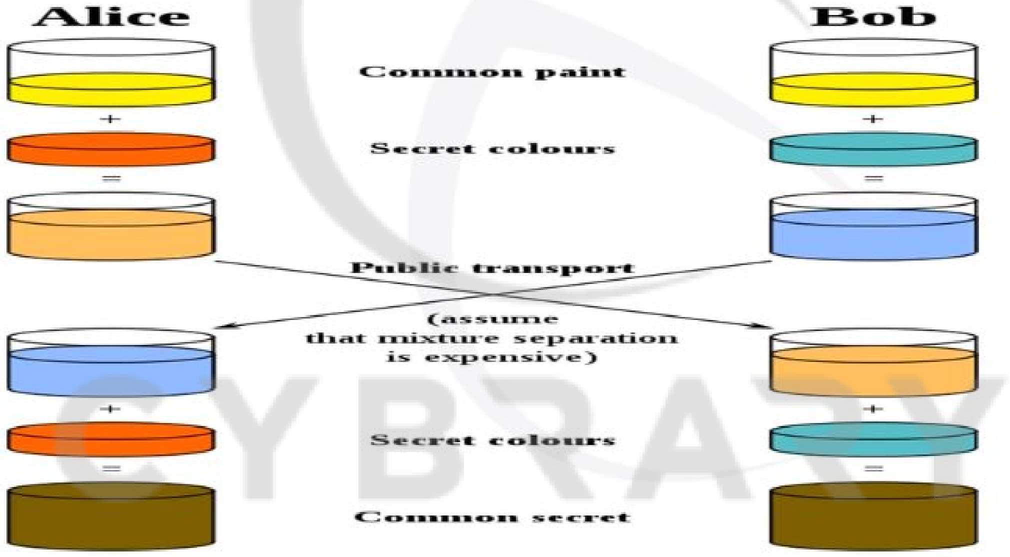
Skills Learned From This Lesson: Crypto Definitions, Types of Cryptography, Encryption algorithms

- Symmetric encryption uses a single key for encryption/decryption
- Cryptography - study and practice of techniques for secure communication in the presence of third parties
- Cryptanalysis - study of analyzing information system to study the hidden aspects of the system
- Cipher - algorithm for performing encryption or decryption
- Types
  - Symmetric - uses a single key
  - Asymmetric - uses a public and private key pair
  - Hashing - no key. Plaintext is not recoverable from the ciphertext
- Government Access to Keys - key escrow means that the government has copies of, or enough information to crack, all keys
- Encryption algorithms
  - **Ciphers** - generally substitute the same number of characters that are input
  - **DES** - Data Encryption Standard. 56-bit key size. Insecure but influential
  - **3DES**. - Applies DES 3 times. Symmetric
  - **AES** - Advanced Encryption Standard. Symmetric. 128 bit block size. Key size of 128, 192, 256
  - **RC4** Stream cipher. Insecure. Few first bits are non random. Analyze high volume of messages to discover key
  - **RC5** - data dependent rotations. Rotation dependant on the least significant few bits
  - **RC6** - Block size of 128 bits. Key sizes of 128, 192, 256. Rotation dependant on every bit in the word

Lesson 17.1: Algorithm and Hash Cryptography EH

Skills Learned From This Lesson: Encryption Algorithms, Hashing Algorithms

- Encryption algorithms
    - **Twofish -** Symmetric. Block size of 128. Key size up to 256 bits. Key dependent S-boxes that obscure relationship of key and cipher
    - **Digital Signature Algorithm (DSA)**
        - 2 choices for key generation
            - Choice of algorithm parameters (shared between different users)
            - Computes public and private keys for user
        - ECDSA - Playstation 3, failOverflow
    - **Rivert Shamir Adleman (RSA) -** Asymmetric
    - **Diffie-Hellman -** Asymmetric



- Hashing
    - **MD5 (Message Digest Function) -** produces 128-bit value. Non identical messages can have the same hash value (collision)
    - **SHA (Secure Hashing Algorithm)**
        - SHA-1 - 160-bit hash value
        - SHA-2 - 224,256,384, and 512 bit values
        - SHA-3 - 512 bit value. Sponge construction

  - **RIPEMD - 160 -** RACE Integrity Primitives Evaluation Message Digest). 160 bits. Avalanche effect behaviour
  - **HMAC -** Hash-based message authentication code. Cryptographic hash function and cryptographic key. Integrity and authentication

Lesson 17.2: Cryptography Tools EH
Skills Learned From This Lesson: Cryptography Tools

- Hash Calculators - Input/output. Hashcalc in labs. Cyberchef.io online
- Advanced Encryption Package 2017 - has over 20 encryption algorithms
- Bctextencoder -
- Whispercore - works with older Android OS

Lesson 17.3: PKI Disk Encrypt Email Cryptography EH
Skills Learned From This Lesson: PKI, Email Encryption, Disk Encryption

- Public Key Infrastructure (PKI)
  - Roles, policies, procedures needed to create manage, distribute, store and revoke digital certificates
  - Bind public keys to entities
  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Web of trust
- Email Encryption
  - Digital Signature (DSA)
  - SSL isn't used due to POODLE
  - TLS (transport Layer Security)
    - TLS 1.2 - SHA-256. Removed SSL Compatibility
    - TLS 1.3 - Removed support for: MD5, SHA-224, weak elliptic curves
  - Pretty Good Privacy (PGP)
    - End to end
    - Open PGP Standard (RFC 4880)
    - Symmetric/Asymmetric
    - GNU Privacy Guard
- Disk Encryption
  - Full disk, every bit of data encrypted, MBR or similar areas not encrypted often

Lesson 17.4: Cryptography Lab Part 1 EH

Skills Learned From This Lesson: Skills Learned From This Lesson: What Are Hashes?, Installing Hashcalc, Verifying Hashes

- This lab is done in any Windows Environment
- Hashes are one way
- Hashes can be used to verify integrity of files
- From a web browser search for Hashcalc
- Install Hashcalc (Slavasoft)
- Open Hashcalc - find Hxdset.zip -select calculate to verify hash against hash on the website
- Install HxD Hex Editor

Lesson 17.5: Cryptography Lab Part 2 EH

Skills Learned From This Lesson: Open Files in HxD Hex Editor, Basic Hex Editing

- Open a web browser - search for any photo - download the image
- Open HxD Hex Editor - file open the image you downloaded
- FF D8 FF - means jpeg file
- Scroll to the bottom of the page in
- After the last text, type whatever you want
- Save it as another file name

Lesson 17.6: Photo Cryptography Lab EH

Skills Learned From This Lesson: Photo Forensics, Calculating Hashes of Files Using HashCalc,

- No visual difference in the edited and unedited files
- Files are the same size
- Open HashCalc - open each photo file -calculate the hash (MD5)
- File hashes are not the same
- Open HxD Hex Editor to review the hex of the files

Lesson 17.7: Bonus Cryptography Lab EH

Skills Learned From This Lesson: Checking Certificates of Websites

- You can check the certificates of pages by clicking the lock icon of pages
- The open certificate
- It will show you the Certificate Authority, date range, etc…
- You can check the certification path

Lesson 17.8: Cryptography Final EH

Skills Learned From This Lesson: Types of Cryptanalysis, Cryptography Attacks

- Cryptanalysis
    - Linear Cryptanalysis
        - Construct linear equations relating to plaintext, ciphertext and key bits that are likely to be close to 1 or 0
        - Use the discovered linear equations, along with known plaintext-ciphertext pairs to figure out the key bits
        - Used in block and stream cipher attacks
    - Differential Cryptanalysis
        - Non-random behaviour in ciphers
        - Method
            - Chosen-plaintext attack (must have ciphertext for a set of plaintext)
            - Method uses pair of plaintext (related by constant difference: XOR)
            - Ciphertext patterns
    - Integral Cryptanalysis
        - Uses set/multisets of chosen plaintexts
        - Part of plaintexts will be constant with others being variable
        - Example: 256 plaintexts that have all but 8 bits that are the same
- Cryptography Attacks
    - Brute-Force - passwords/passphrases
    - Birthday: depends on more collisions found between random attack attempts
    - Meet-in-the-middle: space-time tradeoff
    - DHUK - Don't Use Hard-coded Keys
    - Rainbow Table

Module 18: Reports

Lesson 18.0: Reporting EH

Skills Learned From This Lesson: Sections of Penetration Testing Report, Stages of Testing

- Introduction - Who are you
- Scope - What are we testing. What are we invited to test.Why were we chosen.
- Executive Summary - Major Headlines
- Executive Recommendations - Things to be fixed right away
- Further Information - Drill down on the information in the report
- Main Body
  - Introduction - Outline the test that were done. Time frame
  - Summary of Methodology Used - Black, white, grey box testing
  - Definitions
- System Description - describe the infrastructure as we've been able to see it
  - Infrastructure
  - Key or critical points - high value assets
  - Network ranges - included and excluded
  - Documented configuration and architecture
- Technical Analysis
  - CVEs or misconfigurations
  - Assessed impact of current risks
  - Significant Threat Attack Vectors
- Stages of Testing
  - Classic Penetration Testing Methodology
  - Box by Box
- Security Policy Documentation
  - Policy Compliance
  - Why Live System must meet Policy Requirements
  - Security Mechanisms encountered
- Annexes

Module 19: Summary

Lesson 19.0: Course Summary EH

Skills Learned From This Lesson: Module Overview

- Module Overview
- Download extra resources
- Practice hands on skills - Cybrary has labs and other great tools!