Study Guide

Course Name

Created By: Arnav Banerjee, Teaching Assistant

Module 1: Introduction

Lesson 1.1: Nmap: What It Is and Why It's Important – NM
Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- Open-source scanner.
- Developed in 1997 by Gordon Lyon, a.k.a., Fyodor.
- Suite of tools, includes, Zenmap, Npcap, Ncat, Nping and Ndiff.
    - Zenmap- GUI tool for Nmap.
    - Npcap- Pcap library for Nmap.
    - Others help in Nmap's functioning.
- Why Nmap?
    - Most commonly used.
    - Flexible, powerful and portable.
    - Easy, free and well-documented.

Lesson 1.2: About the Instructor – NM
Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- Masters in CyberSec with CISSP and CEH with nearly 25 years of experience.
- Linkedin: therobthurston.

Lesson 1.3: Course Overview and Prerequisites – NM
Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- Free ebook at Nmap's site: https://nmap.org/book/toc.html, covers most of the features.
- Module foci:
    - Mod-2: Nmap Basics: Installing and Removing, running scans from Command-line, intro to Zenmap Gui.

    - Mod-3: TCP/IP protocol suite, TCP, UDP and ICMP headers, how Nmap crafts packets, wireshark analysis of package, nmap and Ipv6, etc.
    - Mod-4: Popular nmap scans, host discovery, port scanning, service and application version detection and OS detection.
- Pre-requisites:
    - General understanding of TCP/IP protocol suite.
    - 3-5 years of experience.
    - CompTIA Network+, Security+ or Cisco CCNA.

Lesson 1.4: Ethics and Legality of Scanning – NM
Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- Ethics of Scanning
- Legalities of scanning
- Seek legal advice
- Obtain written authorization
- References:
    - https://nmap.org/book/man-legal.html
    - https://nmap.org/book/legal-issues.html
    - Computer Fraud and Abuse Act of America, Section 1030(a)(5)(B).
    - Lawyer Ethan Preston's Papers.

Module 2: Nmap Basics

Lesson 2.1: Installing Nmap on Windows – NM
Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- Download: https://nmap.org/download.html
- Windows Setup info and tweaks: https://nmap.org/book/inst-windows.html
- Stable release self-installer is all inclusive, however, command-line installer requires Npcap and MS Visual C++ 2013 Redist. separately.
- Test scan: **nmap scanme.nmap.org**

Lesson 2.2: Installing Nmap on Linux – NM
Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- Nmap origins: Started on Linux/Unix.
- Linux setup and tweaks: https://nmap.org/book/inst-linux.html

- Installation with dpkg or apt is possibly a version behind.
- RPM installation commands:
  - rpm -vhU https://nmap.org/dist/nmap-7.80-1.x86_64.rpm
  - rpm -vhU https://nmap.org/dist/zenmap-7.80-1.noarch.rpm
  - rpm -vhU https://nmap.org/dist/ncat-7.80-1.x86_64.rpm
  - rpm -vhU https://nmap.org/dist/nping-0.7.80-1.x86_64.rpm
- Debian-based distro (Ubuntu and similar) command sequence:
  - sudo apt-get update
  - sudo apt-get install nmap
  - sudo apt-get install zenmap -y
- Test scan: **nmap scanme.nmap.org**

Lesson 2.3: Installing Nmap on Mac – NM

Skills Learned From This Lesson: Nmap, ZenMap, NPCap, Ncat, Nping, Ndiff.

- MacOS setup and tweaks: https://nmap.org/book/inst-macosx.html
- Latest stable release installer can be found on Nmap's website and the ".dmg" can be installed.
- Homebrew is a package manager for MacOS (https://brew.sh).
- Installs packages in their own directory and symlinks them to /usr/local.
- Homebrew installation commands:
  - /usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
  - brew install wget –with-libressl
  - brew update
  - brew upgrade
  - brew install nmap
  - brew cask install zenmap
- Test scan: **nmap scanme.nmap.org**

Lesson 2.4: Kali Linux: A Hacker's Best Friend – NM

Skills Learned From This Lesson: Nmap, ZenMap, Kali Linux.

- Kali Linux made and managed by Offensive Security.
- Previously called Backtrack and re-built on Debian.
- Useful for Pentesting, Security Research, Computer Forensics and Reverse Engineering.

- Free, Open-Source and FHS Compliant.
- Download: kali.org/downloads.
- Can be run as main OS, dual-boot with Mac or Windows, as a VM or as a "Live CD/DVD".

Lesson 2.5: Kali Linux Lab: Running it Live - NM
Skills Learned From This Lesson: Nmap, ZenMap, Kali Linux, VirtualBox.

- Download 64-bit Kali Light from Kali website.
- Virtualbox Download: virtualbox.org
- Slavasoft HashCalc download: slavasoft.com/hashcalc
- Copy the Hash from kali website and right click on the Kali file>> CRC SHA>> SHA-256. Compare the 2 values.
- Creating Kali VM in VirtualBox – Click "New">> Name = "Kali Light">> Type = "Linux">> Version = "Debian (64-bit)" >> Click "Next" >> *Leave Memory size as default* >> Click "Next" >> Select "Do not add a virtual hard disk" >> Click "Create" >> Click "Continue".
- Loading Kali Image – Right click on "Kali Light">> Click "Settings">> Click "Storage">> Click on "Empty" (Under Controller IDE)>> Check "Live CD/DVD" (On the right)>> Click on the "CD" icon>> Click "Choose Virtual Optical Disk File">> Browse to and Double-Click the Kali image>> Click "OK".
- Default Username: "root" and default password: "toor".
- Open Terminal and Test scan: **nmap scanme.nmap.org**.

Lesson 2.6: Removing Nmap from Windows - NM
Skills Learned From This Lesson: Nmap, ZenMap, cipher.

- Open command prompt in Windows as Administrator.
- Nmap files are most commonly in "Program Files (x86)".
- Open "Programs and Features" in Control Panel and uninstall Npcap and then Nmap.
- Traces and few files are left behind by Nmap uninstaller.
- Deleting files in filesystem only deallocates the memory/storage associated with the file.
- To remove traces of the application: **cipher /w:Nmap**.

Lesson 2.7: Removing Nmap from Linux - NM
Skills Learned From This Lesson: Nmap, ZenMap, apt-get.

- Open terminal and remove Zenmap, first, using: sudo apt-get remove --auto-remove zenmap.
- Then remove nmap: sudo apt-get remove --auto-remove nmap.

Lesson 2.8: Removing Nmap from Mac - NM
Skills Learned From This Lesson: Nmap, ZenMap, brew.

- Open terminal and remove Zenmap, first, using: brew cask uninstall zenmap.
- Then remove nmap: brew uninstall nmap.

Lesson 2.9: Getting Help - NM
Skills Learned From This Lesson: Nmap, ZenMap, cipher.

- All OS commands:
  - "nmap -V" -> Nmap version information, platform running on and how it was compiled.
  - "nmap" or "nmap -h" -> Provides the list of simple scan options available, with examples.
  - "nmap –script-help <script-name>" -> Provides details of the script, as published by the author.
- Linux/Unix/macOS:
  - "man nmap" -> Manual page for nmap
  - "man zenmap" (no macOS). -> Manual page for nmap
- Man page gives more information than the help switch for the command.
- Online contents/help:
  - Nmap docs: https://nmap.org/docs.html
  - Reference Guide: https://nmap.org/book/man.html
  - Zenmap GUI help: https://nmap.org/book/zenmap.html
  - Book: https://nmap.org/book/
  - Subscribe to Nmap hackers: https://nmap.org/download.html
- Conferences and Social Media:
  - FB: facebook.com/nmap
  - Twitter: twitter.com/nmap
  - USENIX: usenix.org
  - DefCon: defcon.org
  - BlackHat: blackhat.com

Lesson 2.10: Phases of the Nmap Scan - NM

Skills Learned From This Lesson: Nmap, ZenMap, traceroute, r-DNS, NSE.

- Reference: https://nmap.org/book/nmap-phases
- Knowing scan phases helps in tuning the scan and also, constructing the required nmap scan.
- Scan Phases of Nmap:
    - Phase 1: Script Pre-scanning
        - Occurs while running NSE scans.
        - Scripts that only have to be run once per Nmap execution.
    - Phase 2: Target Enumeration
        - Occurs with every scan.
        - Determines hosts to scan.
    - Phase 3: Host Discovery
        - "Ping Scanning".
        - Determines which targets are online.
        - Can be skipped.
        - Improves performance if not used or needed.
    - Phase 4: Reverse-DNS resolution
        - Occurs by default when specifying IPs.
        - Hostnames can provide valuable insight about the host.
        - Can be skipped or forced, based on requirement.
    - Phase 5: Port Scanning
        - Backbone of Nmap usage.
        - Significant but is only a single component.
        - Probes sent; responses evaluated.
        - Default for every Nmap scan but can be skipped.
    - Phase 6: Version Detection
        - Port open – Determine server software.
        - Compares responses to known signatures.
        - Can be enabled on any scan.
    - Phase 7: OS Detection
        - Optional, but part of some default scans.
        - Can be run in any scan.
        - Compares responses to known signatures.
        - Provides a degree of likelihood.

        - Can be enhanced with several NSE script scans.
    - Phase 8: Traceroute
        - Enhanced traceroute engine.
        - Can be forced on any scan.
        - Determines route to target, then runs reverse-DNS lookup.
        - Reverse-DNS lookup occur in parallel for enhanced performance.
    - Phase 9: Script scanning
        - Most of the script scan is done in this phase.
    - Phase 10: Output
        - Final phase of most scans.
        - O/p results to screen or to a file.
        - Sometimes the most important phase.
        - Can be both searchable and/or report quality.
    - Phase 11: Script post-scanning
        - Theoretical so far.
        - Can process results and deliver final reports and statistics.
        - Not used by any official NSE script, so far.
        - Likely to change.
        - Custom Scripts in Lua can be processed by this.

Lesson 2.11: Constructing an Nmap Scan – NM

Skills Learned From This Lesson: Nmap, ZenMap, NSE.

- Requirements:
    - Command prompt/terminal should be as privileged user.
    - Check Environment variable/Path variable and availability of Nmap through them.
    - Basic scan – "nmap <target>"
- Order of options is not fixed but create a pattern for convenience.
- Important stuff:
    - Target: hostname(s), IP address(es), network(s) (in CIDR notation).
    - Output: -oN (normal/text file), -oX (XML file), -oS (Script-kiddie format), -oG (Greppable format), -oA (in all the formats: -oN, -oX, -oG), -v or -vv.
- Regular vs Script scan:
    - Regular: "nmap <option(s)> <target(s)>"
    - Script:
        - nmap <option(s)> -sC target ➔ All default NSE scripts are run.

- nmap <option(s)> --script= <script-name> <target(s)>

Lesson 2.13: General Considerations – NM
Skills Learned From This Lesson: Nmap, ZenMap, NSE.

- GUI or CLI: Based on available situation but start with CLI.
- Benefits of using Zenmap:
  - Point and Click.
  - Graphical Environment is sometimes easier.
  - Can create and save custom scan profiles.
  - Good way to learn nmap.
  - NSE scripts guide is useful.
- Reference: https://nmap.org/book/zenmap.html

Lesson 2.14.1: Custom Scan Profiles Part 1 - NM
Skills Learned From This Lesson: Nmap, ZenMap, NSE.

- Custom scan profile is a graphical mechanism to set scan options.
- Saves across Zenmap sessions.
- Easy to create and modify.
- Importance:
  - Easy environment to set options.
  - Good way to learn order of options – Not relevant but helps understand the phasing of options, standard for building command line scans and at times increases scan speed.
  - Can save, modify and run many times.

Module 3: Nmap Basics

Lesson 3.1: IPv4 for Nmap - NM
Skills Learned From This Lesson: Nmap, ZenMap, CIDR notation.

- TCP/IP stack still used in WANs and LANs.
- 2 Protocols: TCP: Layer 4 Transport layer protocol and IP: Layer 3 Network layer protocol.
- Connection-oriented: State is maintained in order to make sure delivery successful delivery of packets.

- Uses 3-way handshake: SYN→ SYN-ACK→ ACK.
- TCP and UDP both use ports to identify the type of data, application and service running.
- IP Addressing:
    - 4-octets (max value is composed of 8 bits, hence octet) separated by a decimal point with numbers in their decimal form.
    - ipconfig – Windows and ifconfig – linux, unix and mac os.
    - The physical address of the host cannot be determined remotely. Need physical access to switch/router/host to determine the address. Exception- when the scanning device sits on span or mirrored port.
- CIDR:
    - Classless Inter-Domain Routing.
    - CIDR notation: <IP address(es)>***/***<Set bits from Subnet mask>.
    - Nmap allows use of CIDR notation.
- DNS:
    - Domain Name System.
    - Name to IP address resolution.
    - Nmap allows use of FQDN for target.
    - By default, it uses the DNS service of the scanning system. This can be changed for using alternate name servers.

Lesson 3.2: IP, TCP, UDP, and ICMP Headers - NM

Skills Learned From This Lesson: Nmap, ZenMap, packet headers.

- Encapsulation:
    - Process of adding headers and trailers to data.
    - Datagram name w.r.t. Layers: Application: Datagram, Transport: Segment, Network: Packet, Link Layer: Frame.
    - Nmap manipulates it's scan using each of the layers.
    - Reference: https://youtu.be/xaKvGnnuYmk
- 3-way handshake:
    - This makes it possible for TCP to be a connection-oriented protocol.
    - The process: SYN-> SYN-ACK->ACK->" Connection Established"
    - SYN and ACK are 2 flags in the packet.
    - Nmap can manipulate TCP flags to generate responses that can give greater details about the host.

    - This uses the Nmap packet crafter: Nping, for this purpose.
    - Reference: https://youtu.be/LyDqA-dAPW4
- TCP Header:
    - Important Components for Nmap in TCP header: Source port, Destination port, TCP flags.
    - Source port is determined by Nmap when initiating the connection.
    - Destination port can be determined by the user or by Nmap based on the scan option set.
    - TCP SYN scan: nmap -sS
    - TCP ACK scan: nmap -sA
    - TCP full connect scan: nmap -sT
    - X-mas scan: nmap -sX -> Sets up all the flags in TCP header.
    - Other switches in TCP header: U: Urgent, P: Push, R: Reset, F: Finish.
    - Reference: https://youtu.be/M-zX_6FuFKg
- UDP header:
    - Important Components: Source port, Destination port.
    - UDP scan: nmap -sU
    - DNS uses TCP/UDP port 53, NTP uses UDP port 123, NetBIOS uses UDP port 137, LDAP uses UDP port 389.
- IP header:
    - Important Component: Version, Protocol, Source and Destination IP address.
    - Version: for IPv4 the value is 4. But IPv6 has a different header structure.
    - Protocol: protocol used in the creation of the package. TCP: 6, UDP: 17, ICMP: 1
    - IP protocol scan: nmap -sO
    - By default, nmap scans for all possible 256 Protocol values.
    - Reference: https://youtu.be/UrO-9Uagn24
- ICMP header:
    - Important Component: Type, Code.
    - Ping scan is not the same as ICMP scan.
    - ICMP scan: nmap -sn -PE
    - Reference: https://youtu.be/FprZF9agJJI

Lesson 3.3.1: Nmap and Wireshark Part 1 - NM
Skills Learned From This Lesson: Nmap, ZenMap, Wireshark.

- Wireshark by default does not capture all network traffic. To do that, we need to set it to Promiscuous mode.
- Wireshark with Nmap provides an insight to how Nmap works and analyse granular details on requests made by Nmap.
- Wireshark Cheat Sheet: https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

Lesson 3.3.1: Nmap and Wireshark Part 2 – NM
Skills Learned From This Lesson: Nmap, ZenMap, Wireshark.

- Nmap sets the Push, Urgent and Finish flags in the TCP requests in case of an Xmas Scan.
- UDP scans do not have flags so targeted ports can be verified from Wireshark.
- TCP SYN scans only have SYN set but never responds with ACK, so ACK packets cannot be seen.

Lesson 3.4: Nmap & IPv6 - NM
Skills Learned From This Lesson: Nmap, ZenMap, IPv6.

- Nmap supports IPv6 since 2002.
- Nmap's popular features work fine with IPv6.
- IPv6 is complicated, hence preferably use hostnames.
- Output is pretty much the same.
- Scan requirements for IPv6:
    - Source and Target must be configured for IPv6.
    - In case, IPv6 is not provided, use tunnel broker service.
    - Or use 6-to-4 tunneling.
    - Free service: https://tunnelbroker.net/
- Syntax and Command Line:
    - nmap -6 <target> or nmap –ipv6 <target>
    - nmap -6 -S <source> <target> ## IPv6 Spoofing.
    - nmap -6 –hop-limit
    - https://nmap.org/book/nping-man-ip6-options.html

Lesson 4.1: Target Specification Review+ - NM
Skills Learned From This Lesson: Nmap, ZenMap, nping.

- Common Target Specification:
  - nmap <ip-address>
  - nmap <ip-address-range>
  - nmap <network in CIDR notation>
  - nmap <fqdn>
  - nmap <Domain name in CIDR>
  - nmap <ip1> <ip2> <ip3>
  - nmap -iL <targets.txt>
  - nmap -iR <number of targets to scan>
  - nmap –exclude <ip>
  - nmap –excludefile <exclude.txt>
  - Reference: https://nmap.org/book/man-target-specification.html

Lesson 4.3: Scan Techniques - NM

Skills Learned From This Lesson: Nmap, ZenMap, nping.

- Scan technique implies Protocol and Flags to use.
- TCP – RFC 793 and TCP/IP Protocol Suite – RFC 1180
- Suggested format: nmap [scan technique] [ports] [targets] [output]
- Reference: https://nmap.org/book/man-port-scanning-techniques.html
- Most Popular Scan techniques:
  - Default (TCP SYN Scan)- nmap -sS
  - Default for no Raw packet privilege (TCP Connect Scan)- nmap -sT
  - UDP scan- nmap -sU
  - IP Protocol scan- nmap -sO
  - SCTP INIT scan- nmap -sY
  - TCP ACK scan- nmap -sA
  - TCP Window scan- nmap -sW
  - TCP Maimon scan- nmap -sM
  - Out of State scan techniques and FW evasion:
    - Null Scan- nmap -sN
    - FIN Scan- nmap -sF
    - Xmas Scan- nmap -sX
    - FTP Bounce scan- nmap -b

Lesson 4.5.1: Host Discovery Part 1 - NM

Skills Learned From This Lesson: Nmap, ZenMap, nping.

- Scanning entire network results in quicker blocking.
- To narrow down potential targets.
- Reference: https://nmap.org/book/man-host-discovery.html
- Host discovery options:
    - List Scan: nmap -sL
    - No port/ping scan or ping sweep: nmap -sn
    - No ping: nmap -Pn
    - Additional features/options:
        - -n : No DNS resolution
        - -R : resolve all using DNS
        - --traceroute : Trace path to host
        - --dns-servers <server1>, <server2>, … : Custom DNS server for PTR lookup.
    - Other Host Discovery Options:
        - nmap -PS (Syn Ping), -PA (Ack Ping), -PU (UDP Ping), -PY (SCTP Init Ping), -PO (IP Protocol Ping).
        - nmap -PE, -PP, -PM – Results in nmap sending ICMP pings.
        - Nmap -PR (arp ping) – Provides MAC Addresses of the target.
        - Additionally:
            - --disable-arp-ping
            - --system-dns

Lesson 4.6: TCP & UDP Port Scanning – NM

Skills Learned From This Lesson: Nmap, ZenMap, nping.

- 3 types of ports: Well-known ports(up to 1023), Registered ports(1024-49151) and Dynamic ports (49152-65535).
- Port Scanning is the act of remotely testing numerous ports to determine in what state they are.
- Port states recognized by Nmap:
    - Open: Actively accepting incoming requests.
    - Closed: Port responds to NMAP probes but does not have a service running.
    - Filtered: NMAP cannot determine if it's open or not.

    - Unfiltered: Port is accessible but NMAP is unable to determine if it's open or close.
    - Open| Filtered: Port might be open or filtered.
    - Closed| Filtered: Port might be closed or filtered.
- Help InfoSec to determine attack surface.
- Open ports are possible points of breach.
- Information from this helps in asset tracking, n/w design mapping and policy compliance checks.
- Reference: https://nmap.org/book/port-scanning.html
- Useful commands:
    - Nmap <target> -> 1000 ports SYN scan
    - Nmap -F <target> -> Popular 100 ports scan.
    - Nmap -p <ports/service name> <target>
    - Nmap -sU -p < ports/service name> <target>
    - Nmap -sS -sU -p <ports> <target>
    - Nmap <scan technique> -p <ports> <target>

Lesson 4.8.1: Service and Application Version Detection Part 1 - NM
Skills Learned From This Lesson: Nmap, ZenMap, nping.

- Nmap matches the response for a port scan against the internal DB to determine the service in use.
- NMAP uses CPE from NIST for result reporting on services.
- Basic command: namp -sV <target>
- A more organized command: nmap <scan technique> <ports> -sV <target>
- Useful switches for versioning:
    - –version-intensity <level>
    - –version-light
    - –version-all
    - –version-trace
- Reference: https://nmap.org/book/vscan.html
- Reference: https://nvd.nist.gov/products/cpe/

Lesson 4.9.1: Operating System Detection and Fingerprinting Part 1 - NM
Skills Learned From This Lesson: Nmap, ZenMap, nping.

- Basic Command: nmap -O
- Organised Command Structure: nmap -O –script=smb-os-discovery -v <target>
- Useful OS versioning switches:
  - –osscan-limit
  - –osscan-guess or –fuzzy
  - –max-os-tries <values>
  - -A
- Reference: https://nmap.org/book/osdetect.html

Lesson 4.10.1: NSE, Vulnerability Testing & Exploitation Part 1 - NM
Skills Learned From This Lesson: Nmap, ZenMap, nsc.

- Nmap scripting engine uses Lua, an interpreted language.
- Script categories:
  - Auth, Broadcast, Brute, Default, Discovery, DoS, Exploit, External, Fuzzer, Intrusive, Malware, Safe, Version, Vuln.
- Large set of scripts pre-built and available.
- Triggering nmap scripting engine:
  - Nmap -sC <target>
  - Nmap –script <name/category> <target>
- Reference: https://nmap.org/book/nse.html

Lesson 4.11.1: Timing and Performance Part 1 - NM
Skills Learned From This Lesson: Nmap, ZenMap, nsc, nmap options.

- Performance can be impacted by:
  - Scan technique used.
  - Large n/w scans with default options.
  - Firewalls with response-rate limiting.
- Basic optimization:
  - Goal oriented scanning.
  - Leave out unnecessary tests.
  - Using updated Nmap.
  - Optimizing timing parameters.

Lesson 4.11.2: Timing and Performance Part 2 - NM
Skills Learned From This Lesson: Nmap, ZenMap, nsc, nmap options.

- Timing templates:
  - T0- Paranoid (for IDS evasion)
  - T1- Sneaky (for IDS evasion)
  - T2- Polite (for less bandwidth and resource consumption
  - T3- Normal (Default)
  - T4- Aggressive (Assumed to be on a fast and reliable network)
  - T5- Insane (Very fast network, with preference for speed over accuracy)
- Fine grain timing options take precedence over timing templates.
- Fine grained timing controls:
  - –host-timeout <time>
  - –min-rtt-timeout/ --max-rtt-timeout/ --initial-rtt-timeout <time>
  - –min-hostgroup/ --max- hostgroup <num hosts>
  - –min-parallelism/ --max- parallelism <num probes>
  - –scan-delay/ --max-scan-delay <time>
  - –max-retries <tries>
  - –min-rate/ --max-rate <number> (number of packets sent per minute)
- Time specs in nmap can be ms, s, m, h.
- Reference: https://nmap.org/book/performance-timing-templates.html.