# Capstone Project - Phase 2 - Identify Targets and Run Scans

* ***Goal***: Identify the tools and techniques to be used to perform host discovery and enumeration
* ***Procedure***: List out the tools you plan on using to perform network scans, the purpose for using them, and how you will use them. For example:
  + Tool: Nmap
    - Purpose: Obtain info on hosts and the services and operating systems they’re running
    - Commands: <List commands to be used for identifying live hosts, banner grabbing, OS fingerprinting, open ports, etc.>
* ***Deliverable***: Provide a minimum 2-page description of the tools you plan on using for the network scans, your reasoning for selecting them, and how they will be used. Be sure to include any challenges and potential drawbacks or limitations. Deliverable should cover at least 5 tools/resources.
* *Course content reference*: There are two optional labs, [Reconnaissance from the WAN](https://www.springboard.com/workshops/cyber-security-career-track/learn/#/curriculum/27756/27762) and [Scanning the Network on the LAN](https://www.springboard.com/workshops/cyber-security-career-track/learn/#/curriculum/27756/27764), that may help you with this step
* **NOTE**: Kali is not a tool; it is a Linux distribution or collection of tools, so do not include it in your list.

## Submission

### Nessus

* + About:
    - <https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/>
    - <https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus>
    - Vulnerability scanner by Tenable, Inc
    - Remote scanning tool, scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network
    - Lowest false positive rate with six-sigma accuracy
    - Tests each port on a computer, determining what service it is running
    - Available for Linux, Unix, FreeBSD
    - Client is available for Unix-based OS and Windows-based OS
  + Purpose:
    - Scanning vulnerabilities that could allow unauthorized control or access to sensitive data on a system
    - Misconfiguration scanning (ex. Open mail relay)
    - Denials of service scanning for vulnerabilities
    - Scanning for default passwords, common passwords, blank/absent passwords on system accounts
    - Other capabilities include scheduled security audits, detection of security holes in local or remote hosts, simulated attacks, to pinpoint vulnerabilities, detection of missing security updates and patches
  + Commands:
    - Ports that can be scanned range from 1 to 65535
    - The steps that are followed during scanning are:
      * Define scan parameters
      * Create scan
      * Launch scan
      * Analyze scan results
    - Step 1: creating a scan
      * After installing/launching Nessus, you can create a scan:
        + In the top navigation bar, click Scans
        + In the upper-right corner of the My Scans page, click the New Scan button
    - Step 2: Choose a Scan Template
      * Next, click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set. For a detailed explanation of all the options available, refer to [Scan and Policy Settings](https://docs.tenable.com/nessus/8_2/Content/TemplateSettings.htm) in the Nessus User Guide.
      * A scan policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more information, see [Create a Policy](https://docs.tenable.com/nessus/Content/CreateAPolicy.htm) in the Nessus User Guide.
      * The Nessus interface provides brief explanations of each template in the product. Some templates are only available when you purchase a fully licensed copy of Nessus Professional.
      * To see a full list of the types of templates available in Nessus, see [Scan and Policy Templates](https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm). To quickly get started with Nessus, use the Basic Network Scan template.
    - Step 3: Configure Scan Settings
      * Prepare your scan by configuring the [settings](https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm) available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.
      * Follow these steps to run a basic scan:
        + 1. Configure the settings in the Basic Settings section.
        + The following are Basic settings:

| Setting | Description |
| --- | --- |
| Name | Specifies the name of the scan or policy. This value is displayed on the Nessus interface |
| Description | (Optional) Specifies a description of the scan or policy. |
| Folder | Specifies the folder where the scan appears after being saved. |
| Targets | Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets. |

* + - * + 2. Configure remaining settings

Although you can leave the remaining settings at their pre-configured default, Tenable recommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure they are appropriate for your environment.

For more information, see the [Scan Settings](https://docs.tenable.com/nessus/Content/TemplateSettings.htm) documentation in the Nessus User Guide.

* + - * + 3. Configure Credentials

Optionally, you can configure Credentials for a scan. This allows credentialed scans to run, which can provide much more complete results and a more thorough evaluation of the vulnerabilities in your environment.

* + - * + 4. Launch Scan

After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.

If you want to launch the scan immediately, click the down button, and then click Launch. Launching the scan will also save it.

The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

* + - Step 4: Viewing your Results
      * Viewing scan results can help you understand your organization’s security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan’s data.
      * You can view scan results in one of several views:

| **Page** | **Description** |
| --- | --- |
| Hosts | Displays all scanned targets |
| Vulnerabilities | List of identified vulnerabilities, sorted by severity |
| Remediations | If the scan’s results include remediation information, this list displays all remediation details, sorted by the number of vulnerabilities |
| Notes | Displays additional information about the scan and the scan’s results |
| History | Displays a list of scans: Start Time, End Time, and the Scan Statuses |

* + - * Viewing scan results by vulnerabilities gives you a view into potential risks on your assets
      * To view vulnerabilities:
        + In the top navigation bar, click Scans.
        + Click the scan for which you want to view results.
        + Do one of the following:
        + Click a specific host to view vulnerabilities found on that host.
        + Click the Vulnerabilities tab to view all vulnerabilities.
        + (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.
        + Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.
    - Step 5: Reporting Your Results
      * Chances are your job isn’t done yet. You need to report your findings to your team.
      * Scan results can be exported in several file formats. Some of these report formats are customizable, while others are designed to be imported into another application or product, such as Microsoft Excel or Tenable.sc. For an explanation of the various report formats and the purpose of each, see the [Nessus User Guide.](https://docs.tenable.com/nessus/8_2/Content/ScanReportFormats.htm)
      * To Export a Scan Report:
        + Start from a scan's results page
        + In the upper-right corner, click Export.
        + From the drop-down box, select the format in which you want to export the scan results.
        + Click Export to download the report.
  + drawbacks/limitations
    - Although nessus is an industry leading scanner, it is not all-encompassing; Tenable actually recommends to use a variety of scanners and agents to ensure full visibility into the entire network
    - Operators may not know the technical terms, so someone more professional will need to be managing the scanner
    - Potential to flood a network
    - Causing false network security events
    - Port knocking and passive ports may not be seen

### Nmap

* + About:
    - <https://www.varonis.com/blog/nmap-commands/>
    - Network mapper
    - a free and open-source network scanner created by Gordon Lyon
    - used to discover hosts and services on a computer network by sending packets and analyzing the responses
    - provides a number of features for probing computer networks, including host discovery and service and operating system detection
    - Perform port scans, ping scans, OS scans, version scans, etc.
  + Purpose:
    - Used to find live hosts on a network
    - Used for performing port scanning, ping sweeps, OS detection, and version detection
    - Used ideally as part of an integrated Data Security Platform
    - Provides information on:
      * 1. Every active IP so you can determine if an IP is being used by a legitimate service or an external attacker
      * 2. Your network as a whole, including live hosts, open ports and the OS of every connected device
      * 3. Vulnerabilities - scan your own server to simulate the process that a hacker would use to attack your site
    - Nmap functions (common)
      * Ping scanning
      * Port scanning
      * Host scanning
      * OS Scanning
      * Scan Top Ports
      * Output to Files
      * Disable DNS Resolution
  + Commands:
    - Prerequisites
      * (fundamental) Familiarity with command-line interfaces
      * (advanced) Know how to write scripts to automate tasks
      * [Install Nmap](https://www.varonis.com/blog/the-mirai-botnet-attack-and-revenge-of-the-internet-of-things/)
    - How to run a ping scan
      * Use the command
        + # nmap - sp 192.100.1.1/24
        + This command then returns a list of hosts on your network and the total number of assigned IP addresses
        + If you spot any hosts or IP addresses on this list you can’t account for, you can then run more commands to investigate them further
    - How to run a host scan
      * This actively sends ARP request packets to all the hosts connected to your network
      * Each host then responds to this packet with another ARP packet containing its status and MAC address
      * Use the command:
        + # nmap -sp <target IP range>
        + This returns info on every host, their latency, their MAC address, and also any description associated with this address. It’s a powerful way too spot suspicious hosts connected to your network
        + If you see anything unusual in this list, run a DNS query on a specific host by using:

# nmap -sL <IP address>

This returns a list of names associated with the scanned IP. this description provides info on what the IP is actually for

* + - Ping sanning
      * Command:
        + #
    - Port scanning
      * Command:
        + # sS TCP SYN scan

Most basic, gives most users all the info they need

Scans thousands of ports per second, doesn’t arouse suspicion bc it doesn’t complete a TCP connection

* + - * + # sT TCP connect scan

Alternative to above

Actively queries each host, requests a response

Takes longer than a SYN scan, but can return more reliable info

* + - * + # sU UDP scans

Similar to TCP scan but uses UDP packets to scan DNS, SNMP, and DHCP ports

Most frequently targeted ports by hackers, so this scan type is useful for checking for vulnerabilities

* + - * + # sY SCTP INIT scan

Covers diff set of services (SS7 and SIGTRAN)

Used to avoid suspicion when scanning an external network bc it doesn’t complete the full SCTP process

* + - * + # sN TCP NULL

Crafty; uses a loophole in the TCP system that can reveal the status of ports without directly querying them, which means you can see their status even where they’re protected by a firewall

* + - Host scanning
      * Command
        + # nmap -sp <target IP range>
    - OS scanning
      * Command:
        + nmap -0 <target IP>
    - Scanning popular ports
      * Command:
        + nmap --top-ports 20 192.168.1.106
        + Replace the “20” with the number of ports to scan, and Nmap quickly scans that many ports
    - Output to a file
      * If you want to output results of your Nmap scans to a file, you can add an extension to your commands to do that. Simply add:
      * Commands:
        + -oN output.txt
        + -oX output.xml
    - Disable DNS Name Resolution
      * Speed up your nmap scans by using the -n parameter to disable reverse DNS resolution
      * Useful if you want to scan a large network
      * Command:
        + # nmap -sp -n 192.100.1.1/24
  + Drawbacks/limitations:
    - Although it is versatile for TCP/UDP port scanning and detection capabilities, port scanning can congest networks when weaker devices are found, causing an unintentional DOS or network slowdown
    - Port scans are considered noisy (not very stealthy), but they require generating a lot of network traffic, so there’s an inverse relationship between stealth and speed.
    - This might trigger security alarms

### [Wireshark](https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it)

* + About:
    - Network protocol analyzer application
    - Network packet capture tool
    - Helps look at packets on a granular level
    - Filtering: capable of slicing and dicing random live data using filters, which allow you to obtain the information you want to see
    - Visualization: you can look into the very middle of a network packet to see entire conversations and network streams
  + Purpose:
    - Helps to put network traffic under a microscope
    - Utilized for filtering and drilling down into the network packets, zooming in on the root cause of the problems, assisting with network analysis and network security
    - Troubleshooting networks that have performance issues
    - Tracing connections, viewing the contents of suspect network transactions and identify bursts of network traffic
  + Commands:
    - Color Coding in Wireshark

| **Color in Wireshark** | **Packet Type** |
| --- | --- |
| Light Purple | TCP |
| Light Blue | UDP |
| Black | Packets with errors |
| Light green | HTTP traffic |
| Light Yellow | Windows-specific traffic, including Server Message Blocks (SMB) and NetBIOS |
| Dark Yellow | Routing |
| Dark gray | TCP SYN, FIN and ACK traffic |

* + - How to Filter and Inspect Packets in Wireshark
      * You can apply filters in 2 ways:
        + 1. In the Display Filter window at the top of the screen
        + 2. By highlighting a packet (or a portion of a packet) and right-clicking on the packet
      * Wireshark filters use key phrases, such as:

| ip.addr | Specifies an IPv4 address |
| --- | --- |
| ipv6.addr | Specifies an IPv6 address |
| src | Source - where the packet came from |
| dst | Destination - where the packet is going |

* + - * You can use the following values:

| && | Means “and,” as in, “Choose the IP address of 192.168.2.1 and 192.168.2.2” |
| --- | --- |
| == | Means “equals,” as in “Choose only IP address 192.168.2.1” |
| ! | Means “not,” as in, do not show a particular IP address or source port |

* + - * Additional filters include:

| tcp.port==8080 | Filters packets to show a port of your own choosing - in this case, port 8080 |
| --- | --- |
| ! (ip.src == 162.248.16.53) | Shows all packets except those originating from 162.248.16.53 |
| ! (ipv6.dst == 2607:f8b0:400a:15:b) | Shows all packets except those going to the IPv6 address of 2607:f8b0:400a:15::b |
| ip.addr == 192.168.4.1 && ip.addr = 192.168.4.2 | Shows both 192.168.4.1 and 192.168.4.2 |
| http.request | Shows only http requests = useful when troubleshooting or visualizing web traffic |

* + drawbacks/limitations
    - Filters may be difficult to remember or formulate; simple filter conditions might be easier to utilize and more efficient/quick
    - The user interface is not as user-friendly as many might have hoped; it’s designed for pure functionality, not ease-of-use
    - Lack of product support/training
    - The dashboard could be revamped and provide more insights

### Metasploit

* + [About](https://www.varonis.com/blog/what-is-metasploit/):
    - Used to be a way to gather public exploits into one place by a single researcher, HD Moore
    - Is now a commercial suite (used to be Rapid7, now Metasploit Pro)
    - Open source version is Metasploit Framework
    - A one-stop shop for reconnaissance, building exploits, remotely controlling them and exfiltrating data, and maintaining a collection of compromised computers and devices
    - One of the most powerful and widely used tools for pentesting
  + Purpose:
    - Use the kali distribution as an ethical hacker to use the tools for pentesting
    - The free version is similar to the commercial version
    - To probe systematic vulnerabilities in networks and servers
    - Open-source framework which is customizable and used with most OS
    - Can use ready-made or custom code and intro it to a network to probe for weak points
    - Once flaws are identified/documented, the info can be used to address systemic weaknesses and prioritize solutions
  + [Commands](https://www.tutorialspoint.com/metasploit/metasploit_quick_guide.htm):
    - help - shows a list of core commands in Metasploit along with their descriptions
    - msfupdate - an important admin command; used to update Metasploit with the latest vulnerability exploits
      * After running this command, you’ll have to wait several minutes until the update completes
    - search - powerful command to find what you want to locate
      * Ex. if you want to find exploits related to Microsoft, then the command will be -
        + msf >search name:Microsoft type:exploit
        + Here, search is the command, name is the name of the object you’re looking for, and type is the kind of script that you’re searching for
    - info - provides info regarding a module or a platform, such as where it’s used, who the author is, vulnerability reference, and its payload restriction
    - Parameters
      * -sV will detect the services with their version details
      * -O is to detect the version of OS
      * -T4 is the time that we let the scan to finish
    - Exploit using command prompt
      * Command:
        + msf > use “exploit path”

To use an exploit that works for you

* + - * + msf > show options

In order to see what parameters you have to set to make it functional

* + - * + msf > set RHOST 192.168.1.101
        + msf > set RPORT 21
        + msf > run
        + msf > show payloads
        + set PAYLOAD payload/path
  + drawbacks/limitations
    - Lack of options to manage payloads, exporting the results or integrating with reporting tools could use improvements
    - Improved dashboard usability to allow C level management to better understand concerns in a simpler manner
    - The chance to damage targeted systems increases exponentially as the experience of the user goes down
    - Lack of support caused the software to slow down since there are increasing use cases

### Spyse

* + About:
    - Records of the internet connected assets available for search and download
    - Allows (like Shodan/Zoomeye) to put in diff information that may have documented/recorded by the Spyse backend and you can pull info
    - Free to use (has a paid program too)
    - Offers different types of data:
      * Domains and Subdomains with their descriptions, SSL/ TSL certificates, DNS records etc. They also hold the largest subdomain database which is why it is considered as the best subdomain search engine on the web world.
      * IPv4 hosts with Geodata, domains on IP, ISP etc. with open ports for services and protocols.
      * SSL/ TSL Certificates with their types and the info of the issuers or providers on the domains and subdomains
      * DNS records
      * Autonomous Systems with much more interesting data such as the number of organizations, type of domain on AS and much more.
      * Whois information to check the authority of the websites with so many important information of a particular domain.
      * The same platform will provide more information and functionality of the domains in the next few months after completing its beta testing.
  + Purpose:
    - Designed with the latest development and OSINT techniques to scan the Internet world and to gather useful data from websites
    - Their database is constantly increasing as the search engine scans for new websites and new data regularly
    - Since it provides regular scans of websites, it makes it easier for new users to get quick results when they search for something on this Search Engine
  + Commands:
    - As a search engine, you simply type in the name of the organization you’d like to perform recon on, so for the dropdown menu on the left of the search bar, choose “Organization” and type in “Artemis” for this example
    - The results are now shown. You can click on the organization name and click “view details” to get the details of that organization.
    - It pulled data from crunchbase to provide details about the organization’s we’re trying to perform recon on; it shows details like AS numbers having a similar name, CIDRs with similar ISP name, SSL Certificates having similar issuer organization name, etc.
    - You can narrow down the pathway and perform recon on the domain from the top left pane; then clicking on the website details of the organization will take us to a different page with other information (whois details, emails, current and historical DNS records, certificates, technologies being used, subdomains, etc.)
    - Clicking on subdomains is more useful; we’ll see more details identified by Spyse’s tool that gives DNS A records CNAME, TLS/SSL versions used, title of website, and other metadata.
    - Click on subdomains to give more related IPs, SSL/TLS certs, and other details
    - Click “view details” to see other pages related to the asset - we’ll be able to see the number of CVE’s associated with the subdomain found by the scanners
    - It’s possible to filter out results to find particular SSL certificates that are used, then find the subdomains or domains that are associated with those in particular.
    - Clicking on certificates and then “find related domains” will allow us to find more domains related to the certificate, which allows ethical hackers to find as many assets as possible to locate vulnerabilities for bug bounty submissions
    - There’s a tool in the menu called “subdomain finder” which allows us to retrieve a list of subdomains identified by Spyse. It then brings us to a different interface that lets us input domain names and results in the subdomain list.
    - Lastly: once we have the list of subdomains, Spyse subscribers will have the option to download the results in either CSV or ND JSON format which can be parsed through and piped into any other tools for further testing.
  + drawbacks/limitations
    - Filter limitations may not allow for specific information to be harvested/pulled from certain sources
    - As an OSINT tool, it may not provide further insight than what the average person could find
    - Doesn’t provide analytics after search results are displayed; a dashboard of “what does x/y/z mean” could help users better grasp what they have pulled from the search engine