



# Network Discovery and Vulnerability Scanning

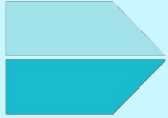
Cybersecurity  
Penetration Testing Day 2



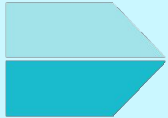
# Class Objectives

---

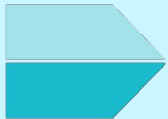
By the end of today's class, you will be able to:



Perform network enumeration using Nmap.



Properly use Nmap options.



Explain what the Nmap Scripting Engine (NSE) is and how it's used.

# Penetration Testing

---

The five phases of an engagement include:

01

Planning and Reconnaissance

02

Scanning

03

Exploitation

04

Post-Exploitation

05

Reporting

# Penetration Testing

---

In today's class we will work on the Scanning portion of a pentest. We will use manual tools to scan networks and enumerate valuable information.

01

Planning and Reconnaissance

02

Scanning

03

Exploitation

04

Post-Exploitation

05

Reporting

# Scanning

Network discovery and vulnerability scanning are essential in the early stages of an engagement. With the proper tools, we can complete the following tasks:

Term	Definition
<b>Network mapping</b>	Using host discovery, we can identify network devices like servers, switches, and routers, and how they're physically interconnected.
<b>Service discovery</b>	Allows us to identify which services are running on which hosts, such as DNS, mail, or web servers.
<b>OS detection</b>	Also known as OS fingerprinting, lets us detect which operating system is running on a networked device, including OS name, vendor, software versions, and estimated device uptime.
<b>Security auditing</b>	The discovery process for finding OS versions and apps running on hosts to determine the depth of vulnerabilities.

# Nmap

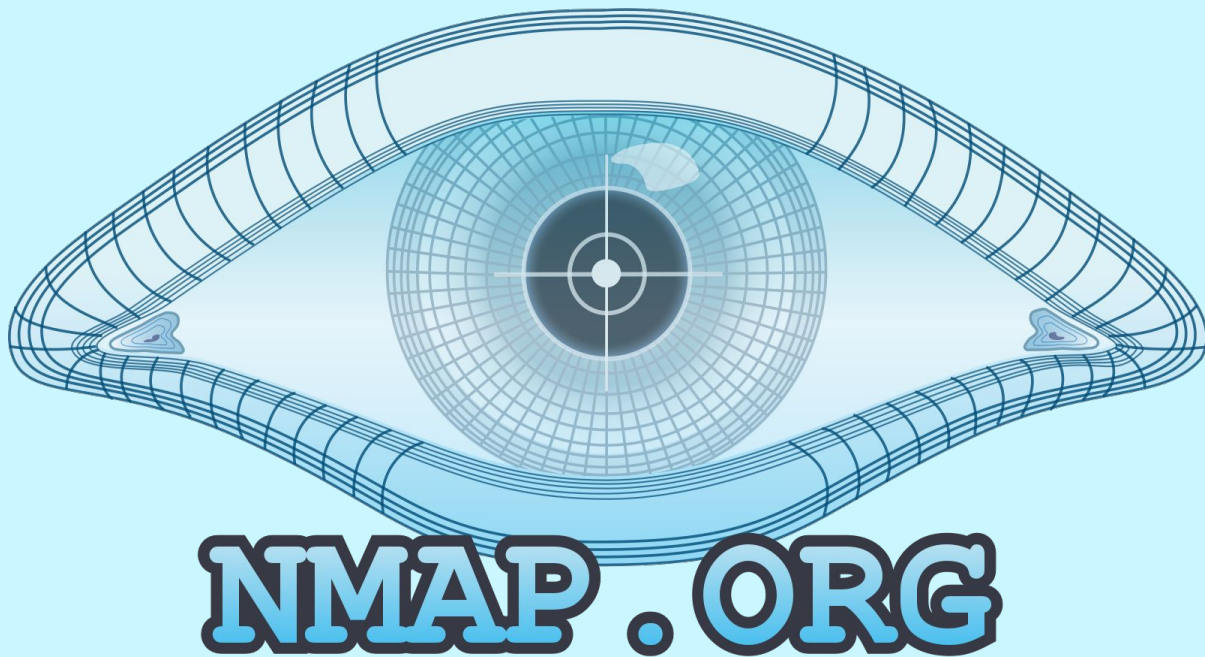
Nmap, short for Network Mapper, is a free, open-source network scanning tool for performing network discovery and vulnerability scans.

Identifying devices running on a network.

Discovering hosts, services, open ports, and IP addresses.

Detecting security risks.

...and much more.



# Nmap

---

The most common Nmap functions include:



Ping scans



Port scans



Host scans



OS detection



Top port scans

# Nmap Scans

Nmap transmits data through scans and listens for responses with information about the network profile and topology.

Nmap's protocols use various packet structures, such as TCP, UDP, and ICMP, which work together to enumerate networks.







Nmap has many scan types and options. Some optimize performance, some optimize stealth, others optimize accuracy. We'll explore several in the next demonstration.

# Is Nmap Legal?

---

Nmap is designed to help network defenders protect their networks from criminal hackers by identifying security vulnerabilities in the system.

But hackers can use Nmap for the same aim: to probe networks for vulnerabilities.

While laws are complicated and vary by region, using Nmap to scan external networks without permission can lead to being banned by your ISP and felony charges.





You should always get  
**written permission** from the  
system owner before engaging  
in any type of network scan.



# Instructor Demonstration

## Nmap



## **Activity:** Port Scanning with Nmap

In this activity, you will experiment with various Nmap scanning options.

**Suggested Time:**  
25 Minutes





**Time's Up!** Let's Review.

# NSE Scripting

# NSE Scripting

The Nmap Scripting Engine (NSE) allows users to write and share scripts that automate a wide variety of networking tasks. Nmap comes with a pre-installed collection of NSE scripts that can be used to modify and create custom scripts for individual needs.

```
instructor@kali:~$ ls /usr/share/nmap/scripts/
```

```
acarsd-info.nse      noscmap-crtsh.nse      ip-geolocation-geoplugin.nse  rsa-vuln-roca.nse
address-info.nse    hostmap-robtx.nse      ip-geolocation-ipinfodb.nse  rsync-brute.nse
afp-brute.nse        http-adobe-coldfusion-apsa1301.nse  ip-geolocation-map-bing.nse  rsync-list-modules.nse
afp-ls.nse           http-affiliate-id.nse   ip-geolocation-map-google.nse  rtsp-methods.nse
afp-path-vuln.nse    http-apache-negotiation.nse  ip-geolocation-map-kml.nse   rtsp-url-brute.nse
afp-serverinfo.nse   http-apache-server-status.nse  ip-geolocation-maxmind.nse   rusers.nse
afp-showmount.nse    http-aspnet-debug.nse      ip-https-discover.nse       s7-info.nse
ajp-auth.nse         http-auth-finder.nse      ipidseq.nse                 samba-vuln-cve-2012-1182.nse
ajp-brute.nse        http-auth.nse           ipmi-brute.nse              script.db
ajp-headers.nse      http-avaya-ipoffice-users.nse  ipmi-cipher-zero.nse       servicetags.nse
ajp-methods.nse      http-awstatstotals-exec.nse    ipmi-version.nse            shodan-api.nse
ajp-request.nse      http-axis2-dir-traversal.nse  ipv6-multicast-mld-list.nse  sip-brute.nse
allseeingeye-info.nse  http-backup-finder.nse      ipv6-node-info.nse          sip-call-spoof.nse
amqp-info.nse        http-barracuda-dir-traversal.nse  ipv6-ra-flood.nse           sip-enum-users.nse
asn-query.nse        http-bigip-cookie.nse       irc-botnet-channels.nse      sip-methods.nse
auth-owners.nse      http-brute.nse            irc-brute.nse                skypev2-version.nse
auth-spoof.nse       http-cakephp-version.nse      irc-info.nse                 smb2-capabilities.nse
backorifice-brute.nse  http-chrono.nse           irc-sasl-brute.nse           smb2-security-mode.nse
backorifice-info.nse  http-cisco-anyconnect.nse     irc-unrealircd-backdoor.nse  smb2-time.nse
bacnet-info.nse      http-coldfusion-subzero.nse   iscsi-brute.nse              smb2-vuln-uptime.nse
banner.nse           http-comments-displayer.nse   iscsi-info.nse               smb-brute.nse
bitcoin-getaddr.nse   http-config-backup.nse       isns-info.nse                smb-double-pulsar-backdoor.nse
bitcoin-info.nse      http-cookie-flags.nse        jdkwp-exec.nse               smb-enum-domains.nse
bitcoinrpc-info.nse   http-cors.nse                jdkwp-info.nse               smb-enum-groups.nse
```



# NSE

---

There's over 600 scripts available in NSE. With these, you can perform almost any infosec research task. For example, we can use NSE scripting to perform:

01

DNS enumeration

02

Brute force attack

03

OS fingerprinting

04

Banner grabbing

05

Vulnerability  
detection

06

Vulnerability exploitation

07

Backdoor identification

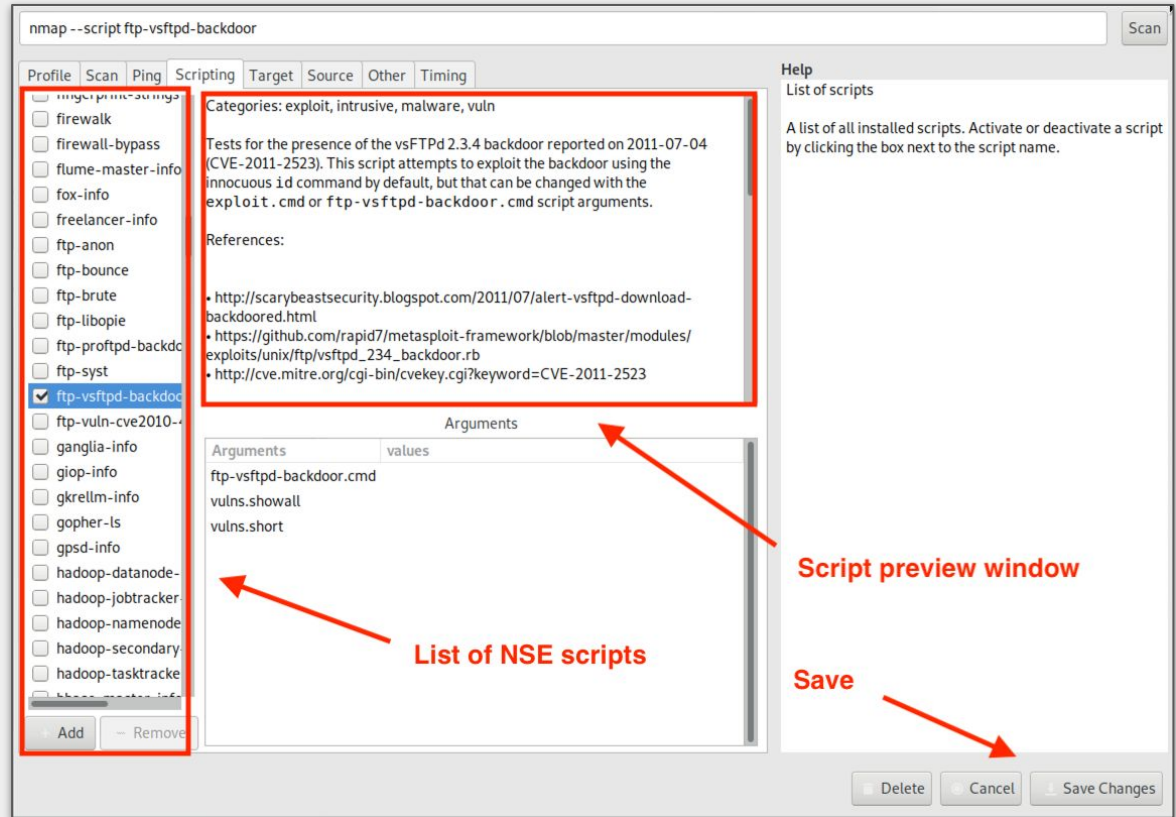
08

Malware discovery

# NSE in Action

We can use NSE to gather information on targets using scans.

While we can run scans directly on the command line, we can pair Nmap with a free, open-source GUI tool called **Zenmap**.



# Zenmap

---

For example, Zenmap displays Nmap output in a convenient GUI display. It can also:  
Zenmap works with Nmap to make it more user-friendly.



Customize display options.



Provide summaries about a single host or a network scan.



Generate topology maps of discovered networks.

# Zenmap

---

Zenmap benefits include:

01

## **Comparison**

Zenmap can compare changes between system scans run at different times, and differences between hosts.

02

## **Convenience and Discoverability**

While Nmap's hundreds of options can be overwhelming for beginners, Zenmap's simple interface helps beginners learn and understand Nmap scans.

03

## **Repeatability**

Zenmap has command profiles that make it easy to run scans more than once.

You can also use preinstalled shell scripts to perform common tasks.



# Instructor Demonstration

Zenmap



## **Activity:** NSE Scripting

In this activity, you will use Zenmap and its associated NSE scripts to gather intelligence about a target.

**Suggested Time:**  
25 Minutes





Countdown timer

15:00

(with alarm)



**Time's Up!** Let's Review.



# Vulnerability Scanning

# NSE Scripts vs. Vulnerability Scanning

---

While NSE has its advantages, it also has disadvantages when compared to other vulnerability scanners.



NSE is not fully comprehensive, meaning many vulnerabilities are not covered.



NSE cannot perform a large number of scans simultaneously.



NSE is most efficient when performing single host scans.



NSE is most useful when doing basic information gathering or enumeration tasks.

# Vulnerability Scanning

---

Vulnerability scanners such as **Nessus** can be used to identify vulnerabilities and create inventories of all interconnected systems.



# Vulnerability Scanning

---

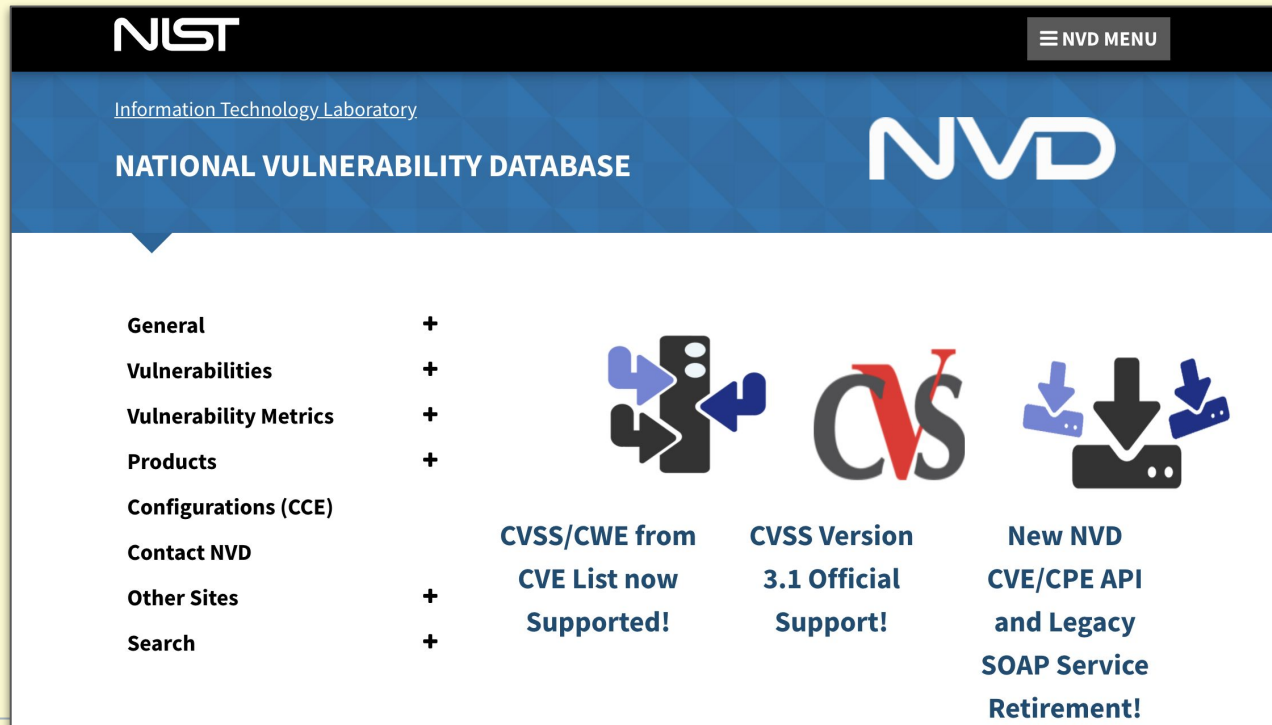
Most vulnerability scanners will attempt to log into systems using default passwords or other credentials in order to establish a more detailed picture of the network infrastructure.

After establishing an inventory list, vulnerability scanners check each item against one or more databases of known vulnerabilities. This identifies which items are associated with specific threats.



# NVD

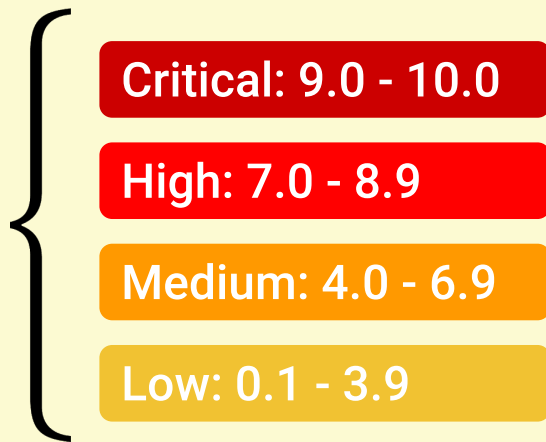
The National Vulnerability Database (NVD) is a source of exploit information that grades each vulnerability based on its severity level.



# NVD

For example, NIST CVE-2016-0800 is detailed on the [nvd.nist.gov](https://nvd.nist.gov) webpage, which provides details, references, and a score of 5.9.

Severity levels are scored using the **Common Vulnerability Scoring System** (CVSS), and have the following ranges:





# Instructor Demonstration

Nessus



## **Activity:** Metasploitable Report

In this activity, you will use Nessus to generate a Metasploitable scan report.

**Suggested Time:**  
25 Minutes







**Time's Up!** Let's Review.

*The  
End*