Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the** System Checker. The System Checker will confirm that your browser and network connection are ready to support virtual labs.

2. **Review the** Common Lab Tasks document. This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.

3. **When you've finished, use the Disconnect button to end your session and create a StateSave**. To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.
   If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.

4. Technical Support **is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.
   Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you’ve identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

Introduction

The hacking process consists of five main steps: footprinting, scanning and vulnerability assessment, enumeration, exploitation (the actual attacks), and post-attack activities, including covering tracks and planting backdoors. Black-hat hackers do this surreptitiously, but ethical hackers add an additional step at the beginning: they obtain written authorization from the target, their client, to perform the scanning and vulnerability assessment on a live production network. The difference between the ethical hacker and an attacker is written permission, complete transparency, and professional accountability.

Successful scanning and vulnerability assessment of a network is all about using the right tools to map the network and identify any vulnerabilities that could be the opening for a future attack. Nmap, and its graphical user interface Zenmap, is the most popular tool used to perform an initial IP host discovery as well as port/services scan for the first part of the scanning and vulnerability assessment step of the hacking process. Nessus performs the second part of this hacking step, the vulnerability assessment. Nessus can assess Linux, Windows, and network infrastructures, and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices. Any known vulnerabilities or bugs will be flagged and identified by Nessus. These two tools work together to complete the scanning and vulnerability assessment phase of the ethical hacking process and lay the groundwork for the third phase (enumeration).

In this lab, you will use Nmap commands within the Zenmap application to scan the virtual network and identify the devices on the network and the operating systems and services running on them. You will also use Nessus to conduct a vulnerability assessment and record the high risk vulnerabilities identified by the tool. Finally, you will use the information you gathered from the report to discover mitigations for those risks and make mitigation recommendations based on your findings.

Learning Objectives

Upon completing this lab, you will be able to:

1. Identify risks, threats, and vulnerabilities in an IP network infrastructure using Zenmap to perform an IP host, port, and services scan

2. Perform a vulnerability assessment scan on a targeted IP subnetwork using Nessus

3. Compare the results of the Zenmap scan with a Nessus vulnerability assessment scan

4. Assess the findings of the vulnerability assessment scan and identify critical vulnerabilities

5. Make recommendations for mitigating the identified risks, threats, and vulnerabilities as

described on the CVE database listing

Lab Overview

Each section of this lab is assigned at your instructor's discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.

SECTION 1 of this lab has three parts, which should be completed in the order specified.

1. In the first part of the lab, you will use Nmap commands in Zenmap to scan the 172.30.0.0/24 network.

2. In the second part of the lab, you will use the Nessus Vulnerability Scanner to assess the security posture of targeted hosts discovered during the Zenmap scan.

3. In the third part of the lab, you will compare the results of the Nmap and Nessus scans and make recommendations for mitigating any vulnerabilities.

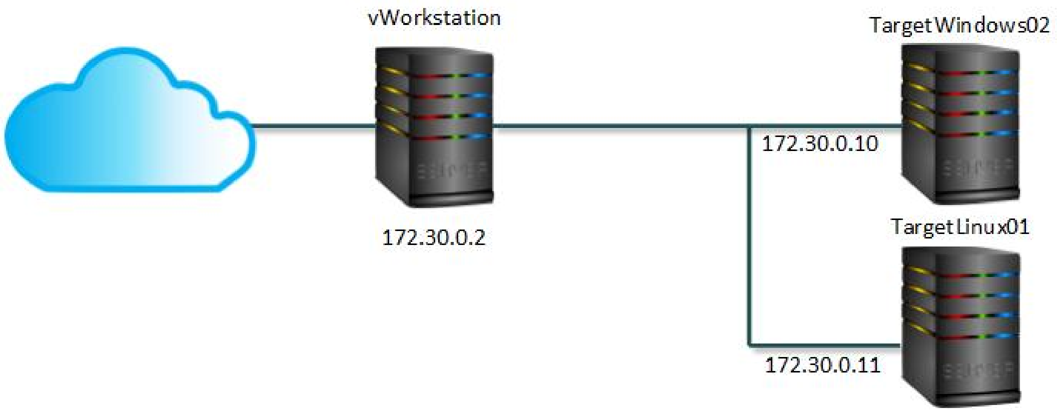
SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab. You will answer questions and complete challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Topology

This lab contains the following virtual devices. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetWindows02 (Windows Server 2016)
- TargetLinux01 (Debian Linux)



Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Nessus
- Zenmap

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1:

1. Lab Report file including screen captures of the following;

- Ports/Hosts tab from the SYN scan for 172.30.0.10;
- Hosts Details tab from the OS scan for 172.30.0.2;
- Ports/Hosts tab from the Service scan for 172.30.0.11;

2. Files downloaded from the virtual environment:

- *yourname*_S1_NessusScan;
- *yourname*_S1_NmapScans;

3. Any additional information as directed by the lab:

- Comparison of Zenmap scans with the HTML version of the scan results;
- Details and possible mitigations for all medium-risk vulnerabilities found on 172.30.0.10;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

SECTION 2:

1. Lab Report file including screen captures of the following:

- Hosts Details tab from the TCP Connect scan for 172.30.0.2;
- Ports/Hosts tab from the SYN scan for 172.30.0.11;
- Ports/Hosts tab from the Service scan for 172.30.0.10;

2. Files downloaded from the virtual environment:

- yourname_S2_NessusScan;
- yourname_S2_NmapScans;

3. Any additional information as directed by the lab:

- Details and possible mitigations for all medium-risk vulnerabilities found on 172.30.0.11;

SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverable(s).

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: Scanning a Network with Zenmap

Note: Zenmap is a graphical interface for Nmap (network mapper), a network and port scanning tool that can quickly identify hosts and detect what operating system and services are running on them, and all without privileged access. Zenmap, and similar tools, are typically used during the scanning and vulnerability phase of the ethical hacking process.

Because of its popularity and effectiveness, Nmap is a very well documented tool. There are several books and online tutorials available. An additional reference is the Nmap Mindmap (http://nmap.org/docs/nmap-mindmap.pdf), a chart of the most frequently-used Nmap options.

In the next steps, you will use Zenmap to scan the target network.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.

2. In the Connections folder, **double-click** the **TargetWindows02 RDP shortcut** to open a remote connection to the TargetWindows02 machine.

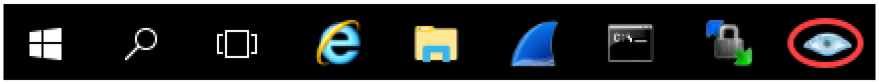
   If prompted, **type** the following credentials and **click OK** to open the remote connection.

   - Username: `Administrator`

    - Password: `P@ssw0rd!`

    The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

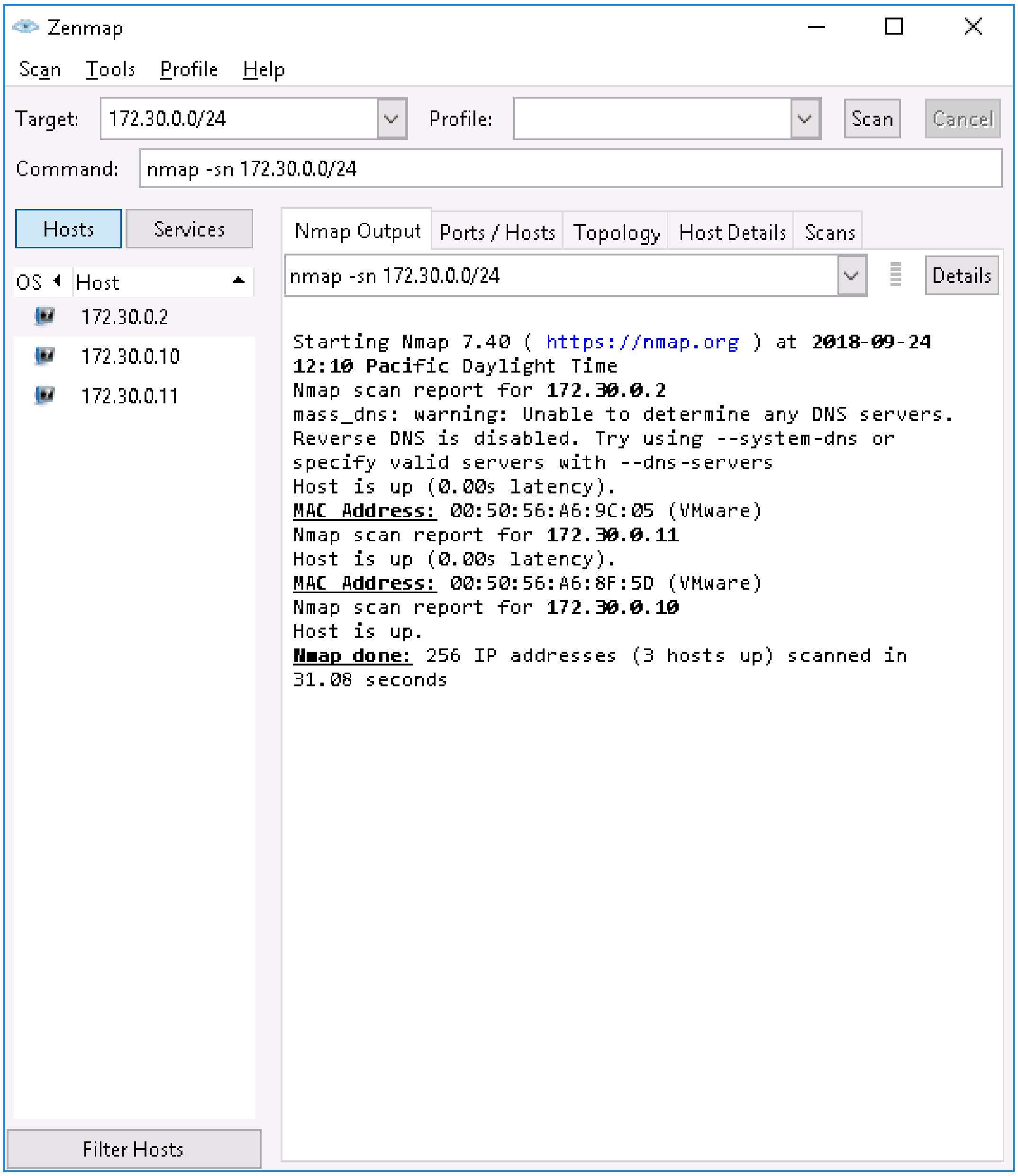
3. On the TargetWindows02 taskbar, **click** the **Nmap - Zenmap GUI icon** (an eye) to open the Zenmap application.



Zenmap icon

4. In the Command box, **highlight** the existing text, then **type** `nmap -sn 172.30.0.0/24` and **press Enter**.

   This command will manually execute a Ping scan (-sn) on all hosts on the 172.30.0.0/24 subnet. The scan should find three hosts on the 172.30.0.0/24 subnet.

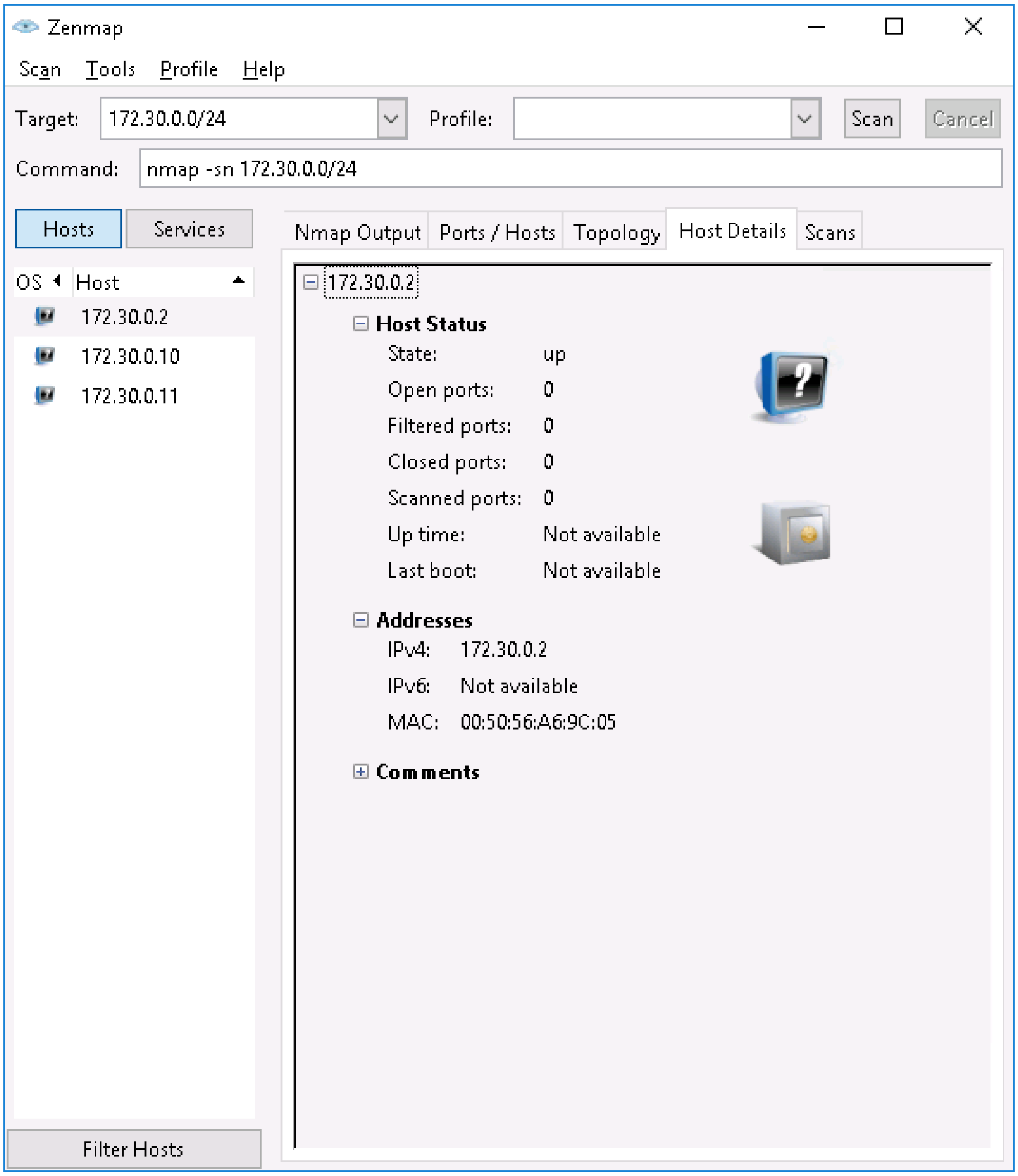


Command: nmap -sn 172.30.0.0/24

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-24
12:10 Pacific Daylight Time
Nmap scan report for 172.30.0.2
mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Host is up (0.00s latency).
MAC Address: 00:50:56:A6:9C:05 (VMware)
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
MAC Address: 00:50:56:A6:8F:5D (VMware)
Nmap scan report for 172.30.0.10
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in
31.08 seconds
```

Nmap Ping scan

5. When the scan is complete, **click** the first host IP in the left pane (**172.30.0.2**) to select it, then **click** the **Host Details tab** to see an organized summary of the information about the host detected during the scan.



Target: 172.30.0.0/24
Profile:
Command: nmap -sn 172.30.0.0/24

172.30.0.2
172.30.0.10
172.30.0.11

172.30.0.2

Host Status

State: up
Open ports: 0
Filtered ports: 0
Closed ports: 0
Scanned ports: 0
Up time: Not available
Last boot: Not available

Addresses

IPv4: 172.30.0.2
IPv6: Not available
MAC: 00:50:56:A6:9C:05

Comments

Nmap Host Details tab

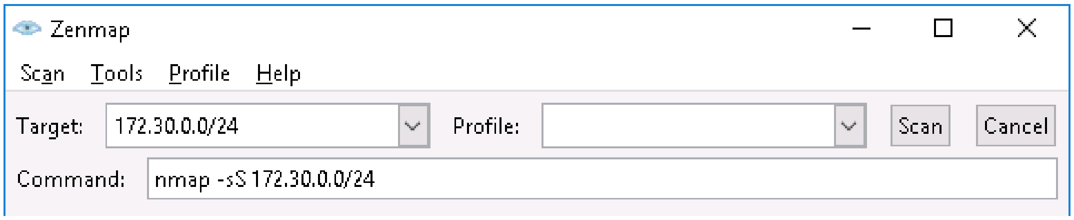
The Ping scan confirms that the machine is available, but can't identify ports, operating systems, or services. The host icon in the Host Details tab matches the one in the OS column of the left pane. These icons indicate that the scan was unable to determine the operating system (OS) of the host.

Take time to explore the details provided in the Ports/Hosts and Host Details tab for each host in the scan. The raw data from the Nmap Output tab is grouped into a more readable format on these tabs.

6. **Click** the **Nmap Output tab** to return to the complete scan results.

7. In the Command box, **highlight -sn**, then **type** `-sS` and **press Enter** to overwrite the existing command and begin a SYN scan of the subnet.

   The SYN scan is a form of TCP scanning that is less intrusive to the target host. The scanner, Zenmap, can identify open ports without completing a TCP handshake, which might be noticed by network administrators.



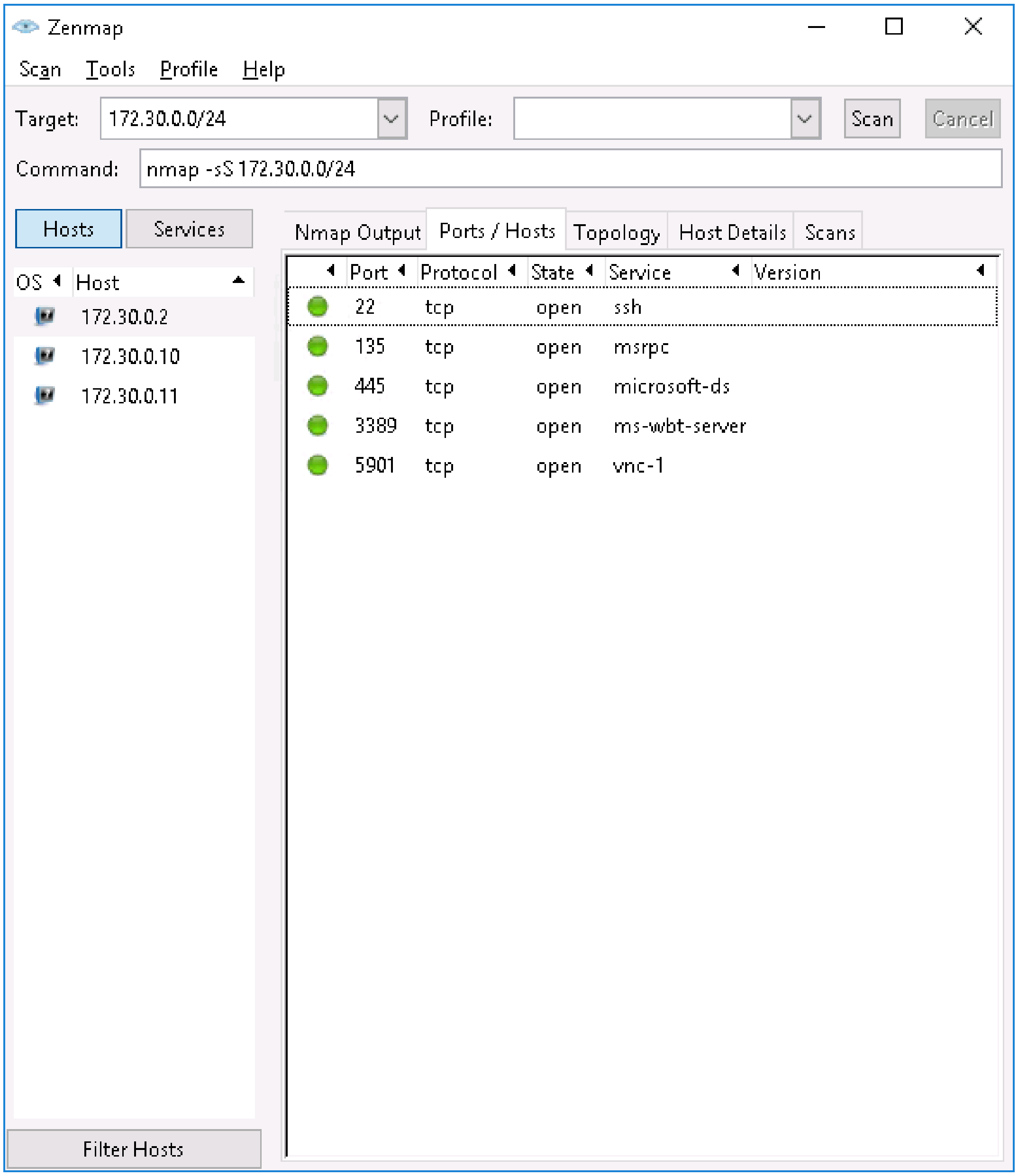
Target: 172.30.0.0/24

Command: nmap -sS 172.30.0.0/24

Nmap SYN scan command

8. When the scan is complete, **click** the first host IP in the left pane (**172.30.0.2**) to select it, then **click** the **Ports/Host tab** to see the services using the TCP protocol.

   Notice that the SYN scan can identify the services (e.g. FTP, HTTP, SSH, etc.), but not the versions of these applications. You will discover that information in a later step.



Target: 172.30.0.0/24

Profile:

Command: nmap -sS 172.30.0.0/24

OS	Host
	172.30.0.2
	172.30.0.10
	172.30.0.11

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	
●	135	tcp	open	msrpc	
●	445	tcp	open	microsoft-ds	
●	3389	tcp	open	ms-wbt-server	
●	5901	tcp	open	vnc-1	

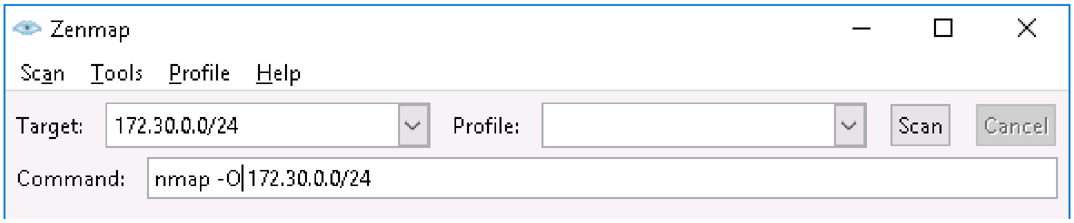
Services found with the SYN scan

9. In the left pane, **click** each remaining **host IP address** to review the Ports/Hosts tab for all identified hosts.

10. **Make a screen capture** showing the contents of the **Ports/Hosts tab from the SYN scan for 172.30.0.10** and **paste** it in your Lab Report file.

11. **Click** the **Nmap Output tab** to return to the complete scan results.

12. In the Command box, **highlight -sS**, then **type** **`-O`** and **press Enter** to begin an OS fingerprinting scan and determine which operating systems (OS) are running on the network hosts.



Target: 172.30.0.0/24

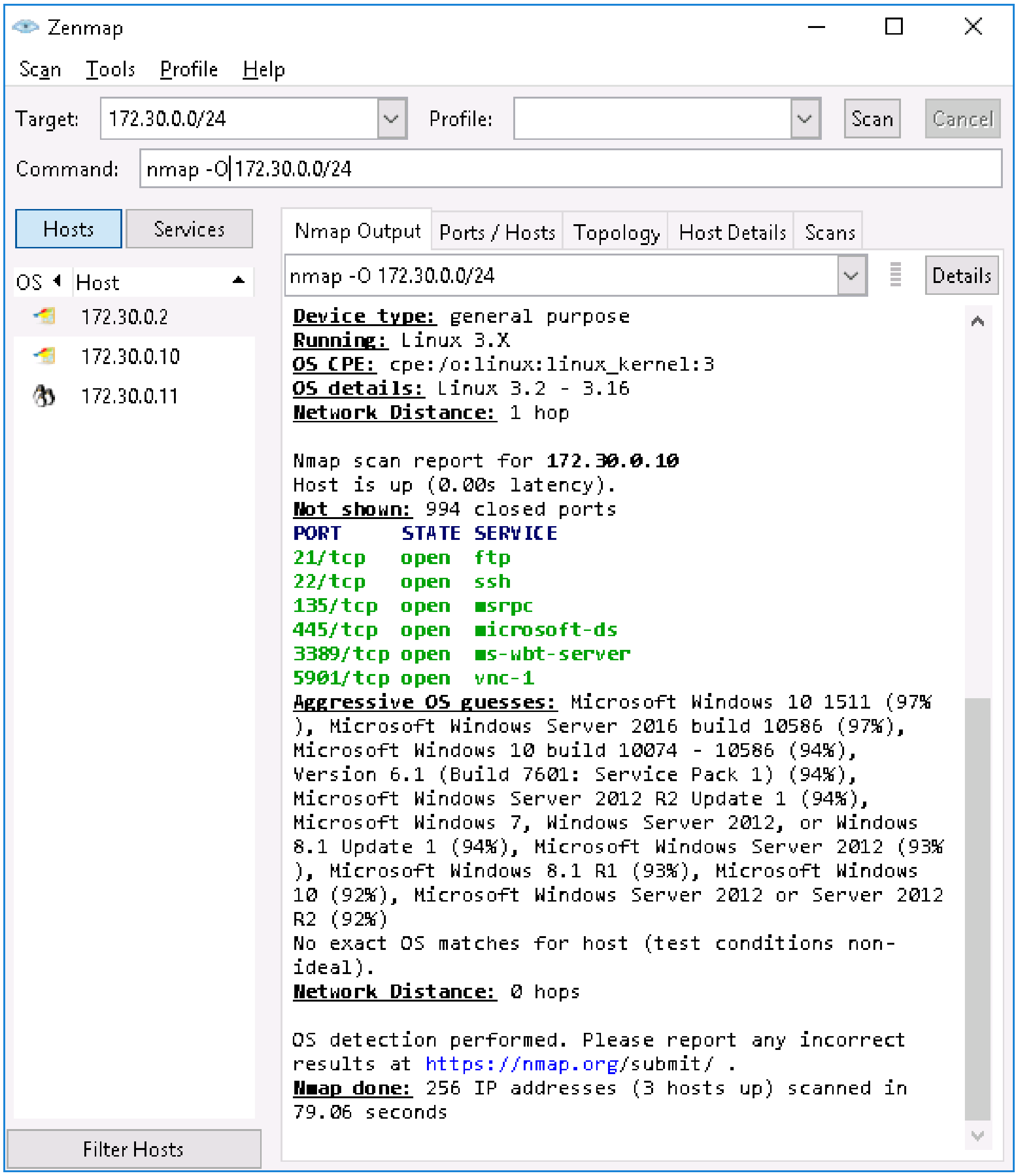
Profile:

Command: nmap -O 172.30.0.0/24

OS fingerprinting scan command

13. When the scan is complete, **review** the **scan results** in the Nmap Output tab.

    This scan not only discovered both open TCP ports (as did the SYN scan), but it also made a guess at the operating system for each host. The OS icon in the left pane changed as a result of that guess. The window icon (for 172.30.0.2 and 172.30.0.10) represents Windows machines and the trio of penguins (for 172.30.0.11) represents Linux machines.



```
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop

Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5901/tcp open  vnc-1
Aggressive OS guesses: Microsoft Windows 10 1511 (97%
), Microsoft Windows Server 2016 build 10586 (97%),
Microsoft Windows 10 build 10074 - 10586 (94%),
Version 6.1 (Build 7601: Service Pack 1) (94%),
Microsoft Windows Server 2012 R2 Update 1 (94%),
Microsoft Windows 7, Windows Server 2012, or Windows
8.1 Update 1 (94%), Microsoft Windows Server 2012 (93%
), Microsoft Windows 8.1 R1 (93%), Microsoft Windows
10 (92%), Microsoft Windows Server 2012 or Server 2012
R2 (92%)
No exact OS matches for host (test conditions non-
ideal).
Network Distance: 0 hops

OS detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in
79.06 seconds
```

Operating system scan results

Note: Zenmap detects the OS by using TCP/IP stack fingerprinting and comparing the results with a database. However, this database is not comprehensive; therefore, it is still possible that Zenmap will identify the OS incorrectly.

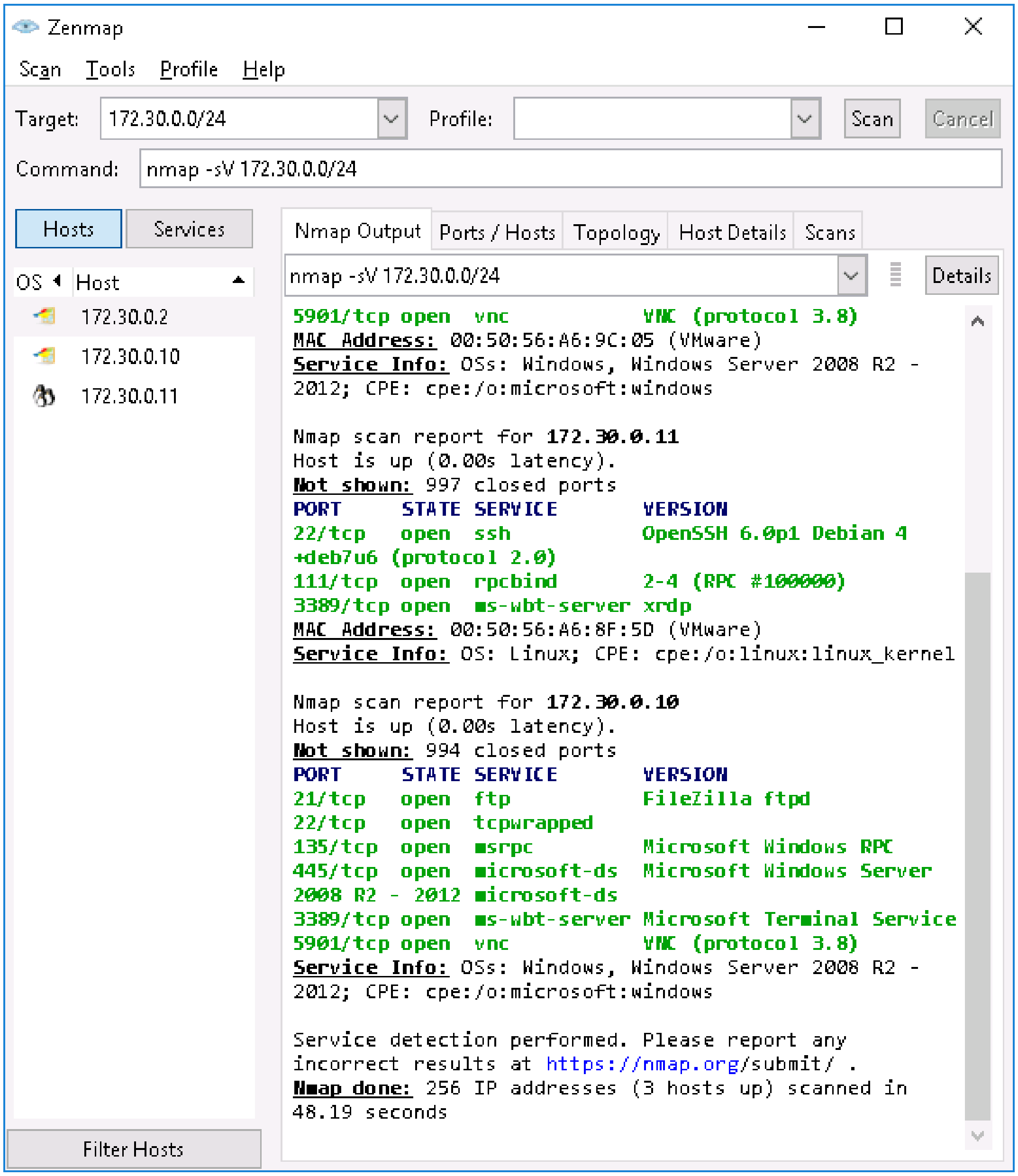
14. In the left pane, **click** the first host IP (**172.30.0.2**) to select it, then **click** the **Host Details tab** to see an organized summary of the information about the host detected during the scan.

15. In the left pane, **click** each remaining **host IP address** to review the Host Details tab for all identified hosts.

16. **Make a screen capture** showing the contents of the **Host Details tab from the OS scan for 172.30.0.2** and **paste** it in your Lab Report file.

17. In the Command box, **highlight -O**, then **type** `-sV` and **press Enter** to begin a Service scan.

    In the SYN scan from earlier in the lab, Zenmap identified the services running on the machines, but not the versions. This scan will discover the versions of the software on open TCP ports and will make a guess at the OS based on the services. As a result, the Service (–sV) scan can detect OS types better than the -O option and will take a little longer to run than the previous scans.



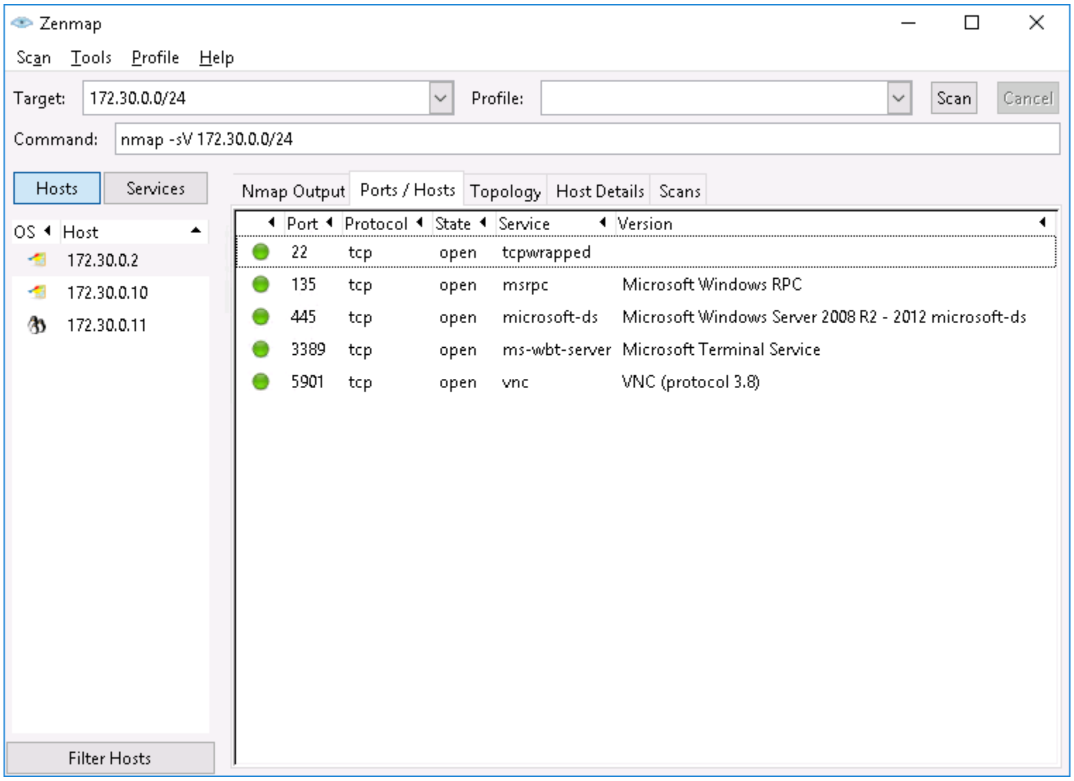
Target: 172.30.0.0/24
Profile:
Command: nmap -sV 172.30.0.0/24

```
nmap -sV 172.30.0.0/24

5901/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:50:56:A6:9C:05 (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 -
2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 6.0p1 Debian 4
+deb7u6 (protocol 2.0)
111/tcp  open  rpcbind       2-4 (RPC #100000)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 00:50:56:A6:8F:5D (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd
22/tcp   open  tcpwrapped
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds  Microsoft Windows Server
2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Service
5901/tcp open  vnc           VNC (protocol 3.8)
Service Info: OSs: Windows, Windows Server 2008 R2 -
2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in
48.19 seconds
```

Service scan results

18. When the scan is complete, **click** the first host IP in the left pane (**172.30.0.2**) to select it, then **click** the **Ports/Hosts tab**.

    The version for the services running on the TCP protocol are now visible in the Ports/Hosts tab.



Target: 172.30.0.0/24

Command: nmap -sV 172.30.0.0/24

OS	Host
	172.30.0.2
	172.30.0.10
	172.30.0.11

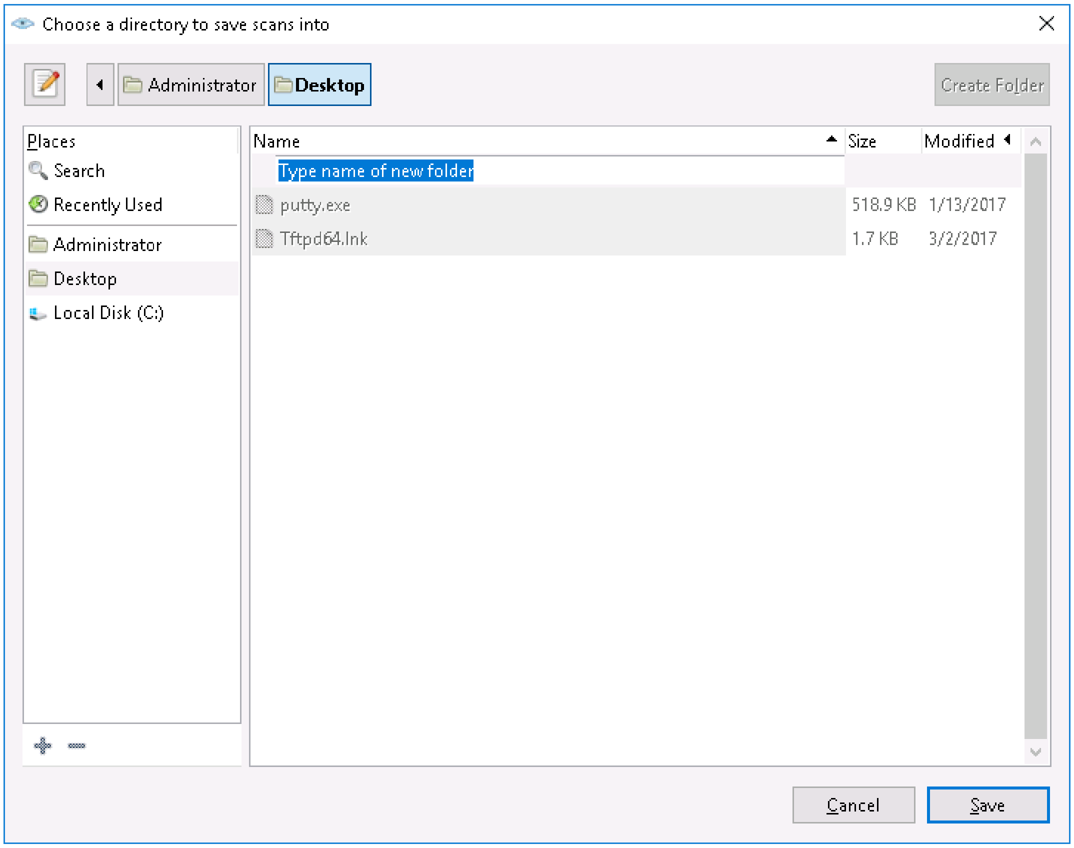
	Port	Protocol	State	Service	Version
●	22	tcp	open	tcpwrapped	
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	445	tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
●	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
●	5901	tcp	open	vnc	VNC (protocol 3.8)

Ports/Hosts tab after Service scan

19. In the left pane, **click** each remaining **host IP address** to review the Ports/Hosts tab for all identified hosts.

20. **Make a screen capture** showing the details in the **Ports/Hosts tab from the Service scan for 172.30.0.11** and **paste** it in your Lab Report file.

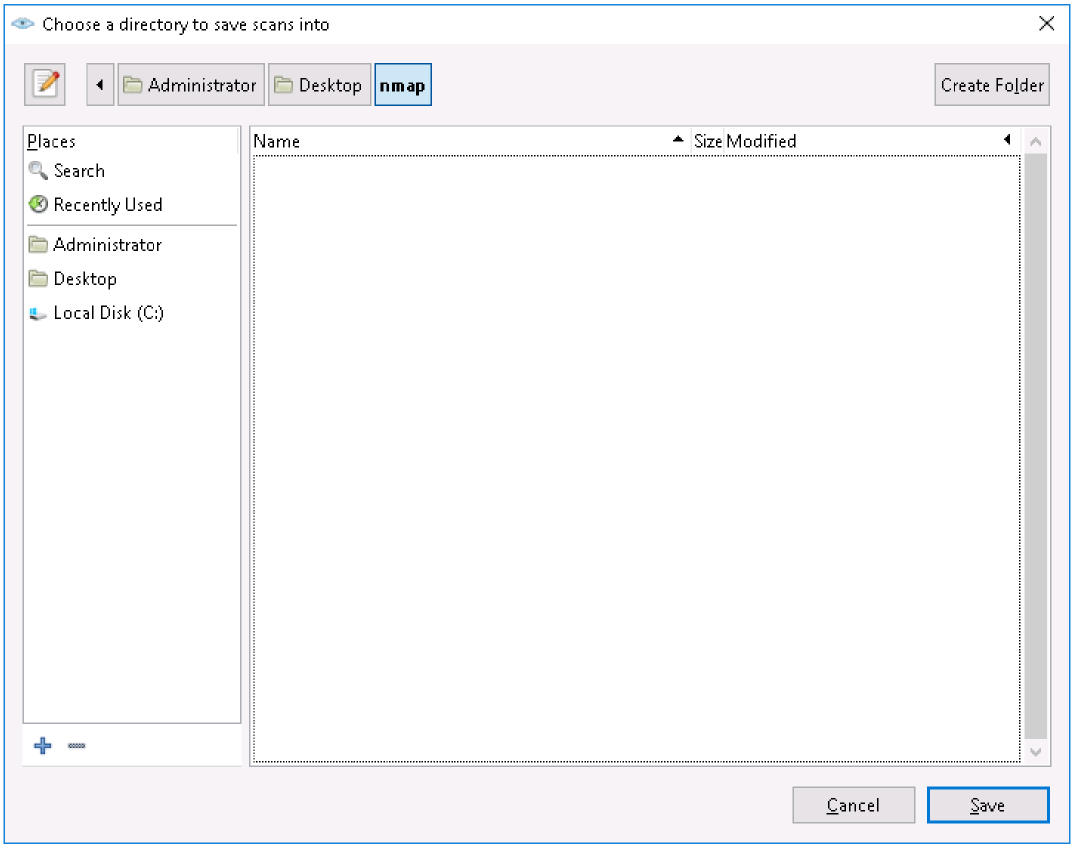
21. From the Zenmap menu bar, **select Scan > Save All Scans to Directory**, then **click** the **Desktop folder** and **click Create Folder** to create a new folder on the desktop.



Name	Size	Modified
Type name of new folder		
putty.exe	518.9 KB	1/13/2017
Tftpd64.lnk	1.7 KB	3/2/2017

Create a new folder

22. When prompted to name the new folder, **type** **nmap** and **press Enter**, then **click Save** to save the scans to the new nmap folder on the desktop.



Save all scans

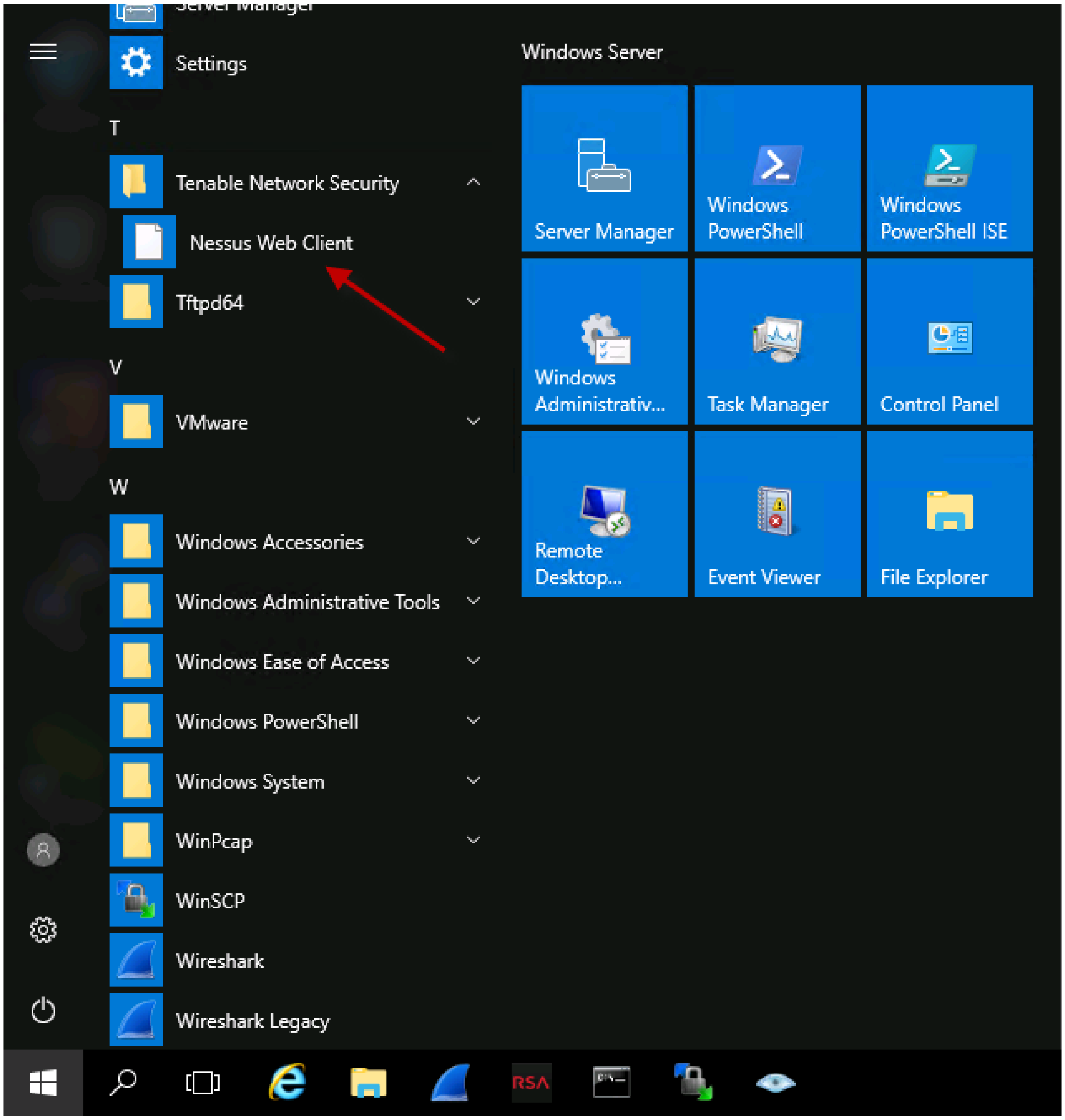
23. **Close** the **Zenmap window**.

Part 2: Conducting a Vulnerability Scan with Nessus

Note: Nessus, and similar tools, perform vulnerability assessments of Unix, Windows, and network infrastructures and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices. These tools are typically used to complete the scanning and vulnerability assessment phase of the ethical hacking process once the network mapping scan (that you conducted in Part 1 of this lab) is completed. Conducting a vulnerability scan on entire subnets can be noisy (making them easily detected) and time-consuming. You can limit the breadth and scope of the scan by specifying the hosts you want to scan in a simple text file.

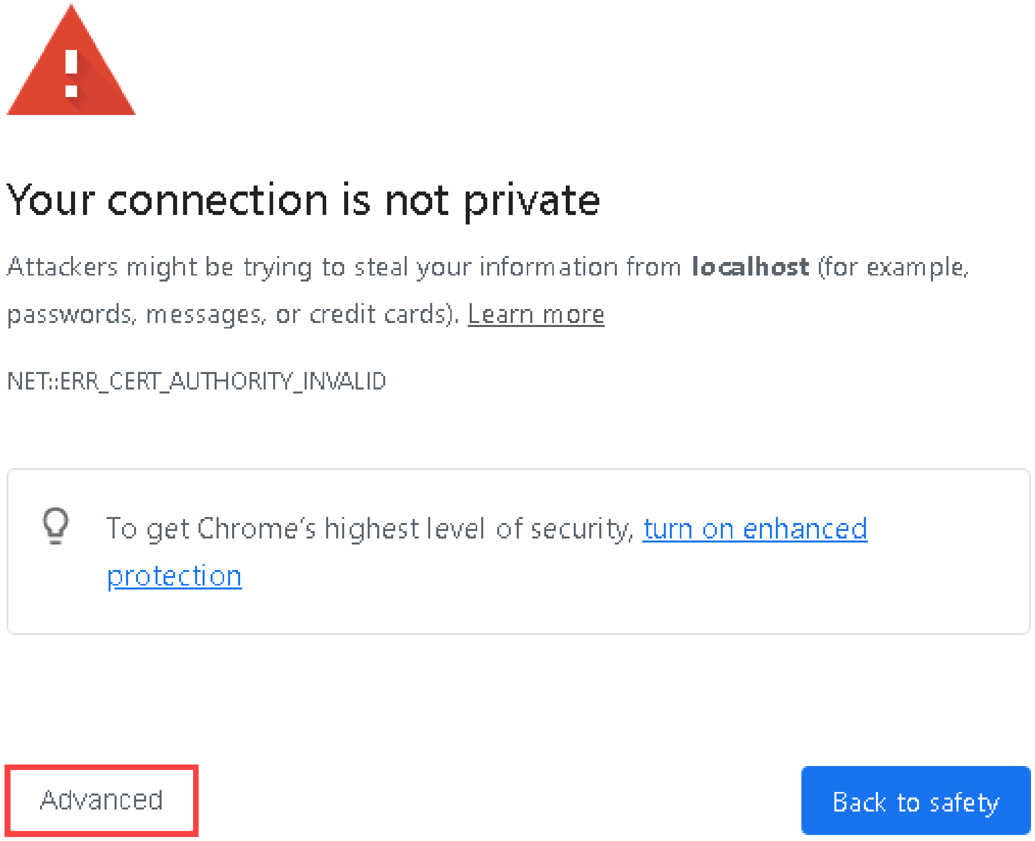
1. On the TargetWindows02 taskbar, **click** the **Windows Start icon**, then **select Tenable**

Network Security > Nessus Web Client to open the Nessus Web Client in Google Chrome.



Nessus menu location

2. When prompted with a security warning, **click** the **Advanced button**, then **click** the **Proceed to localhost (unsafe)** to continue.



Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Security warning

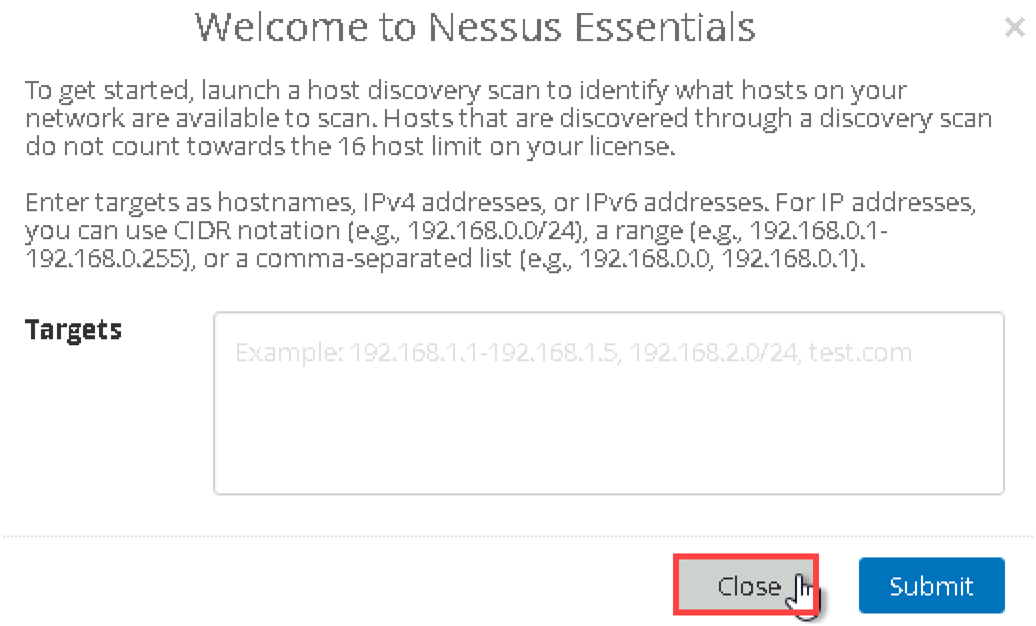
Note: This warning appears when visiting a website that either has an expired certificate, a mismatched certificate, or a self-signed certificate. For the purposes of this lab, you can disregard this warning.

3. At the Nessus log-in screen, **type** the following credentials and **click Login** to open the Nessus web client.

    - Username: `Administrator`
    - Password: `P@ssw0rd!`

    If prompted to save your password, **click Not for this site** to continue.

4. If prompted, **click** the **Close button** to close the Welcome dialog box.



Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

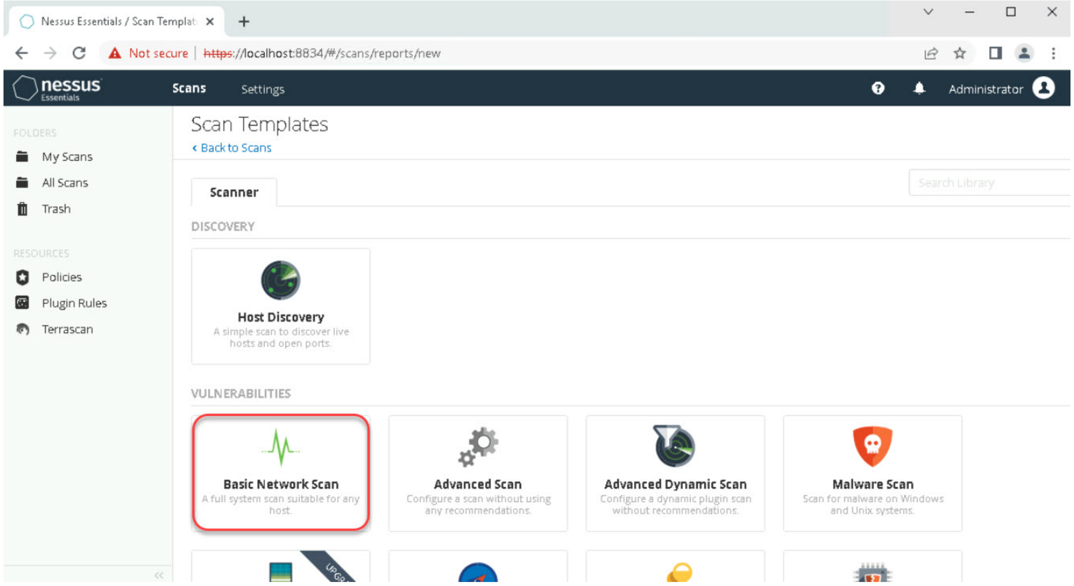
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Welcome dialog box

5. In the upper-right corner of the Scans page, **click** the **New Scan button** to open the Scan Templates Library of preconfigured network scans.

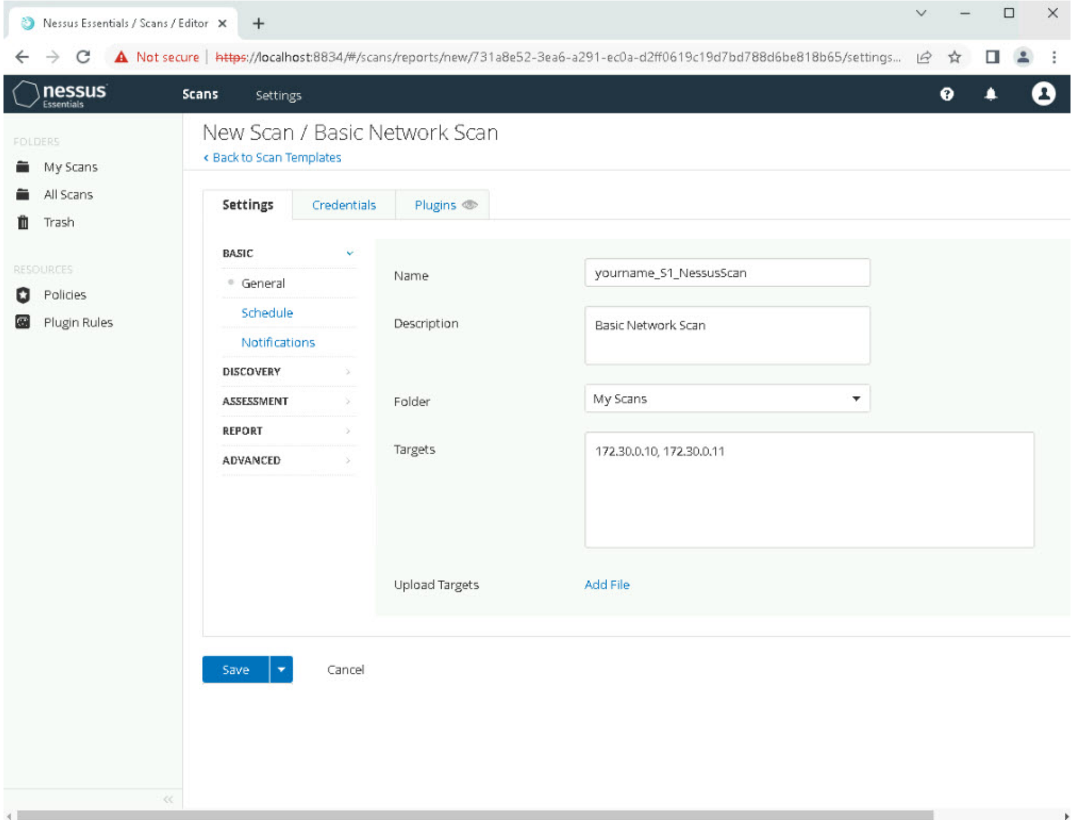
6. On the Scan Templates page, **click** the **Basic Network Scan button** to create a new Basic Network Scan.


Nessus Essentials / Scan Templat
Not secure
https://localhost:8834/#/scans/reports/new
nessus Essentials
Scans
Settings
Administrator
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Scan Templates
‹ Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.

Select a scan

7. In the New Scan / Basic Network Scan form, **type** the following information:

    - Name: ***`yourname_S1_NessusScan`***, replacing *yourname* with your own name
    - Description: **`Basic Network Scan`**
    - Folder: **`My Scans`**
    - Targets: **`172.30.0.10, 172.30.0.11`**



New Scan / Basic Network Scan

Name: yourname_S1_NessusScan

Description: Basic Network Scan

Folder: My Scans

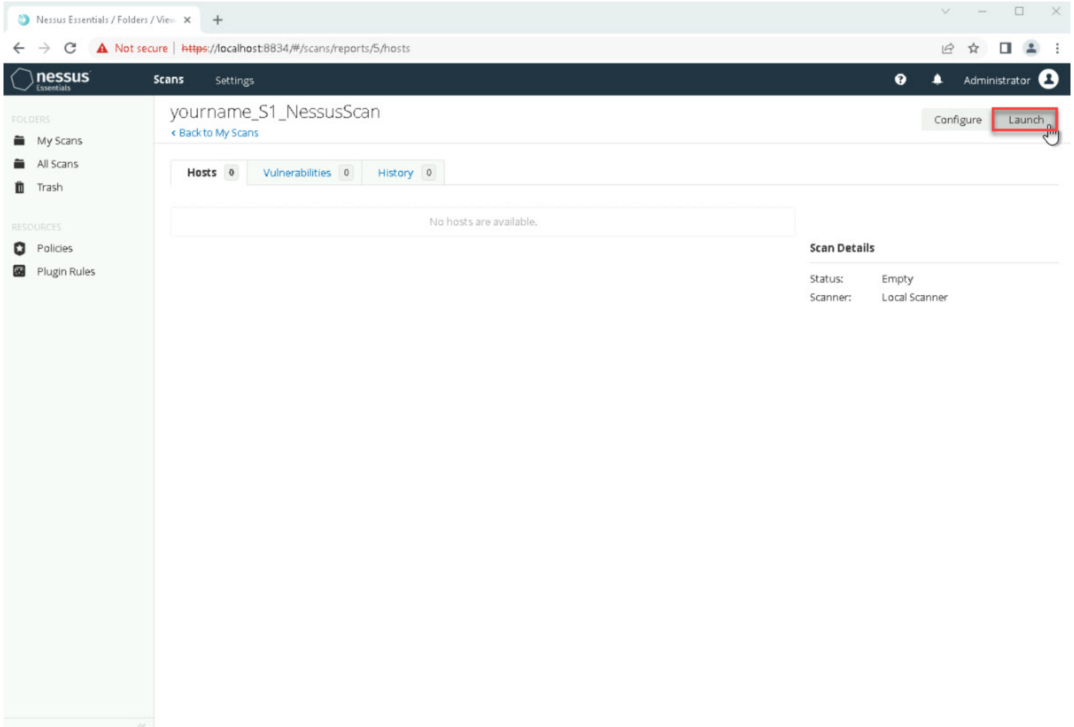
Targets: 172.30.0.10, 172.30.0.11

Nessus configuration form

8. At the bottom of the form, **click** the **Save button** to save the new configuration and open the My Scans page.

9. On the My Scans page, **click** the ***yourname*_S1_NessusScan checkbox** to select your Basic Scan.

10. In the upper-right corner of the *yourname*_S1_NessusScan page, **click** the **Launch button** to start the scan.



No hosts are available.

Scan Details

Status: Empty
Scanner: Local Scanner

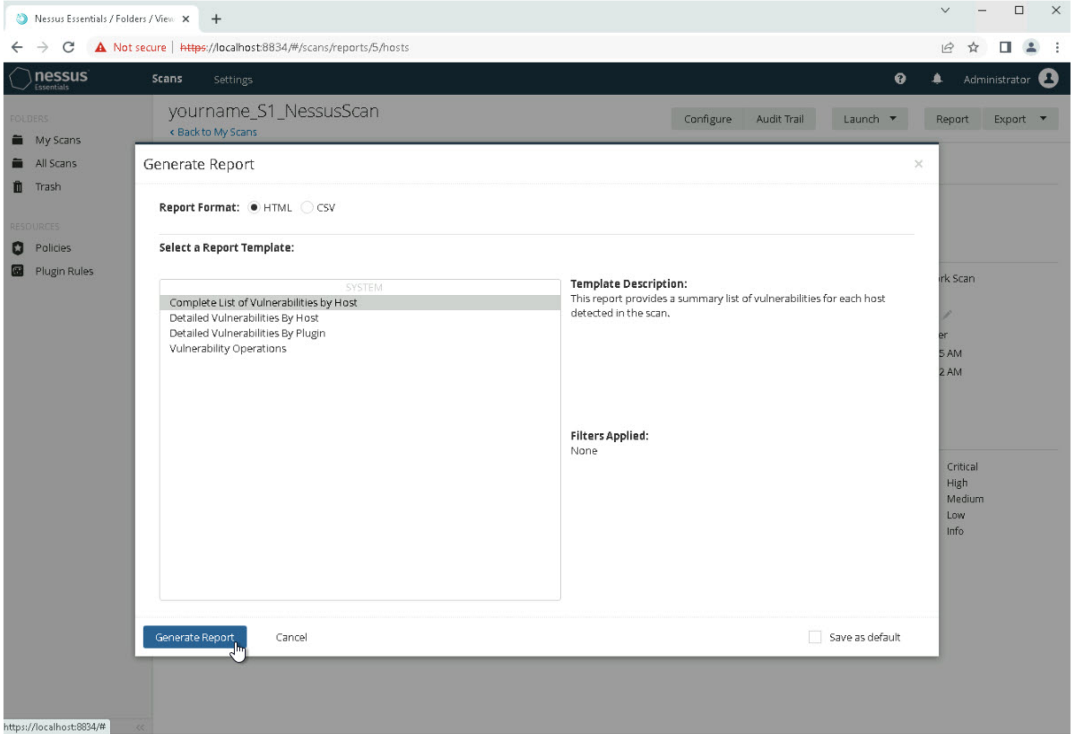
Launch scan

Note: Scanning will take about 5 to 7 minutes to complete. The green refresh symbol will spin as long as the scan is running. The refresh symbol will change to a check mark when the scan is complete.

11. When the scan is complete, **click *yourname*_S1_NessusScan** to open the scan results.

    The report summary includes both a bar chart and a pie chart showing the distribution of vulnerability findings for each host.

12. In the upper-right corner of the scan results page, **click Report** and **select Complete List of Vulnerabilities by Host** to export the scan results as an HTML file. Then **click** the **Generate Report button.**



Report Format: ● HTML ○ CSV

Select a Report Template:

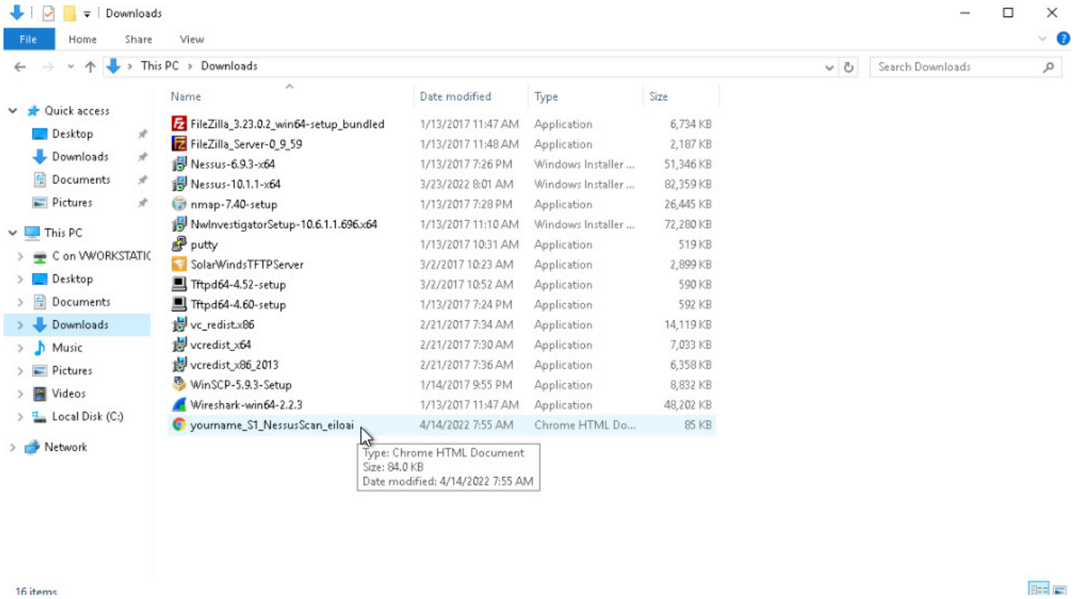
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Export report

13. In File Explorer, **navigate to the This PC/Downloads folder** and **locate the HTML report** that was exported (**yourname_S1_NessusScan_***).



Name	Date modified	Type	Size
FileZilla_3.23.0.2_win64-setup_bundled	1/13/2017 11:47 AM	Application	6,734 KB
FileZilla_Server-0_9_59	1/13/2017 11:48 AM	Application	2,187 KB
Nessus-6.9.3-x64	1/13/2017 7:26 PM	Windows Installer ...	51,346 KB
Nessus-10.1.1-x64	3/23/2022 8:01 AM	Windows Installer ...	82,359 KB
nmap-7.40-setup	1/13/2017 7:28 PM	Application	26,445 KB
NwInvestigatorSetup-10.6.1.1.696.x64	1/13/2017 11:10 AM	Windows Installer ...	72,280 KB
putty	1/13/2017 10:31 AM	Application	519 KB
SolarWindsTFTPServer	3/2/2017 10:23 AM	Application	2,899 KB
Tftpd64-4.52-setup	3/2/2017 10:52 AM	Application	590 KB
Tftpd64-4.60-setup	1/13/2017 7:24 PM	Application	592 KB
vc_redist.x86	2/21/2017 7:34 AM	Application	14,119 KB
vcredist_x64	2/21/2017 7:30 AM	Application	7,033 KB
vcredist_x86_2013	2/21/2017 7:36 AM	Application	6,358 KB
WinSCP-5.9.3-Setup	1/14/2017 9:55 PM	Application	8,832 KB
Wireshark-win64-2.2.3	1/13/2017 11:47 AM	Application	48,202 KB
yourname_S1_NessusScan_eiloai	4/14/2022 7:55 AM	Chrome HTML Do...	85 KB

Type: Chrome HTML Document
Size: 84.0 KB
Date modified: 4/14/2022 7:55 AM

Locating the exported nessus report

14. In File Explorer, **copy** the **yourname_S1_NessusScan_* file** to **This PC/Desktop.**

15. On This PC/Desktop, **rename** the **yourname_S1_NessusScan_* HTML file** to yourname_S1_NessusScan, replacing *yourname* with your own name

16. **Close** the **Nessus browser window**.

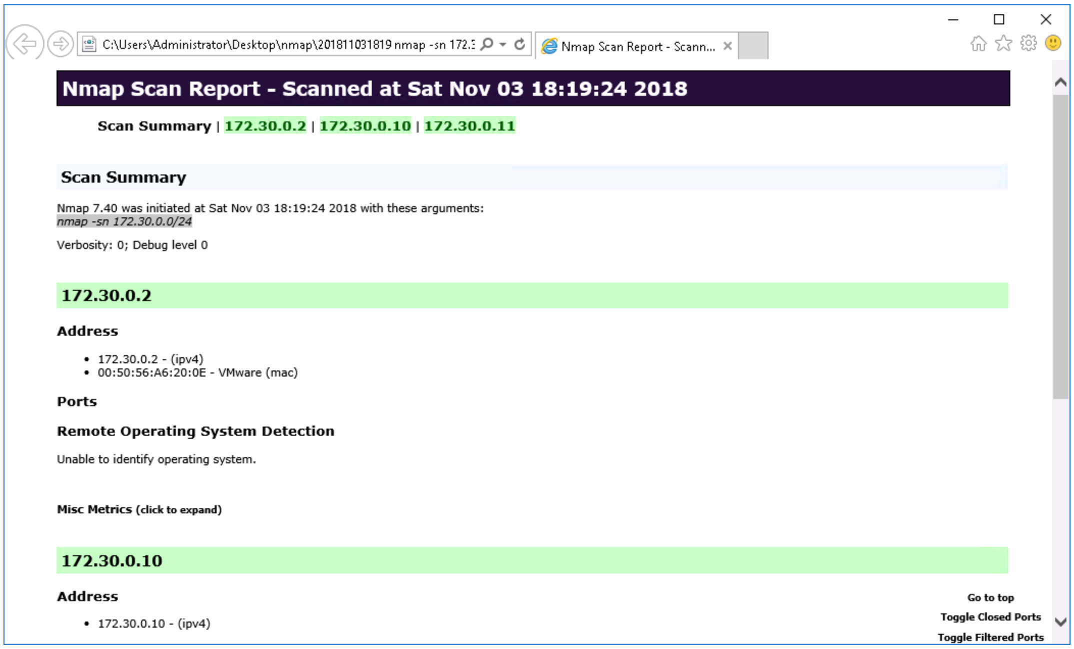
Part 3: Evaluate your Findings

Note: In the next steps, you will review the vulnerabilities identified in the Nessus scan and research the details for several risks using multiple resources. You will use that information to locate possible solutions. First, you will review the files you saved earlier in the lab.

1. On the TargetWindows02 desktop, **double-click** the **nmap folder** to open the folder in a new File Explorer window.

2. In the nmap folder, **double-click** the **first nmap file** to open the scan results in a new browser window.

   If prompted, **click Allow Blocked Content** to dismiss the popup window. Each host appears as a link in the header of the report. Click the host IP to navigate to the discovery data for that machine. Compare the presentation of the findings with the results of the Zenmap scan in Part 1 of this lab by reopening Zenmap or reviewing your screenshots.


C:\Users\Administrator\Desktop\nmap\201811031819 nmap -sn 172.3
Nmap Scan Report - Scann...
Go to top
Toggle Closed Ports
Toggle Filtered Ports

Nmap Scan Report - Scanned at Sat Nov 03 18:19:24 2018

Scan Summary | **172.30.0.2** | **172.30.0.10** | **172.30.0.11**

Scan Summary

Nmap 7.40 was initiated at Sat Nov 03 18:19:24 2018 with these arguments:
nmap -sn 172.30.0.0/24

Verbosity: 0; Debug level 0

172.30.0.2

Address

- 172.30.0.2 - (ipv4)
- 00:50:56:A6:20:0E - VMware (mac)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

172.30.0.10

Address

- 172.30.0.10 - (ipv4)

Nmap scan

3. **Repeat step 2** for each file in the nmap folder.

4. In your Lab Report file, **compare** the presentation of the HTML report with the presentation of the native Zenmap results.

5. **Close** the **browser window**.

6. **Close** the **File Explorer window**.

Note: In the next steps, you will copy the deliverable files to the vWorkstation desktop so that you can continue to work with the reports.

7. From the TargetWindow02 desktop, **select any deliverable files** you saved in the course of this lab and **copy** them to the Windows clipboard.

- **nmap folder** (includes all Zenmap scans)
- ***yourname*_S1_NessusScan.html**

8. **Minimize** the **remote TargetWindows02 connection** to return to the vWorkstation.

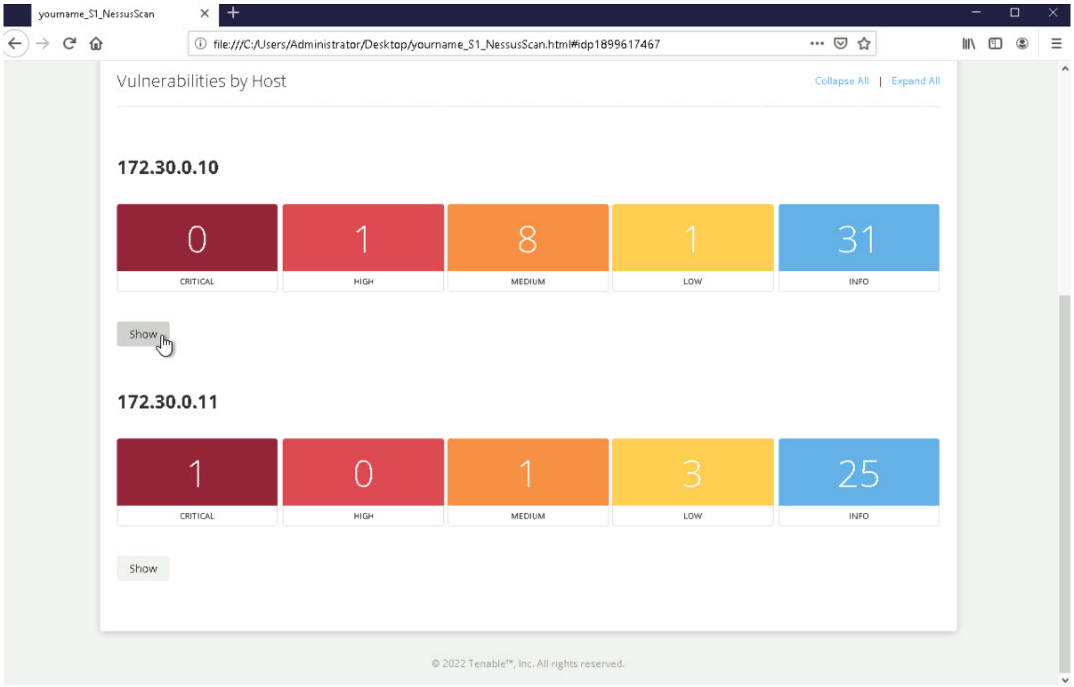
   If necessary, **minimize** the **Connections folder**.

9. On the vWorkstation, **paste** the copied files to the desktop.

10. On the vWorkstation desktop, **double-click** the ***yourname*_S1_NessusScan file** to open the Nessus Scan Report in a new browser window.

    If prompted, **click Allow blocked content**.

11. In the Nessus Scan Report's Table of Contents, **click** the **172.30.0.10 link** to skip to the summary for the TargetWindows02 host, then **click** the **Show button** below 172.30.0.10 to open the summary.



file:///C:/Users/Administrator/Desktop/yourname_S1_NessusScan.html#idp1899617467

Vulnerabilities by Host

Collapse All | Expand All

172.30.0.10

0	1	8	1	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show

172.30.0.11

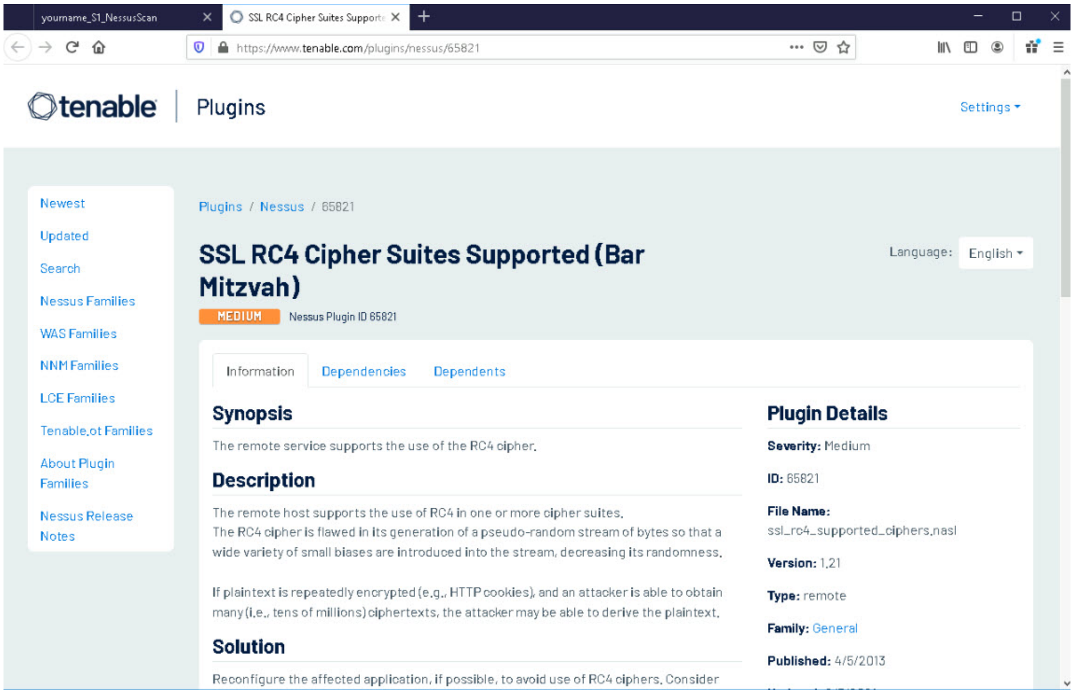
1	0	1	3	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show

© 2022 Tenable™, Inc. All rights reserved.

Opening the summary of the 172.30.0.10 scan

12. In the Plugin Id column, **click** the **65821 link** to open details for the Bar Mitzvah vulnerability in a new tab.



SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM Nessus Plugin ID 65821

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider

Plugin Details

Severity: Medium

ID: 65821

File Name: ssl_rc4_supported_ciphers.nasl

Version: 1.21

Type: remote

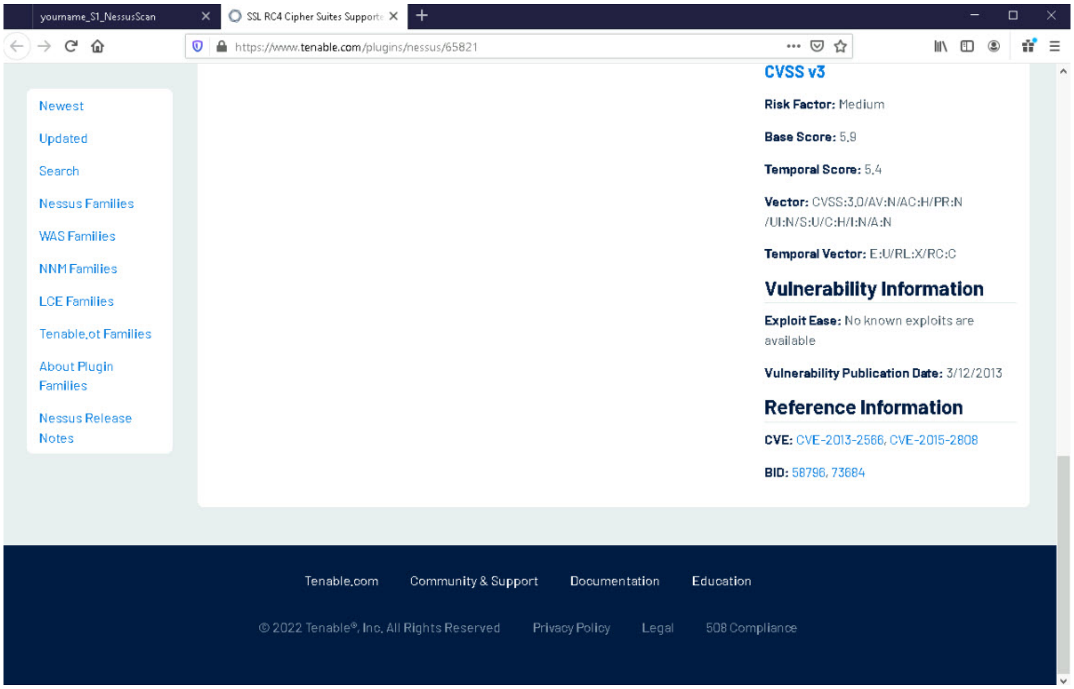
Family: General

Published: 4/5/2013

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Note: Each vulnerability identified in the report will include a corresponding Plugin ID. A Plugin is a vulnerability test script, written to detect a specific vulnerability or set of vulnerabilities. If a plugin's vulnerability check matches a CVE description, it is added to the plugin. CVE stands for Common Vulnerabilities and Exposures. The MITRE Corporation (www.mitre.org) launched the CVE List in 1999 as a community effort to document publicly known cybersecurity vulnerabilities. The CVE List also serves as the foundation for the U.S. National Vulnerability Database (NVD), a vulnerability database launched by the National Institute of Standards and Technology (NIST) in 2005. Building upon the CVE List, the NVD enhances each CVE entry with information about how to mitigate the vulnerability with software patches and updates. Although the two are separate resources, the NVD is fully synchronized with the CVE List, and both are sponsored by the United States Department of Homeland Security and the Cybersecurity and Communications office of the United States Computer Emergency Readiness Team (US-CERT). More information on discovered vulnerabilities (and their mitigation strategies) can be found at http://cve.mitre.org.

13. On the Nessus Plugins tab, **review** the description of the problem and the solution options, then **locate** the **CVE IDs** at the bottom of the page.



CVSS v3

Risk Factor: Medium

Base Score: 5.9

Temporal Score: 5.4

Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Temporal Vector: E:U/RL:X/RC:C

Vulnerability Information

Exploit Ease: No known exploits are available

Vulnerability Publication Date: 3/12/2013

Reference Information

CVE: CVE-2013-2566, CVE-2015-2808

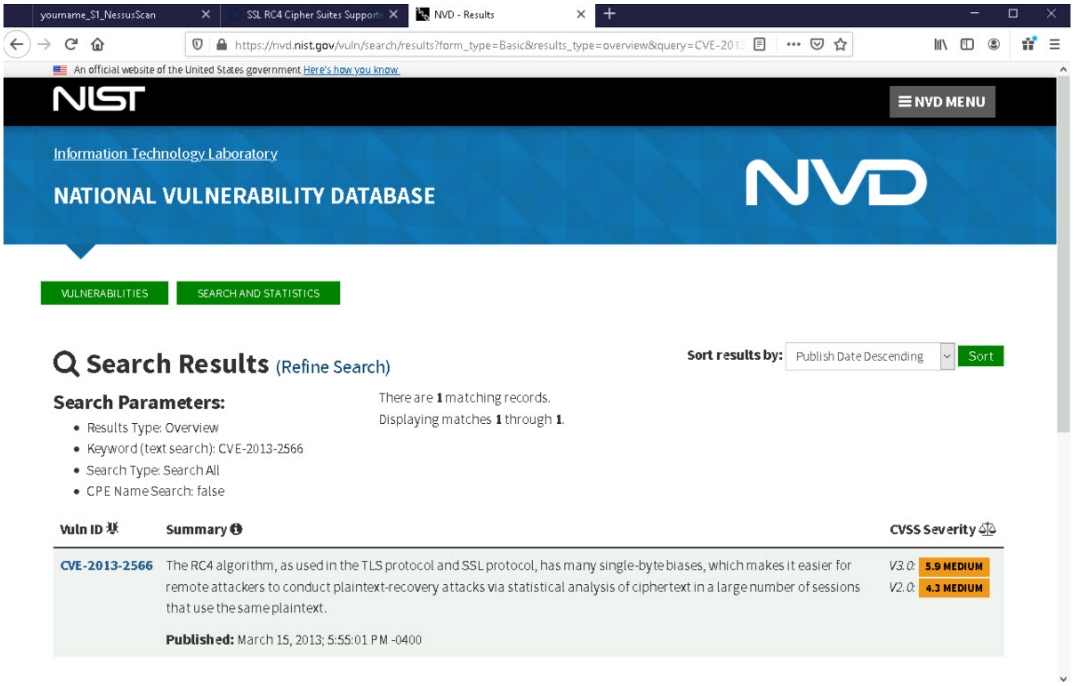
BID: 58796, 73684

CVE IDs

14. On the Firefox toolbar, **click** the **new tab button**, then **type** **`http://nvd.nist.gov/vuln/search`** in the address box and **press Enter** to open the NVD search page.

15. In the Keyword Search field, **type** **`CVE-2013-2566`** (the first CVE ID associated with this vulnerability) and **click** the **Search button** to search the National Vulnerability Database for the CVE ID supplied by the Nessus report.

    The database lists only a brief summary of the vulnerability in the search results, but includes a link to more information.


yourname_S1_NessusScan
SSL RC4 Cipher Suites Support
NVD - Results
https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-201
An official website of the United States government Here's how you know
NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2013-2566
- Search Type: Search All
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2013-2566	The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext. **Published:** March 15, 2013; 5:55:01 PM -0400	V3.0: 5.9 MEDIUM V2.0: 4.3 MEDIUM

NVD summary of the vulnerability

16. On the Search Results page, **click** the **CVE-2013-2566 link** to view more information about this vulnerability.

    Review the additional information available on this page and compare the information provided in the database to the information provided by Nessus.

17. On the Firefox toolbar, **click** the **Nessus Scan Report tab** to return to the full report.

18. In your Lab Report file, **document** all of the **medium-risk security vulnerabilities for 172.30.0.10** identified by the scan and **make recommendations** for mitigating one of those risks based on your review of the information in the vulnerability scan.

19. **Close** the **Firefox window**.

Note: This completes Section 1 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

20. On the vWorkstation desktop, **double-click** the **nmap folder** to open it.

21. In the nmap folder, **press CTRL** and **click all four files** to select them.

22. With the cursor over the highlighted files, **right-click** and select **Send to > Compressed (zipped) folder** from the context menu to combine the files into an archive file.

    When prompted, **type** ***`yourname`*****`_S1_NmapScans`**, replacing *yourname* with your own name, and **press Enter** to save the archive file.

23. In the Nmap folder, **drag and drop** the ***yourname*****_S1_NmapScans file** to the desktop, then **close** the **File Explorer**.

24. On the vWorkstation desktop, **drag and drop** the following files into the File Transfer folder to complete the download to your local computer.

    - ***yourname*****_S1_NmapScans**
    - ***yourname*****_S1_NessusScan**

Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
   a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.

   b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.

3. **Proceed** with **Part 1**.

Part 1: Scanning a Network with Zenmap

Note: Zenmap is a graphical interface for Nmap (network mapper), a network and port scanning tool that can quickly identify hosts and detect what operating system and services are running on them, and all without privileged access. Zenmap, and similar tools, are typically used during the scanning and vulnerability phase of the ethical hacking process.

Because of its popularity and effectiveness, Nmap is a very well documented tool. There are several books and online tutorials available. An additional reference is the Nmap Mindmap (http://nmap.org/docs/nmap-mindmap.pdf), a chart of the most frequently-used Nmap options.

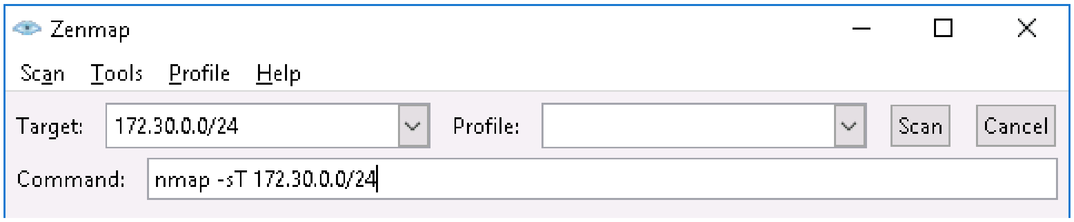
In the next steps, you will use Zenmap to scan the target network.

1. **Open a remote connection** to the **TargetWindows02** machine.

2. **Launch** the **Zenmap application**.

3. Using the Command box, **execute** **`nmap -sT 172.30.0.0/24`** to run a TCP connect scan (-sT) on all hosts on the 172.30.0.0/24 subnet.

   This scan will take several minutes to complete. A TCP connection scan takes longer to run because a connection is established with the target and can be run when a user does not have permission to use raw packets. Once complete, the scan should find three hosts on the 172.30.0.0/24 subnet.



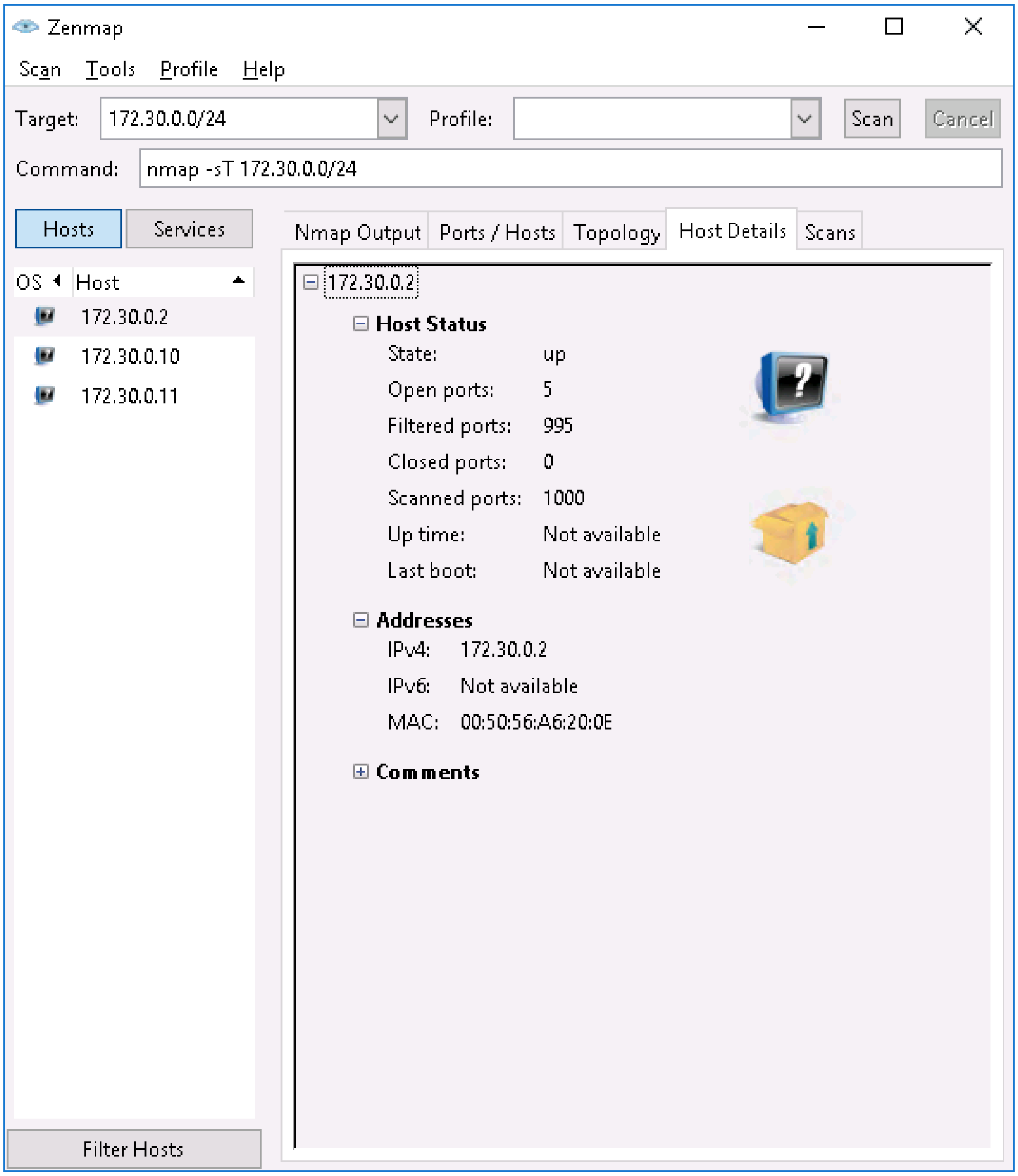
Target: 172.30.0.0/24

Command: nmap -sT 172.30.0.0/24

Nmap TCP scan

4. When the scan is complete, **select** the **first host** and **review** the **Host Details tab**.

   The question mark host icon in the Host Details tab matches the one in the OS column of the left pane. These icons indicate that the scan was unable to determine the operating system (OS) of the host.



Target: 172.30.0.0/24

Command: nmap -sT 172.30.0.0/24

172.30.0.2
172.30.0.10
172.30.0.11

172.30.0.2

Host Status

State:	up
Open ports:	5
Filtered ports:	995
Closed ports:	0
Scanned ports:	1000
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	172.30.0.2
IPv6:	Not available
MAC:	00:50:56:A6:20:0E

Comments

Nmap Host Details tab

5. **Review** the **Host Details tab** for each remaining host IP address.

6. **Make a screen capture** showing the **Host Details tab from the TCP Connection scan for 172.30.0.2** and **paste** it in your Lab Report file.

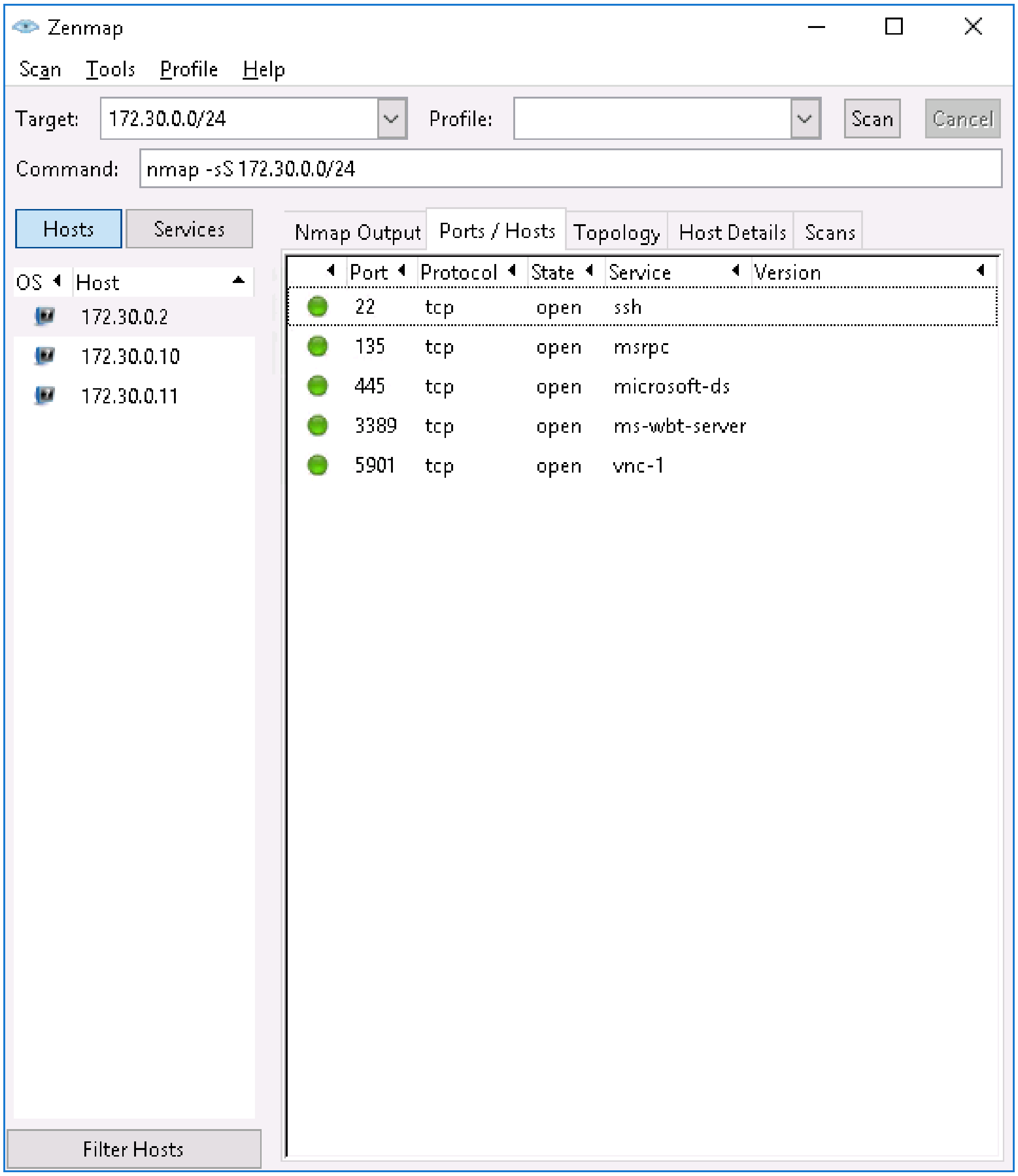
7. **Click** the **Nmap Output tab** to return to the complete scan results.

8. Using the Command box, **execute the command** to run a SYN scan on all hosts on the 172.30.0.0/24 subnet.

   The SYN scan (-sS) is a form of TCP scanning that is less intrusive on the target host. The scanner, Zenmap, can identify open ports without completing a TCP handshake, which might be noticed by network administrators.

9. **Select** the **first host** and **review** the **Ports/Hosts tab** to see the services using the TCP protocol.

   Notice that the SYN scan can identify the services (e.g. FTP, HTTP, SSH, etc.), but not the versions of these applications. You will discover that information in a later step.



Target: 172.30.0.0/24

Command: nmap -sS 172.30.0.0/24

OS	Host
	172.30.0.2
	172.30.0.10
	172.30.0.11

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	
●	135	tcp	open	msrpc	
●	445	tcp	open	microsoft-ds	
●	3389	tcp	open	ms-wbt-server	
●	5901	tcp	open	vnc-1	

Services found with the SYN scan

10. **Review** the **Ports/Host tab** for each remaining host IP address.

11. **Make a screen capture** showing the **Host Details tab from the SYN scan for 172.30.0.11** and **paste** it in your Lab Report file.

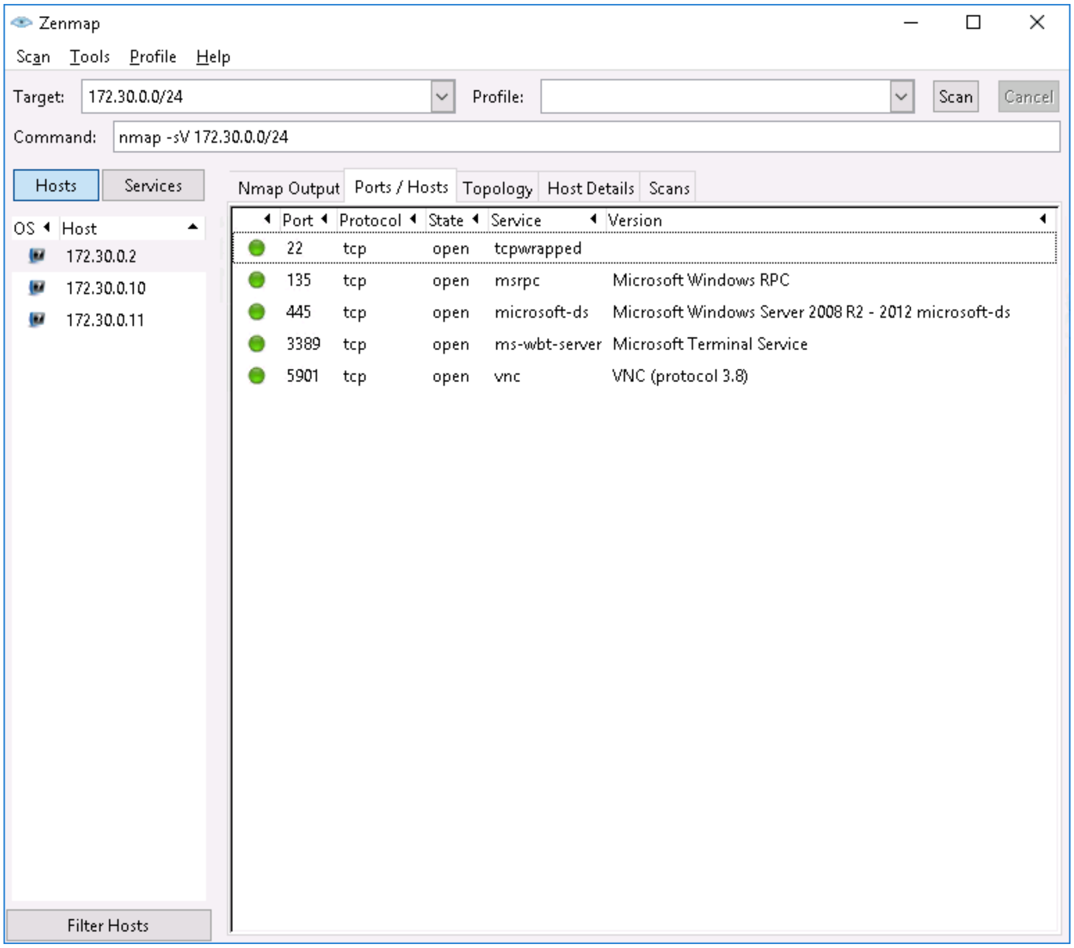
12. **Click** the **Nmap Output tab** to return to the complete scan results.

13. Using the Command box, **execute the command** to run a service scan on all hosts on the 172.30.0.0/24 subnet.

    In the SYN scan, Zenmap identified the services running on the machines, but not the versions. The service scan will discover the versions of the software on open TCP ports and will make a guess at the OS based on the services. The attempted OS identifications are available within the body of the Nmap output (see Service Info), but will not be rendered in the Host Details tab.

14. **Click** the **Ports/Hosts tab**.

    The versions for the services running on the TCP protocol are now visible in the Ports/Hosts tab.



Target: 172.30.0.0/24

Command: nmap -sV 172.30.0.0/24

OS	Host
	172.30.0.2
	172.30.0.10
	172.30.0.11

	Port	Protocol	State	Service	Version
●	22	tcp	open	tcpwrapped	
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	445	tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
●	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
●	5901	tcp	open	vnc	VNC (protocol 3.8)

Ports/Hosts tab after Service scan

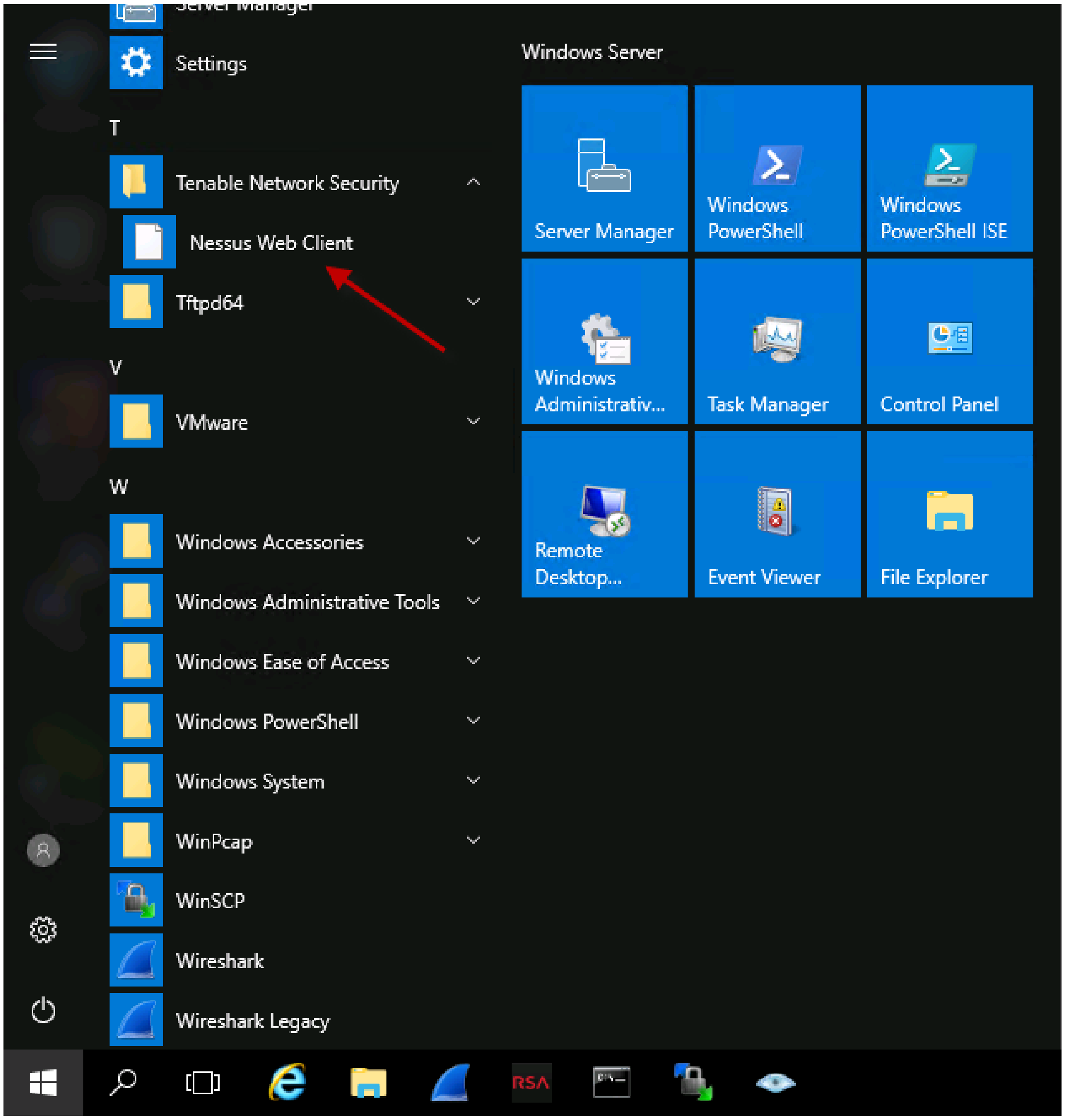
15. **Make a screen capture** showing the details in the **Ports/Hosts tab from the Service scan for 172.30.0.10** and **paste** it in your Lab Report file.

16. **Save all scans** to a new directory (**S2nmap**) on the TargetWindows02 desktop and **close** the **Zenmap window**.

Part 2: Conducting a Vulnerability Scan with Nessus

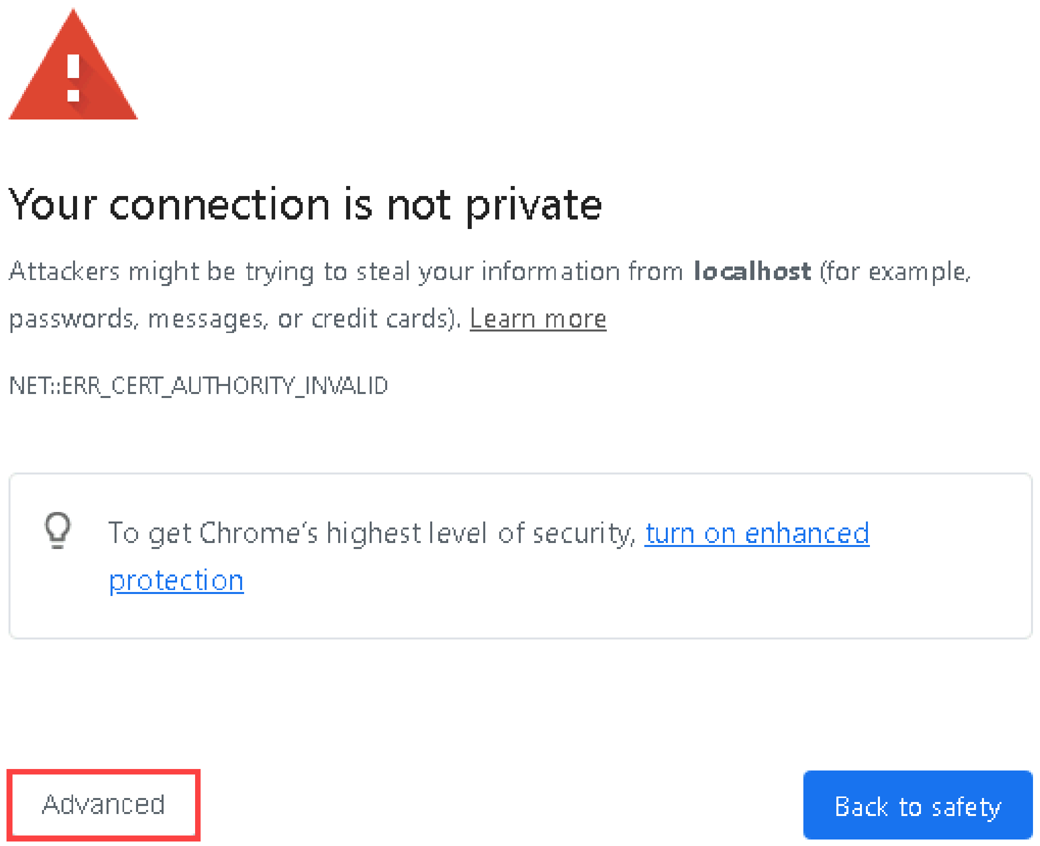
Note: Nessus, and similar tools, perform vulnerability assessments of Unix, Windows, and network infrastructures and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices. These tools are typically used to complete the scanning and vulnerability assessment phase of the ethical hacking process once the network mapping scan (that you conducted in Part 1 of this lab) is completed. Conducting a vulnerability scan on entire subnets can be noisy (making them easily detected) and time-consuming. You can limit the breadth and scope of the scan by specifying the hosts you want to scan in a simple text file.

1. On the TargetWindows02 taskbar, **click** the **Windows Start icon**, then **select Tenable Network Security > Nessus Web Client** to open the Nessus Web Client in Google Chrome.



Nessus menu location

2. When prompted with a security warning, **click** the **Advanced button**, then **click** the **Proceed to localhost (unsafe)** to continue.



Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

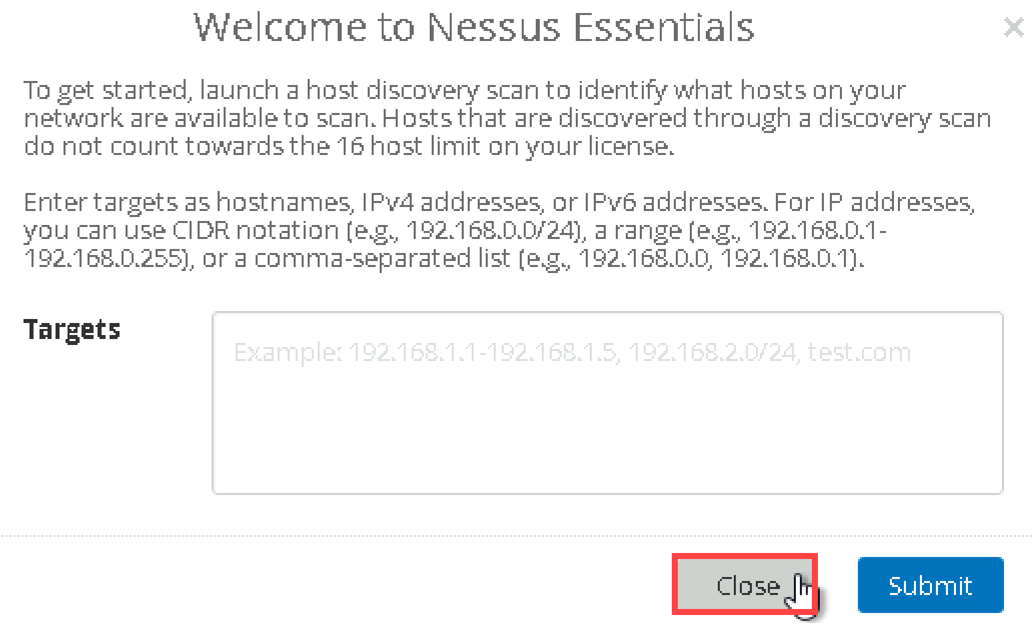
Security warning

Note: This warning appears when visiting a website that either has an expired certificate, a mismatched certificate, or a self-signed certificate. For the purposes of this lab, you can disregard this warning.

3. When prompted, **type** the following credentials and **click Login** to open Nessus.

    - Username: `Administrator`
    - Password: `P@ssw0rd!`

4. If prompted, **click** the **Close button** to close the Welcome dialog box.


Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

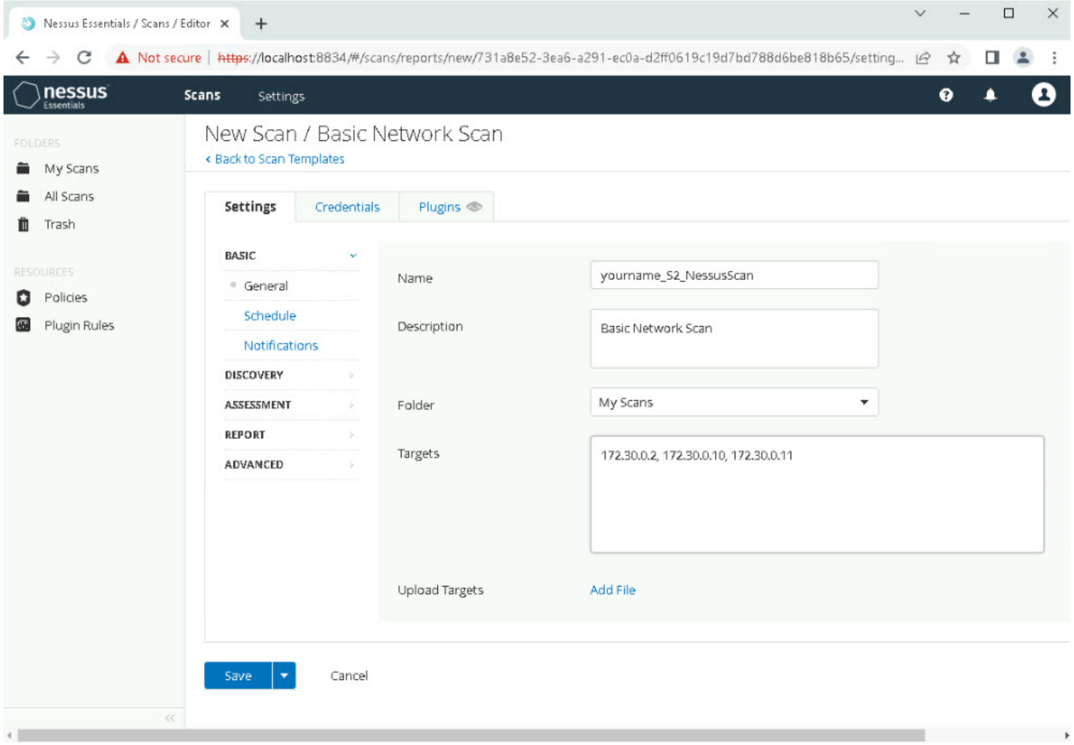
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Welcome dialog box

5. **Create** a new **Basic Network Scan** of all of the hosts identified by Zenmap using the following configuration.

   - Name: ***yourname*****_S2_NessusScan**, replacing *yourname* with your own name
   - Description: **Basic Network Scan**
   - Folder: **My Scans**
   - Target: **172.30.0.2, 172.30.0.10, 172.30.0.11**



New Scan / Basic Network Scan

Name: yourname_S2_NessusScan

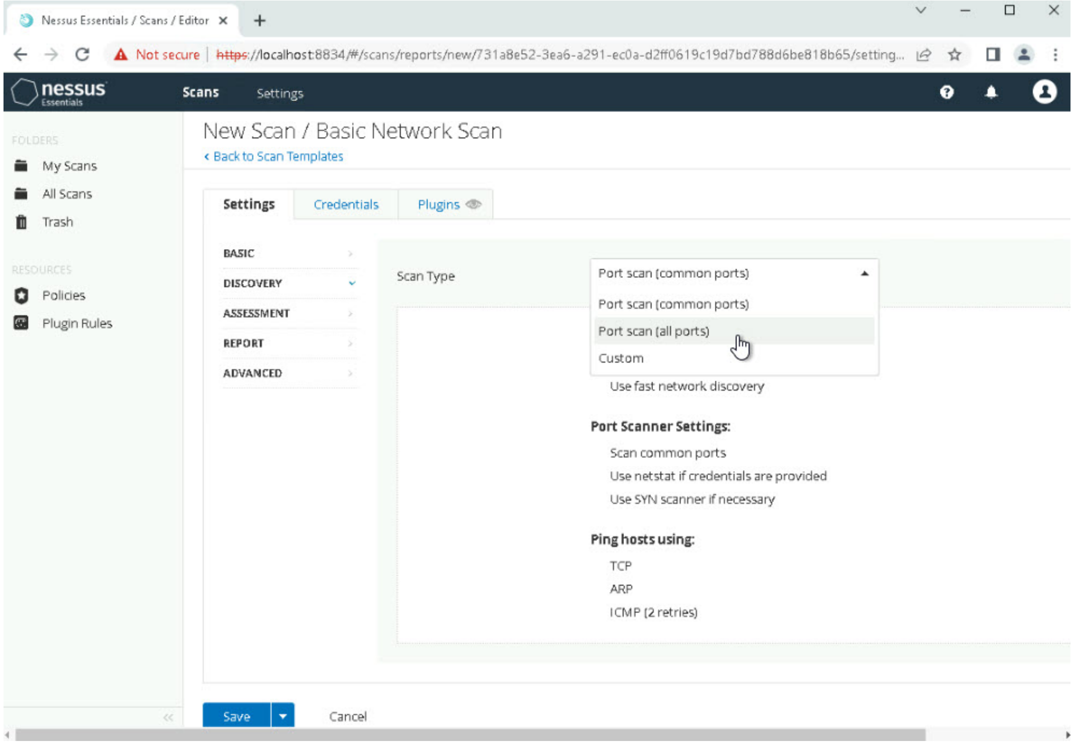
Description: Basic Network Scan

Folder: My Scans

Targets: 172.30.0.2, 172.30.0.10, 172.30.0.11

Nessus configuration form

6. In the left pane, **click Discovery** to open the Discovery settings, then **select Port scan (all ports)** from the Scan Type drop down list and **save** the new scan configuration.



New Scan / Basic Network Scan

Scan Type: Port scan (common ports)

- Port scan (common ports)
- Port scan (all ports)
- Custom

Use fast network discovery

Port Scanner Settings:

Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary

Ping hosts using:

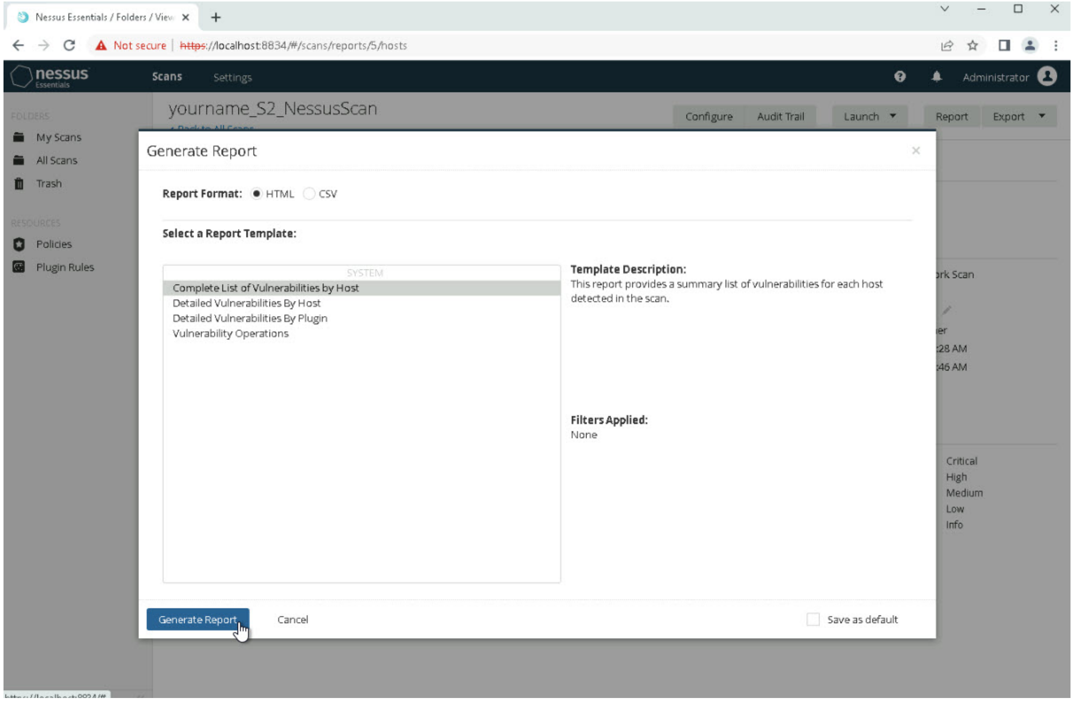
TCP
ARP
ICMP (2 retries)

Scan all ports

7. **Launch** a new scan using the ***yourname*_S2_NessusScan** configuration.

Note: Scanning will take around 20 minutes to complete. The green refresh symbol will spin as long as the scan is running. The refresh symbol will change to a check mark when the scan is complete.

8. In the upper-right corner of the scan results page, **click Report** and **select Complete List of Vulnerabilities by Host** to export the scan results as an HTML file. Then **click** the **Generate Report button.**



yourname_S2_NessusScan

Generate Report

Report Format: ● HTML ○ CSV

Select a Report Template:

SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Generate Report   Cancel   □ Save as default

Export report

9. In File Explorer, **navigate to the This PC/Downloads folder** and **locate the HTML report** that was exported (**yourname_S2_NessusScan_***).

10. In File Explorer, **copy** the **yourname_S2_NessusScan_* file** to **This PC/Desktop** and then **rename the file to** yourname_S2_NessusScan, replacing *yourname* with your own name.

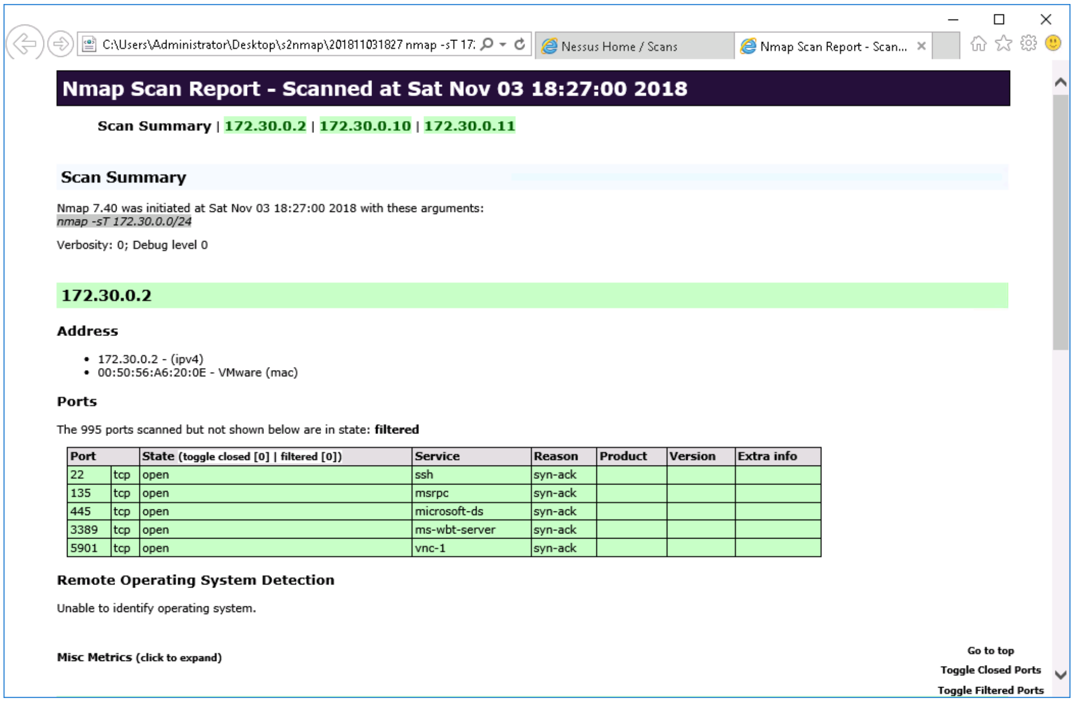
11. **Close** the **Nessus browser window**.

Part 3: Evaluate your Findings

Note: In the next steps, you will review the vulnerabilities identified in the Nessus scan and research the details for several risks using multiple resources. You will use that information to locate possible solutions. First, you will review the files you saved earlier in the lab.

1. From the S2nmap folder on the TargetWindows02 desktop, **review** all **Nmap scans**.

   If prompted, **click Allow Blocked Content** to dismiss the popup window. The scan report will open in Firefox. Each host appears as a link in the header of the report. Click the host IP to navigate to the discovery data for that machine.


C:\Users\Administrator\Desktop\s2nmap\201811031827 nmap -sT 17:
Nessus Home / Scans
Nmap Scan Report - Scan...

Nmap Scan Report - Scanned at Sat Nov 03 18:27:00 2018

Scan Summary | **172.30.0.2** | **172.30.0.10** | **172.30.0.11**

Scan Summary

Nmap 7.40 was initiated at Sat Nov 03 18:27:00 2018 with these arguments:
nmap -sT 172.30.0.0/24

Verbosity: 0; Debug level 0

172.30.0.2

Address

- 172.30.0.2 - (ipv4)
- 00:50:56:A6:20:0E - VMware (mac)

Ports

The 995 ports scanned but not shown below are in state: **filtered**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack			
135	tcp	open	msrpc	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
5901	tcp	open	vnc-1	syn-ack			

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Nmap scan

Note: In the next steps, you will copy the deliverable files to the vWorkstation desktop so that you can continue to work with the reports.

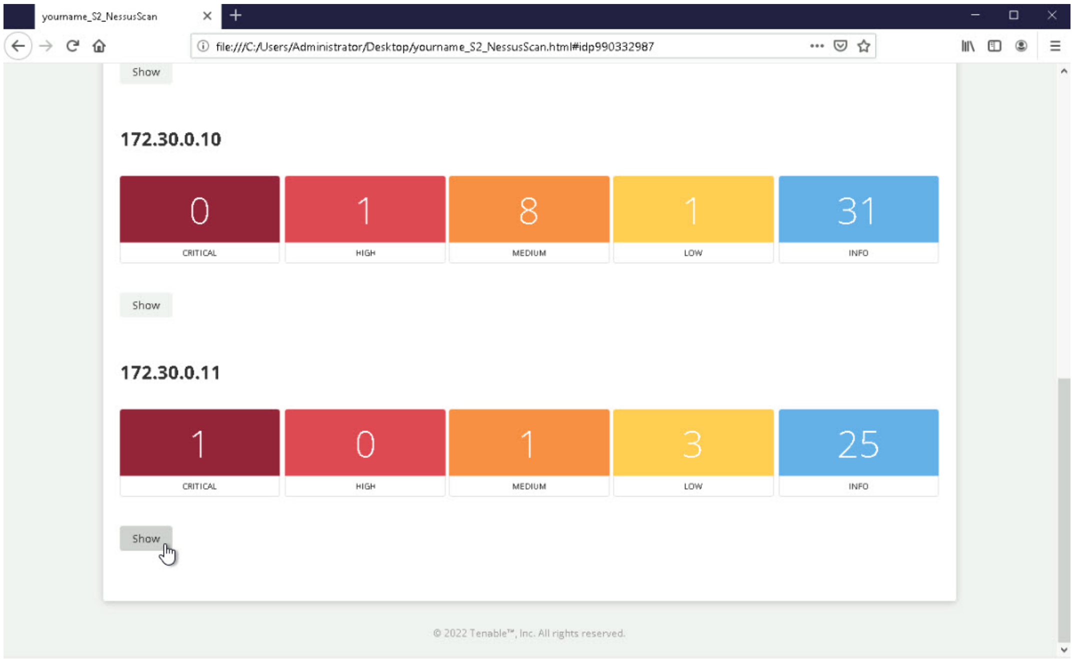
2. **Compress** all **Nmap files** into a new archive file (***yourname*_S2_NmapScans**), replacing *yourname* with your own name, and save the new file to the TargetWindows02 desktop.

3. From the TargetWindows02 desktop, **copy the scan files** you saved earlier in this lab and **paste** them to the vWorkstation desktop.

   - ***yourname*_S2_NessusScan**
   - ***yourname*_S2_NmapScans**

4. From the vWorkstation desktop, **open *yourname*_S2_NessusScan** in Firefox.

5. **Navigate** to the Summary for **172.30.0.11** and **click** the **Show button** to expand the summary.



file:///C:/Users/Administrator/Desktop/yourname_S2_NessusScan.html#idp990332987

172.30.0.10

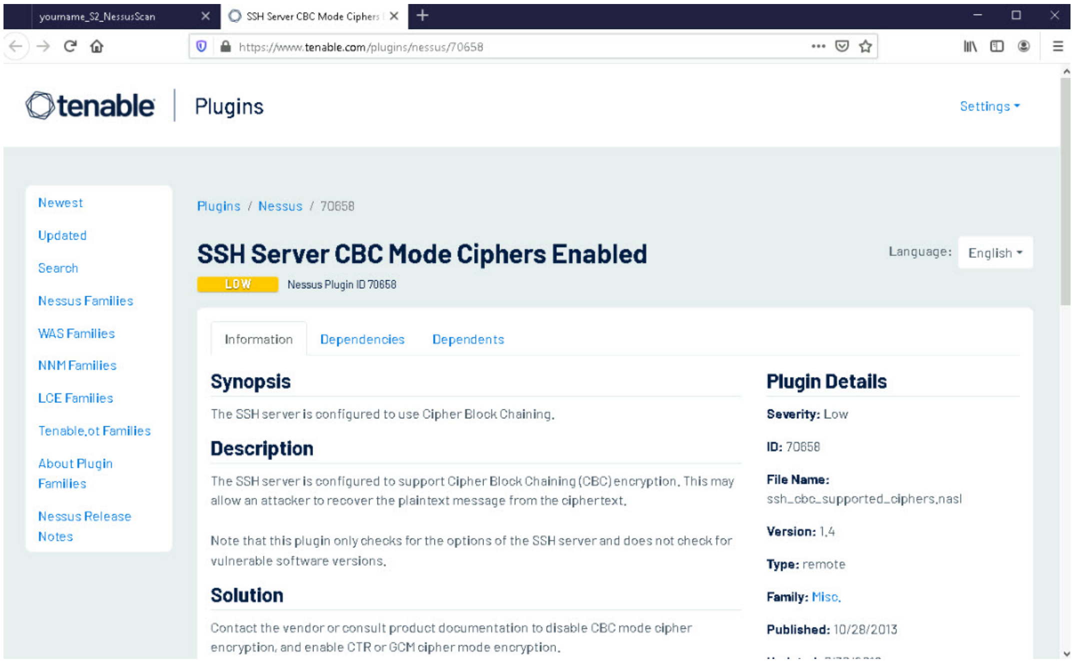
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	8	1	31

172.30.0.11

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	0	1	3	25

Opening the summary of 172.30.0.11

6. **Click** the **70658 link** to view additional details for the SSH Server CBC Mode Ciphers Enabled vulnerability.



SSH Server CBC Mode Ciphers Enabled

Nessus Plugin ID 70658

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Plugin Details

Severity: Low

ID: 70658

File Name: ssh_cbc_supported_ciphers.nasl

Version: 1.4

Type: remote

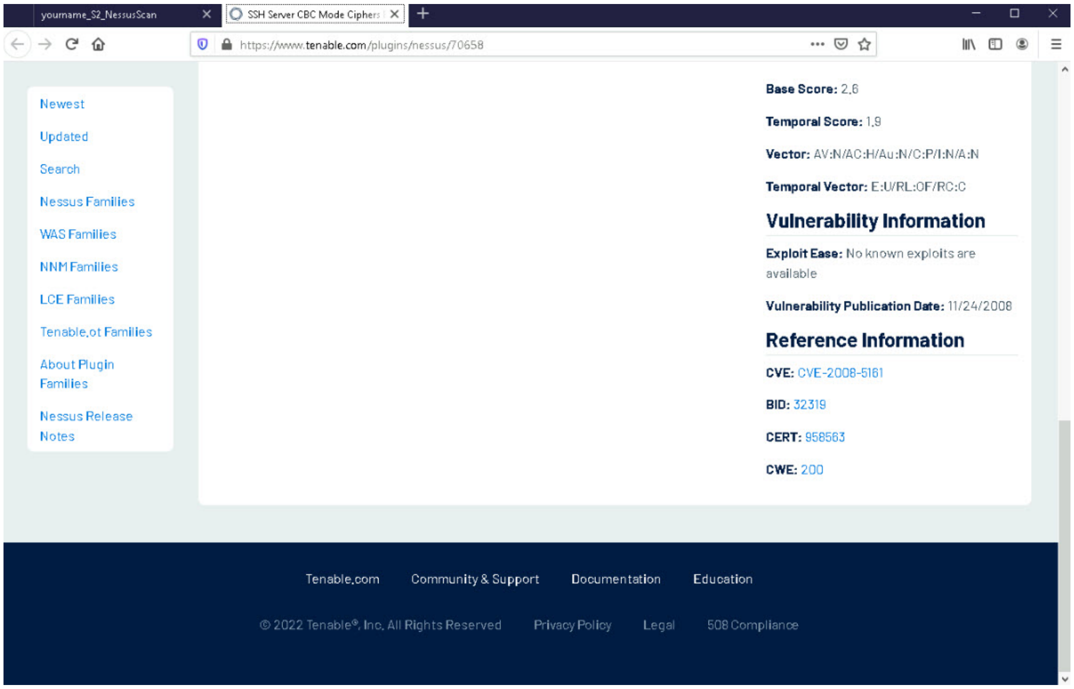
Family: Misc.

Published: 10/28/2013

SSH Server CBC Mode Ciphers Enabled

Note: Each vulnerability identified in the report will include a corresponding Plugin ID. A Plugin is a vulnerability test script, written to detect a specific vulnerability or set of vulnerabilities. If a plugin's vulnerability check matches a CVE description, it is added to the plugin. CVE stands for Common Vulnerabilities and Exposures. The MITRE Corporation (www.mitre.org) launched the CVE List in 1999 as a community effort to document publicly known cybersecurity vulnerabilities. The CVE List also serves as the foundation for the U.S. National Vulnerability Database (NVD), a vulnerability database launched by the National Institute of Standards and Technology (NIST) in 2005. Building upon the CVE List, the NVD enhances each CVE entry with information about how to mitigate the vulnerability with software patches and updates. Although the two are separate resources, the NVD is fully synchronized with the CVE List, and both are sponsored by the United States Department of Homeland Security and the Cybersecurity and Communications office of the United States Computer Emergency Readiness Team (US-CERT). More information on discovered vulnerabilities (and their mitigation strategies) can be found at http://cve.mitre.org.

7. **Review** the description of the problem and the solution options, then **locate** the **CVE ID**.



Base Score: 2.6

Temporal Score: 1.9

Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Temporal Vector: E:U/RL:OF/RC:C

Vulnerability Information

Exploit Ease: No known exploits are available

Vulnerability Publication Date: 11/24/2008

Reference Information

CVE: CVE-2008-5161

BID: 32319

CERT: 958563

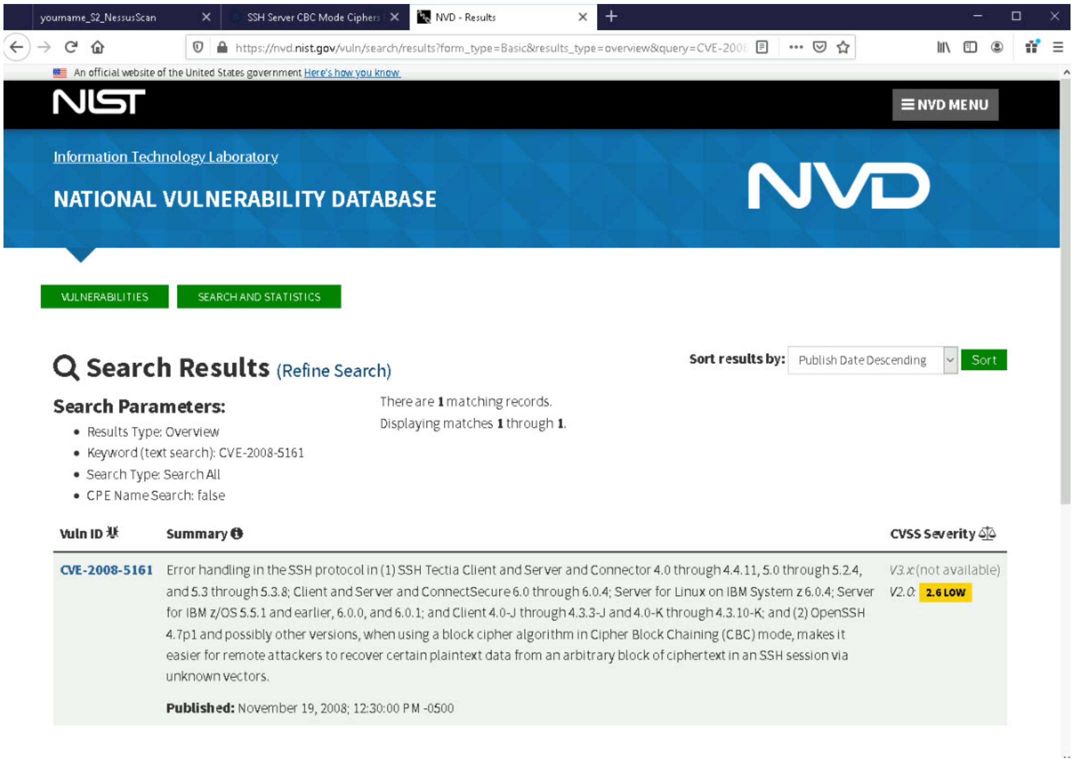
CWE: 200

CVE ID

8. **Open** a **new browser tab** and **navigate** to **`http://nvd.nist.gov/vuln/search`**.

9. **Search** the NVD for CVE ID **`CVE-2008-5161`**.

   The database lists only a brief summary of the vulnerability in the search results, but includes a link to more information.


yourname_S2_NessusScan
SSH Server CBC Mode Ciphers
NVD - Results
https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2008
An official website of the United States government Here's how you know
NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
SEARCH AND STATISTICS
Sort results by:
Publish Date Descending
Sort

Search Results (Refine Search)

There are **1** matching records.
Displaying matches **1** through **1**.

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2008-5161
- Search Type: Search All
- CPE Name Search: false

Vuln ID	Summary	CVSS Severity
CVE-2008-5161	Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors. **Published:** November 19, 2008; 12:30:00 PM -0500	*V3.x:* (not available) *V2.0:* **2.6 LOW**

CVE List's summary of the vulnerability

10. **Click** the **CVE-2008-5161 link** to view more information about this vulnerability.

    Review the additional information available on this page and compare the information provided in the database to the information provided by Nessus. You may notice that they both provide many of the same references, but Nessus simplifies the discovery.

11. **Click** the **Nessus Scan Report browser tab** to return to the Nessus report.

12. In your Lab Report file, **document** all of the **medium-risk security vulnerabilities for 172.30.0.11** identified by the scan and **make recommendations** for mitigating those risks based on your review of the information in the vulnerability scan.

13. **Close** the **browser**.

Note: This completes Section 2 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

14. On the vWorkstation desktop, **drag and drop** the following files into the File Transfer folder to complete the download to your local computer.

    - ***yourname*_S2_NessusScan**
    - ***yourname*_S2_NmapScans**

Section 3: Lab Challenge and Analysis

Note: The following questions are provided to allow you the opportunity for independent, unguided research, similar to what you will encounter in a real situation. Some questions will challenge you to find command line syntax for tasks you performed in the lab, others may ask you to extend your learning from the lab. Use screen captures where possible to illustrate your answers.

Part 1: Analysis and Discussion

Zenmap identified three hosts on the 172.30.0.0/24 subnet. What operating system version did the scan reveal for each host?

Part 2: Tools and Commands

In this lab, you learned a few basic, but powerful, Nmap commands for Zenmap. Research the Internet to find more about Nmap commands and how Zenmap (or Nmap by itself) can be used for network reconnaissance. Then, construct an Nmap command that could probe a firewalled network in a stealthy manner. Explain how your command works. Use the network subnet 172.30.0.0/24 in your command syntax.

Part 3: Challenge Exercise

In the lab, you made recommendations for the medium risk vulnerabilities identified by Nessus based on research in the Nessus itself and the CVE database. These are not your only resources. Research the Internet to find the recommended solution and a download link for the SSL RC4 Cipher Suites Supported (Bar Mitzvah) vulnerability discussed in Section 1.