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

To be good at their job, hackers and cybercriminals do not need to understand everything about how networks work or how they are vulnerable to attack. All they really need to know is one vulnerability, or how to use one automated tool that attacks that vulnerability. Defenders, on the other hand, need to have a comprehensive knowledge of networks and networking protocols. Defenders also need to understand how to identify and test for vulnerabilities in computer systems, routers, switches, firewalls, and other network devices. They need to find and close as many vulnerabilities as possible, as soon as possible.

Hackers traditionally follow a five-step approach to seek out and compromise targeted hosts: reconnaissance, scanning, vulnerability analysis (enumeration), exploitation (the actual attack), and post-attack activities, including remediation of the vulnerabilities. The first step, reconnaissance, begins with identifying the target and learning as much as possible about the target. During and after the reconnaissance phase, hackers may scan a target to identify IP hosts, open ports, and services enabled on servers and workstations.

In this lab, you will explore the common tools available in the virtual lab environment. You will use Wireshark to capture and analyze network traffic, use Nessus to scan the network, review a sample collection of data using NetWitness Investigator, connect to a remote Windows machine and explore two file transfer applications, FileZilla and Tftpd64. You will use PuTTY to connect to a Linux machine and run several Cisco commands to display statistics for the network interfaces. Finally, you will use Zenmap to perform a scan of the network and create a network topology chart.

Learning Objectives

Upon completing this lab, you will be able to:

1. Explore common network scanning and analysis tools

2. Perform network reconnaissance and probing on the machines in the Virtual Security Cloud Lab (VSCL)

3. Use Zenmap to perform an Intense scan on an entire subnetwork (172.30.0.0/24)

4. Create a Fisheye Bubble chart to explain the relationships between devices on a network

5. Explain how attackers use common network scanning and analysis tools to compromise networks

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 explore the tools used within the virtual lab environment.
2. In the second part of the lab, you will use PuTTY to connect to a Linux server and perform several Cisco IOS operations.
3. In the third part of the lab, you will use Zenmap to perform a basic reconnaissance of the targeted machine.

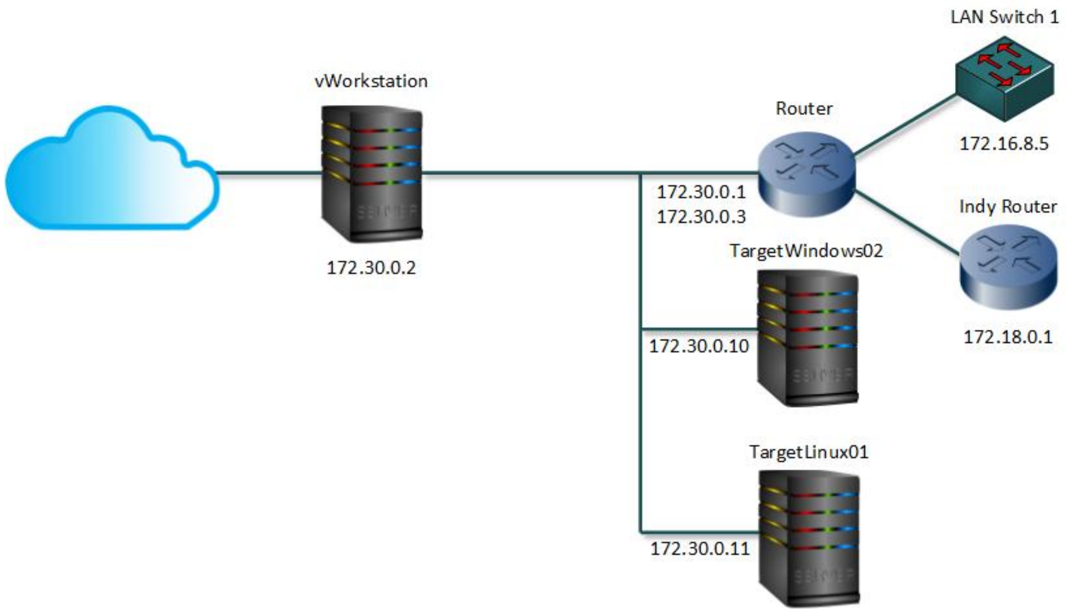
SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

Finally, if assigned by your instructor, you will explore the virtual environment on your own in **SECTION 3** of this lab to answer a set of questions and 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)
- Cisco IOS Emulator
  - Router
  - LAN Switch 1
  - Indy Router



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.

- FileZilla
- RSA NetWitness Investigator
- Nessus
- PuTTY
- Tftpd64
- Wireshark
- 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;

- Arrival Time for the Wireshark ICMP traffic;
- filename of the attachment in the NetWitness Investigator Demo Collection;
- Fisheye Bubble chart from Zenmap scan;

2. Files downloaded from the virtual environment:

- *yourname*_S1_zenmap.xml;

3. Any additional information as directed by the lab:

- results of Cisco command tests;
- tests run as part of the Intense scan;

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

SECTION 2:

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

- Arrival Time for the Wireshark ICMP traffic;
- file details of the creditcards.txt attachment in NetWitness Investigator;
- successful TFTP file transfer;
- output from the Cisco command issued in PuTTY;
- Fisheye Bubble chart from Zenmap scan;
- results of the second Zenmap scan;

2. Files downloaded from the virtual environment:

- *yourname*_S2_wireshark_capture.pcap;
- *yourname*_S2_BasicScan.txt;

3. Any additional information as directed by the lab;

- results of VLAN command test;
- type of Zenmap scan that uses the command -T4 -F;

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**.

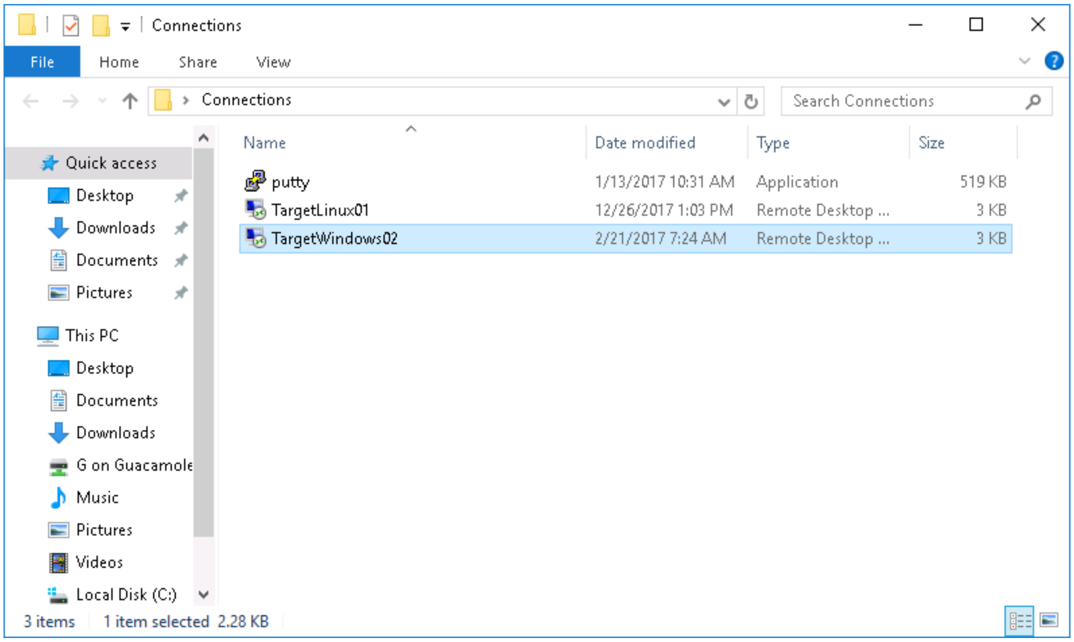
Part 1: Exploring the Tools used in the Virtual Lab Environment

Note: In the next steps, you will explore several of the applications and tools available in the virtual lab environment to help familiarize you with their intended purpose.

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

Connections folder

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



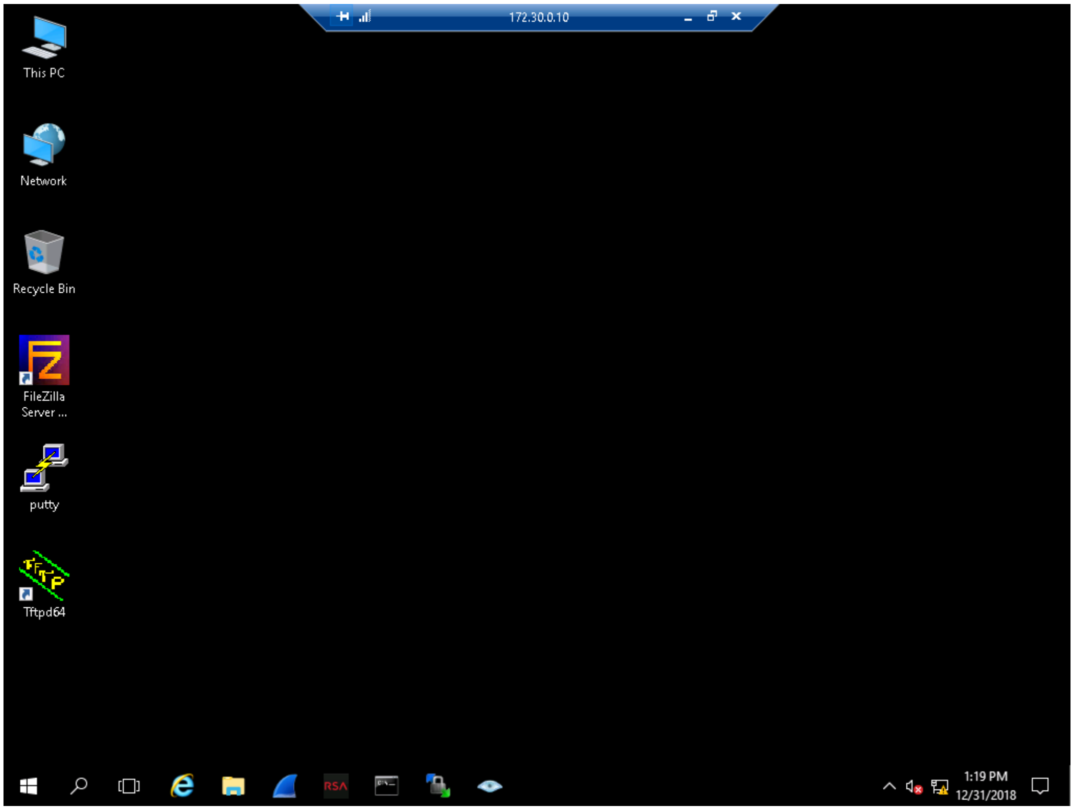
Name	Date modified	Type	Size
putty	1/13/2017 10:31 AM	Application	519 KB
TargetLinux01	12/26/2017 1:03 PM	Remote Desktop ...	3 KB
TargetWindows02	2/21/2017 7:24 AM	Remote Desktop ...	3 KB

TargetWindows02 RDP Shortcut

If prompted, **type** the following credentials and **click OK**.

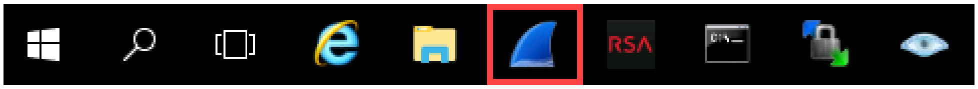
- Username: `Administrator`
- Password: `P@ssw0rd!`

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



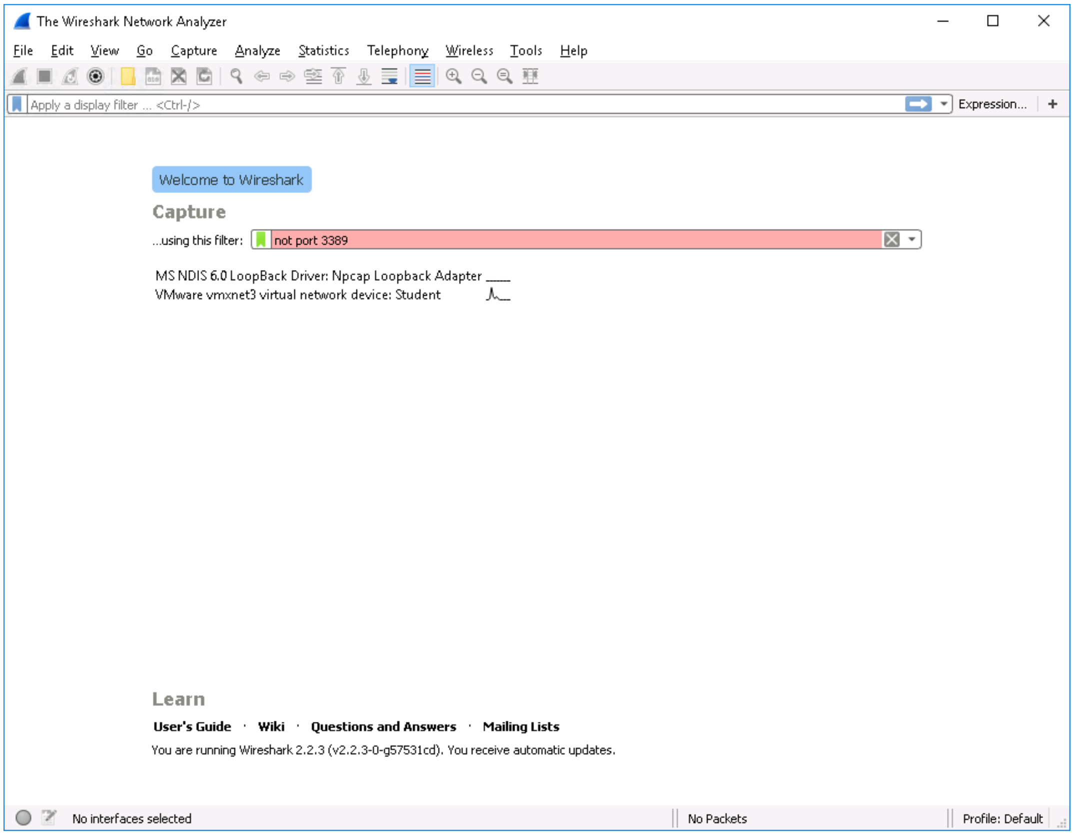
TargetWindows02 desktop

3. On the TargetWindows02 taskbar, **click** the **Wireshark icon** (a blue shark fin) to open the Wireshark application.



Wireshark icon

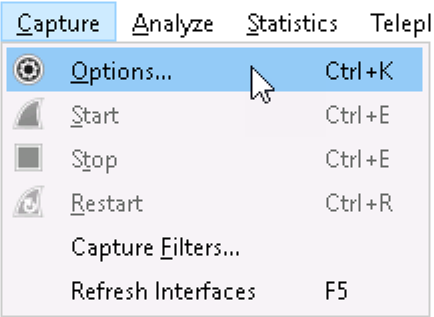
Note: Wireshark is a protocol analyzer tool (sometimes called a “packet sniffer”). It is used to capture IP traffic from a variety of sources. The main screen of Wireshark includes details about the current capture configuration. From this screen, analysts can select common filters from the drop-down menu, or type a custom filter command to quickly sort the captured data. Your welcome screen may not match the figure below.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Welcome to Wireshark
Capture
…using this filter:
not port 3389
MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter
VMware vmxnet3 virtual network device: Student
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.3 (v2.2.3-0-g57531cd). You receive automatic updates.
No interfaces selected
No Packets
Profile: Default

Wireshark main screen

4. If necessary, **maximize** the **Wireshark window**.

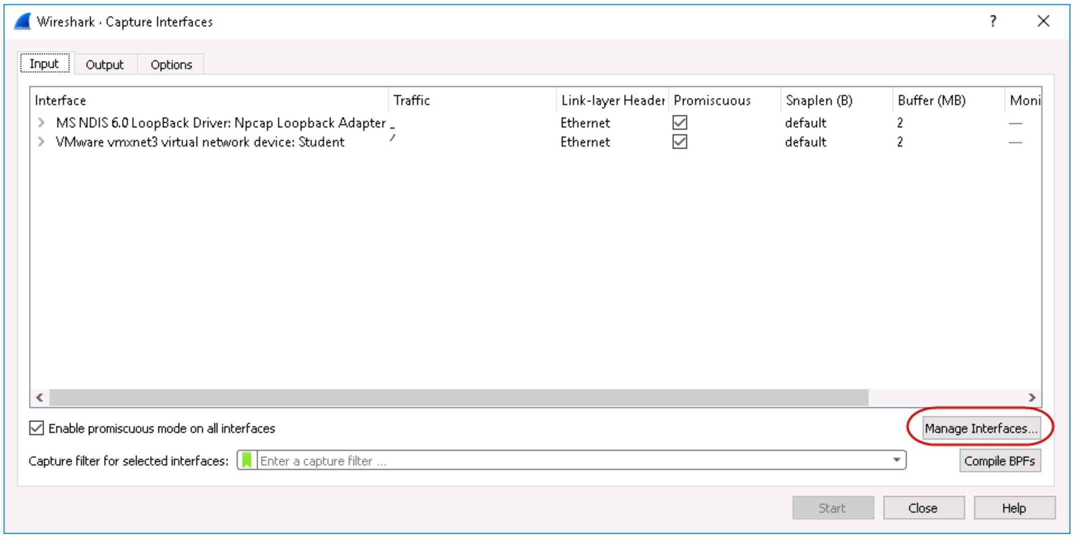
5. From the Wireshark menu bar, **click Capture** and **select Options** to open the Capture Interfaces dialog box.



Capture menu

Note: You may also press CTRL+K to open the Capture Interfaces dialog box.

6. In the Capture Interfaces dialog box, **click** the **Manage Interfaces button** to open the Manage Interfaces dialog box.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Moni
MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter		Ethernet	☑	default	2	—
VMware vmxnet3 virtual network device: Student		Ethernet	☑	default	2	—

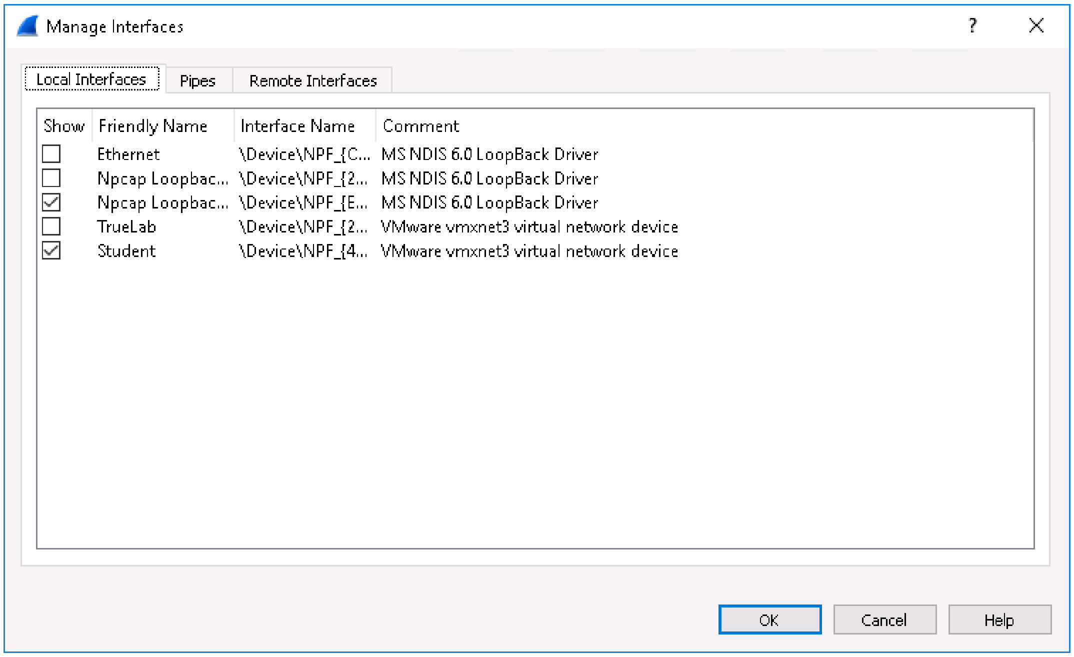
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Manage Interfaces button

7. In the Manage Interfaces dialog box, **confirm** that only the **Student** and **Npcap Loopback Adapter interfaces** are selected, as shown in the following figure.

   The student interface is the network interface for the lab environment that you are working in. Selecting this interface ensures that Wireshark can analyze traffic from areas of the network that are visible to students.



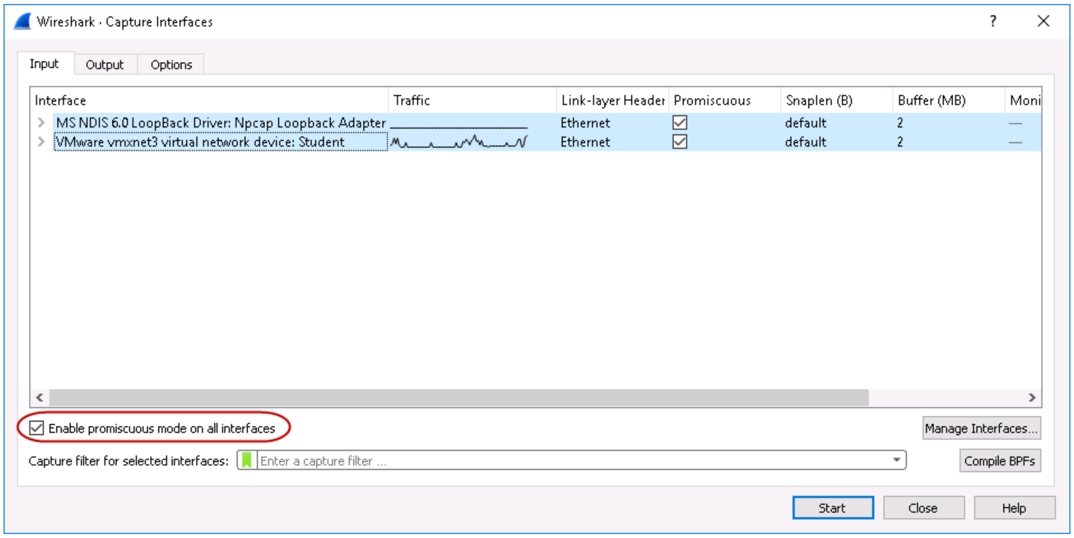
Show	Friendly Name	Interface Name	Comment
□	Ethernet	\Device\NPF_{C...	MS NDIS 6.0 LoopBack Driver
□	Npcap Loopbac...	\Device\NPF_{2...	MS NDIS 6.0 LoopBack Driver
☑	Npcap Loopbac...	\Device\NPF_{E...	MS NDIS 6.0 LoopBack Driver
□	TrueLab	\Device\NPF_{2...	VMware vmxnet3 virtual network device
☑	Student	\Device\NPF_{4...	VMware vmxnet3 virtual network device

Verify interface selection

8. In the Manage Interfaces dialog box, **click OK** to close the dialog box.

9. In the Capture Interfaces dialog box, **confirm** that the **Enable promiscuous mode on all interfaces checkbox** is selected.

   Promiscuous mode allows Wireshark (or any other application) to capture packets destined to any host on the same subnet or virtual LAN (VLAN). Without this option selected, Wireshark would only capture packets to and from TargetWindows02.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Moni
MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter		Ethernet	☑	default	2	—
VMware vmxnet3 virtual network device: Student		Ethernet	☑	default	2	—

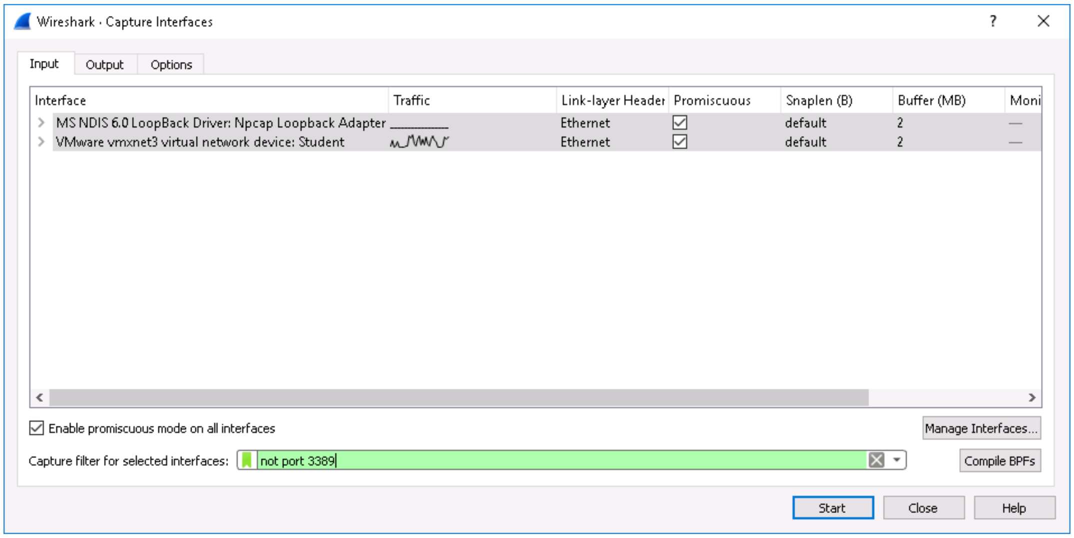
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Verify promiscuous mode

10. In the Capture Interfaces dialog box, **hold down** the **CTRL key** and **click** the **Student** and **Npcap Loopback Adapter interfaces** to select both interfaces.

11. In the Capture filter for selected interfaces box, **type** `not port 3389` to filter out the RDP traffic generated between the vWorkstation and TargetWindows02 systems.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Moni
MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter		Ethernet	☑	default	2	—
VMware vmxnet3 virtual network device: Student		Ethernet	☑	default	2	—

☑ Enable promiscuous mode on all interfaces

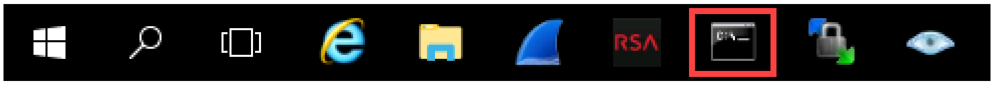
Capture filter for selected interfaces: not port 3389

Select interfaces

12. In the Capture Interfaces dialog box, **click Start** to close the Capture Interfaces dialog box and begin the packet capture.

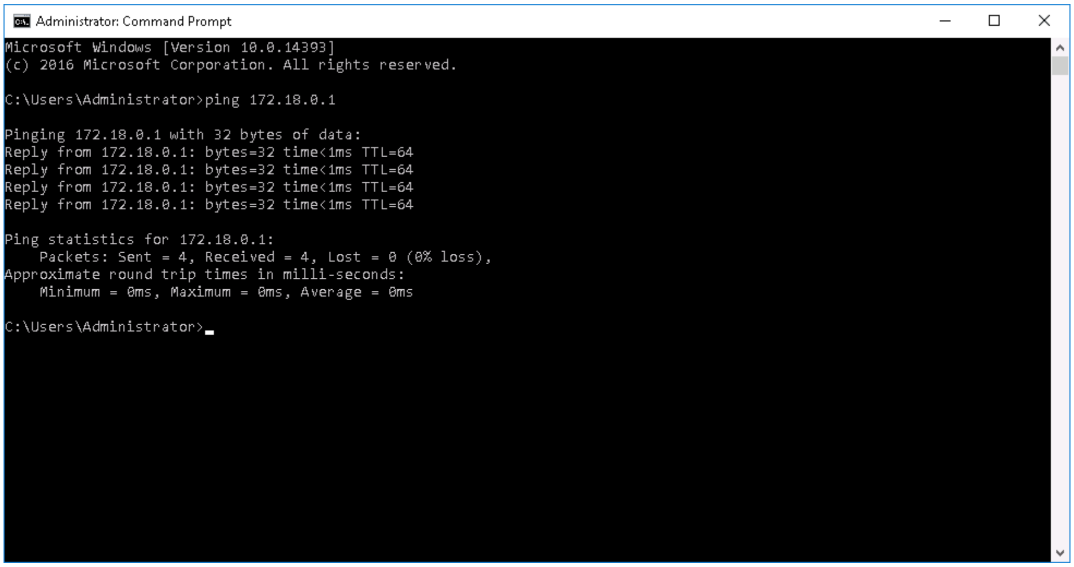
Note: In the next steps, you will generate traffic for Wireshark to capture.

13. On the TargetWindows02 taskbar, **click** the **Command Prompt icon** to open a new command prompt window.



Command Prompt icon

14. At the command prompt, **type** `ping 172.18.0.1` (the IP address for the Indy Router interface) and **press Enter** to ping the Indy Router and begin generating network traffic for Wireshark to capture.

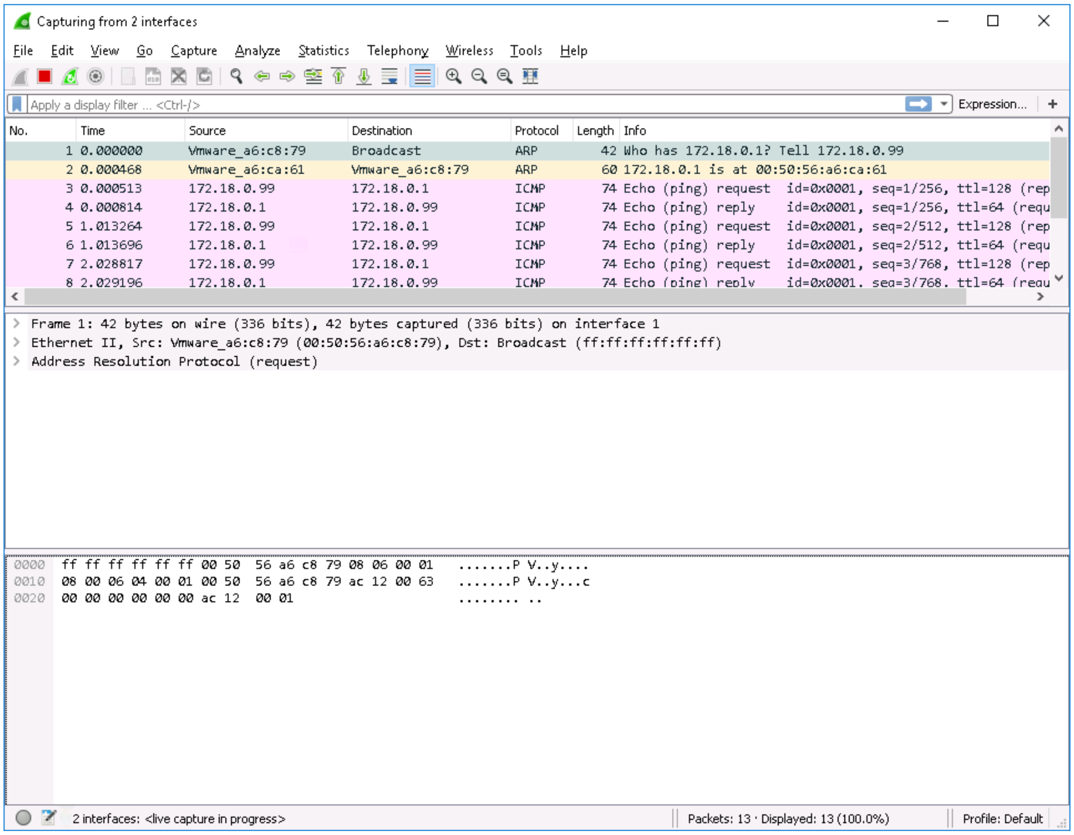


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.18.0.1

Pinging 172.18.0.1 with 32 bytes of data:
Reply from 172.18.0.1: bytes=32 time<1ms TTL=64
Reply from 172.18.0.1: bytes=32 time<1ms TTL=64
Reply from 172.18.0.1: bytes=32 time<1ms TTL=64
Reply from 172.18.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.18.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Generate capture data

15. When the command prompt reappears, **type** `exit` and **press Enter** to close the command prompt window and return to the Wireshark window.

    Because Wireshark is capturing live data, your screen will not match the following figure. However, you will still see that Wireshark has captured the Ping traffic as packets using the ICMP protocol (Internet Control Message Protocol).


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  Vmware_a6:c8:79    Broadcast          ARP          42 Who has 172.18.0.1? Tell 172.18.0.99
   2 0.000468  Vmware_a6:ca:61    Vmware_a6:c8:79    ARP          60 172.18.0.1 is at 00:50:56:a6:ca:61
   3 0.000513  172.18.0.99        172.18.0.1         ICMP         74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (rep
   4 0.000814  172.18.0.1         172.18.0.99        ICMP         74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (requ
   5 1.013264  172.18.0.99        172.18.0.1         ICMP         74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (rep
   6 1.013696  172.18.0.1         172.18.0.99        ICMP         74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (requ
   7 2.028817  172.18.0.99        172.18.0.1         ICMP         74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (rep
   8 2.029196  172.18.0.1         172.18.0.99        ICMP         74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (requ
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 1
> Ethernet II, Src: Vmware_a6:c8:79 (00:50:56:a6:c8:79), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 50  56 a6 c8 79 08 06 00 01   .......P V..y....
0010  08 00 06 04 00 01 00 50  56 a6 c8 79 ac 12 00 63   .......P V..y...c
0020  00 00 00 00 00 00 ac 12  00 01                     ........ ..
```

2 interfaces: <live capture in progress>   Packets: 13 · Displayed: 13 (100.0%)   Profile: Default

Wireshark window

Exploring Wireshark

The Wireshark window opens with the detailed information about the packets captured in three panes. Use your mouse to drag the borders of any pane up or down to change its size.

- The top pane of the Wireshark window contains all of the packets that Wireshark has captured, in time order, and provides a summary of the contents of the packet in a format close to human readable. Keep in mind that the content will be different depending on where you capture packets in the network. Also remember that the “source” and “destination” are relative to where a packet is captured. This area of the Wireshark window is referred to as the *frame summary* or *packet list* pane.

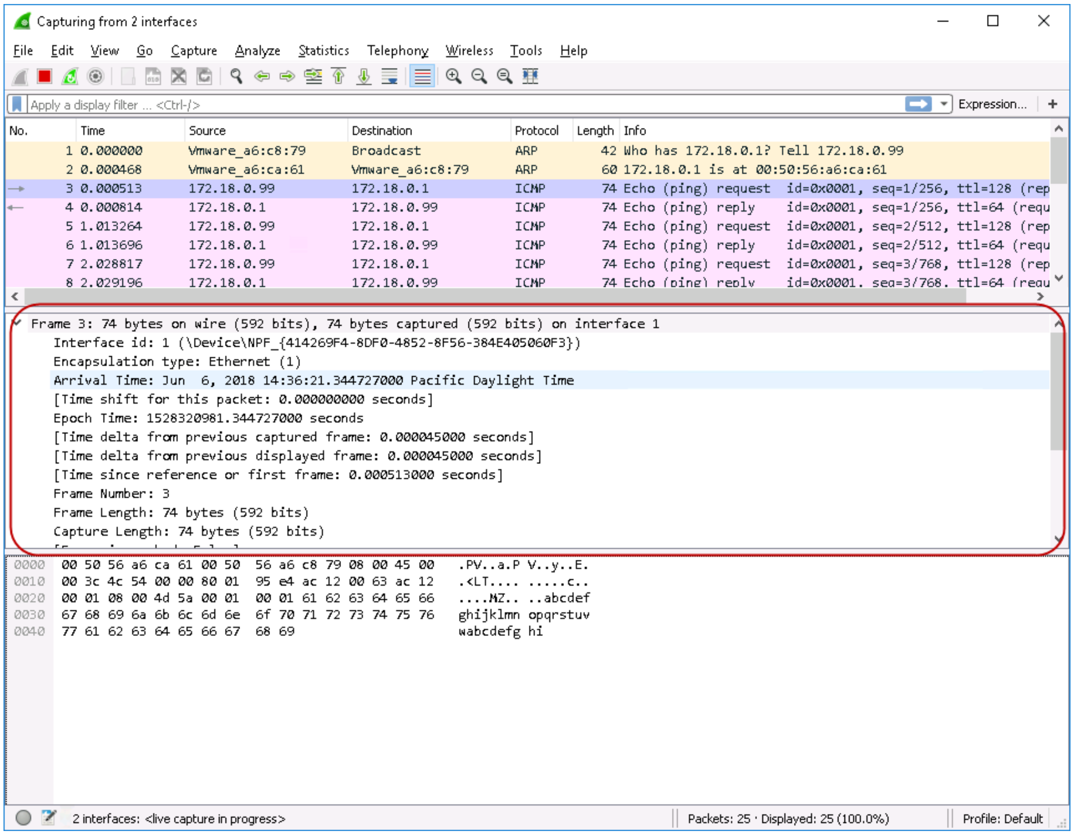
- The middle pane of the Wireshark window is used to display the packet structure and contents of fields within the packet. This area of the Wireshark window is referred to as the *frame details* or *packet details* pane.

- The bottom pane of the Wireshark window displays the hex data. All of the information in the packet is displayed in hexadecimal on the left and in decimal, in characters when possible, on the right. This can be a useful feature, especially if the passwords you are looking for are unencrypted. This area of the Wireshark window is referred to as the *hex data* or *packet bytes* pane.

16. In the frame summary pane, **review** the **Protocol column** and **click** the **first ICMP frame** to select it.

17. In the frame detail pane, **click** the **arrow** to the left of the frame number to expand the detail.

    In the frame detail pane, Wireshark displays information about the time the data was captured.



```
No.      Time        Source              Destination         Protocol  Length  Info
     1 0.000000    Vmware_a6:c8:79     Broadcast           ARP           42 Who has 172.18.0.1? Tell 172.18.0.99
     2 0.000468    Vmware_a6:ca:61     Vmware_a6:c8:79     ARP           60 172.18.0.1 is at 00:50:56:a6:ca:61
     3 0.000513    172.18.0.99         172.18.0.1          ICMP          74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (rep
     4 0.000814    172.18.0.1          172.18.0.99         ICMP          74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (requ
     5 1.013264    172.18.0.99         172.18.0.1          ICMP          74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (rep
     6 1.013696    172.18.0.1          172.18.0.99         ICMP          74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (requ
     7 2.028817    172.18.0.99         172.18.0.1          ICMP          74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (rep
     8 2.029196    172.18.0.1          172.18.0.99         ICMP          74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (requ
```

```
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1
    Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun  6, 2018 14:36:21.344727000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1528320981.344727000 seconds
    [Time delta from previous captured frame: 0.000045000 seconds]
    [Time delta from previous displayed frame: 0.000045000 seconds]
    [Time since reference or first frame: 0.000513000 seconds]
    Frame Number: 3
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
```

```
0000  00 50 56 a6 ca 61 00 50  56 a6 c8 79 08 00 45 00   .PV..a.P V..y..E.
0010  00 3c 4c 54 00 00 80 01  95 e4 ac 12 00 63 ac 12   .<LT.... .....c..
0020  00 01 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ....MZ.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

2 interfaces: <live capture in progress>
Packets: 25 · Displayed: 25 (100.0%)
Profile: Default

Frame detail for ICMP traffic

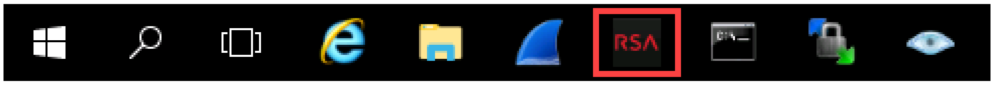
18. **Make a screen capture** showing the **Arrival Time** for the ICMP traffic that you captured and **paste** it into your Lab Report file.

19. On the Wireshark toolbar, **click** the red **Stop button** to stop the packet capture process, then **close** the **Wireshark window**.

20. When prompted, **click** the **Quit without Saving button** to close the application without saving the packet capture.

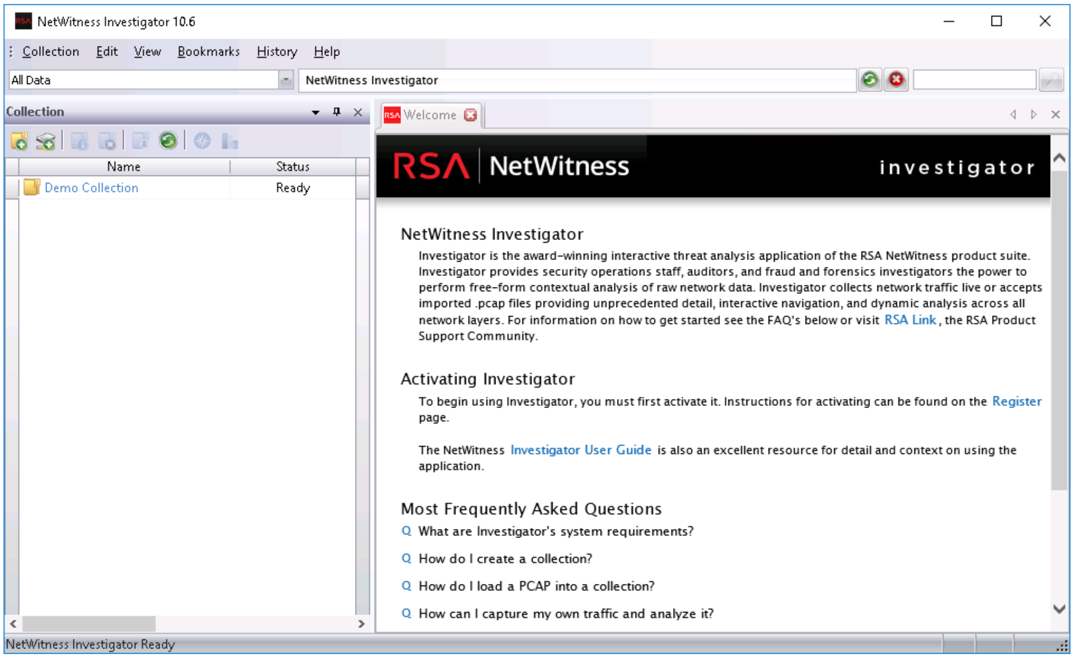
Note: In the next steps, you will explore the RSA NetWitness Investigator application. NetWitness Investigator provides a high-level overview of all the traffic in a packet capture file. While Wireshark looks at every packet, NetWitness categorizes and organizes traffic so that anomalous patterns become more apparent.

21. On the TargetWindows02 taskbar, **click** the **RSA icon** to open the NetWitness Investigator application.



NetWitness Investigator icon

22. If necessary, **maximize** the **NetWitness Investigator window**.



NetWitness Investigator

Investigator is the award-winning interactive threat analysis application of the RSA NetWitness product suite. Investigator provides security operations staff, auditors, and fraud and forensics investigators the power to perform free-form contextual analysis of raw network data. Investigator collects network traffic live or accepts imported .pcap files providing unprecedented detail, interactive navigation, and dynamic analysis across all network layers. For information on how to get started see the FAQ's below or visit RSA Link, the RSA Product Support Community.

Activating Investigator

To begin using Investigator, you must first activate it. Instructions for activating can be found on the Register page.

The NetWitness Investigator User Guide is also an excellent resource for detail and context on using the application.

Most Frequently Asked Questions

Q What are Investigator's system requirements?

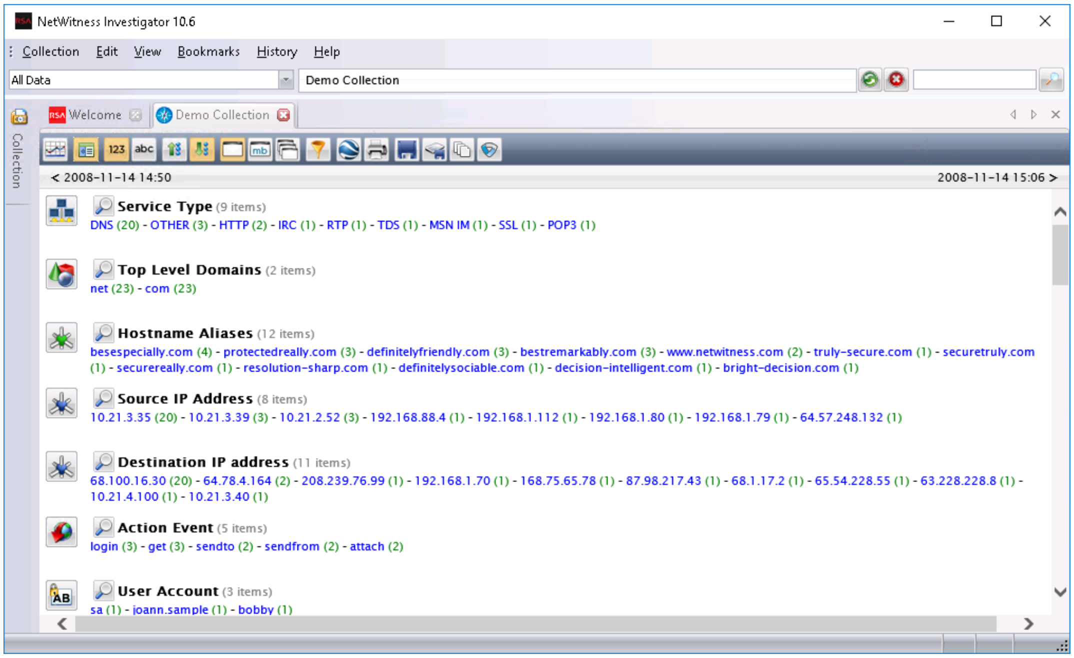
Q How do I create a collection?

Q How do I load a PCAP into a collection?

Q How can I capture my own traffic and analyze it?

NetWitness Investigator home page

23. In the Collections pane, **double-click** the **Demo Collection** to open the Demo Collection in NetWitness Investigator and see how NetWitness Investigator collects and presents traffic types and security events.



< 2008-11-14 14:50 | 2008-11-14 15:06 >

Service Type (9 items)
DNS (20) - OTHER (3) - HTTP (2) - IRC (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POP3 (1)

Top Level Domains (2 items)
net (23) - com (23)

Hostname Aliases (12 items)
besespecially.com (4) - protectedreally.com (3) - definitelyfriendly.com (3) - bestremarkably.com (3) - www.netwitness.com (2) - truly-secure.com (1) - securetruly.com (1) - securereally.com (1) - resolution-sharp.com (1) - definitelysociable.com (1) - decision-intelligent.com (1) - bright-decision.com (1)

Source IP Address (8 items)
10.21.3.35 (20) - 10.21.3.39 (3) - 10.21.2.52 (3) - 192.168.88.4 (1) - 192.168.1.112 (1) - 192.168.1.80 (1) - 192.168.1.79 (1) - 64.57.248.132 (1)

Destination IP address (11 items)
68.100.16.30 (20) - 64.78.4.164 (2) - 208.239.76.99 (1) - 192.168.1.70 (1) - 168.75.65.78 (1) - 87.98.217.43 (1) - 68.1.17.2 (1) - 65.54.228.55 (1) - 63.228.228.8 (1) - 10.21.4.100 (1) - 10.21.3.40 (1)

Action Event (5 items)
login (3) - get (3) - sendto (2) - sendfrom (2) - attach (2)

User Account (3 items)
sa (1) - joann.sample (1) - bobby (1)

Demo Collection viewed in NetWitness Investigator

24. Use the scrollbar to **review** the **NetWitness Investigator report**.

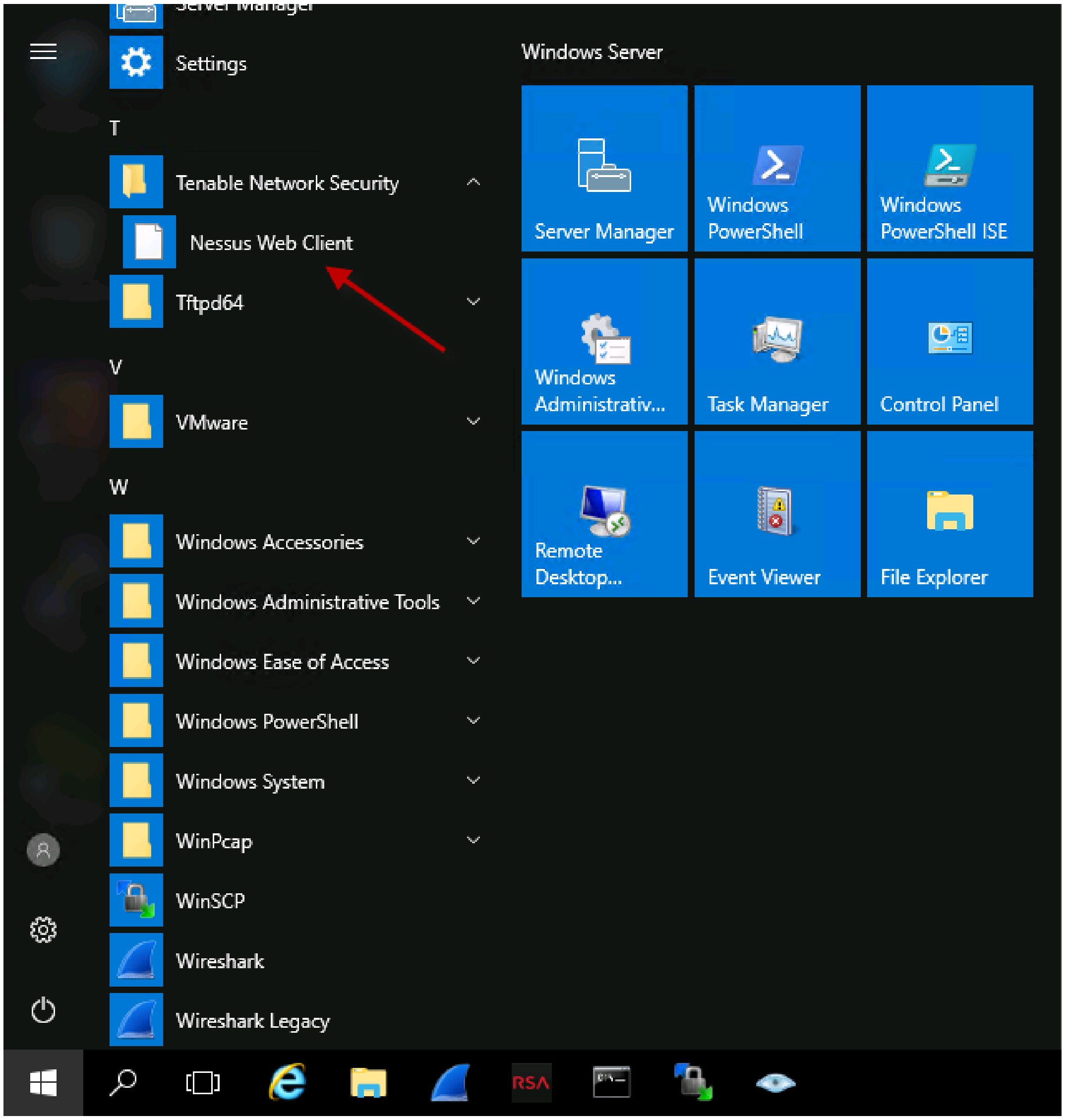
    Notice that NetWitness Investigator has specified the source and destination IP addresses in this collection, identified the user accounts found in the collection, and even recognized attachments.

25. **Make a screen capture** showing the **filename of the attachment** in this collection and **paste** it into your Lab Report file.

26. **Close** the **NetWitness Investigator window**.

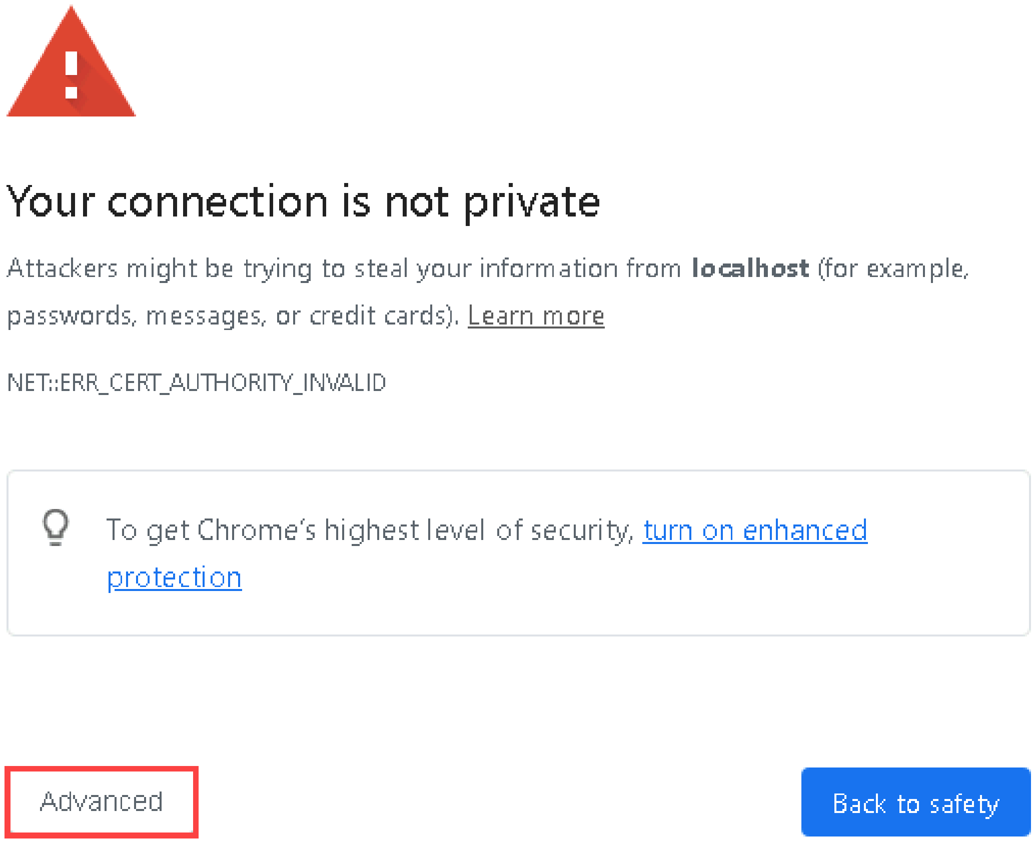
Note: In the next steps, you will explore the Nessus Web Client. Nessus performs remote scans and audits of Unix, Windows, and network infrastructures, and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices.

27. 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

28. 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

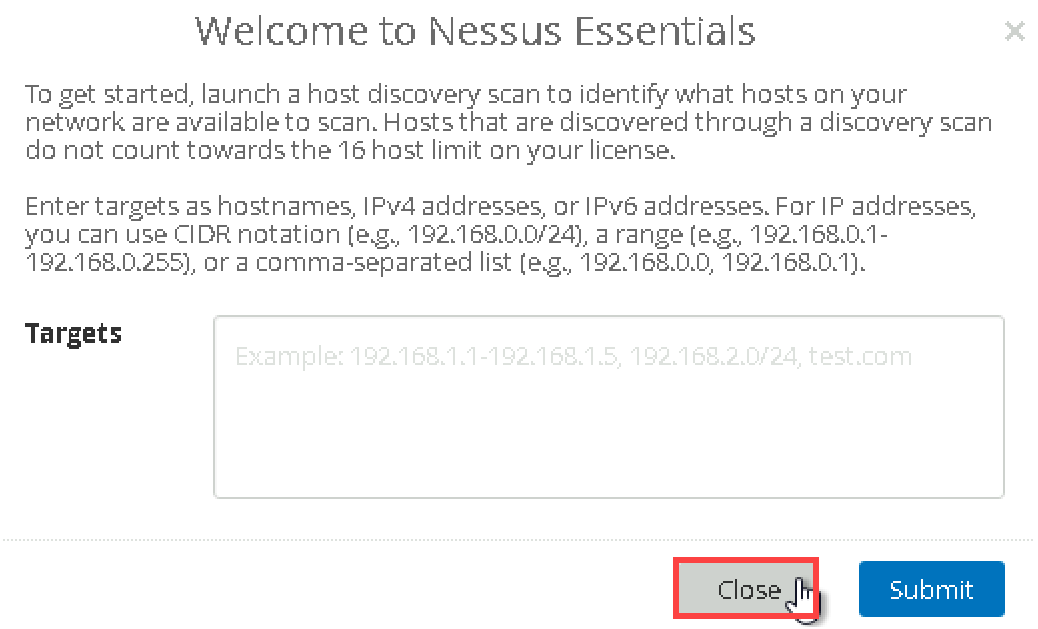
Note: This warning appears when visiting a website that either has an expired certificate, a mismatched certificate, or a self-signed certificate. For the purposes of this lab, you can disregard this warning.

29. 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**.

30. 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.

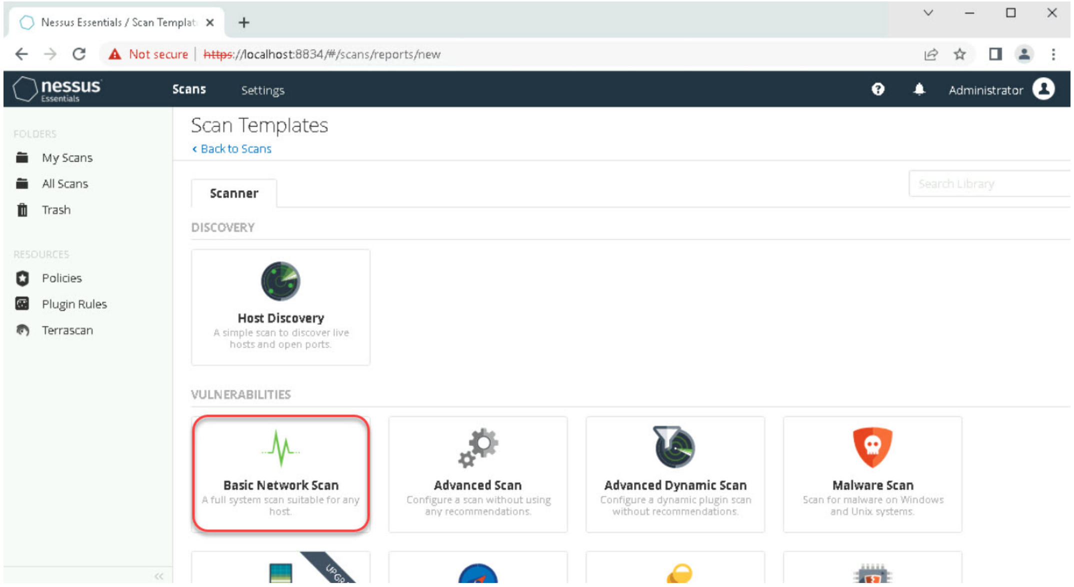
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Welcome dialog box

31. If necessary, **maximize** the **Nessus window**.

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

33. 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

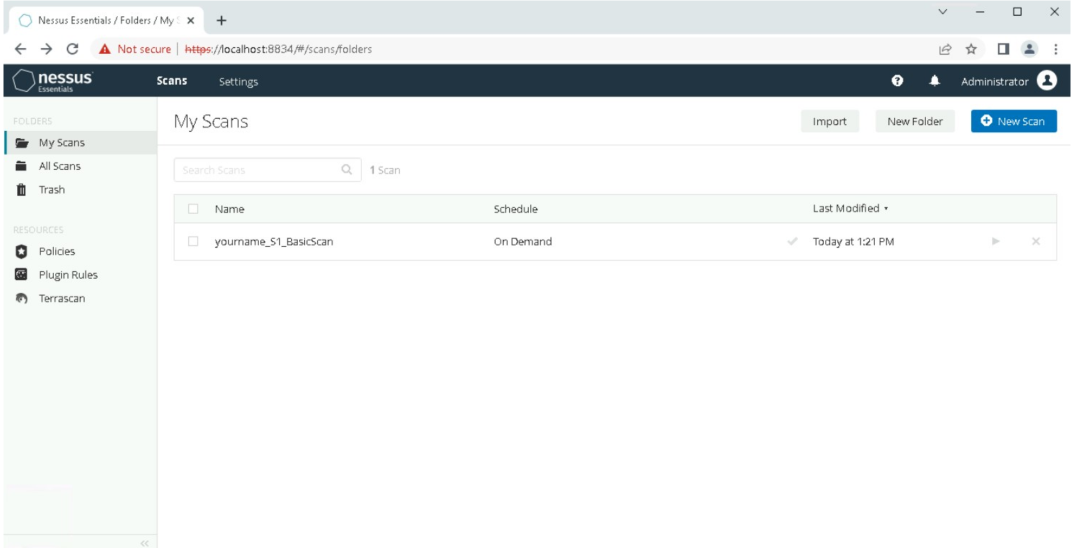
34. In the New Scan / Basic Network Scan form, **type** the following information:

    - Name: ***yourname*_S1_BasicScan**
    - Description: ***Current date and time***
    - Folder: **My Scans**
    - Targets: **172.30.0.11**

    The Targets box defines the IP address for the target of the scan - in this case, the TargetLinux01 machine. It can be directed at one or more machines. It can also be populated by uploading a text file.

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

36. On the My Scans page, **click** the ***yourname*_S1_BasicScan** scan that you just created to open the *yourname*_S1_BasicScan scan page.



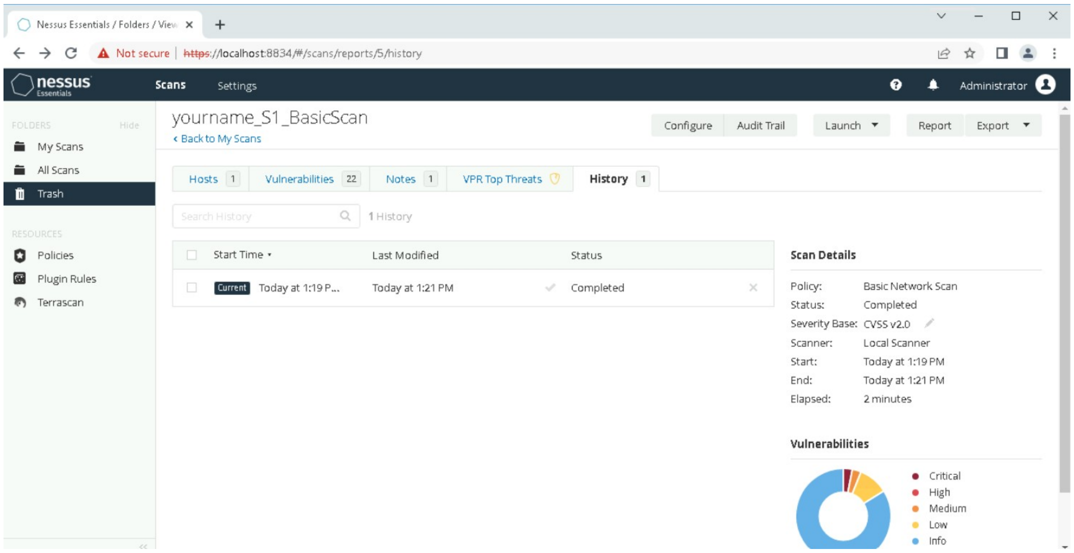
My Scans

Name	Schedule	Last Modified ▾
yourname_S1_BasicScan	On Demand	Today at 1:21 PM

My Scans

37. In the upper-right corner of the *yourname*_S1_BasicScan page, **click** the **Launch button** to start the scan.

    This scan may take 3-5 minutes to complete. When it is finished, the word *Completed* will be displayed in the Status column.



yourname_S1_BasicScan

‹ Back to My Scans

Start Time ▾	Last Modified	Status
Current Today at 1:19 P...	Today at 1:21 PM	Completed

Scan Details

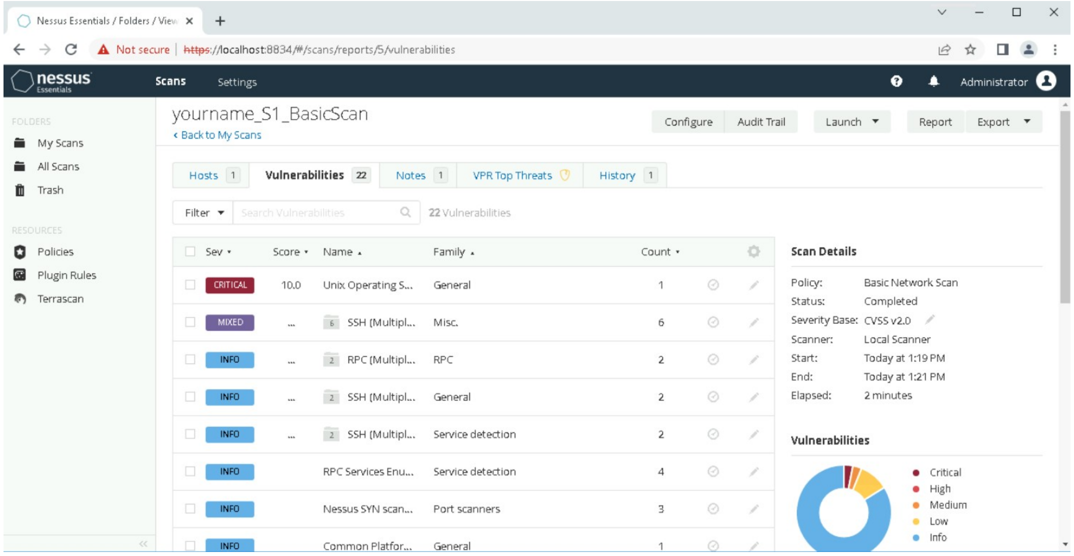
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	Today at 1:19 PM
End:	Today at 1:21 PM
Elapsed:	2 minutes

Vulnerabilities

Completed scan

38. When the scan is finished, **click** the **Vulnerabilities link** at the top of the page to view details about the security vulnerabilities identified by Nessus.

    Clicking on any vulnerability will enable you to drill down to gain additional information about the nature of the issue and possible solutions.



yourname_S1_BasicScan
‹ Back to My Scans

22 Vulnerabilities

□	Sev	Score	Name	Family	Count
□	CRITICAL	10.0	Unix Operating S...	General	1
□	MIXED	...	6 SSH (Multipl...	Misc.	6
□	INFO	...	2 RPC (Multipl...	RPC	2
□	INFO	...	2 SSH (Multipl...	General	2
□	INFO	...	2 SSH (Multipl...	Service detection	2
□	INFO		RPC Services Enu...	Service detection	4
□	INFO		Nessus SYN scan...	Port scanners	3
□	INFO		Common Platfor...	General	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 1:19 PM
End: Today at 1:21 PM
Elapsed: 2 minutes

Vulnerabilities

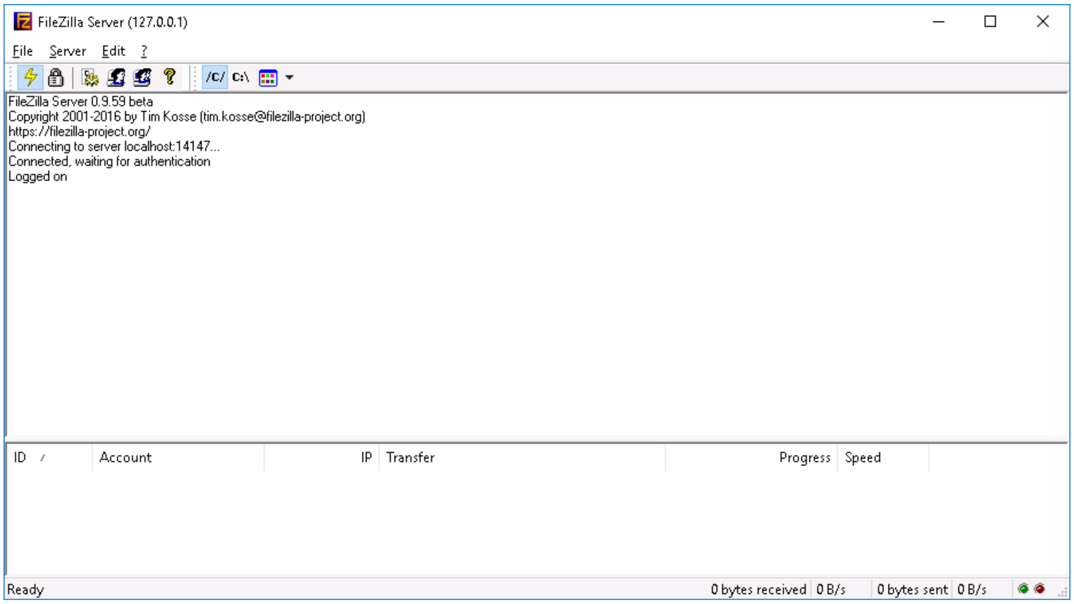
Vulnerability report

39. **Close** the **Nessus window**.

Note: In the next steps, you will explore the FileZilla application.

40. On the TargetWindows02 desktop, **double-click** the **FileZilla Server Interface icon** to open

the FileZilla Server application.

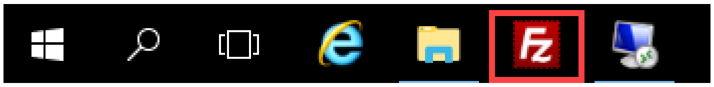


```
FileZilla Server 0.9.59 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
```

FileZilla Server application

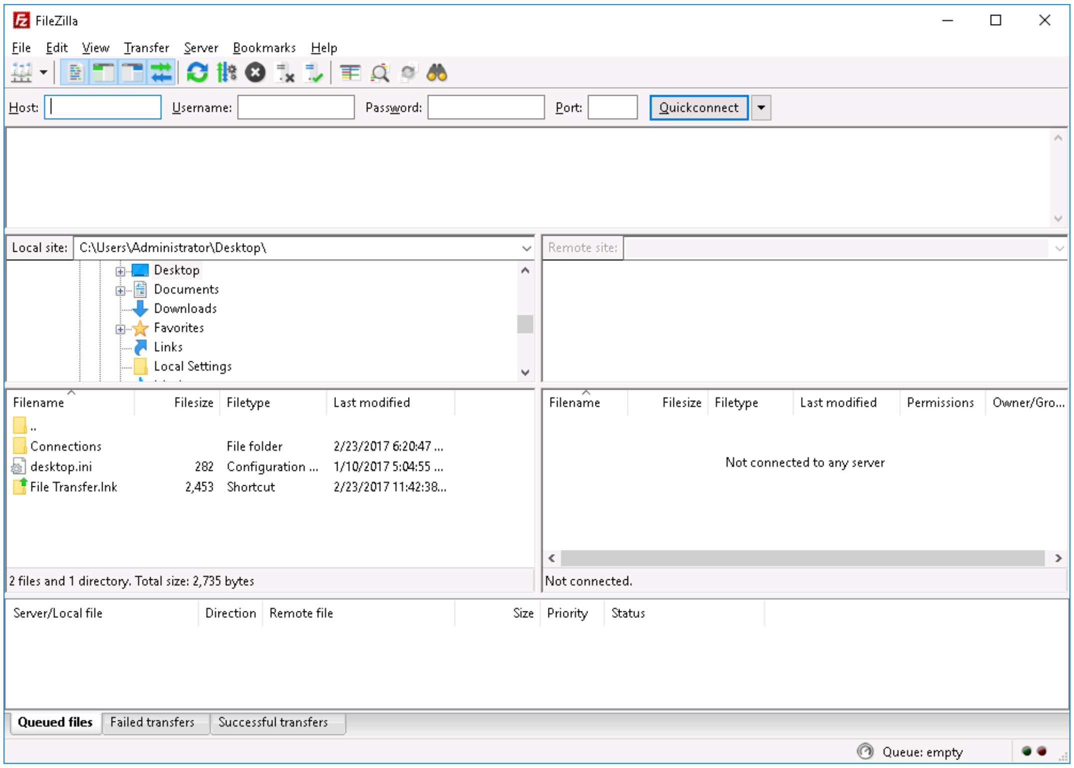
41. **Minimize** the **remote TargetWindows02 connection** to return to the vWorkstation.

42. On the vWorkstation taskbar, **click** the **FileZilla Client icon** to open the FileZilla Client application.



FileZilla Client icon

43. If necessary, **maximize** the **FileZilla window**.


FileZilla
File Edit View Transfer Server Bookmarks Help
Host: Username: Password: Port: Quickconnect
Local site: C:\Users\Administrator\Desktop\
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Remote site:
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers
Queue: empty

Filename	Filesize	Filetype	Last modified
..			
Connections		File folder	2/23/2017 6:20:47 ...
desktop.ini	282	Configuration ...	1/10/2017 5:04:55 ...
File Transfer.lnk	2,453	Shortcut	2/23/2017 11:42:38...

2 files and 1 directory. Total size: 2,735 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...

Not connected to any server

Not connected.

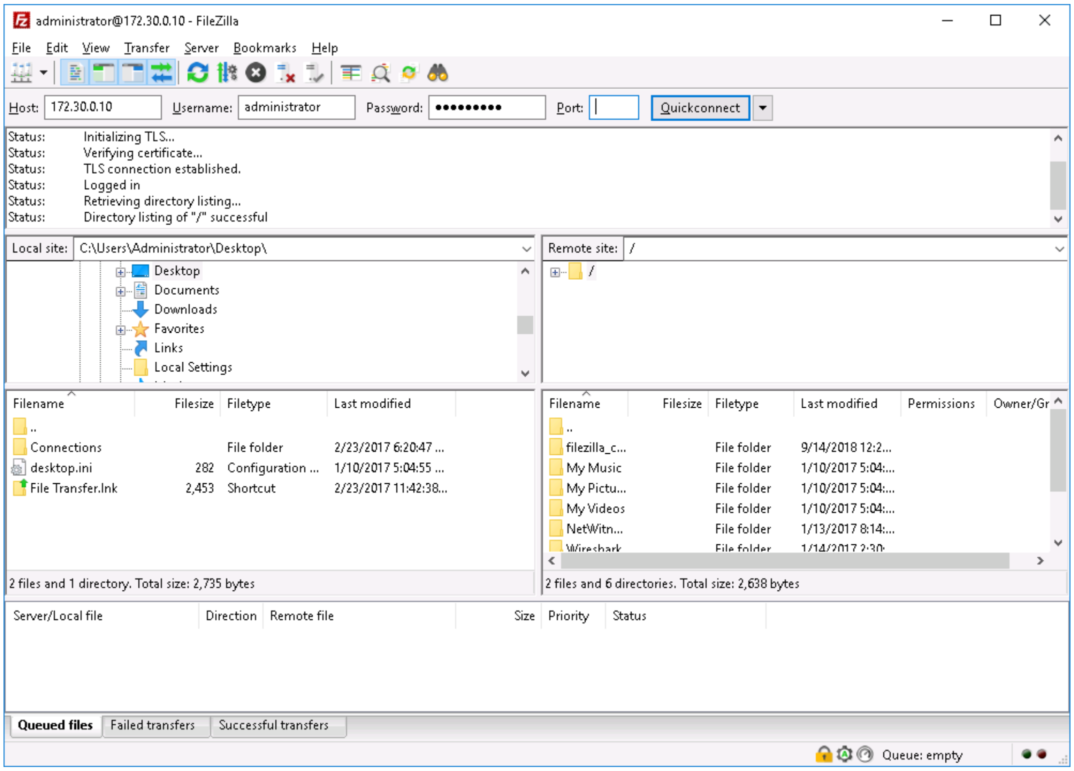
FileZilla Client application

44. In the FileZilla Quickconnect bar, **type** the following details and **click** the **Quickconnect button** to connect to the FileZilla Server application on TargetWindows02.

    When prompted with a security notification, **click** the **OK button** to continue.

    - Host: `172.30.0.10`
    - Username: `administrator`
    - Password: `P@ssw0rd!`
    - Port: `21`

    Use the mouse to drag the horizontal borders to explore the application window.



Host: 172.30.0.10 Username: administrator Password: ●●●●●●●●● Port:

```
Status:     Initializing TLS...
Status:     Verifying certificate...
Status:     TLS connection established.
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Directory listing of "/" successful
```

Local site: C:\Users\Administrator\Desktop\

Filename	Filesize	Filetype	Last modified
..			
Connections		File folder	2/23/2017 6:20:47 ...
desktop.ini	282	Configuration ...	1/10/2017 5:04:55 ...
File Transfer.lnk	2,453	Shortcut	2/23/2017 11:42:38...

2 files and 1 directory. Total size: 2,735 bytes

Remote site: /

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gr
..					
filezilla_c...		File folder	9/14/2018 12:2...		
My Music		File folder	1/10/2017 5:04:...		
My Pictu...		File folder	1/10/2017 5:04:...		
My Videos		File folder	1/10/2017 5:04:...		
NetWitn...		File folder	1/13/2017 8:14:...		
Wireshark		File folder	1/14/2017 2:30:		

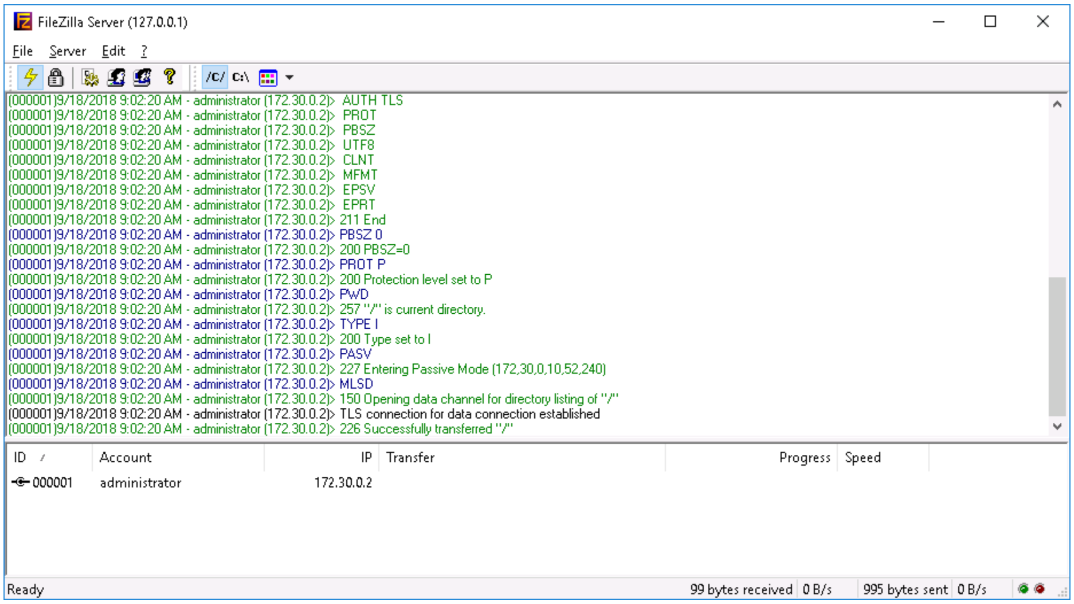
2 files and 6 directories. Total size: 2,638 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status

FileZilla Client connection

45. From the vWorkstation taskbar, **restore** the **remote TargetWindows02 connection** to view the FileZilla Server logs showing the connection activity.

    The information captured in log files can be instrumental during an investigation of a security incident.



```
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  AUTH TLS
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  PROT
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  PBSZ
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  UTF8
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  CLNT
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  MFMT
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  EPSV
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)>  EPRT
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 211 End
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> PBSZ 0
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 200 PBSZ=0
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> PROT P
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 200 Protection level set to P
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> PWD
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 257 "/" is current directory.
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> TYPE I
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 200 Type set to I
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> PASV
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 227 Entering Passive Mode (172,30,0,10,52,240)
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> MLSD
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 150 Opening data channel for directory listing of "/"
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> TLS connection for data connection established
(000001)9/18/2018 9:02:20 AM - administrator (172.30.0.2)> 226 Successfully transferred "/"
```

ID	Account	IP	Transfer	Progress	Speed
000001	administrator	172.30.0.2			

Ready | 99 bytes received | 0 B/s | 995 bytes sent | 0 B/s

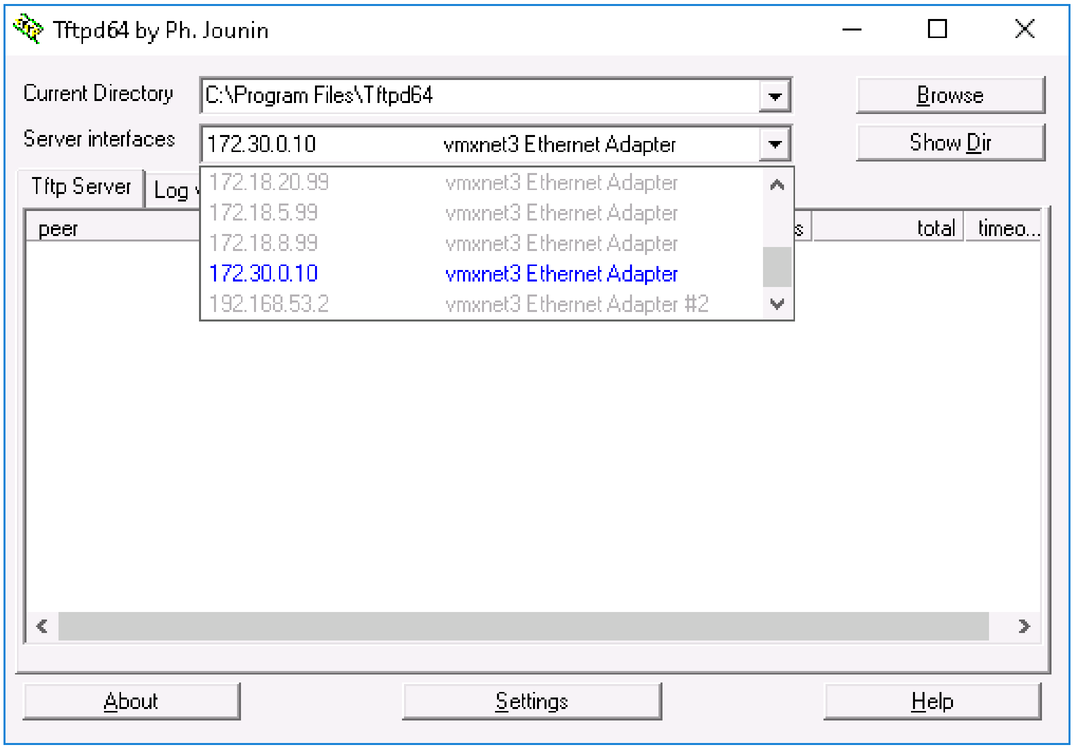
FileZilla Server activity log

46. **Close** the **FileZilla Server window**.

Note: In the next steps, you will explore Tftpd64, another file transfer application. This tool allows files to be shared without the overhead of FTP. The Tftpd64 application uses tFTP (Trivial File Transfer Protocol) to send (put) or receive (get) files between computers, but does not require a username or password to do so. You will not be transferring any files in this section.

47. On the TargetWindows02 desktop, **double-click** the **Tftpd64 icon** to launch the Tftpd64 application.

48. From the Server interfaces drop-down menu, **select 172.30.0.10** (the IP address for TargetWindows02) to establish this machine as the server in a file transfer. To make a connection, you would also need to establish another machine as the client. You will not do that in this section.



Current Directory: C:\Program Files\Tftpd64

Server interfaces: 172.30.0.10 vmxnet3 Ethernet Adapter

```
172.18.20.99    vmxnet3 Ethernet Adapter
172.18.5.99     vmxnet3 Ethernet Adapter
172.18.8.99     vmxnet3 Ethernet Adapter
172.30.0.10     vmxnet3 Ethernet Adapter
192.168.53.2    vmxnet3 Ethernet Adapter #2
```

Select Tftpd64 server

49. **Close** the **Tftpd64 window**.

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

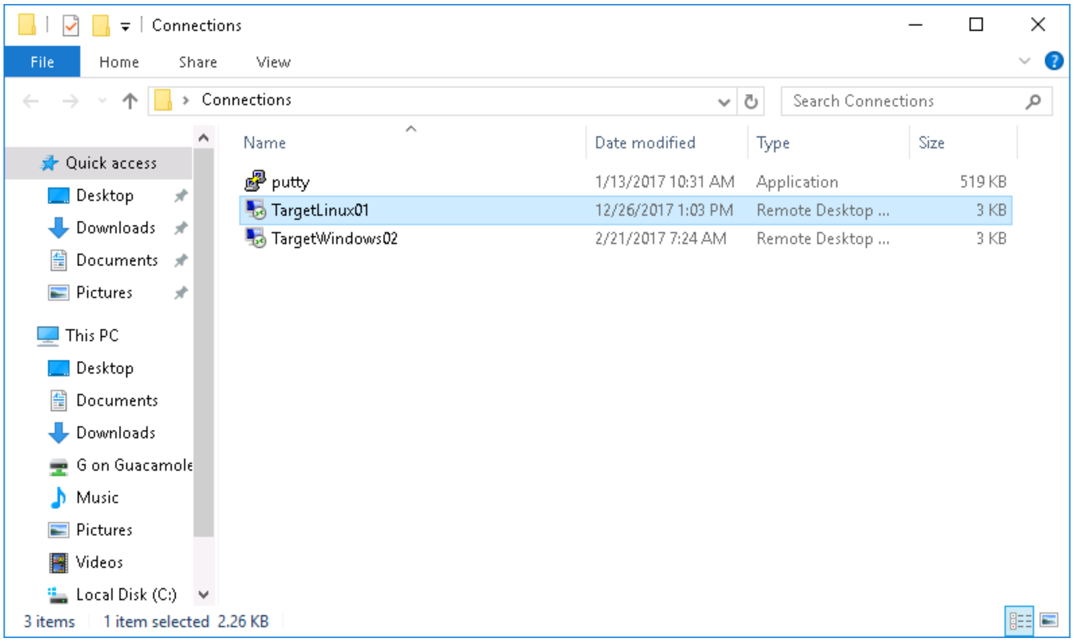
51. **Close** the **FileZilla window**.

Part 2: Connecting to a Linux Machine

Note: Some tools are only available on Linux machines. Unlike Windows machines, most Linux interactions take place from the command line, rather than in an application GUI. The virtual environment in this lab offers two ways to connect to the Linux terminal: a Remote Desktop Connection and PuTTY. In the next steps, you will explore both options.

1. If necessary, **double-click** the **Connections folder** on the vWorkstation desktop.

2. In the Connections folder, **double-click** the **TargetLinux01 shortcut** to open a remote connection to the TargetLinux01 machine.



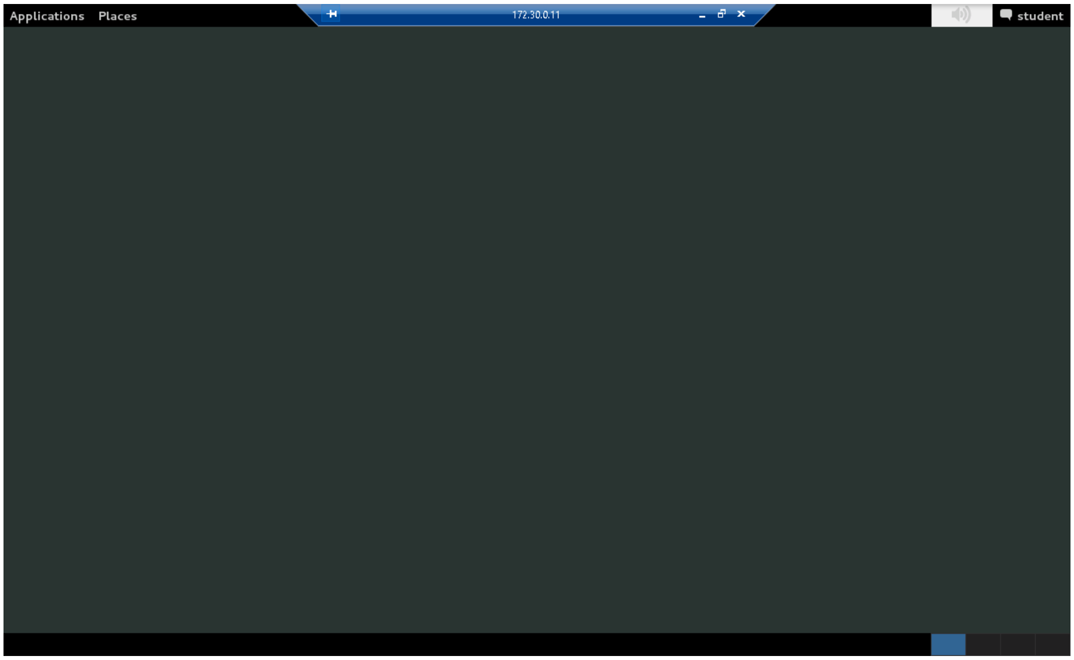
Name	Date modified	Type	Size
putty	1/13/2017 10:31 AM	Application	519 KB
TargetLinux01	12/26/2017 1:03 PM	Remote Desktop ...	3 KB
TargetWindows02	2/21/2017 7:24 AM	Remote Desktop ...	3 KB

TargetLinux01 RDP Shortcut

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

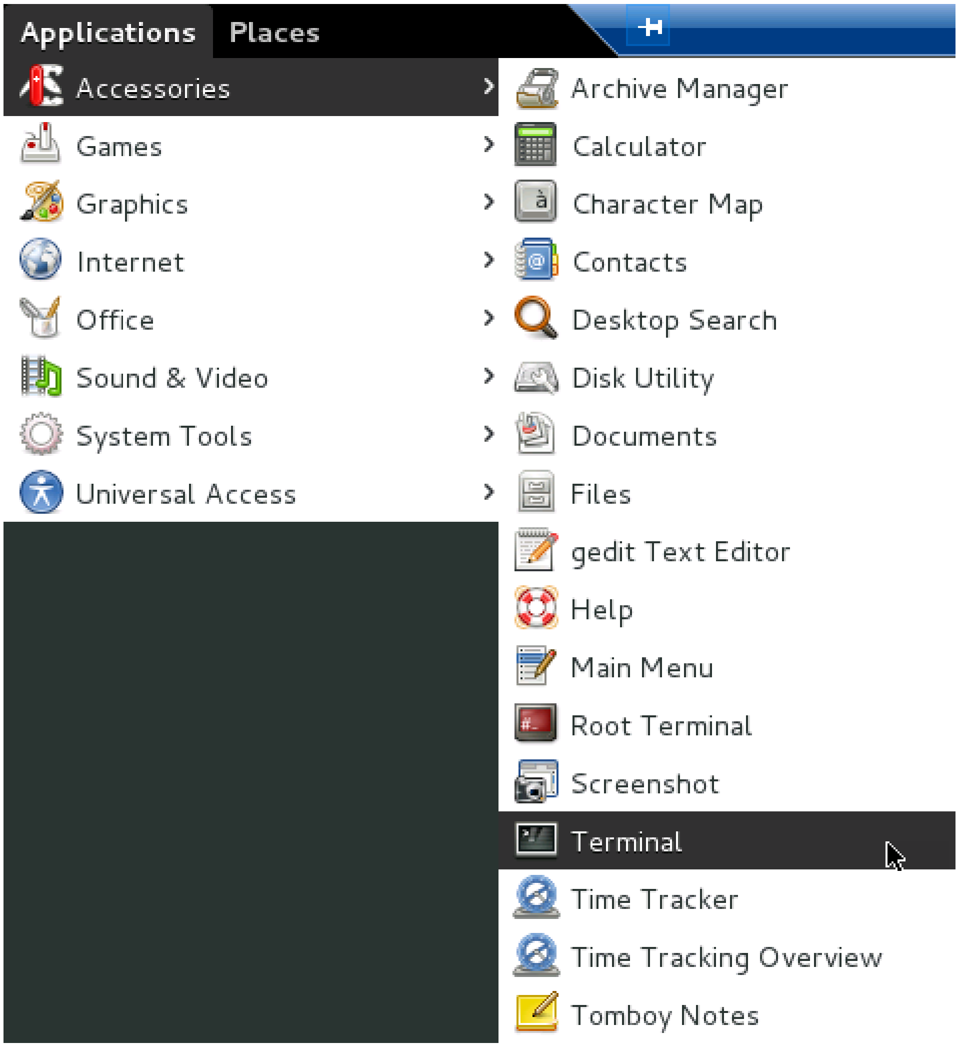
- Username: **`student`**
- Password: **`student`**

The remote desktop opens with the IP address of TargetLinux01 (172.30.0.11) in the title bar at the top of the window.



TargetLinux01 desktop

3. From the TargetLinux01 menu bar, **click Applications** and **select Accessories > Terminal** to open a command prompt window.



Applications Menu

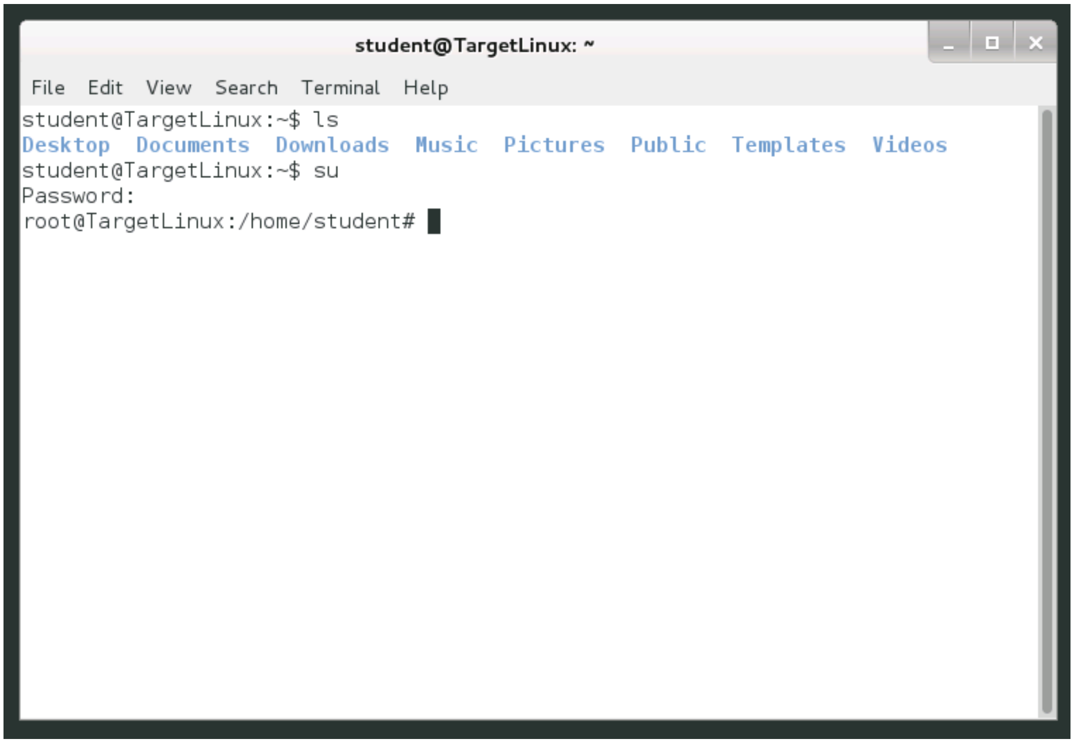
4. At the command prompt, **type** `ls` (list) and **press Enter** to see a list of the directories in the student's home folder.

5. At the command prompt, **type** `su` (switch user / super user) and **press Enter** to switch user accounts to one with elevated privileges.

   Many Linux commands require elevated access and cannot be performed by the student account.

6. When prompted for a password, **type** `toor` and **press Enter**. Please note that your inputs for the password will not appear onscreen; this is normal behavior in a terminal session.

   You are now logged into the TargetLinux01 Debian machine with root-level access. The command prompt has changed to root@TargetLinux:/home/student#.



```
student@TargetLinux:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
student@TargetLinux:~$ su
Password:
root@TargetLinux:/home/student# 
```

Linux command shell

7. At the command prompt, **type** `exit` and **press Enter** to exit root access.

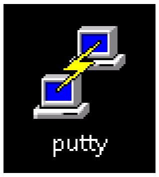
8. At the command prompt, **type** `exit` and **press Enter** to close the terminal window.

9. **Close** the **remote TargetLinux01 connection**.

Note: In the next steps, you will use PuTTY to open a remote connection to the LAN Switch 1 interface.

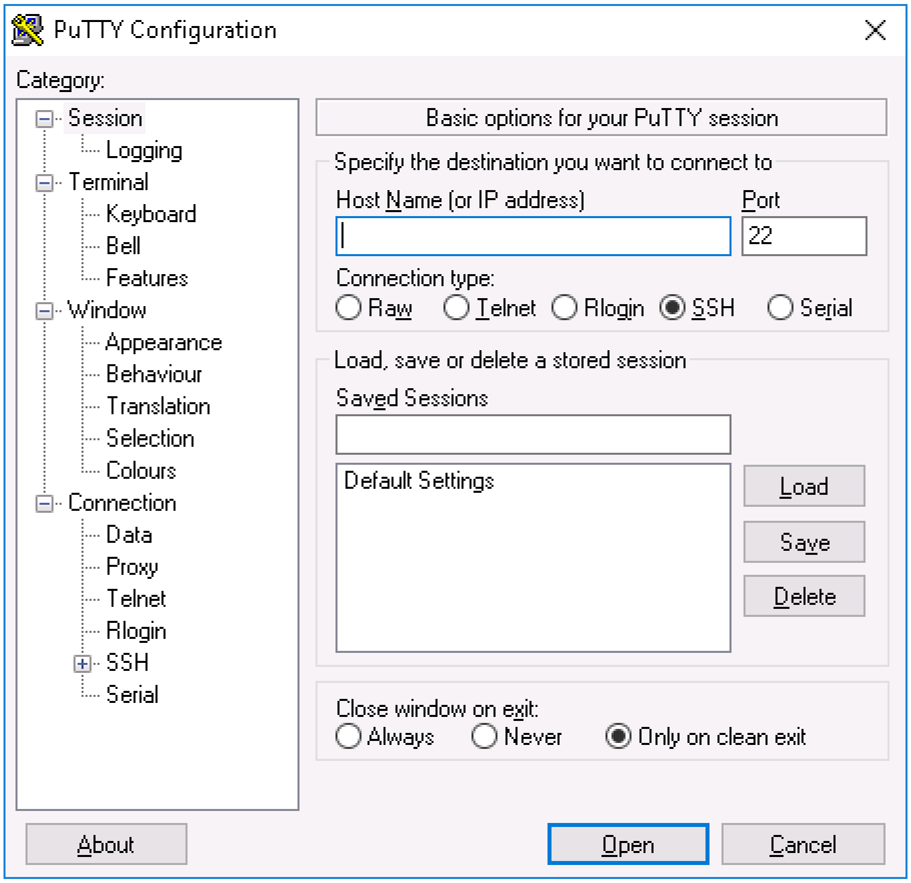
10. **Restore** the **remote TargetWindows02 connection**.

11. On the TargetWindows02 desktop, **double-click** the **putty icon** to open the PuTTY application.



putty icon

PuTTY uses the Secure Shell (SSH) protocol to securely access a remote computer. Once connected, PuTTY displays a terminal shell in which Linux commands can be executed.



Port: 22

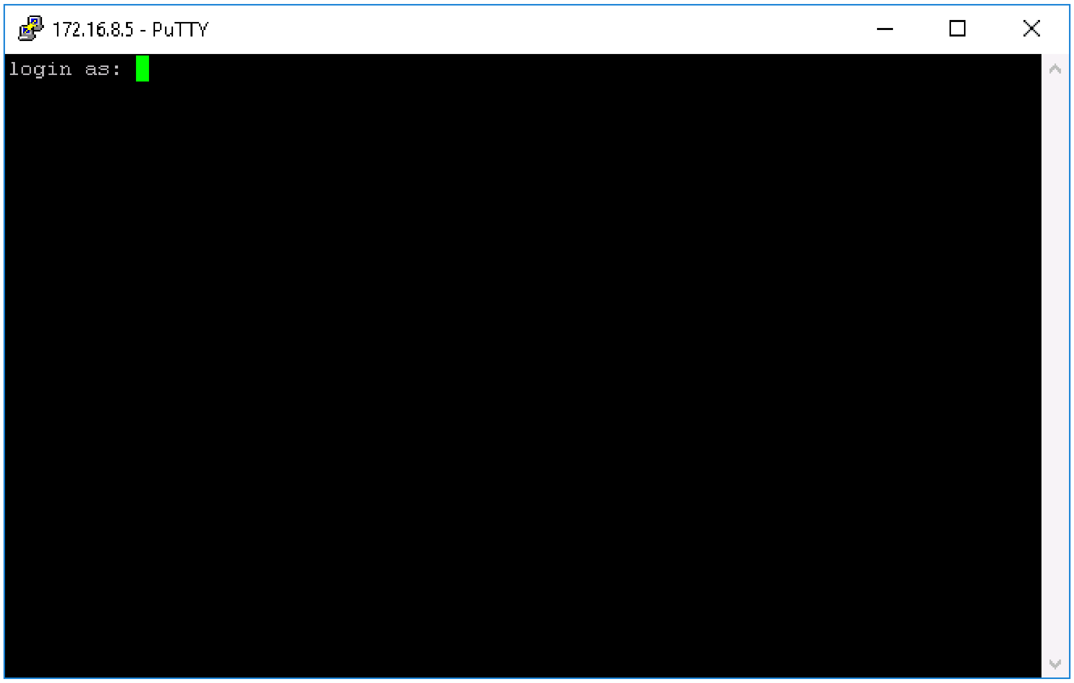
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

PuTTY Configuration window

12. In the Host Name (or IP address) box, **type** **172.16.8.5**, the IP address for LAN Switch 1.

13. **Click Open** to open a PuTTY terminal window and start the connection.



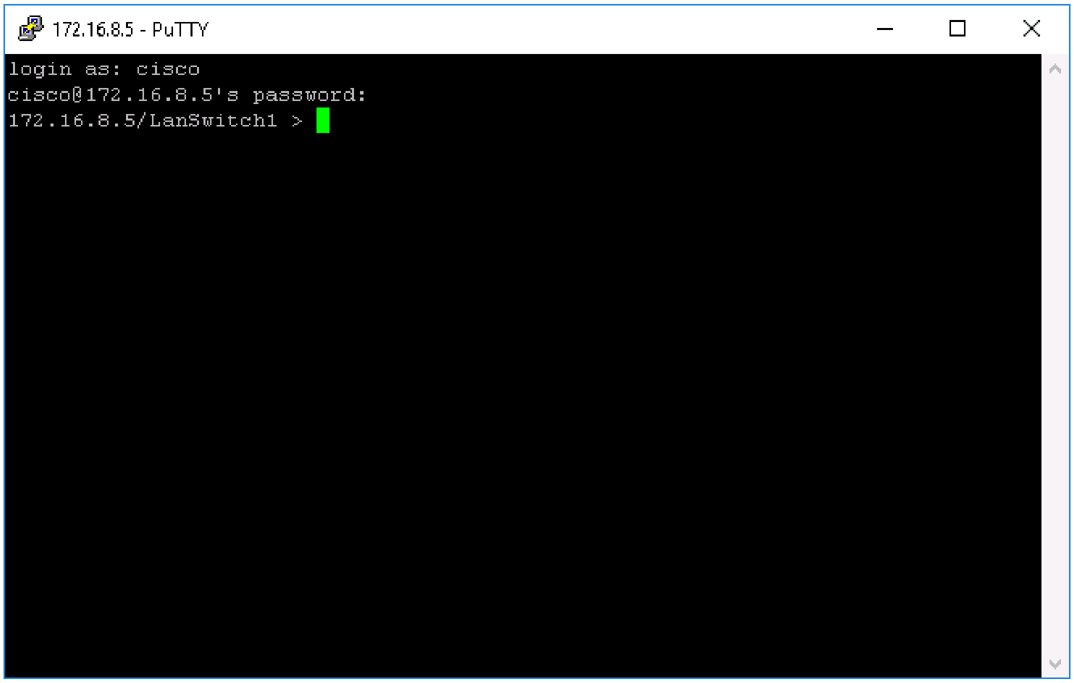
```
login as: 
```

PuTTY Terminal window

14. At the login prompt, **type** the following credentials. **Press Enter** after each entry. For security reasons, the terminal shell will not register your password input on-screen.

    - Login: **`cisco`**
    - Password: **`cisco`**

    Once successfully logged in, the command prompt, 172.16.8.5/LanSwitch1>, is displayed.



```
login as: cisco
cisco@172.16.8.5's password:
172.16.8.5/LanSwitch1 >
```

PuTTY terminal console

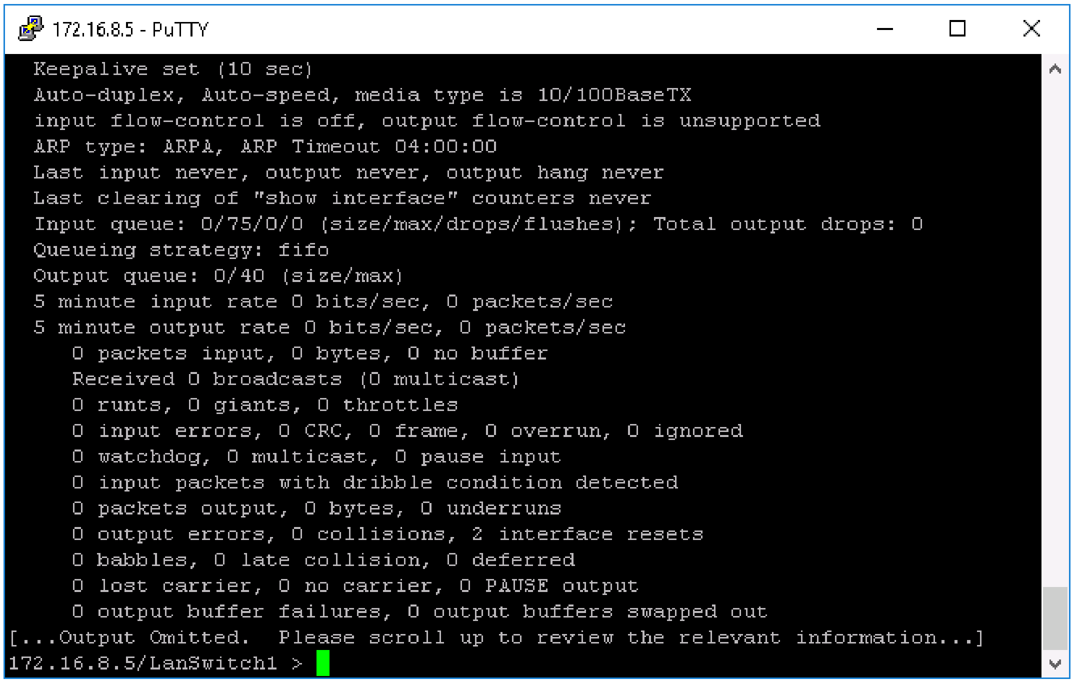
Note: In the next steps, you will use the Cisco IOS (Internetwork Operating System) *show* command to obtain network documentation information from the interface you've connected to (LAN Switch 1). Cisco IOS is a package of routing, switching, and networking commands integrated with a Cisco-specific operating system, of which the *show* command is a key function. Entering a *show* command at the command prompt in the terminal console will return network information specific to the command you entered. There are hundreds of *show* commands in Cisco IOS; availability is based on the *privilege level* of the user. The relevant *show* commands for this lab include those in the following table.

Cisco Commands	Data to Look For and Review
show interface	This command displays physical and logical configuration information about each interface and whether or not the interface is up or down. This command tells you what interfaces are enabled and active. *Look for:* Interface names, number of interfaces, interface up or down (available or unavailable)
show ip interface	This command displays logical IP address and subnet mask address information. It tells you what the IP subnet number, IP host address, and subnet mask address information for all enabled ports.

	Look for: Interface names, interface up or down, IP address, subnet mask address
show ip route	This command displays the IP routing protocol used, the IP routes and network numbers visible to the switch/router, and the physical interface that an IP packet traverses based on the IP routes and IP networks seen (Cisco routers only). *Look for:* IP routing protocol, IP routes and networks
show vlan	This command displays the VLANs configured within the LAN Switch 1 and LAN Switch 2 devices only. *Look for:* VLAN name, VLAN status
show ip arp	This command displays the address resolution table of MAC-layer addresses to assigned IP host addresses. *Look for:* IP address, MAC-layer hardware address, interface name(s)

15. At the command prompt, **type** **`show interface`**, the first Cisco IOS *show* command from the preceding table, and **press Enter**.

    Review the output for this command, being sure to look for the information described in the table. Because this is a LAN switch and not a Router, not all of the commands will be valid for this interface.



```
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
[...Output Omitted.  Please scroll up to review the relevant information...]
172.16.8.5/LanSwitch1 >
```

Output from show interface command

16. In your Lab Report file, **record the results** of the Cisco command.

17. **Repeat steps 15-16** for each of the Cisco commands in the preceding table.

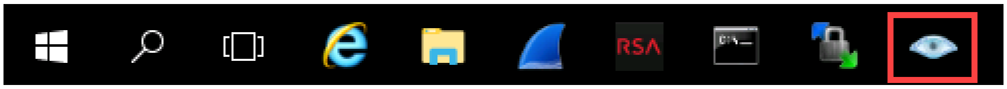
    Because this is a LAN switch and not a Router, not all of the commands will be valid for this interface.

18. At the command prompt, **type** `quit` and **press Enter** to close the PuTTY window.

Part 3: Using Zenmap to Perform Basic Reconnaissance

Note: In the next steps, you will use Zenmap to perform a targeted IP subnetwork Intense Scan, which will identify what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters or firewalls are in use.

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

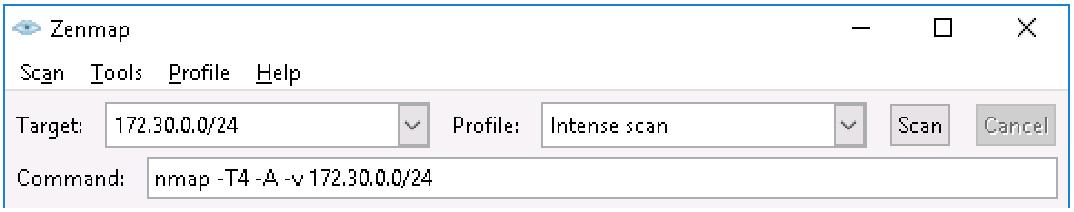


Zenmap icon

2. If necessary, **maximize** the **Zenmap window**.

3. In the Target box, **type `172.30.0.0/24`**, the subnet address for the virtual lab environment.

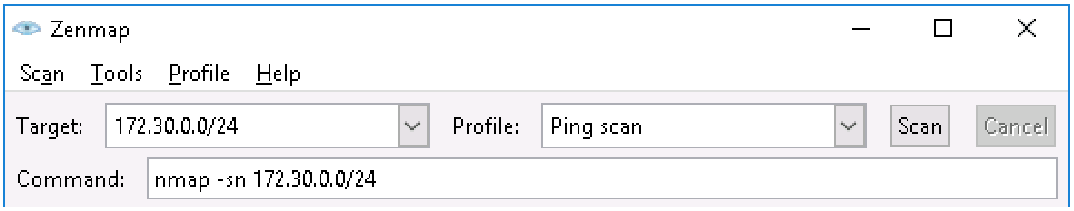
   The Target field allows you to specify or select the networks or subnets you want to connect to.



Target: 172.30.0.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 172.30.0.0/24

Target field

4. From the Profile drop-down menu, **select Ping scan**, then **click Scan** to begin a ping scan of the virtual lab environment.

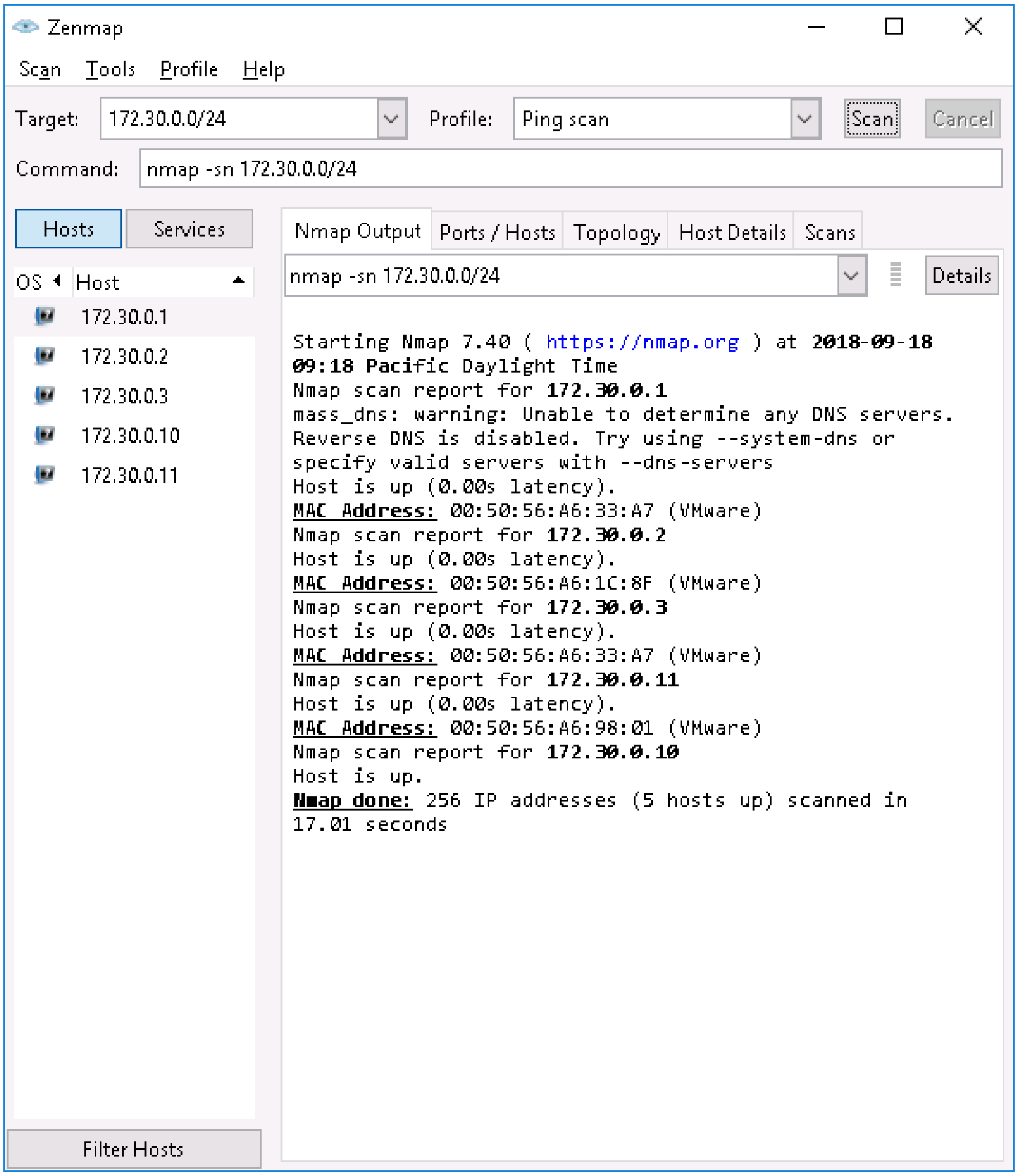


Target: 172.30.0.0/24
Profile: Ping scan
Command: nmap -sn 172.30.0.0/24

Ping scan of 172.30.0.0/24 IP subnet

The Profile field indicates the types of scans you can perform. Notice that the Command box automatically populates the Nmap command as you select the options in these fields. These commands can also be typed manually.

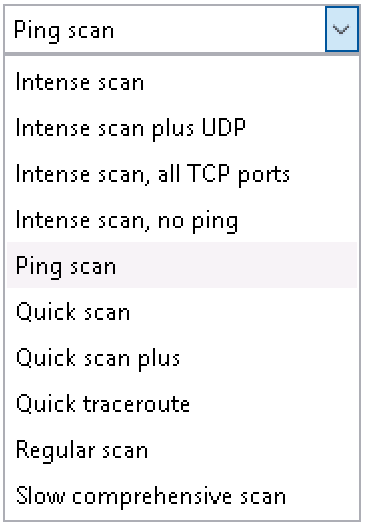
Within a few minutes, the results of the scan will start filling the Nmap Output tab. This scan returns basic information about host availability and MAC addresses. The scan is completed when the final line of the output reads *Nmap done*.



```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-18
09:18 Pacific Daylight Time
Nmap scan report for 172.30.0.1
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:A6:33:A7 (VMware)
Nmap scan report for 172.30.0.2
Host is up (0.00s latency).
MAC Address: 00:50:56:A6:1C:8F (VMware)
Nmap scan report for 172.30.0.3
Host is up (0.00s latency).
MAC Address: 00:50:56:A6:33:A7 (VMware)
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
MAC Address: 00:50:56:A6:98:01 (VMware)
Nmap scan report for 172.30.0.10
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in
17.01 seconds
```

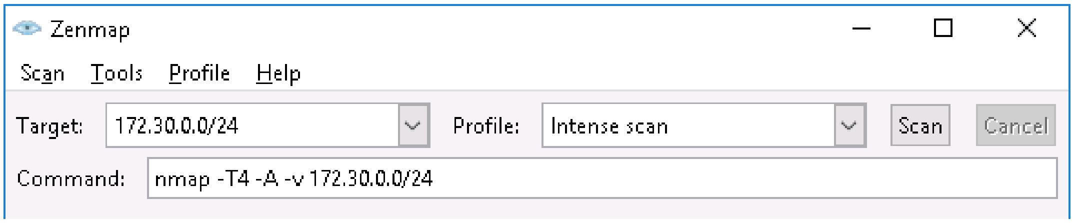
Zenmap Ping scan

5. From the Zenmap toolbar, **click** the **Profile drop-down menu** to see the complete list of scans that Zenmap can perform.



Profile menu

6. From the Profile drop-down menu, **select Intense Scan** and **click Scan** to run a scan that will gather more detailed information.



Target: 172.30.0.0/24

Profile: Intense scan

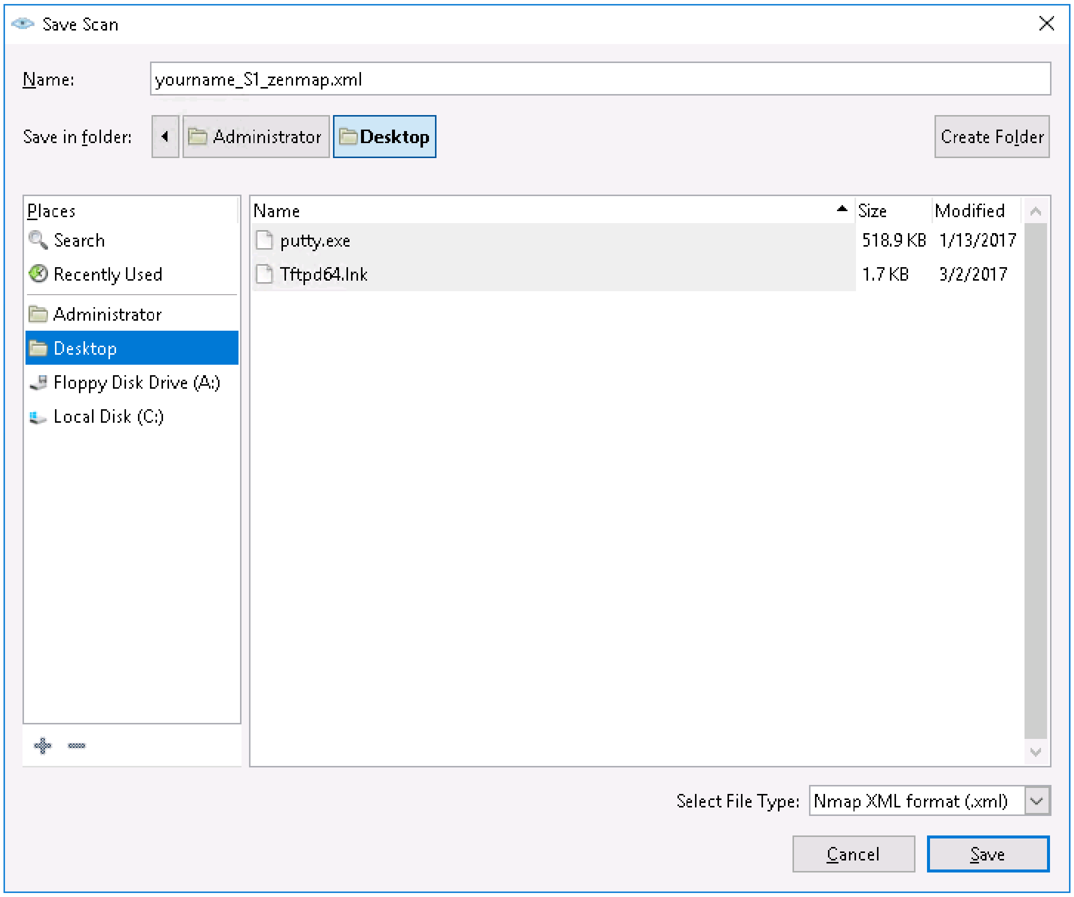
Command: nmap -T4 -A -v 172.30.0.0/24

Intense scan of 172.30.0.0/24 IP subnet

Note: The Intense scan can take 3 to 5 minutes to complete all test scripts. The scan is completed when the final line of the output reads *Nmap done*.

7. From the Zenmap menu bar, **click Scan** and **select Save Scan**, then **select nmap -T4 -A -v 172.30.0.0/24** (the Intense scan) from the drop-down menu and **click Save**.

Save the scan results to TargetWindows02 Desktop as ***yourname*_S1_zenmap.xml**, replacing *yourname* with your own name.



Name: yourname_S1_zenmap.xml

Save in folder: Administrator Desktop

Name	Size	Modified
putty.exe	518.9 KB	1/13/2017
Tftpd64.lnk	1.7 KB	3/2/2017

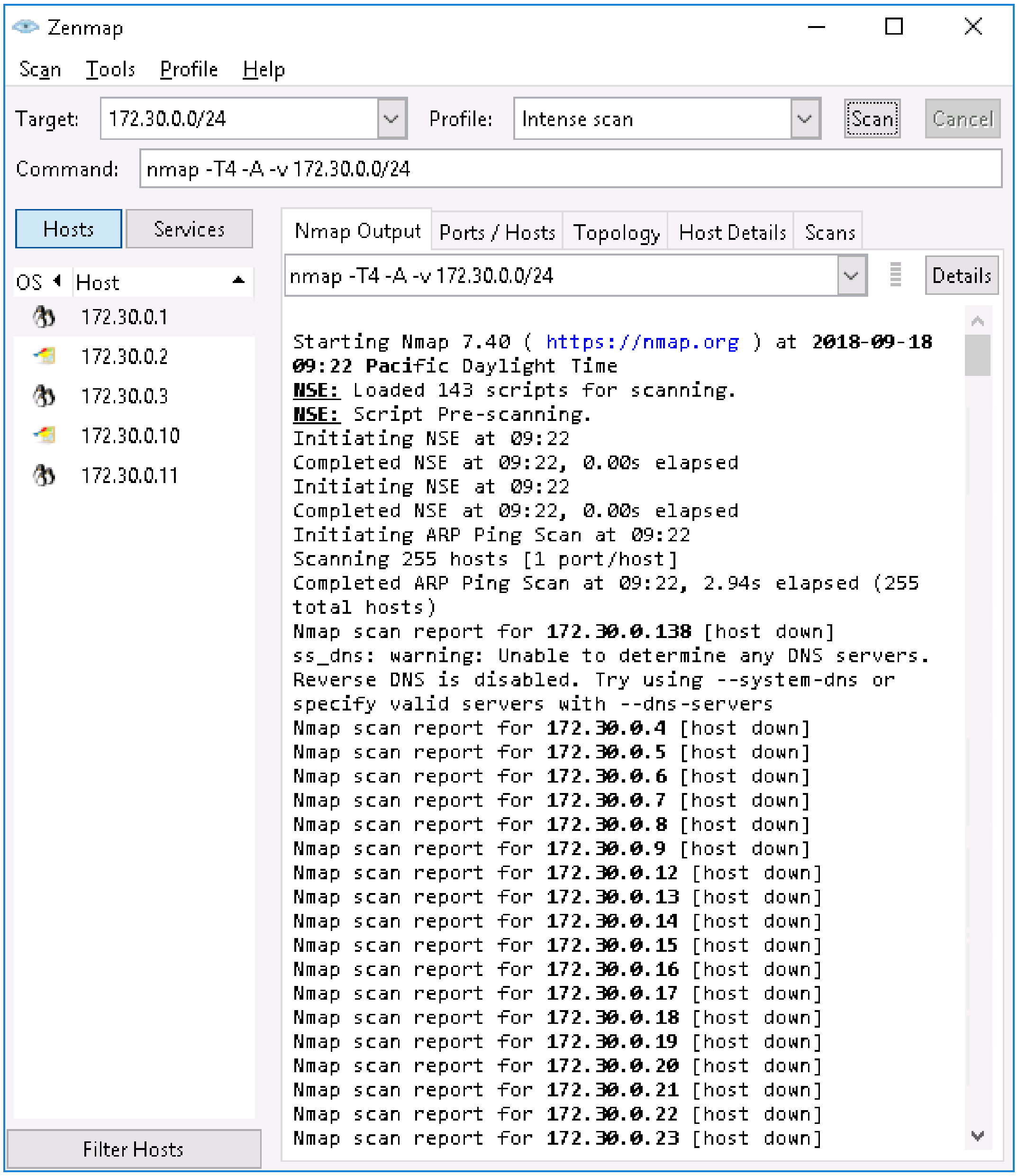
Select File Type: Nmap XML format (.xml)

Save the Zenmap scan

Note: In the next steps, you will review the results (output) of the Zenmap Intense scan in more detail.

8. In the Nmap Output tab, use the scrollbar to **review** the **results of the Intense scan** .

   The Intense scan is actually a collection of several individual tests. The Nmap Output tab shows the raw output, including the name of each scan and its results. For example, the first test in the report, the ARP Ping Scan, scans 255 total hosts on the subnet.



Command: nmap -T4 -A -v 172.30.0.0/24

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-18
09:22 Pacific Daylight Time
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Initiating ARP Ping Scan at 09:22
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 09:22, 2.94s elapsed (255
total hosts)
Nmap scan report for 172.30.0.138 [host down]
ss_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 172.30.0.4 [host down]
Nmap scan report for 172.30.0.5 [host down]
Nmap scan report for 172.30.0.6 [host down]
Nmap scan report for 172.30.0.7 [host down]
Nmap scan report for 172.30.0.8 [host down]
Nmap scan report for 172.30.0.9 [host down]
Nmap scan report for 172.30.0.12 [host down]
Nmap scan report for 172.30.0.13 [host down]
Nmap scan report for 172.30.0.14 [host down]
Nmap scan report for 172.30.0.15 [host down]
Nmap scan report for 172.30.0.16 [host down]
Nmap scan report for 172.30.0.17 [host down]
Nmap scan report for 172.30.0.18 [host down]
Nmap scan report for 172.30.0.19 [host down]
Nmap scan report for 172.30.0.20 [host down]
Nmap scan report for 172.30.0.21 [host down]
Nmap scan report for 172.30.0.22 [host down]
Nmap scan report for 172.30.0.23 [host down]
```

Intense scan

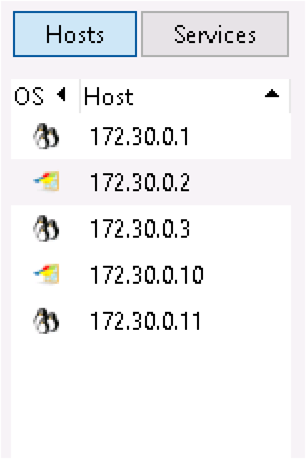
9. In your Lab Report file, **identify each test performed as part of the Intense scan**.

10. In right pane of the Zenmap window, **click each Nmap tab** and **review the data**, being sure to look for the information described in the following table.

Nmap Tab	Information to Look For and Review
Nmap Output	Raw output data
Ports/Hosts	IP hosts and open ports
Topology	Fisheye bubble chart of IP hosts
Host Details	IP host OS fingerprint details
Scans	Completed scans performed

11. In the left pane, **click 172.30.0.2** to select the vWorkstation host, then **click each Nmap tab** and **review the data**. Notice how the information in the Ports/Hosts and Host Details tabs changes.

    The left pane of the Zenmap window lists the hosts or services scanned. It can also identify the operating system for each host.



172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11

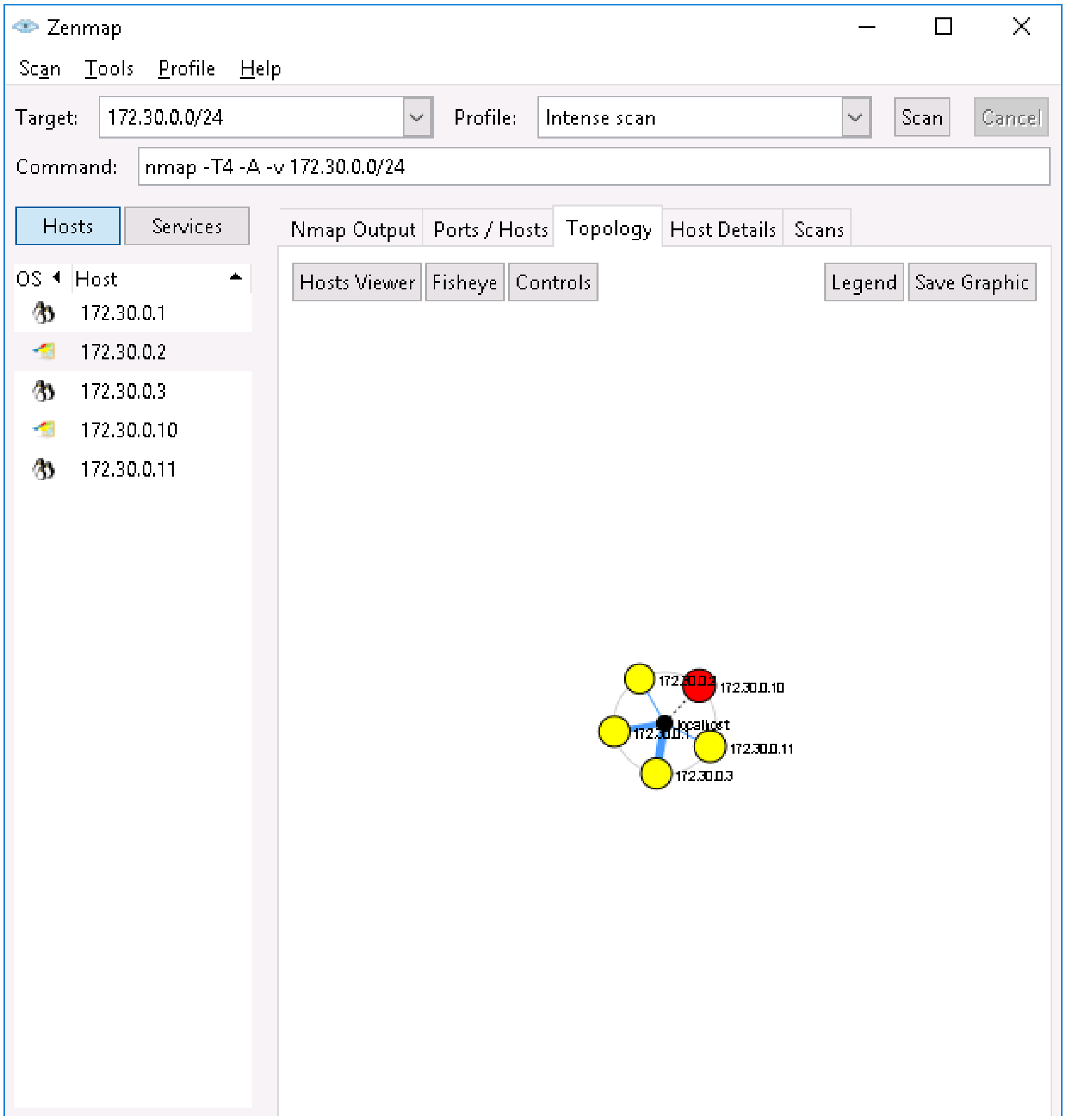
Zenmap Hosts list

12. **Review** the **Ports/Hosts** and **Host Details** tabs for each additional host identified by the scan.

Note: In the next steps, you will create a picture of the scanned network using the tools in the Topology tab. If you have not already done so, maximize the Zenmap window to make this task easier.

13. In the right pane, **click** the **Topology tab**.

    This tab displays a bubble chart of all the IP hosts discovered during the scan. In this report, the bubble chart shows the relative size and connection type of all discovered hosts.

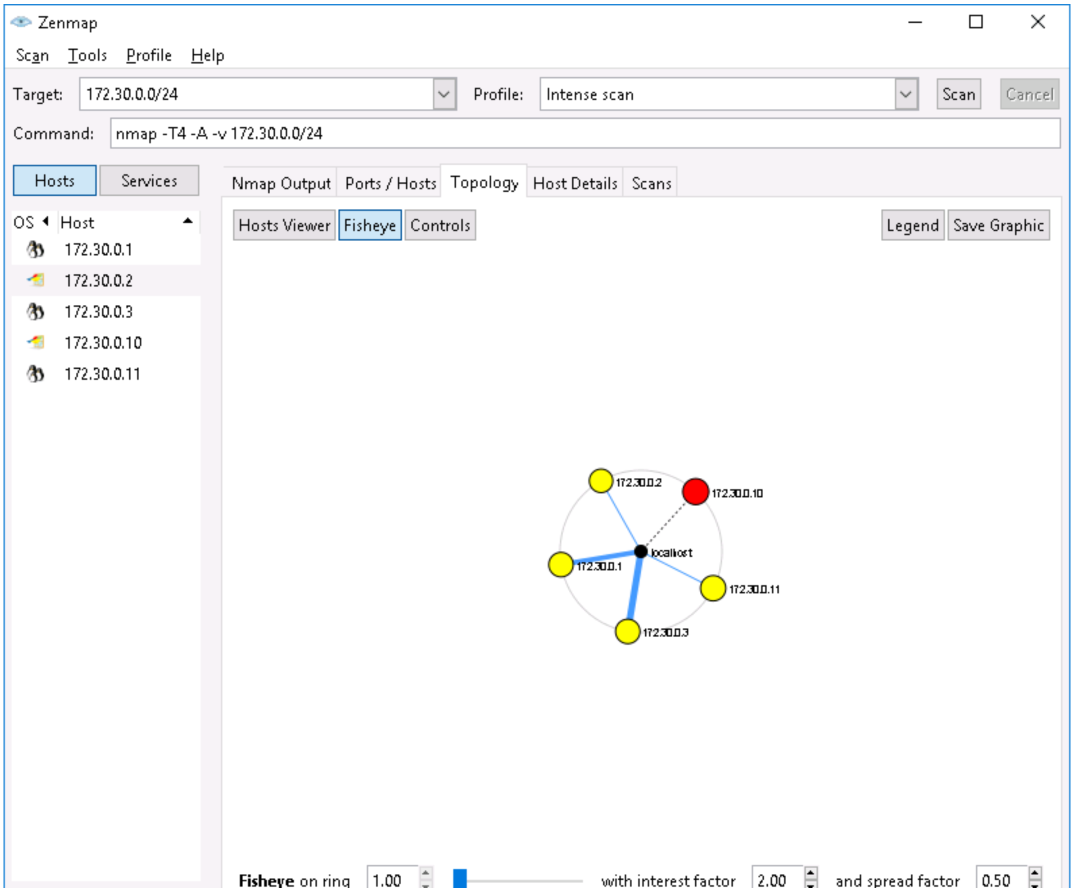


Target: 172.30.0.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 172.30.0.0/24

OS	Host
	172.30.0.1
	172.30.0.2
	172.30.0.3
	172.30.0.10
	172.30.0.11

Topology tab

14. On the Topology tab, **click** the **Fisheye button** to see how the orientation of the chart changes.



Target: 172.30.0.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 172.30.0.0/24

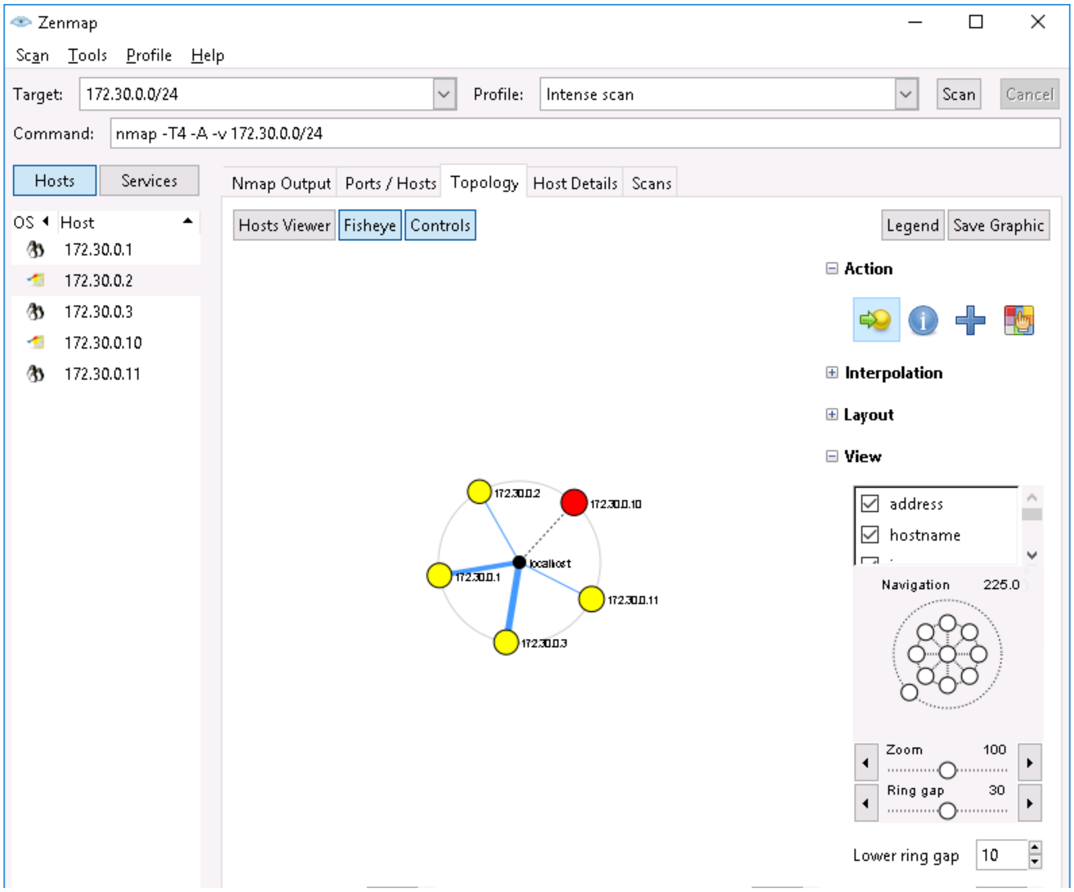
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Fisheye View

Note: A bubble chart is a type of graph used to show relationships, by size, of different variables across an XY axis. A fisheye lens is a tool which can be used to change the shape and orientation of the graph. A fisheye bubble chart combines the two features.

15. On the Topology tab, **click** the **Controls button** to display the chart controls on the right side of the window.



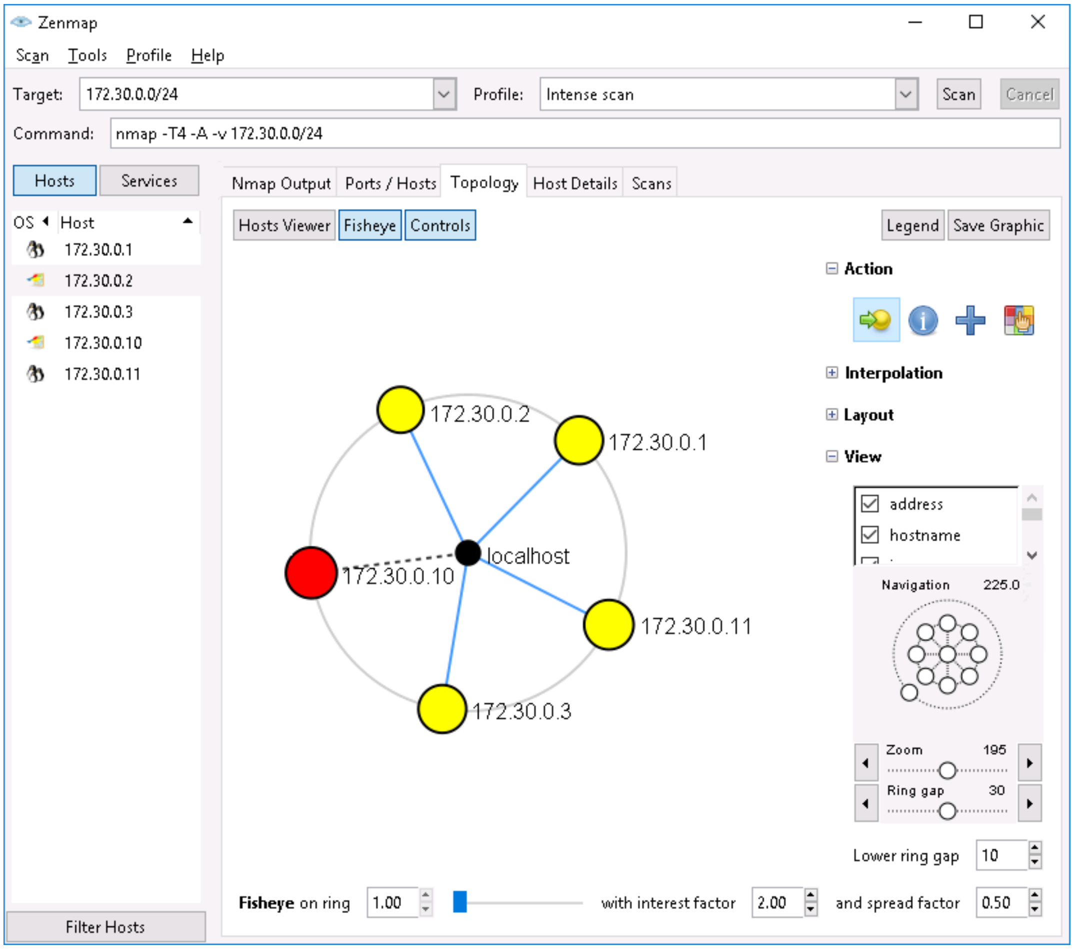
Target: 172.30.0.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 172.30.0.0/24

Topology Chart Controls

16. In the chart controls pane, **drag** the **Zoom** and **Ring Gap sliders** to adjust the size and orientation of the chart until you are satisfied that all of the hostnames and the relationship indicators are clearly readable without any overlapping information.



Target: 172.30.0.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 172.30.0.0/24

172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11

☑ address
☑ hostname

Navigation 225.0

Zoom 195

Ring gap 30

Lower ring gap 10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Resized Fisheye Bubble Chart

17. **Make a screen capture** showing the **fisheye bubble chart** and **paste** it into your Lab Report file.

18. **Close** the **Zenmap window.**

19. When prompted, **click Close anyway** to close Zenmap without saving changes.

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. From the TargetWindows02 desktop, **select any deliverable files** you saved in the course of this lab and **copy** them to the Windows clipboard.

    - ***yourname*_S1_zenmap.xml**

21. **Minimize** the **remote TargetWindows02 connection**.

22. On the vWorkstation desktop, **right-click** any empty area of the desktop and **select Paste** to paste the copied files to the Desktop.

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

23. On the vWorkstation desktop, **drag** the deliverable files into the File Transfer folder to complete the download to your local computer.

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: Exploring the Tools used in the Virtual Lab Environment

Note: In the next steps, you will explore several of the applications and tools available in the virtual lab environment to help familiarize you with their intended purpose.

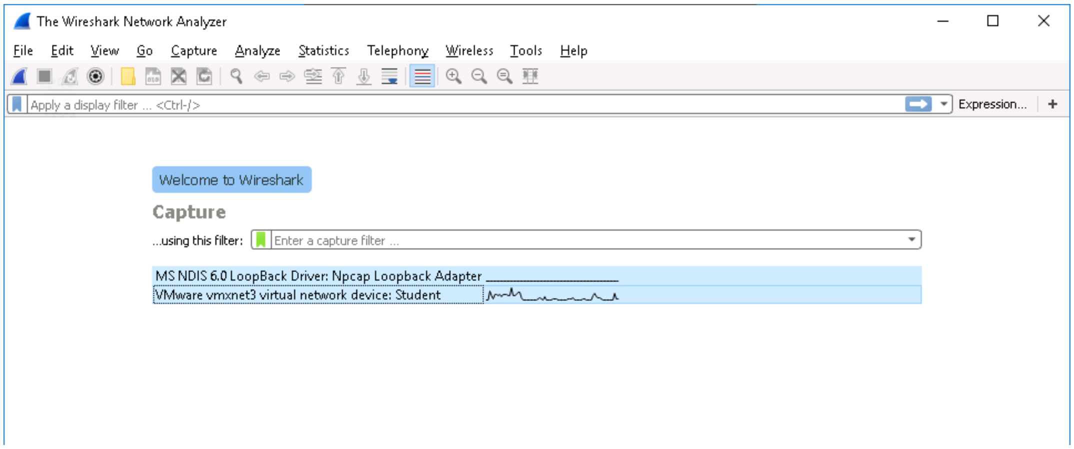
1. **Open a remote connection** to the **TargetWindows02** machine.

2. **Open** the **Wireshark application**.

   Wireshark is a protocol analyzer tool (sometimes called a “packet sniffer”). It is used to capture IP traffic from a variety of sources. The main screen of Wireshark includes details about the current capture configuration. From this screen, analysts can select individual interfaces and enter custom filter commands to quickly sort the captured data.

3. From the main screen, **select** the **Student** and **Npcap Loopback Adapter capture interfaces**.

   The student interface is the network interface for the lab environment that you are working in. Selecting this interface ensures that Wireshark can analyze traffic from areas of the network that are visible to students.



MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter
VMware vmxnet3 virtual network device: Student

Verify interface selection

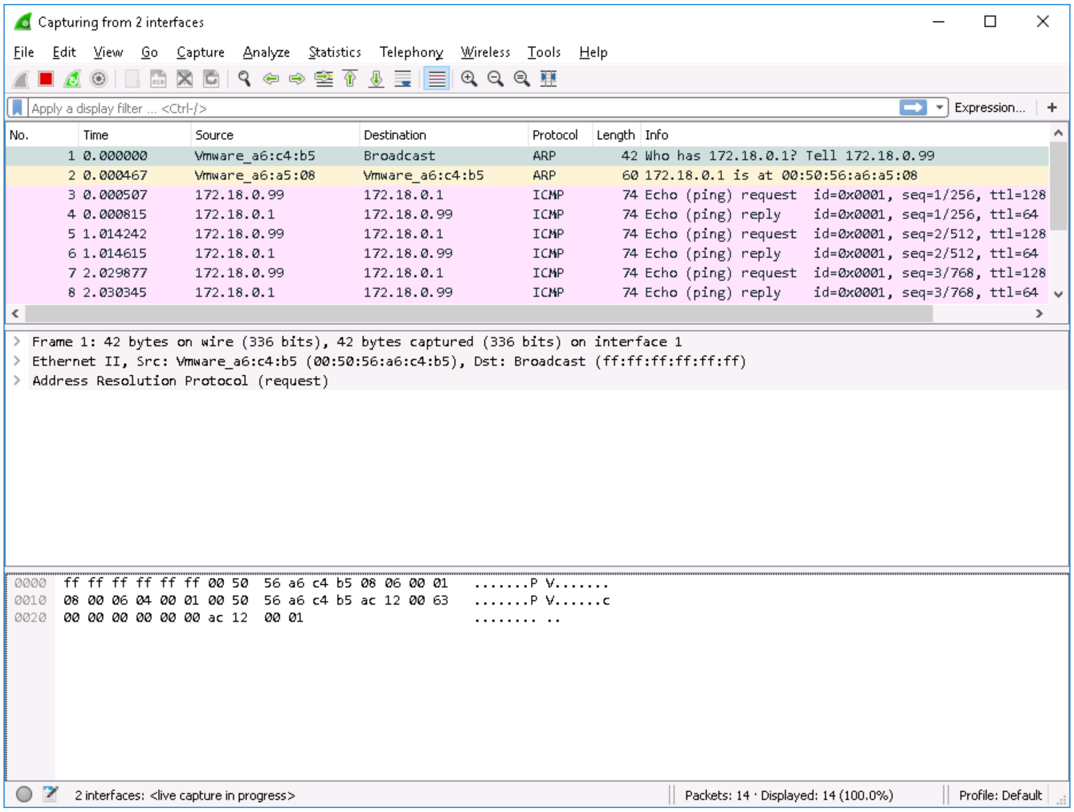
4. **Apply a filter** to exclude RDP traffic generated between the vWorkstation and TargetWindows02 systems, then **start** the packet capture.

Note: In the next steps, you will generate traffic for Wireshark to capture.

5. **Open** a **Command Prompt window** and **ping** the Indy Router at **172.18.0.1**.

6. When the prompt reappears, **close** the **command window** and review the data captured by Wireshark.

   Because Wireshark is capturing live data, your screen will not match the following figure; however, you will still see that Wireshark has captured the Ping traffic as packets using the ICMP protocol (Internet Control Message Protocol).


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_a6:c4:b5	Broadcast	ARP	42	Who has 172.18.0.1? Tell 172.18.0.99
2	0.000467	Vmware_a6:a5:08	Vmware_a6:c4:b5	ARP	60	172.18.0.1 is at 00:50:56:a6:a5:08
3	0.000507	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128
4	0.000815	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64
5	1.014242	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128
6	1.014615	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64
7	2.029877	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128
8	2.030345	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 1
> Ethernet II, Src: Vmware_a6:c4:b5 (00:50:56:a6:c4:b5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 50  56 a6 c4 b5 08 06 00 01   .......P V.......
0010  08 00 06 04 00 01 00 50  56 a6 c4 b5 ac 12 00 63   .......P V......c
0020  00 00 00 00 00 00 ac 12  00 01                     ........ ..
```

2 interfaces: <live capture in progress> Packets: 14 · Displayed: 14 (100.0%) Profile: Default

Wireshark window

Exploring Wireshark

The Wireshark window opens with the detailed information about the packets captured in three panes. Use your mouse to drag the borders of any pane up or down to change its size.

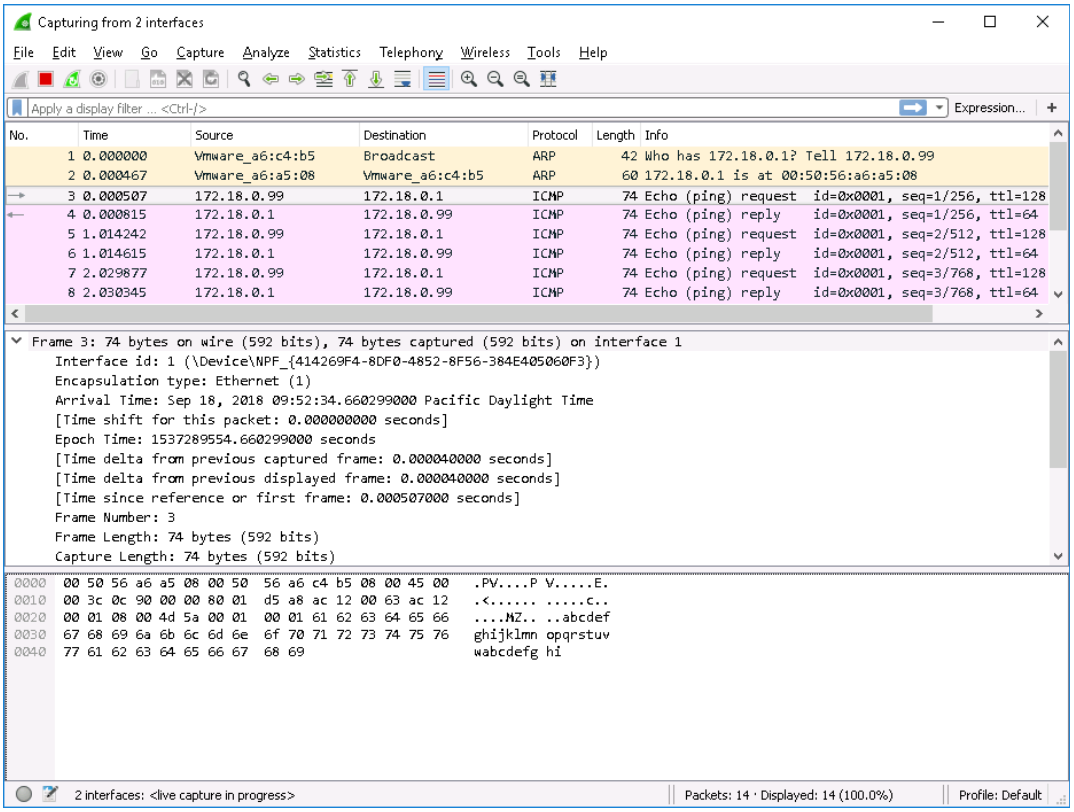
- The top pane of the Wireshark window contains all of the packets that Wireshark has captured, sorted by timestamp, and provides a summary of the contents of the packet in a format close to English. Keep in mind that the content will be different depending on where you capture packets in the network. Also remember that the "source" and "destination" are relative to where a packet is captured. This area of the Wireshark window is referred to as the *frame summary*.

- The middle pane of the Wireshark window is used to display the packet structure and contents of fields within the packet. This area of the Wireshark window is referred to as the *frame detail*.

- The bottom pane of the Wireshark window displays the hex. All of the information in the packet is displayed in hexadecimal on the left and in decimal, in characters when possible, on the right. This can be a useful feature, especially if the passwords you are looking for are unencrypted. This area of the Wireshark window is referred to as the *hex pane*.

7. In the frame summary pane, **select** the **first ICMP frame** and **expand** the **frame detail**.

   In the frame detail, Wireshark displays information about the time the data was captured.


Capturing from 2 interfaces
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Expression...
+
2 interfaces: <live capture in progress>
Packets: 14 · Displayed: 14 (100.0%)
Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_a6:c4:b5	Broadcast	ARP	42	Who has 172.18.0.1? Tell 172.18.0.99
2	0.000467	Vmware_a6:a5:08	Vmware_a6:c4:b5	ARP	60	172.18.0.1 is at 00:50:56:a6:a5:08
3	0.000507	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128
4	0.000815	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64
5	1.014242	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128
6	1.014615	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64
7	2.029877	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128
8	2.030345	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64

```
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1
    Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2018 09:52:34.660299000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1537289554.660299000 seconds
    [Time delta from previous captured frame: 0.000040000 seconds]
    [Time delta from previous displayed frame: 0.000040000 seconds]
    [Time since reference or first frame: 0.000507000 seconds]
    Frame Number: 3
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
```

```
0000  00 50 56 a6 a5 08 00 50  56 a6 c4 b5 08 00 45 00   .PV....P V.....E.
0010  00 3c 0c 90 00 00 80 01  d5 a8 ac 12 00 63 ac 12   .<...... .....c..
0020  00 01 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ....MZ.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Frame detail for ICMP traffic

8. **Make a screen capture** showing the **Arrival Time** for the ICMP traffic that you captured and **paste** it into your Lab Report file.

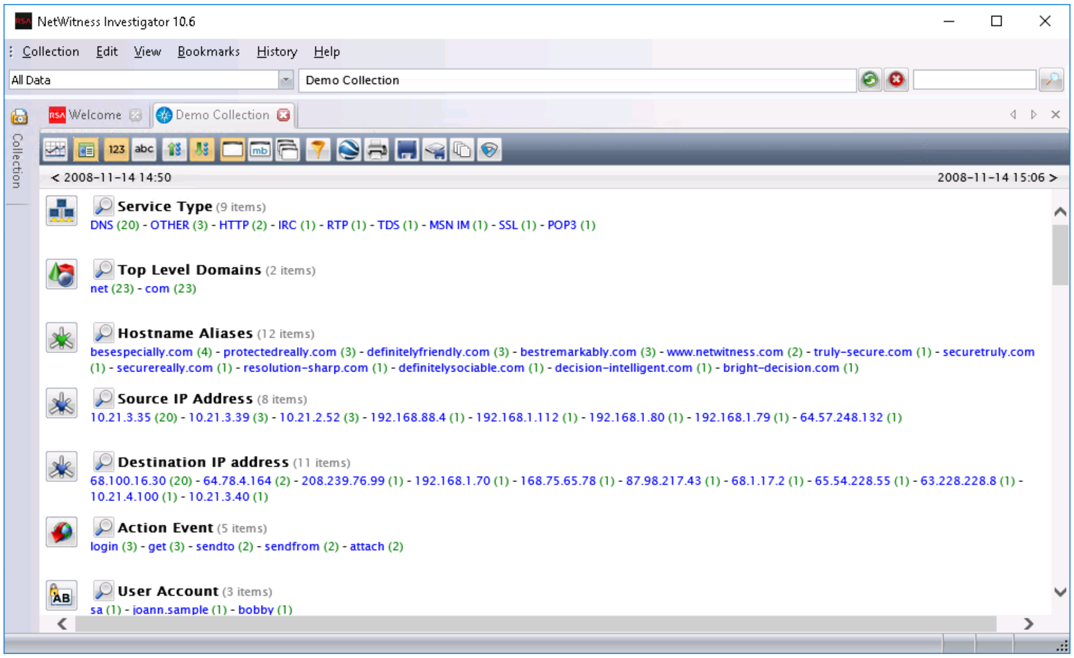
9. **Stop** the **packet capture**, then **save** the Wireshark capture to the TargetWindows02 desktop as ***yourname*****_S2_wireshark_capture.pcap**, replacing *yourname* with your own name, and **close Wireshark**.

Note: In the next steps, you will explore the RSA NetWitness Investigator application. NetWitness Investigator provides a high-level overview of all the traffic in a packet capture file. While Wireshark looks at every packet, NetWitness categorizes and organizes traffic so that anomalous patterns become more apparent.

10. **Open** the **NetWitness Investigator application**.

11. **Open** the **Demo Collection** and review the NetWitness Investigator report.

    Notice that NetWitness Investigator has specified the source and destination IP addresses in this collection, identified the user accounts found in the collection, and even recognized attachments.



< 2008-11-14 14:50 2008-11-14 15:06 >

Service Type (9 items)
DNS (20) - OTHER (3) - HTTP (2) - IRC (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POP3 (1)

Top Level Domains (2 items)
net (23) - com (23)

Hostname Aliases (12 items)
besespecially.com (4) - protectedreally.com (3) - definitelyfriendly.com (3) - bestremarkably.com (3) - www.netwitness.com (2) - truly-secure.com (1) - securetruly.com (1) - securereally.com (1) - resolution-sharp.com (1) - definitelysociable.com (1) - decision-intelligent.com (1) - bright-decision.com (1)

Source IP Address (8 items)
10.21.3.35 (20) - 10.21.3.39 (3) - 10.21.2.52 (3) - 192.168.88.4 (1) - 192.168.1.112 (1) - 192.168.1.80 (1) - 192.168.1.79 (1) - 64.57.248.132 (1)

Destination IP address (11 items)
68.100.16.30 (20) - 64.78.4.164 (2) - 208.239.76.99 (1) - 192.168.1.70 (1) - 168.75.65.78 (1) - 87.98.217.43 (1) - 68.1.17.2 (1) - 65.54.228.55 (1) - 63.228.228.8 (1) - 10.21.4.100 (1) - 10.21.3.40 (1)

Action Event (5 items)
login (3) - get (3) - sendto (2) - sendfrom (2) - attach (2)

User Account (3 items)
sa (1) - joann.sample (1) - bobby (1)

Demo Collection viewed in NetWitness Investigator

12. In the User Account category, **click** the **Joann.sample link** to learn more about that account's activity.

13. In the Attachment category, **click** the **(1) link** following the creditcards.txt link to view information specific to the file.

    Ensure you are clicking the **(1)** link, not the creditcard.txt link.

14. **Make a screen capture** showing the **creditcards.txt file details** and **paste** it into your Lab Report file.

15. **Close** the **NetWitness Investigator window**.

Note: In the next steps, you will explore the Nessus Web Client. Nessus performs remote scans and audits of Unix, Windows, and network infrastructures and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices.

16. **Open** the **Nessus Web Client**.

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

    This warning occurs when a website has either an expired certificate, mismatched certificate, or a self-signing certificate.

18. When prompted, **enter** the following credentials and **click Sign In** to open Nessus.

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

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

19. **Create** a new **Basic Network Scan** using the details provided below and **save** the new scan.

    - Name: ***yourname*_S2_BasicScan**
    - Description: ***Current date and time***

    - Folder: **My Scans**
    - Targets: **`172.30.0.11`**

    The Targets box defines the IP address for the target of the scan. It can be directed to one or more machines. It can also be populated by uploading a text file.

20. **Launch** the ***yourname*_S2_BasicScan** scan.

    This scan may take 3-5 minutes to complete. When it is finished, the word *Completed* will be displayed in the Status column.

21. When the scan is completed, **review** the **security vulnerabilities** identified by Nessus.

    Clicking on any vulnerability will enable you to drill down to gain additional information about the nature of the issue and possible solutions.

22. **Click** the **Unix Operating System Unsupported Version Detection vulnerability** to display additional details about this vulnerability.

23. **Make a screen capture** showing the **vulnerability detail screen** and **paste** it into the Lab Report file.

24. Under the Output section of the vulnerability detail page, **click** the **172.30.0.11 link** to return to the Vulnerabilities list, filtered to show only vulnerabilities related to the TargetLinux01 host.

    In this case, your scan only included one target, so the filtered list of vulnerabilities will be the same as the first vulnerabilities list. However, for scans that include multiple targets, you can use the filtered vulnerabilities list to review vulnerabilities by host.

25. **Export** the scan report as an HTML file and **save** the file to the TargetWindows02 desktop as ***yourname*_S2_BasicScan**, replacing *yourname* with your own name.

26. **Close** the **Nessus window**.

Note: In the next steps, you will explore the FileZilla application.

27. **Open** the **FileZilla Server application**.

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

29. **Open** the **FileZilla Client application**.

30. Use the following details to **connect** to the **TargetWindows02** machine.

    - Host: **`172.30.0.10`**
    - Username: **`Administrator`**
    - Password: **`P@ssw0rd!`**

- Port: **21**

31. **Close** the **FileZilla Client window** and **restore** the **remote TargetWindows02 connection** to view the connection activity in the FileZilla server logs.

32. **Close** the **FileZilla Server window**.

Note: In the next steps, you will explore Tftpd64, another file transfer application. This tool allows files to be shared without the overhead of FTP. Tftpd64 uses TFTP (Trivial File Transfer Protocol) to send (put) or receive (get) files between computers.

33. **Open** the **Tftpd64 application**.

34. **Change** the **Current Directory** to the TargetWindows02 Administrator desktop, then **select 172.30.0.10** from the Server interfaces menu.
    The local TFTP server will now listen on UDP port 69 on the 172.30.0.10 interface for a file transfer. In the next steps, you will transfer a file to the directory shown in the Current Directory box using TFTP.

35. **Minimize** the **remote TargetWindows02 connection**.

36. On the vWorkstation desktop, **create** a **new text document** (***yourname*_S2_tftp**), replacing *yourname* with own name.

37. **Open** a **Command Prompt window**.

38. At the command prompt, **execute** `tftp 172.30.0.10 put c:\users\administrator\desktop\yourname_S2_tftp.txt` to transfer the file to the TargetWindows02 desktop, then **close** the **Command Prompt window**.

39. **Restore** the **remote TargetWindows02 connection**, then **click** the **Show Dir button** in the Tftp64 application to confirm the file transfer.

40. **Make a screen capture** showing the **successful TFTP file transfer** and **paste** it into the Lab Report file.

41. **Close** the **Tftpd64 windows**.

42. **Minimize** the **remote TargetWindows02 connection**.

Part 2: Connecting to a Linux Machine

Note: Some tools are only available on Linux machines. Unlike Windows machines, most Linux interactions take place from the command line, rather than in an application GUI. The virtual environment offers two ways to connect to the Linux terminal: a Remote Desktop Connection and PuTTY. In the next steps, you will explore both options.

1. **Open a remote connection** to the **TargetLinux01 machine**.

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

   - Username: **`student`**
   - Password: **`student`**

2. From the TargetLinux01 menu bar, **open** a **terminal window**.

3. At the command prompt, **execute** **`top`** to display all the systems' top processes.

4. **Press CTRL+ c** to stop the process.

5. At the command prompt, **execute** **`su`** to switch user accounts to the superuser.

   Many Linux commands require elevated access and cannot be performed by the student account.

6. When prompted for a password, **type** **`toor`** and **press Enter**.

You are now logged into the Linux Debian machine with root level access. The command prompt has changed to root@TargetLinux:/home/student#.

7. **Close** the **terminal window**, then **close** the **remote TargetLinux01 connection** to return to the vWorkstation.

8. **Restore** the **remote TargetWindows02 connection**.

9. **Open** the **PuTTY application**.

   PuTTY uses the Secure Shell (SSH) protocol to securely access to a remote computer. Once connected, PuTTY displays a terminal shell in which Linux commands can be executed.

10. In the Host Name (or IP address) box, **type** `172.16.8.5`, the IP address for LAN Switch 1.

11. If necessary, **click** the **SSH radio button**, then **click Open** to start the connection.

12. At the login prompt, **enter** the following credentials.

    - Login: `cisco`
    - Password: `cisco`

    Once successfully logged in, the command prompt, 172.16.8.5/LanSwitch1>, is displayed.

13. **Execute** the **Cisco command** that will list the vlans for LAN Switch 1.

14. **Make a screen capture** showing the **output from the Cisco command** and **paste** it into the Lab Report file.

15. **Execute** `quit` to close the PuTTY window.

Part 3: Using Zenmap to Perform Basic Reconnaissance

Note: In the next steps, you will use Zenmap to perform an Intense Scan on two IP addresses, which will identify the hosts, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters or firewalls are in use.

1. **Open** the **Zenmap application**.

2. **Run** an **Intense scan** on **172.30.0.3** and **172.30.0.11**.

   When listing multiple targets, each IP address should be separated by a single space. This scan will take about 2 minutes. The scan is completed when the final line of the output reads *Nmap done*.

3. When the scan has completed, **examine each Nmap tab** and look for the information in the following table.

Nmap Tab	Information to Look For and Review
Nmap Output	Raw output data
Ports/Hosts	IP hosts and open ports
Topology	Fisheye bubble chart of IP hosts
Host Details	IP host OS fingerprint details
Scans	Completed scans performed

4. **Create** a **Fisheye Bubble chart** for the scan results.

5. **Make a screen capture** showing the Fisheye Bubble chart and **paste** it into your Lab Report file.

6. In the Command box, **type** `nmap -T4 -F 172.16.8.5` and **press Enter** to scan the target.

7. **Make a screen capture** showing the **results of the Zenmap scan** and **paste** it into your Lab Report file.

8. In your Lab Report file, **identify the type of scan that uses the command *-T4 -F*** (hint: use the Profile dropdown menu).

9. **Close Zenmap** without saving changes.

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.

10. **Select any deliverable files** you saved in the course of this lab and **copy** them to the Windows clipboard.

    - ***yourname*_S2_wireshark_capture.pcap**
    - ***yourname*_S2_BasicScan.txt**

11. **Minimize** the **remote TargetWindows02 connection**.

12. On the vWorkstation desktop, **paste** the copied files to the Desktop.

13. On the vWorkstation desktop, **drag** the deliverables files into the File Transfer folder to complete the download to your local computer.

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

In the lab, NetWitness Investigator identified two email addresses found in the Demo Collection. What were they?

Part 2: Tools and Commands

In the lab, you used the filter box in Wireshark to remove traffic from port 3389. What is that port used for? What filter syntax could you use to show only the Ping traffic that was generated in the lab?

Part 3: Challenge Exercise

Repeat a Nessus Basic Scan on the TargetWindows02 machine. Make a screen capture of two different Medium Risk vulnerabilities and using the links provided in the vulnerability detail page, give a brief description of the problem and next steps for each.