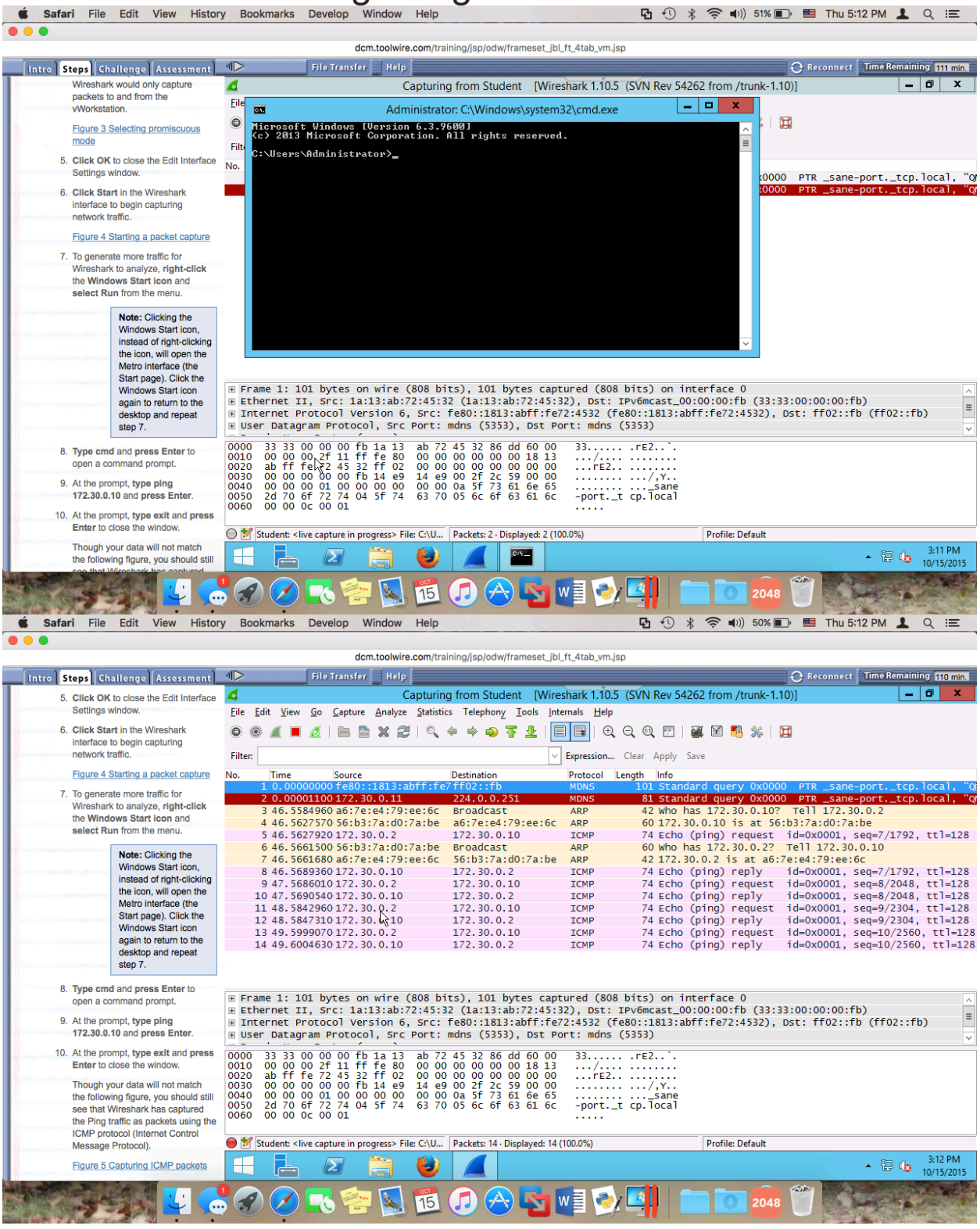
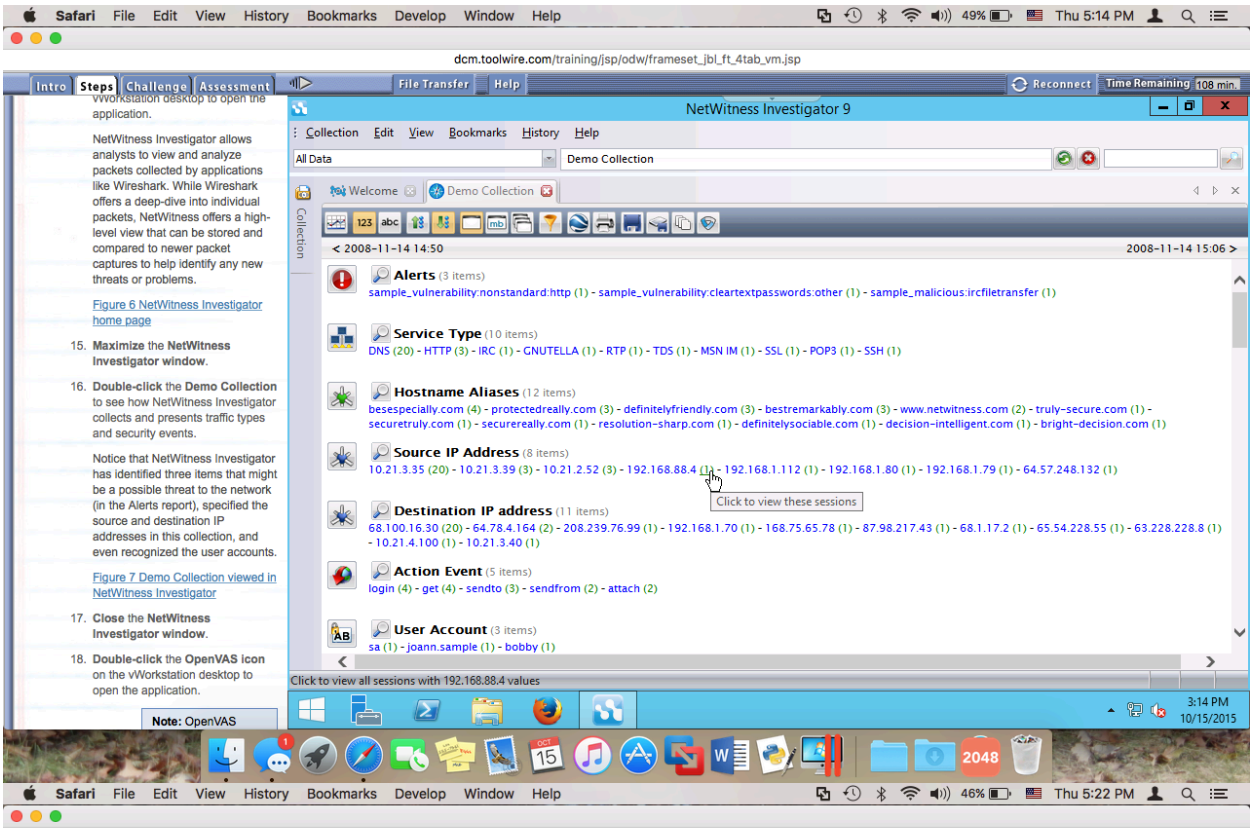
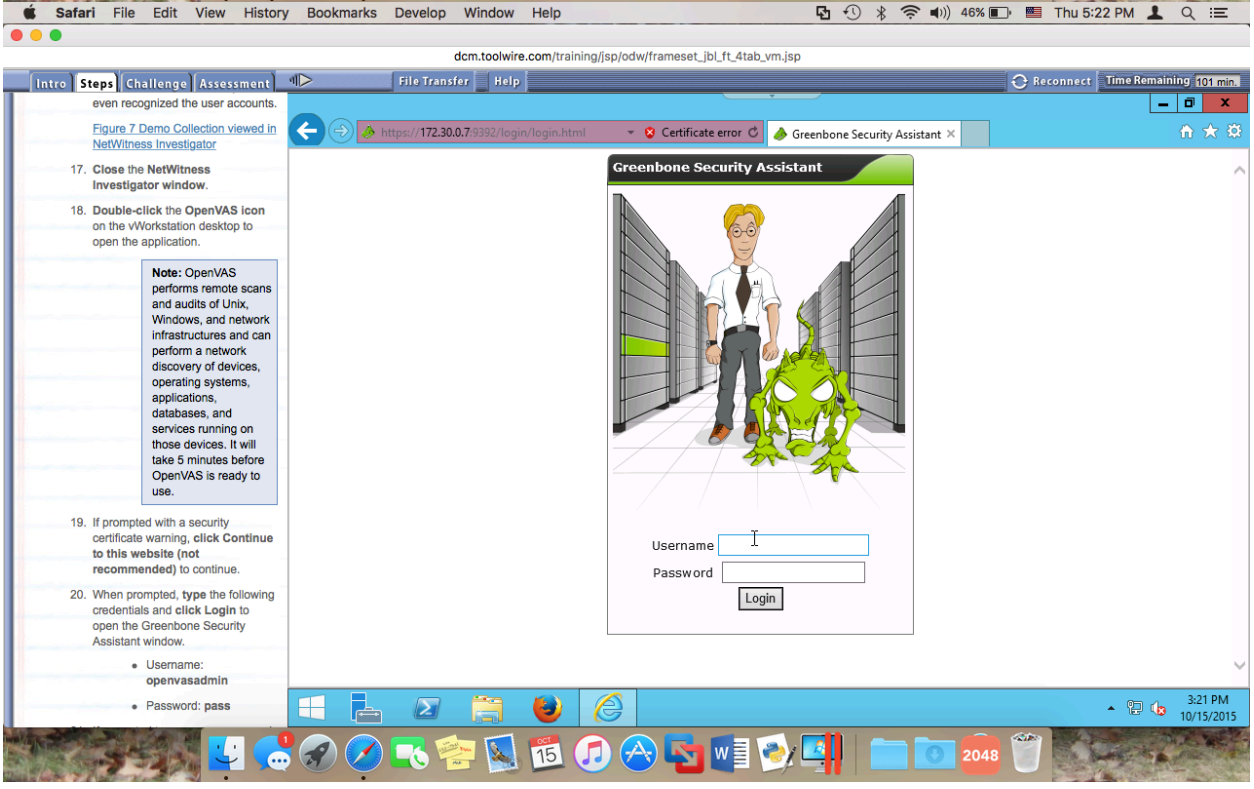
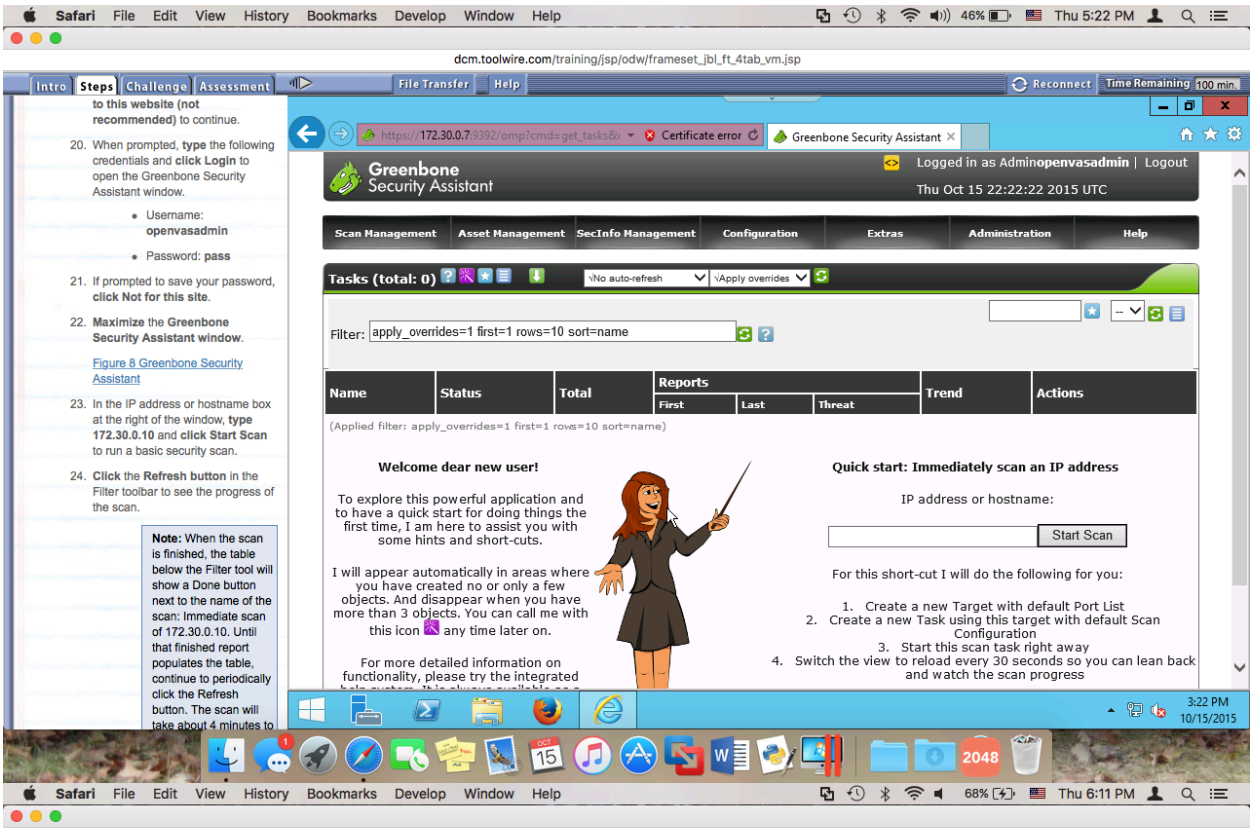
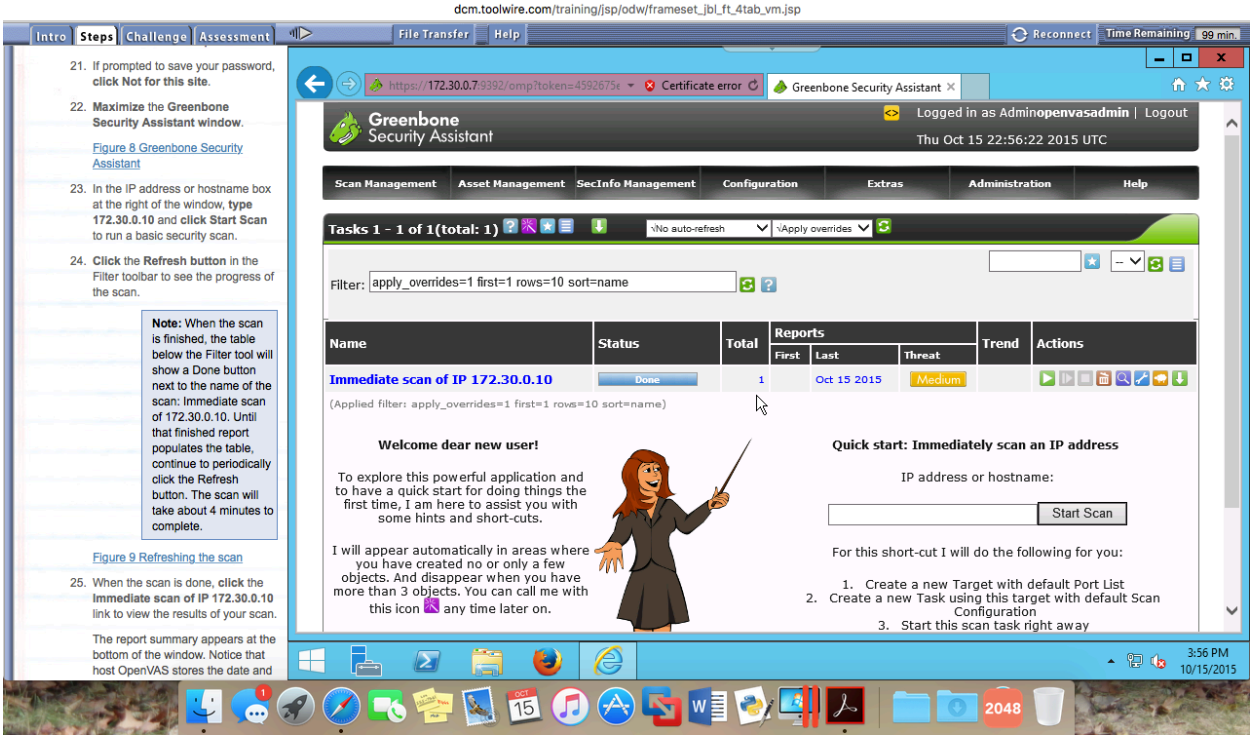
Lab 6
Performing Reconnaissance and Probing using Common Tools

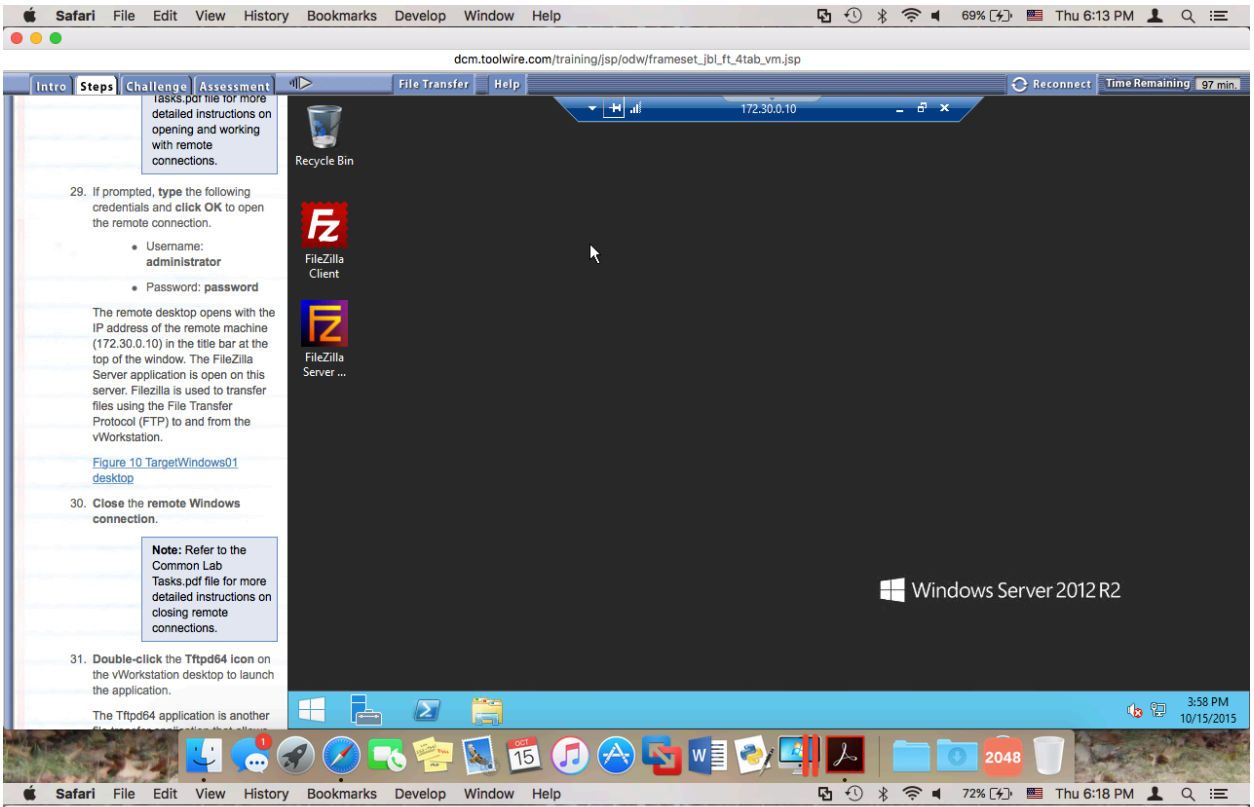


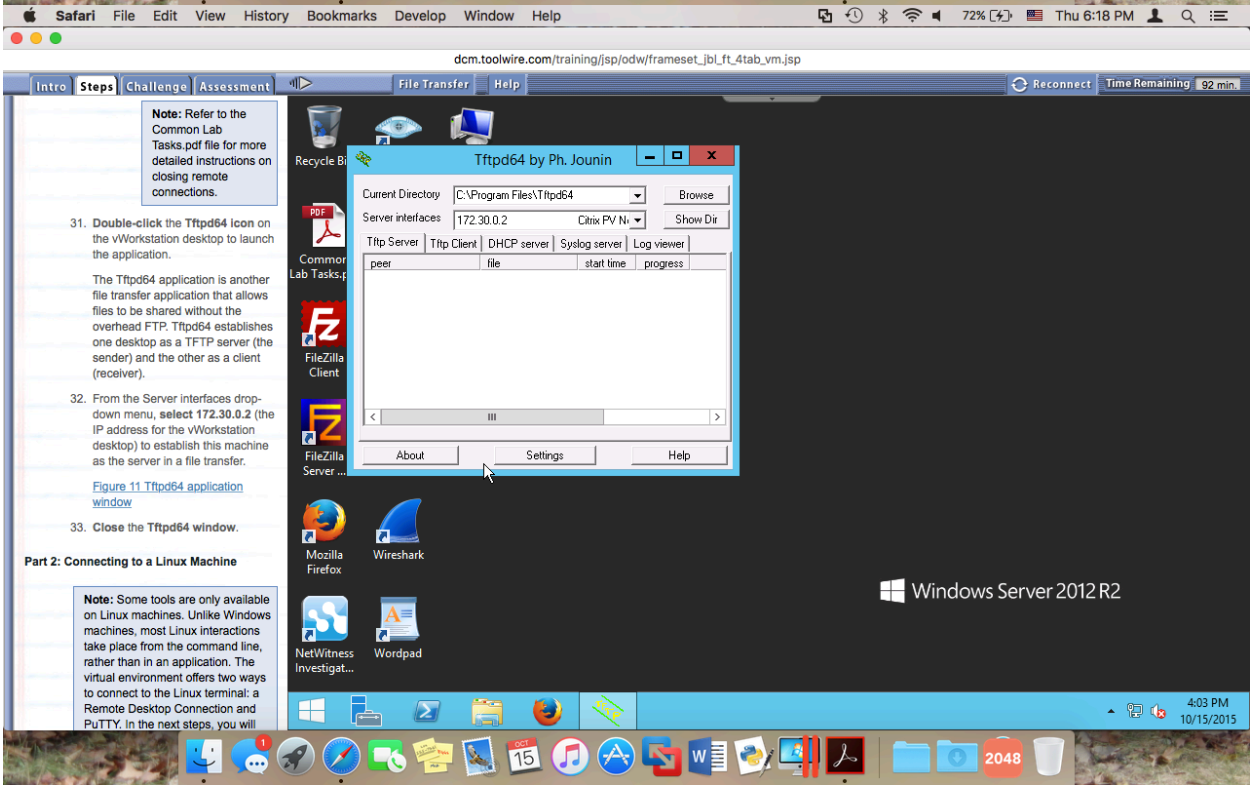

Safari File Edit View History Bookmarks Develop Window Help
Thu 5:14 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 108 min.
vWorkstation desktop to open the application.
NetWitness Investigator allows analysts to view and analyze packets collected by applications like Wireshark. While Wireshark offers a deep-dive into individual packets, NetWitness offers a high-level view that can be stored and compared to newer packet captures to help identify any new threats or problems.
Figure 6 NetWitness Investigator home page
15. Maximize the NetWitness Investigator window.
16. Double-click the Demo Collection to see how NetWitness Investigator collects and presents traffic types and security events.
Notice that NetWitness Investigator has identified three items that might be a possible threat to the network (in the Alerts report), specified the source and destination IP addresses in this collection, and even recognized the user accounts.
Figure 7 Demo Collection viewed in NetWitness Investigator
17. Close the NetWitness Investigator window.
18. Double-click the OpenVAS icon on the vWorkstation desktop to open the application.
Note: OpenVAS
NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
Demo Collection
Welcome
Demo Collection
< 2008-11-14 14:50
2008-11-14 15:06 >
Alerts (3 items)
sample_vulnerability:nonstandard:http (1) - sample_vulnerability:cleartextpasswords:other (1) - sample_malicious:ircfiletransfer (1)
Service Type (10 items)
DNS (20) - HTTP (3) - IRC (1) - GNUTELLA (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POP3 (1) - SSH (1)
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)
Click to view these sessions
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 (4) - get (4) - sendto (3) - sendfrom (2) - attach (2)
User Account (3 items)
sa (1) - joann.sample (1) - bobby (1)
Click to view all sessions with 192.168.88.4 values
3:14 PM
10/15/2015

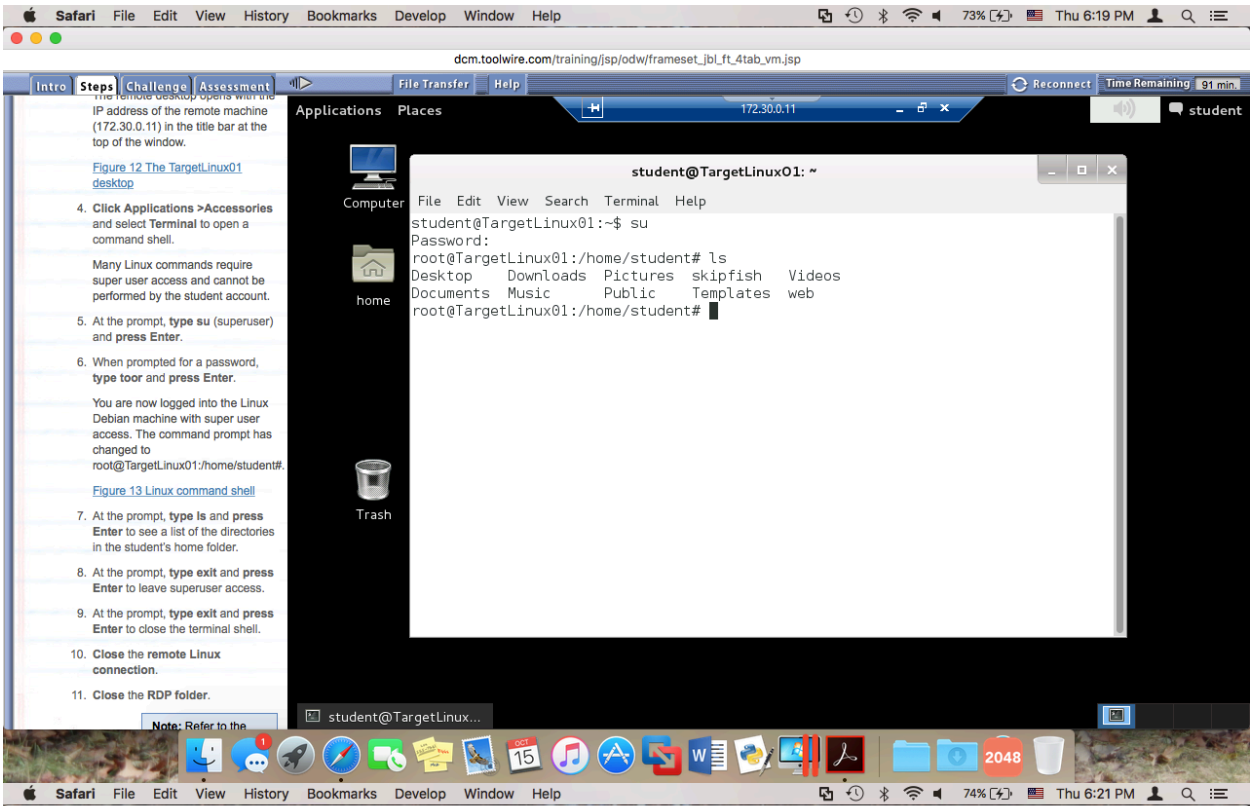

Safari File Edit View History Bookmarks Develop Window Help
Thu 5:22 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 101 min.
even recognized the user accounts.
Figure 7 Demo Collection viewed in NetWitness Investigator
17. Close the NetWitness Investigator window.
18. Double-click the OpenVAS icon on the vWorkstation desktop to open the application.
Note: OpenVAS 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. It will take 5 minutes before OpenVAS is ready to use.
19. If prompted with a security certificate warning, click Continue to this website (not recommended) to continue.
20. When prompted, type the following credentials and click Login to open the Greenbone Security Assistant window.
Username: openvasadmin
Password: pass
https://172.30.0.7:9392/login/login.html
Certificate error
Greenbone Security Assistant
Greenbone Security Assistant
Username
Password
Login
3:21 PM
10/15/2015

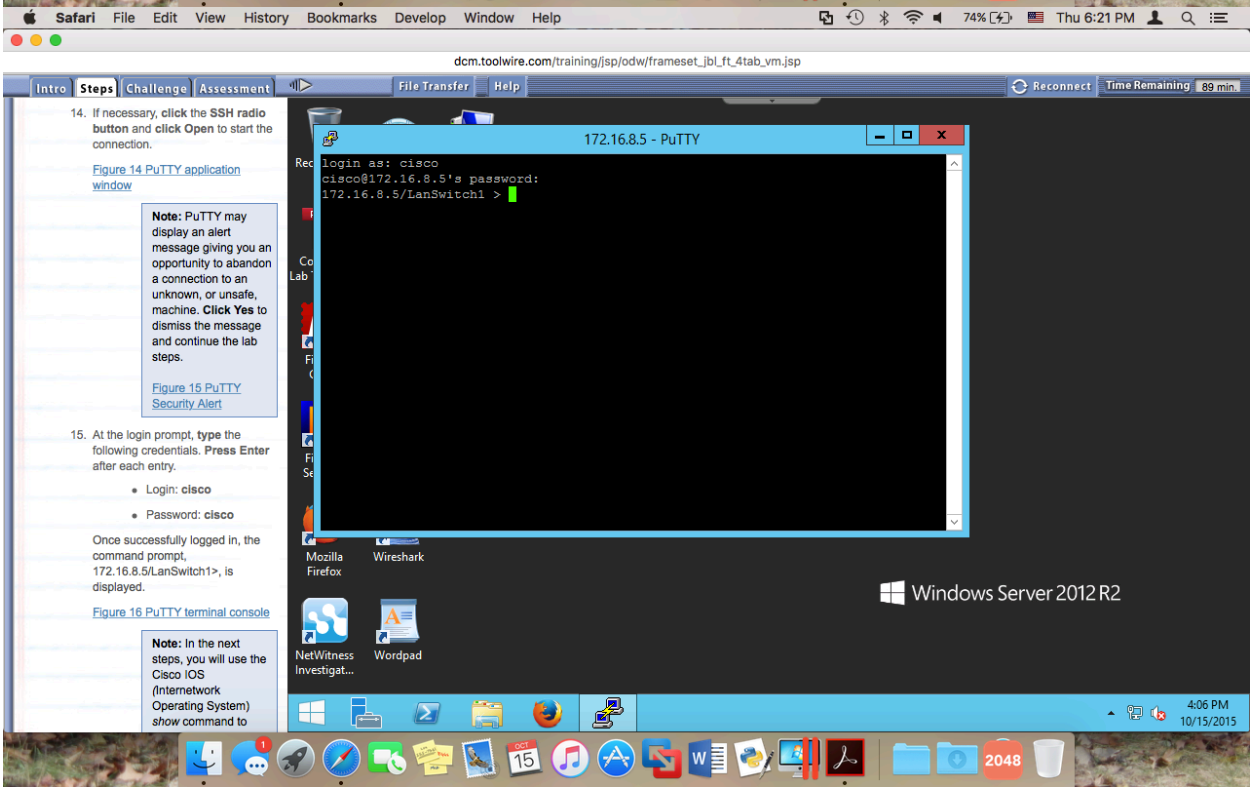

Safari File Edit View History Bookmarks Develop Window Help
Thu 5:22 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 100 min.
to this website (not recommended) to continue.
20. When prompted, type the following credentials and click Login to open the Greenbone Security Assistant window.
Username: openvasadmin
Password: pass
21. If prompted to save your password, click Not for this site.
22. Maximize the Greenbone Security Assistant window.
Figure 8 Greenbone Security Assistant
23. In the IP address or hostname box at the right of the window, type 172.30.0.10 and click Start Scan to run a basic security scan.
24. Click the Refresh button in the Filter toolbar to see the progress of the scan.
Note: When the scan is finished, the table below the Filter tool will show a Done button next to the name of the scan: Immediate scan of 172.30.0.10. Until that finished report populates the table, continue to periodically click the Refresh button. The scan will take about 4 minutes to
Certificate error
Greenbone Security Assistant
Greenbone Security Assistant
Logged in as Adminopenvasadmin | Logout
Thu Oct 15 22:22:22 2015 UTC
Scan Management Asset Management SecInfo Management Configuration Extras Administration Help
Tasks (total: 0)
Filter: apply_overrides=1 first=1 rows=10 sort=name
Name Status Total Reports First Last Threat Trend Actions
(Applied filter: apply_overrides=1 first=1 rows=10 sort=name)
Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.
For more detailed information on functionality, please try the integrated
Quick start: Immediately scan an IP address
IP address or hostname:
Start Scan
For this short-cut I will do the following for you:
1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress
3:22 PM
10/15/2015
Safari File Edit View History Bookmarks Develop Window Help
68%
Thu 6:11 PM

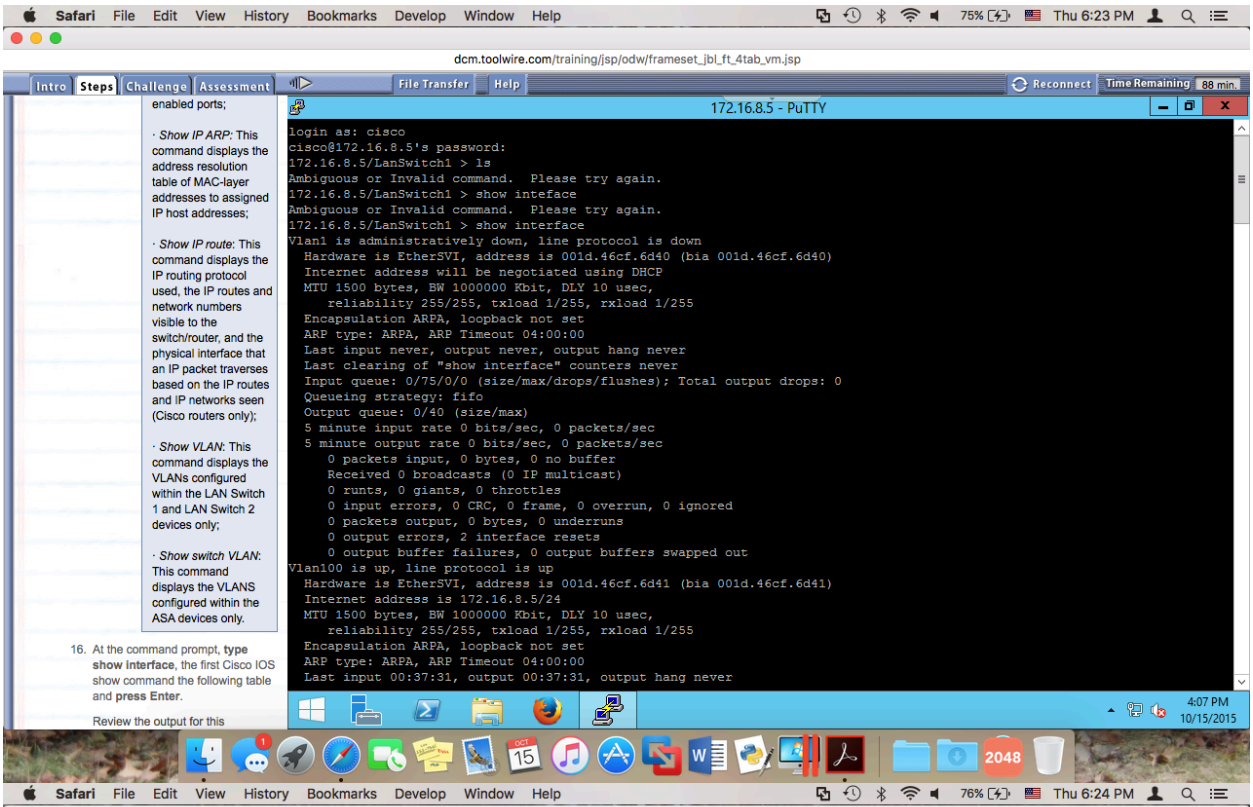

dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 99 min.
21. If prompted to save your password, click Not for this site.
22. Maximize the Greenbone Security Assistant window.
Figure 8 Greenbone Security Assistant
23. In the IP address or hostname box at the right of the window, type 172.30.0.10 and click Start Scan to run a basic security scan.
24. Click the Refresh button in the Filter toolbar to see the progress of the scan.
Note: When the scan is finished, the table below the Filter tool will show a Done button next to the name of the scan: Immediate scan of 172.30.0.10. Until that finished report populates the table, continue to periodically click the Refresh button. The scan will take about 4 minutes to complete.
Figure 9 Refreshing the scan
25. When the scan is done, click the Immediate scan of IP 172.30.0.10 link to view the results of your scan.
The report summary appears at the bottom of the window. Notice that host OpenVAS stores the date and
Certificate error
Greenbone Security Assistant
Greenbone Security Assistant
Logged in as Adminopenvasadmin | Logout
Thu Oct 15 22:56:22 2015 UTC
Scan Management Asset Management SecInfo Management Configuration Extras Administration Help
Tasks 1 - 1 of 1(total: 1)
Filter: apply_overrides=1 first=1 rows=10 sort=name
Name Status Total Reports First Last Threat Trend Actions
Immediate scan of IP 172.30.0.10 Done 1 Oct 15 2015 Medium
(Applied filter: apply_overrides=1 first=1 rows=10 sort=name)
Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.
Quick start: Immediately scan an IP address
IP address or hostname:
Start Scan
For this short-cut I will do the following for you:
1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
3:56 PM
10/15/2015

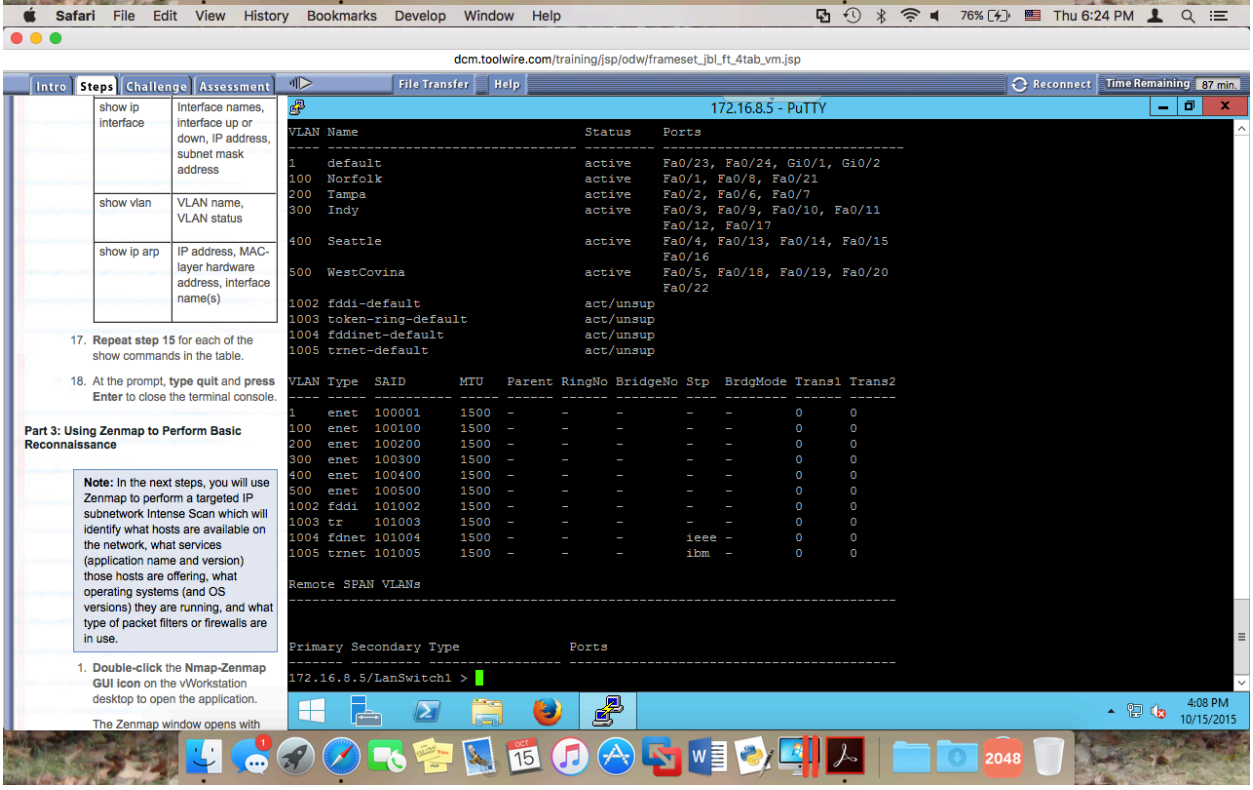

Safari File Edit View History Bookmarks Develop Window Help
69% Thu 6:13 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 97 min.
Tasks.pdf file for more detailed instructions on opening and working with remote connections.
29. If prompted, type the following credentials and click OK to open the remote connection.
Username: administrator
Password: password
The remote desktop opens with the IP address of the remote machine (172.30.0.10) in the title bar at the top of the window. The FileZilla Server application is open on this server. Filezilla is used to transfer files using the File Transfer Protocol (FTP) to and from the vWorkstation.
Figure 10 TargetWindows01 desktop
30. Close the remote Windows connection.
Note: Refer to the Common Lab Tasks.pdf file for more detailed instructions on closing remote connections.
31. Double-click the Tftpd64 icon on the vWorkstation desktop to launch the application.
The Tftpd64 application is another
172.30.0.10
Recycle Bin
FileZilla Client
FileZilla Server ...
Windows Server 2012 R2
3:58 PM
10/15/2015

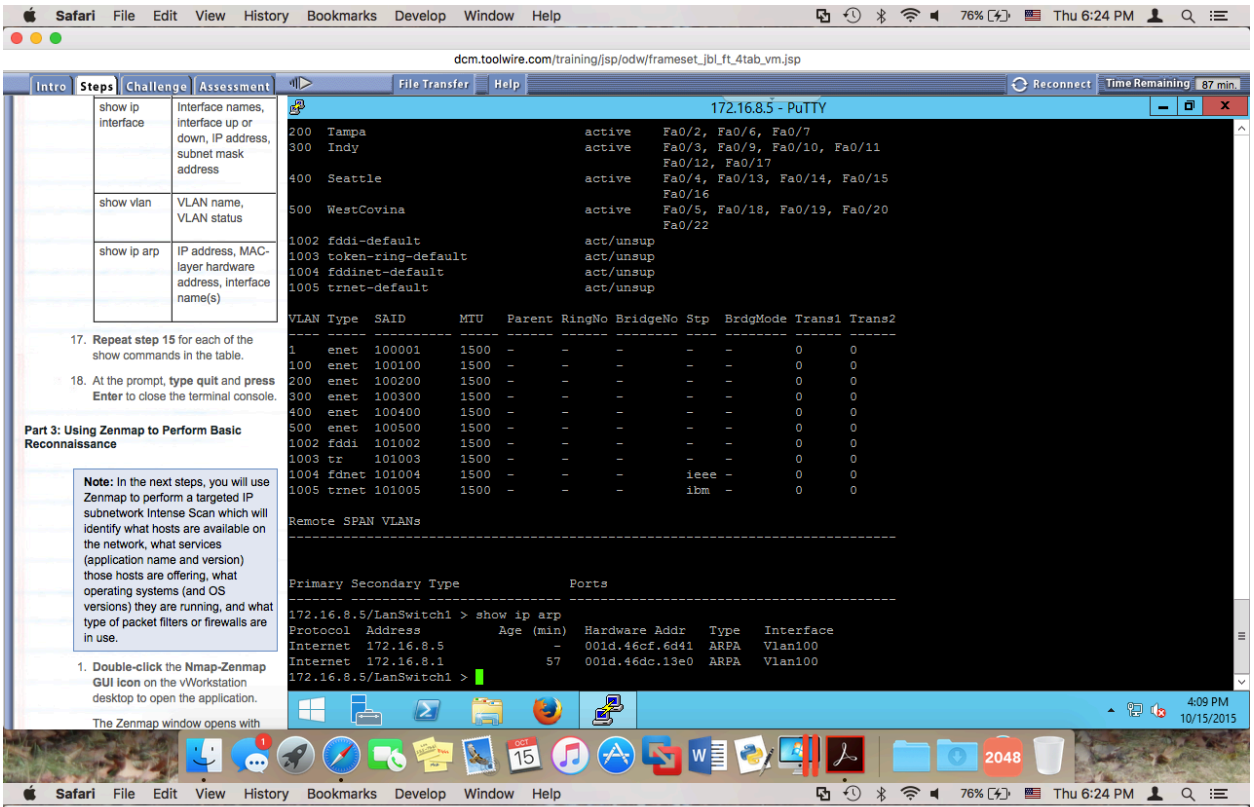

Safari File Edit View History Bookmarks Develop Window Help
72% Thu 6:18 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 92 min.
Note: Refer to the Common Lab Tasks.pdf file for more detailed instructions on closing remote connections.
31. Double-click the Tftpd64 icon on the vWorkstation desktop to launch the application.
The Tftpd64 application is another file transfer application that allows files to be shared without the overhead FTP. Tftpd64 establishes one desktop as a TFTP server (the sender) and the other as a client (receiver).
32. From the Server interfaces drop-down menu, select 172.30.0.2 (the IP address for the vWorkstation desktop) to establish this machine as the server in a file transfer.
Figure 11 Tftpd64 application window
33. Close the Tftpd64 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. The virtual environment offers two ways to connect to the Linux terminal: a Remote Desktop Connection and PuTTY. In the next steps, you will
Tftpd64 by Ph. Jounin
Current Directory C:\Program Files\Tftpd64
Browse
Server interfaces 172.30.0.2
Show Dir
Tftp Server Tftp Client DHCP server Syslog server Log viewer
peer file start time progress
About Settings Help
Recycle Bi
Common Lab Tasks.p
FileZilla Client
FileZilla Server ...
Mozilla Firefox
Wireshark
NetWitness Investigat...
Wordpad
Windows Server 2012 R2
4:03 PM
10/15/2015

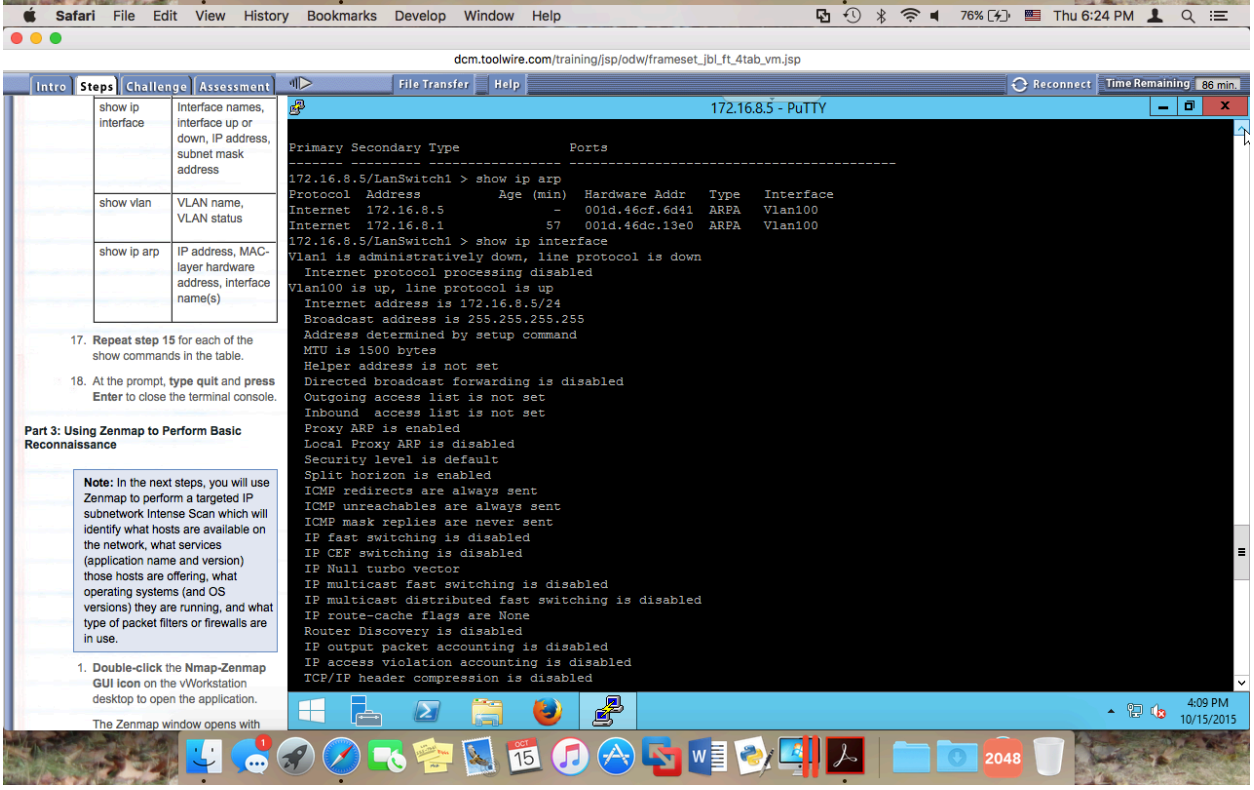

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:19 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 91 min.
Applications Places
172.30.0.11
student
Computer
home
Trash
student@TargetLinux01: ~
File Edit View Search Terminal Help
student@TargetLinux01:~$ su
Password:
root@TargetLinux01:/home/student# ls
Desktop Downloads Pictures skipfish Videos
Documents Music Public Templates web
root@TargetLinux01:/home/student#
student@TargetLinux...
IP address of the remote machine (172.30.0.11) in the title bar at the top of the window.
Figure 12 The TargetLinux01 desktop
4. Click Applications >Accessories and select Terminal to open a command shell.
Many Linux commands require super user access and cannot be performed by the student account.
5. At the prompt, type su (superuser) and press Enter.
6. When prompted for a password, type toor and press Enter.
You are now logged into the Linux Debian machine with super user access. The command prompt has changed to root@TargetLinux01:/home/student#.
Figure 13 Linux command shell
7. At the prompt, type ls and press Enter to see a list of the directories in the student's home folder.
8. At the prompt, type exit and press Enter to leave superuser access.
9. At the prompt, type exit and press Enter to close the terminal shell.
10. Close the remote Linux connection.
11. Close the RDP folder.

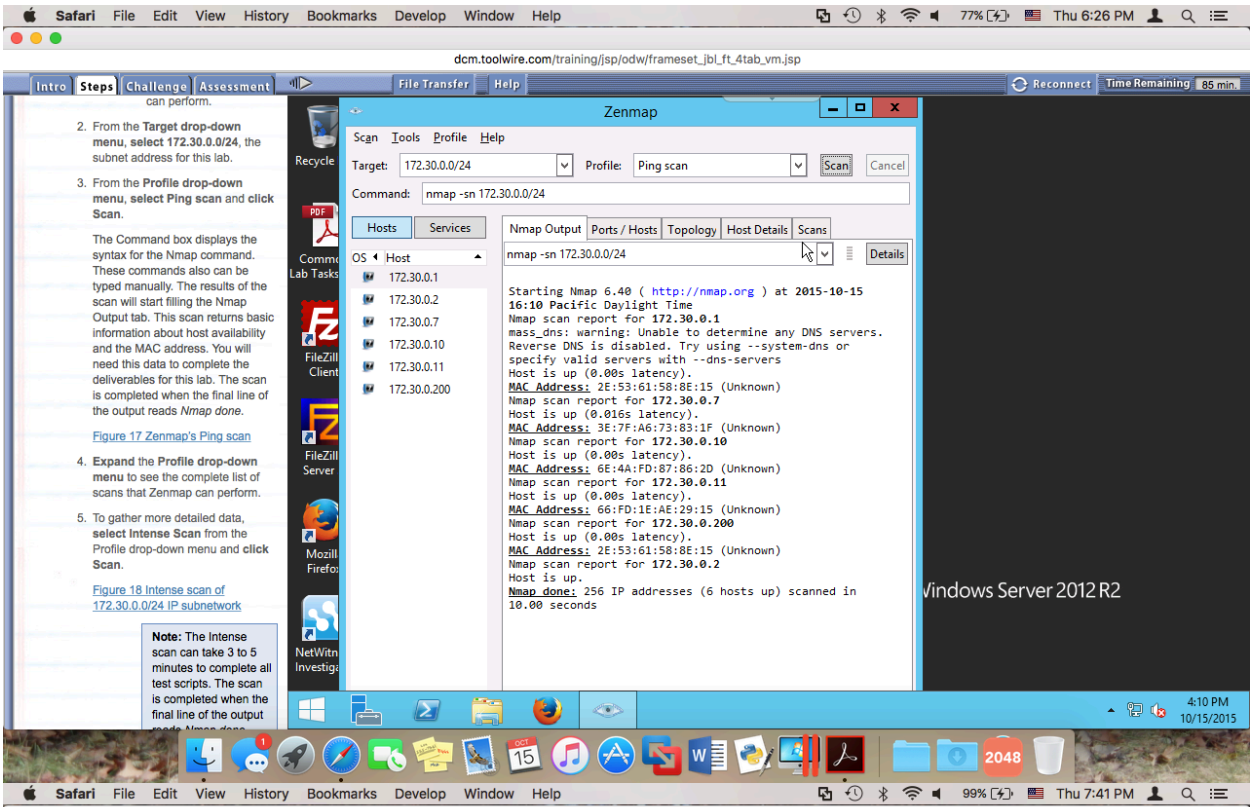

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:21 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 89 min.
172.16.8.5 - PuTTY
login as: cisco
cisco@172.16.8.5's password:
172.16.8.5/LanSwitch1 >
Mozilla Firefox
Wireshark
NetWitness Investigat...
Wordpad
Windows Server 2012 R2
4:06 PM
10/15/2015
14. If necessary, click the SSH radio button and click Open to start the connection.
Figure 14 PuTTY application window
Note: PuTTY may display an alert message giving you an opportunity to abandon a connection to an unknown, or unsafe, machine. Click Yes to dismiss the message and continue the lab steps.
Figure 15 PuTTY Security Alert
15. At the login prompt, type the following credentials. Press Enter after each entry.
• Login: cisco
• Password: cisco
Once successfully logged in, the command prompt, 172.16.8.5/LanSwitch1>, is displayed.
Figure 16 PuTTY terminal console
Note: In the next steps, you will use the Cisco IOS (Internetwork Operating System) show command to

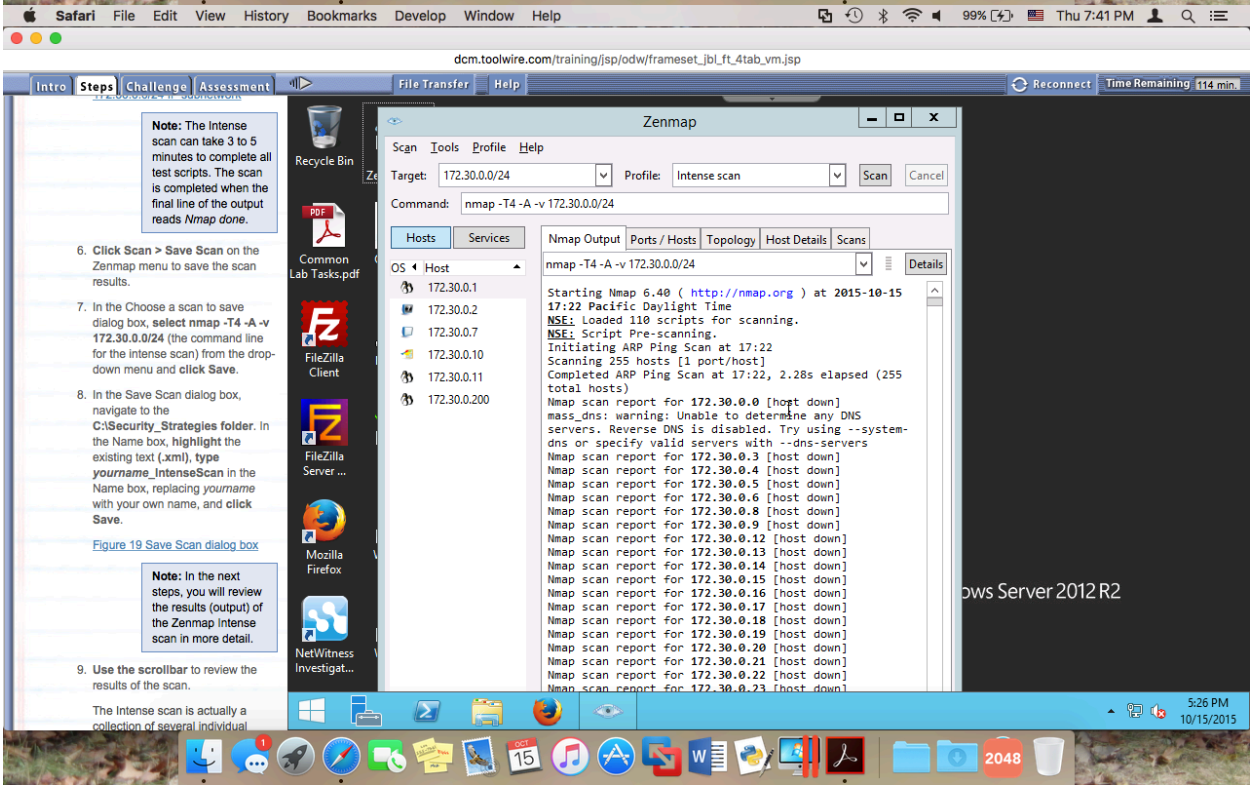

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:23 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 88 min.
172.16.8.5 - PuTTY
enabled ports;
· Show IP ARP: This command displays the address resolution table of MAC-layer addresses to assigned IP host addresses;
· 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);
· Show VLAN: This command displays the VLANs configured within the LAN Switch 1 and LAN Switch 2 devices only;
· Show switch VLAN: This command displays the VLANS configured within the ASA devices only.
16. At the command prompt, type show interface, the first Cisco IOS show command the following table and press Enter.
Review the output for this
login as: cisco
cisco@172.16.8.5's password:
172.16.8.5/LanSwitch1 > ls
Ambiguous or Invalid command. Please try again.
172.16.8.5/LanSwitch1 > show inteface
Ambiguous or Invalid command. Please try again.
172.16.8.5/LanSwitch1 > show interface
Vlan1 is administratively down, line protocol is down
Hardware is EtherSVI, address is 001d.46cf.6d40 (bia 001d.46cf.6d40)
Internet address will be negotiated using DHCP
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
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 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 packets output, 0 bytes, 0 underruns
0 output errors, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
Vlan100 is up, line protocol is up
Hardware is EtherSVI, address is 001d.46cf.6d41 (bia 001d.46cf.6d41)
Internet address is 172.16.8.5/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:37:31, output 00:37:31, output hang never
4:07 PM
10/15/2015

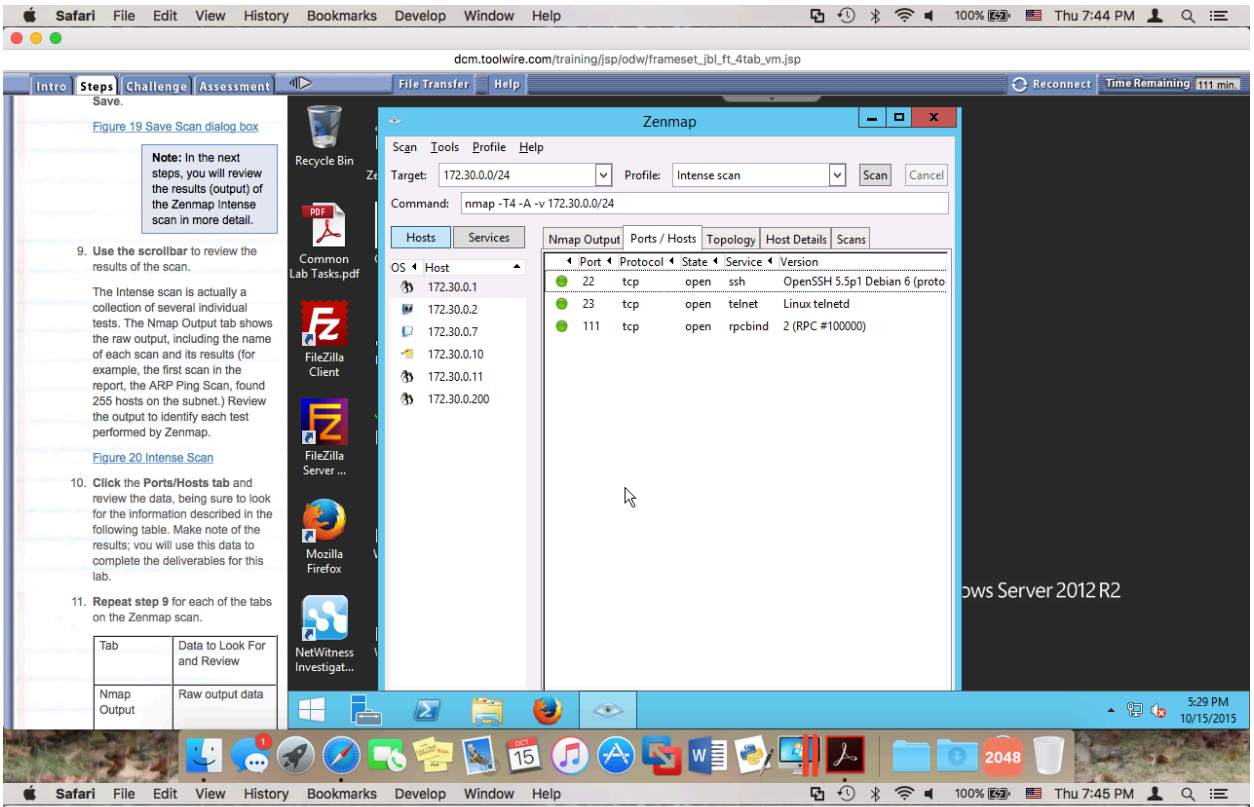

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:24 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 87 min.
172.16.8.5 - PuTTY
show ip interface | Interface names, interface up or down, IP address, subnet mask address
show vlan | VLAN name, VLAN status
show ip arp | IP address, MAC-layer hardware address, interface name(s)
17. Repeat step 15 for each of the show commands in the table.
18. At the prompt, type quit and press Enter to close the terminal console.
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. Double-click the Nmap-Zenmap GUI icon on the vWorkstation desktop to open the application.
The Zenmap window opens with
VLAN Name Status Ports
1 default active Fa0/23, Fa0/24, Gi0/1, Gi0/2
100 Norfolk active Fa0/1, Fa0/8, Fa0/21
200 Tampa active Fa0/2, Fa0/6, Fa0/7
300 Indy active Fa0/3, Fa0/9, Fa0/10, Fa0/11
Fa0/12, Fa0/17
400 Seattle active Fa0/4, Fa0/13, Fa0/14, Fa0/15
Fa0/16
500 WestCovina active Fa0/5, Fa0/18, Fa0/19, Fa0/20
Fa0/22
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
100 enet 100100 1500 - - - - - 0 0
200 enet 100200 1500 - - - - - 0 0
300 enet 100300 1500 - - - - - 0 0
400 enet 100400 1500 - - - - - 0 0
500 enet 100500 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
Remote SPAN VLANs
Primary Secondary Type Ports
172.16.8.5/LanSwitch1 >
4:08 PM
10/15/2015

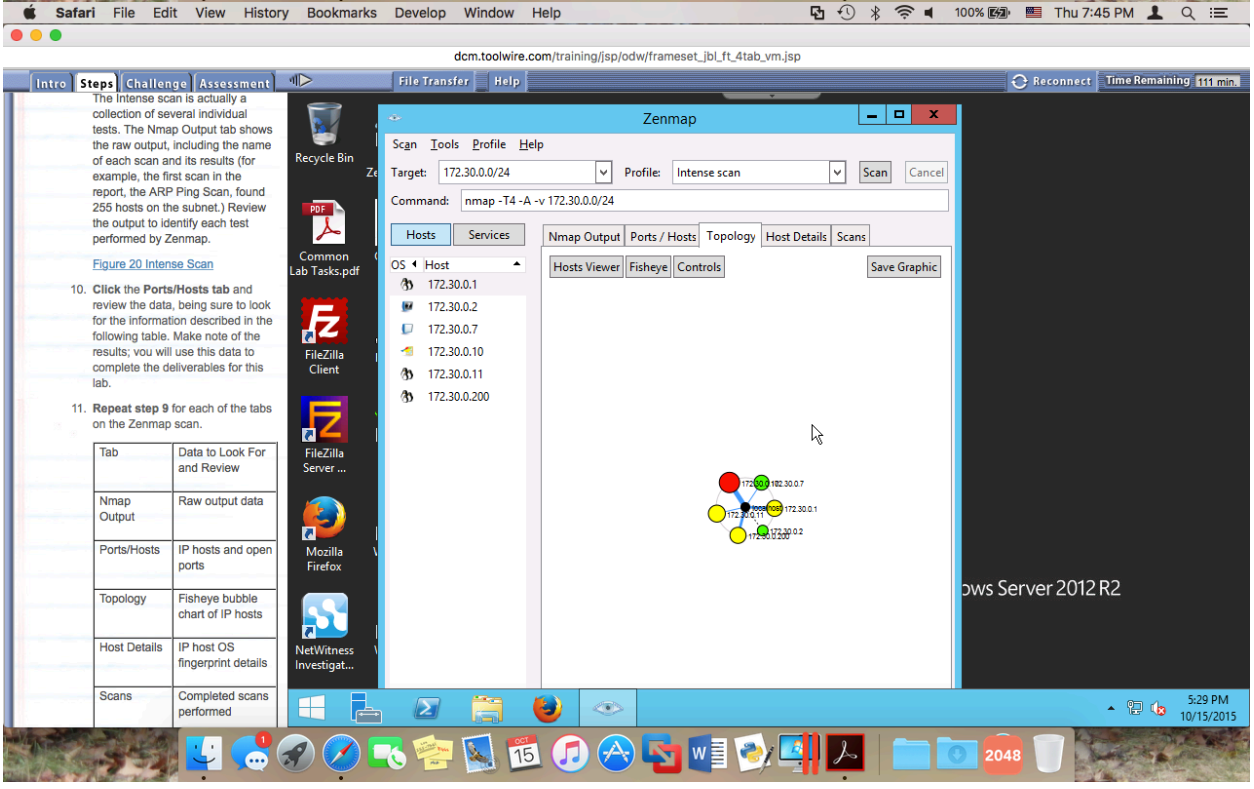

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:24 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 87 min.
172.16.8.5 - PuTTY
show ip interface
Interface names, interface up or down, IP address, subnet mask address
show vlan
VLAN name, VLAN status
show ip arp
IP address, MAC-layer hardware address, interface name(s)
17. Repeat step 15 for each of the show commands in the table.
18. At the prompt, type quit and press Enter to close the terminal console.
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. Double-click the Nmap-Zenmap GUI icon on the vWorkstation desktop to open the application.
The Zenmap window opens with
200 Tampa active Fa0/2, Fa0/6, Fa0/7
300 Indy active Fa0/3, Fa0/9, Fa0/10, Fa0/11
Fa0/12, Fa0/17
400 Seattle active Fa0/4, Fa0/13, Fa0/14, Fa0/15
Fa0/16
500 WestCovina active Fa0/5, Fa0/18, Fa0/19, Fa0/20
Fa0/22
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
100 enet 100100 1500 - - - - - 0 0
200 enet 100200 1500 - - - - - 0 0
300 enet 100300 1500 - - - - - 0 0
400 enet 100400 1500 - - - - - 0 0
500 enet 100500 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
Remote SPAN VLANs
Primary Secondary Type Ports
172.16.8.5/LanSwitch1 > show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 172.16.8.5 - 001d.46cf.6d41 ARPA Vlan100
Internet 172.16.8.1 57 001d.46dc.13e0 ARPA Vlan100
172.16.8.5/LanSwitch1 >
4:09 PM
10/15/2015

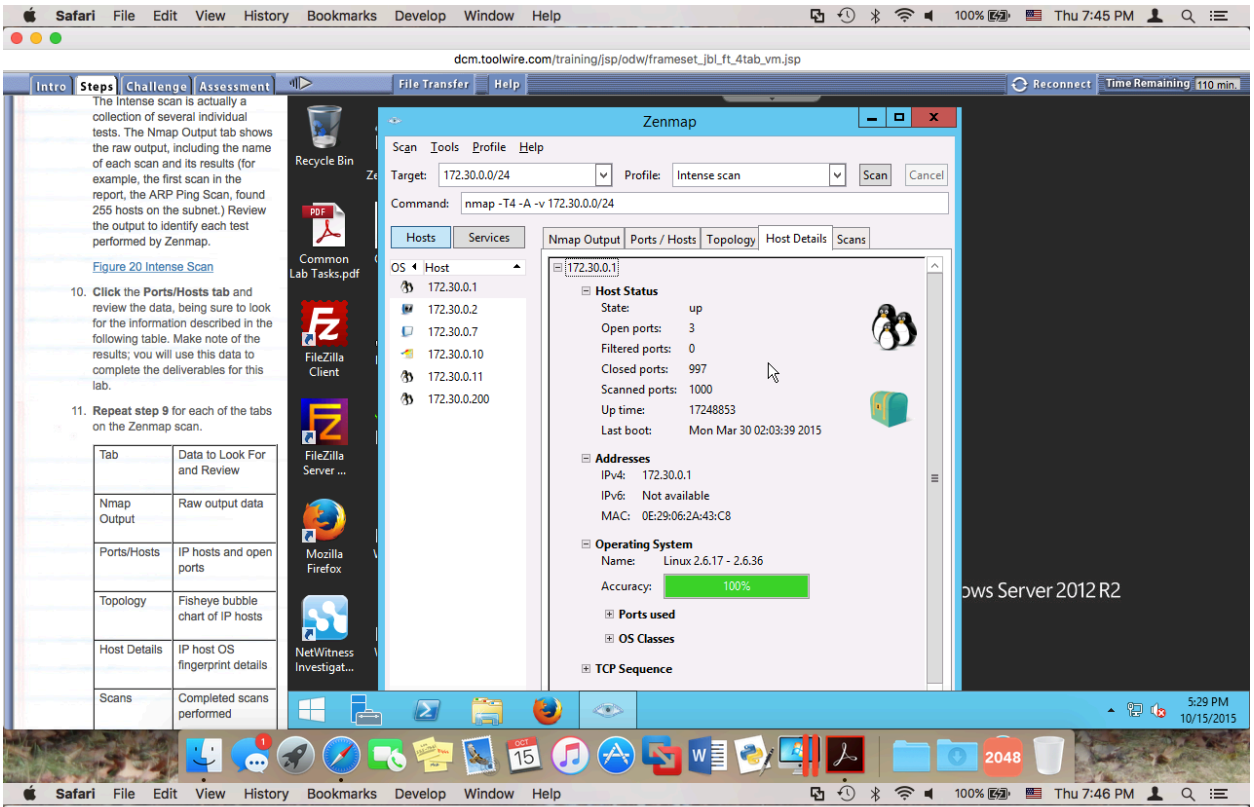

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:24 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 86 min.
172.16.8.5 - PuTTY
show ip interface
Interface names, interface up or down, IP address, subnet mask address
show vlan
VLAN name, VLAN status
show ip arp
IP address, MAC-layer hardware address, interface name(s)
17. Repeat step 15 for each of the show commands in the table.
18. At the prompt, type quit and press Enter to close the terminal console.
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. Double-click the Nmap-Zenmap GUI icon on the vWorkstation desktop to open the application.
The Zenmap window opens with
Primary Secondary Type Ports
172.16.8.5/LanSwitch1 > show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 172.16.8.5 - 001d.46cf.6d41 ARPA Vlan100
Internet 172.16.8.1 57 001d.46dc.13e0 ARPA Vlan100
172.16.8.5/LanSwitch1 > show ip interface
Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled
Vlan100 is up, line protocol is up
Internet address is 172.16.8.5/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP CEF switching is disabled
IP Null turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are None
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
4:09 PM
10/15/2015

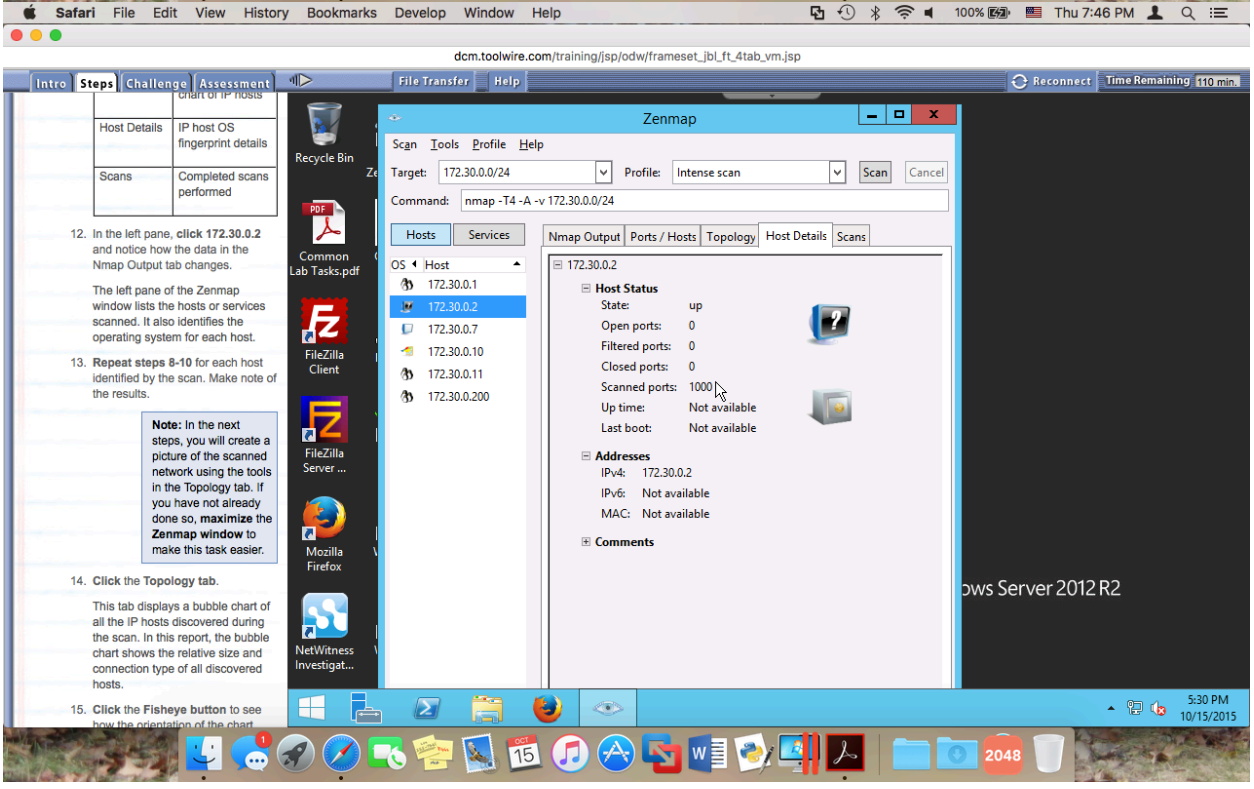

Safari File Edit View History Bookmarks Develop Window Help
Thu 6:26 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 85 min.
can perform.
2. From the Target drop-down menu, select 172.30.0.0/24, the subnet address for this lab.
3. From the Profile drop-down menu, select Ping scan and click Scan.
The Command box displays the syntax for the Nmap command. These commands also can be typed manually. The results of the scan will start filling the Nmap Output tab. This scan returns basic information about host availability and the MAC address. You will need this data to complete the deliverables for this lab. The scan is completed when the final line of the output reads Nmap done.
Figure 17 Zenmap's Ping scan
4. Expand the Profile drop-down menu to see the complete list of scans that Zenmap can perform.
5. To gather more detailed data, select Intense Scan from the Profile drop-down menu and click Scan.
Figure 18 Intense scan of 172.30.0.0/24 IP subnetwork
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
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Ping scan
Scan Cancel
Command: nmap -sn 172.30.0.0/24
Hosts Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sn 172.30.0.0/24
Details
Starting Nmap 6.40 (http://nmap.org) at 2015-10-15 16:10 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: 2E:53:61:58:8E:15 (Unknown)
Nmap scan report for 172.30.0.7
Host is up (0.016s latency).
MAC Address: 3E:7F:A6:73:83:1F (Unknown)
Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
MAC Address: 6E:4A:FD:87:86:2D (Unknown)
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
MAC Address: 66:FD:1E:AE:29:15 (Unknown)
Nmap scan report for 172.30.0.200
Host is up (0.00s latency).
MAC Address: 2E:53:61:58:8E:15 (Unknown)
Nmap scan report for 172.30.0.2
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 10.00 seconds
Windows Server 2012 R2
4:10 PM
10/15/2015

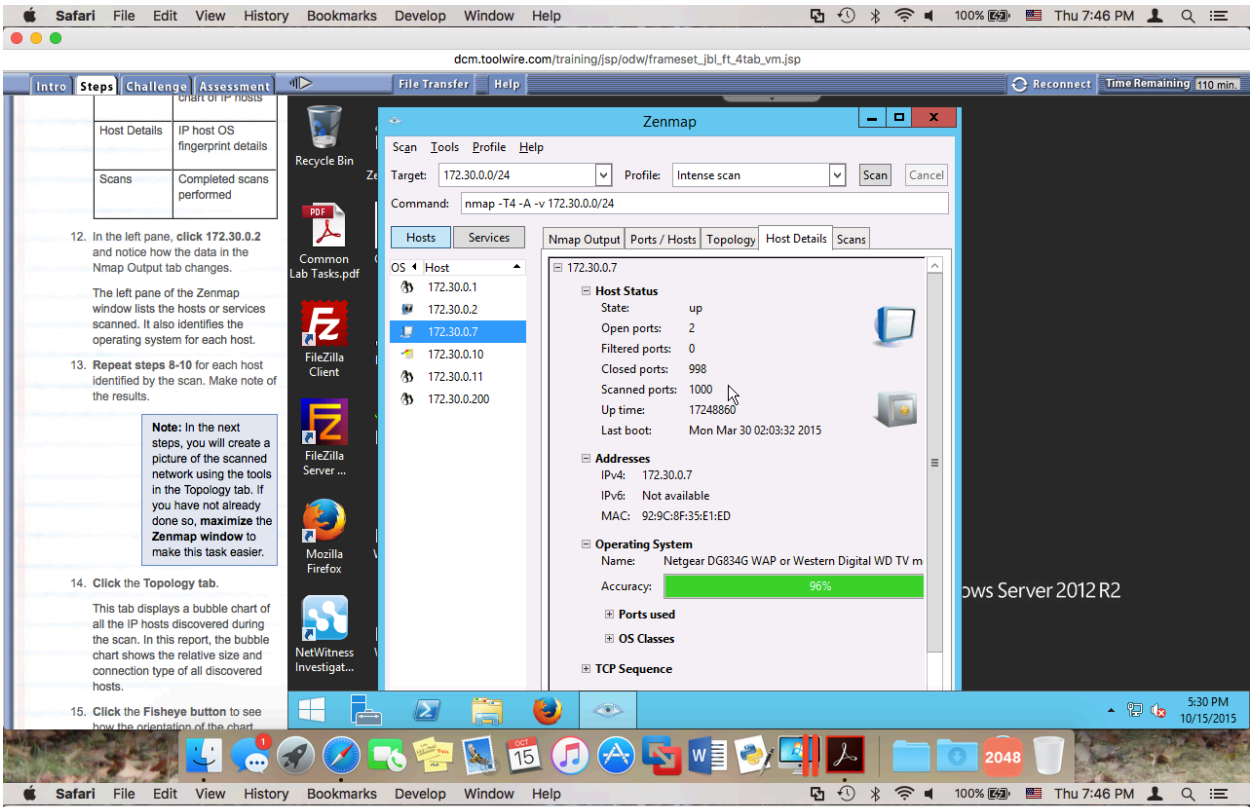

Safari File Edit View History Bookmarks Develop Window Help
Thu 7:41 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 114 min.
Note: The Intense scan can take 3 to 5 minutes to complete all test scripts. The scan is completed when the final line of the output reads Nmap done.
6. Click Scan > Save Scan on the Zenmap menu to save the scan results.
7. In the Choose a scan to save dialog box, select nmap -T4 -A -v 172.30.0.0/24 (the command line for the intense scan) from the drop-down menu and click Save.
8. In the Save Scan dialog box, navigate to the C:\Security_Strategies folder. In the Name box, highlight the existing text (.xml), type yourname_IntenseScan in the Name box, replacing yourname with your own name, and click Save.
Figure 19 Save Scan dialog box
Note: In the next steps, you will review the results (output) of the Zenmap Intense scan in more detail.
9. Use the scrollbar to review the results of the scan.
The Intense scan is actually a collection of several individual
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 172.30.0.0/24
Details
Starting Nmap 6.40 (http://nmap.org) at 2015-10-15 17:22 Pacific Daylight Time
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 17:22
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 17:22, 2.28s elapsed (255 total hosts)
Nmap scan report for 172.30.0.0 [host down]
mass_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 172.30.0.3 [host down]
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 172.30.0.8 [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]
ows Server 2012 R2
5:26 PM
10/15/2015

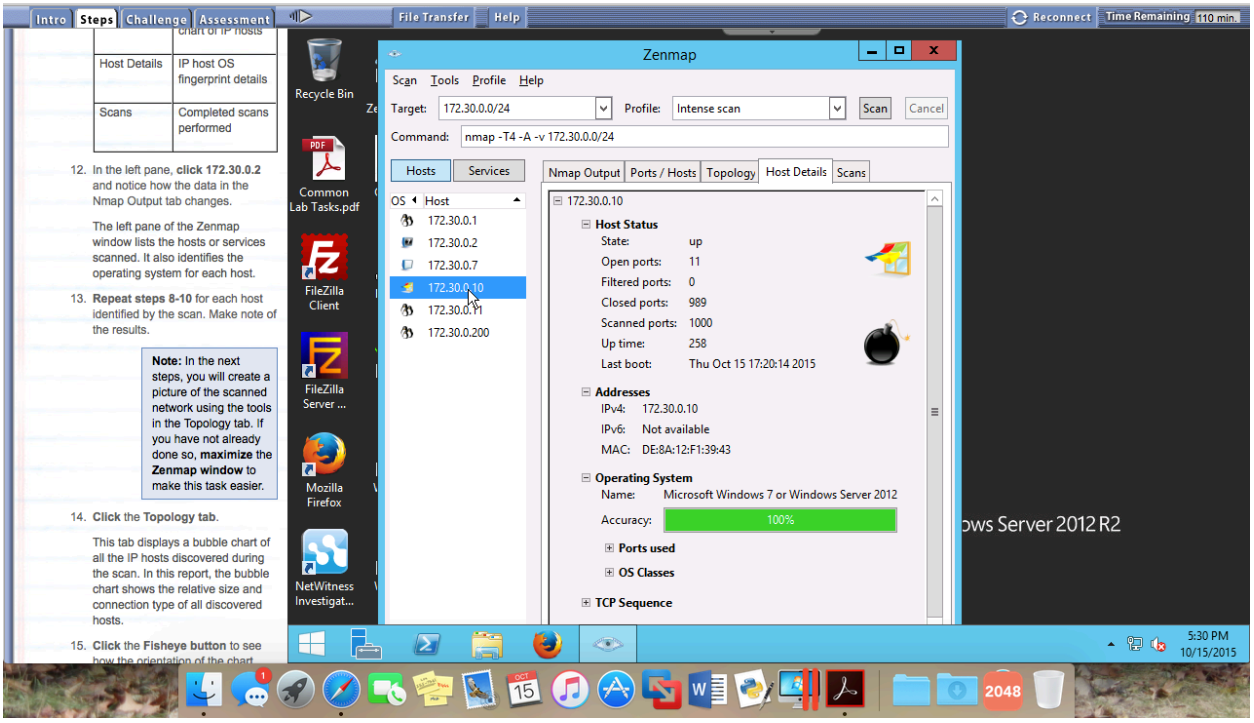

Safari File Edit View History Bookmarks Develop Window Help
100% Thu 7:44 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 111 min.
Save.
Figure 19 Save Scan dialog box
Note: In the next steps, you will review the results (output) of the Zenmap Intense scan in more detail.
9. Use the scrollbar to review the results of the 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 scan in the report, the ARP Ping Scan, found 255 hosts on the subnet.) Review the output to identify each test performed by Zenmap.
Figure 20 Intense Scan
10. Click the Ports/Hosts tab and review the data, being sure to look for the information described in the following table. Make note of the results; you will use this data to complete the deliverables for this lab.
11. Repeat step 9 for each of the tabs on the Zenmap scan.
Tab
Data to Look For and Review
Nmap Output
Raw output data
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Port Protocol State Service Version
22 tcp open ssh OpenSSH 5.5p1 Debian 6 (proto
23 tcp open telnet Linux telnetd
111 tcp open rpcbind 2 (RPC #100000)
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
ows Server 2012 R2
5:29 PM
10/15/2015

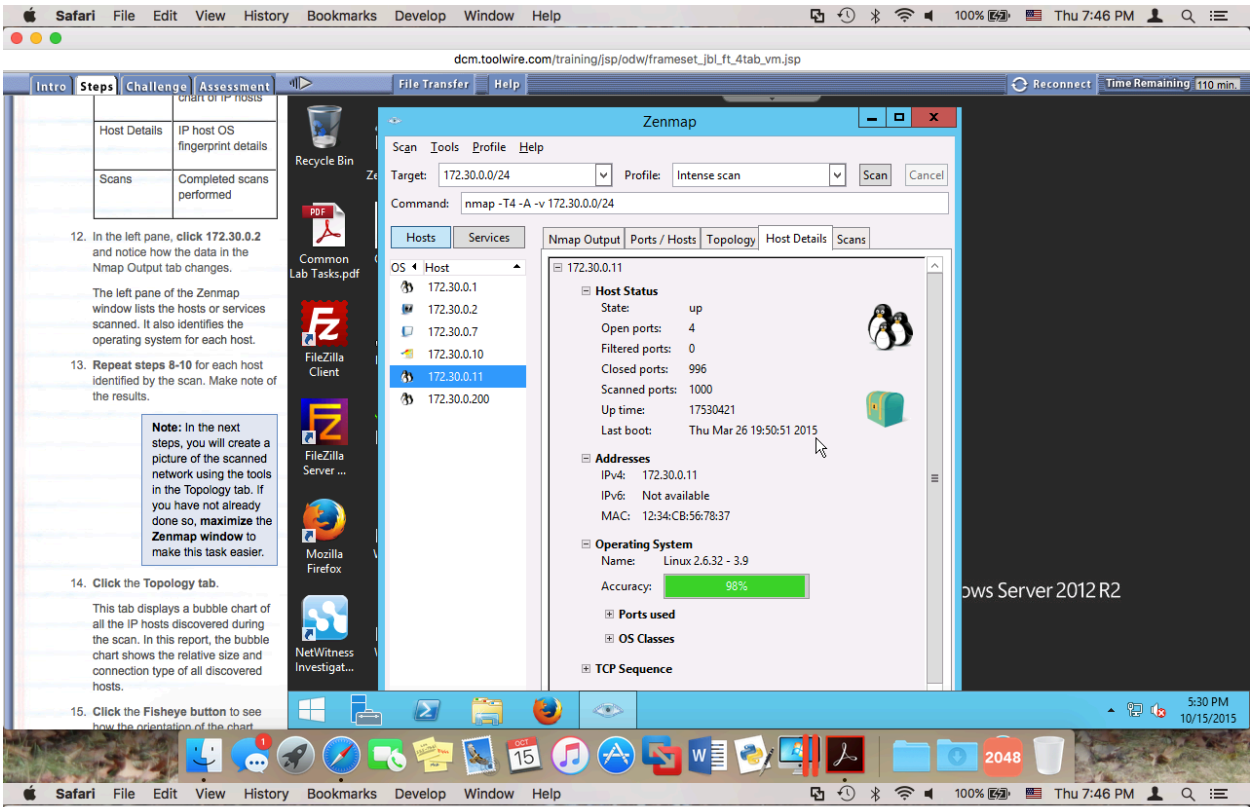

Safari File Edit View History Bookmarks Develop Window Help
100% Thu 7:45 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 111 min.
The Intense scan is actually a collection of several individual tests. The Nmap Output tab shows the raw output, including the name of each scan and its results (for example, the first scan in the report, the ARP Ping Scan, found 255 hosts on the subnet.) Review the output to identify each test performed by Zenmap.
Figure 20 Intense Scan
10. Click the Ports/Hosts tab and review the data, being sure to look for the information described in the following table. Make note of the results; you will use this data to complete the deliverables for this lab.
11. Repeat step 9 for each of the tabs on the Zenmap scan.
Tab
Data 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
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls Save Graphic
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
ows Server 2012 R2
5:29 PM
10/15/2015

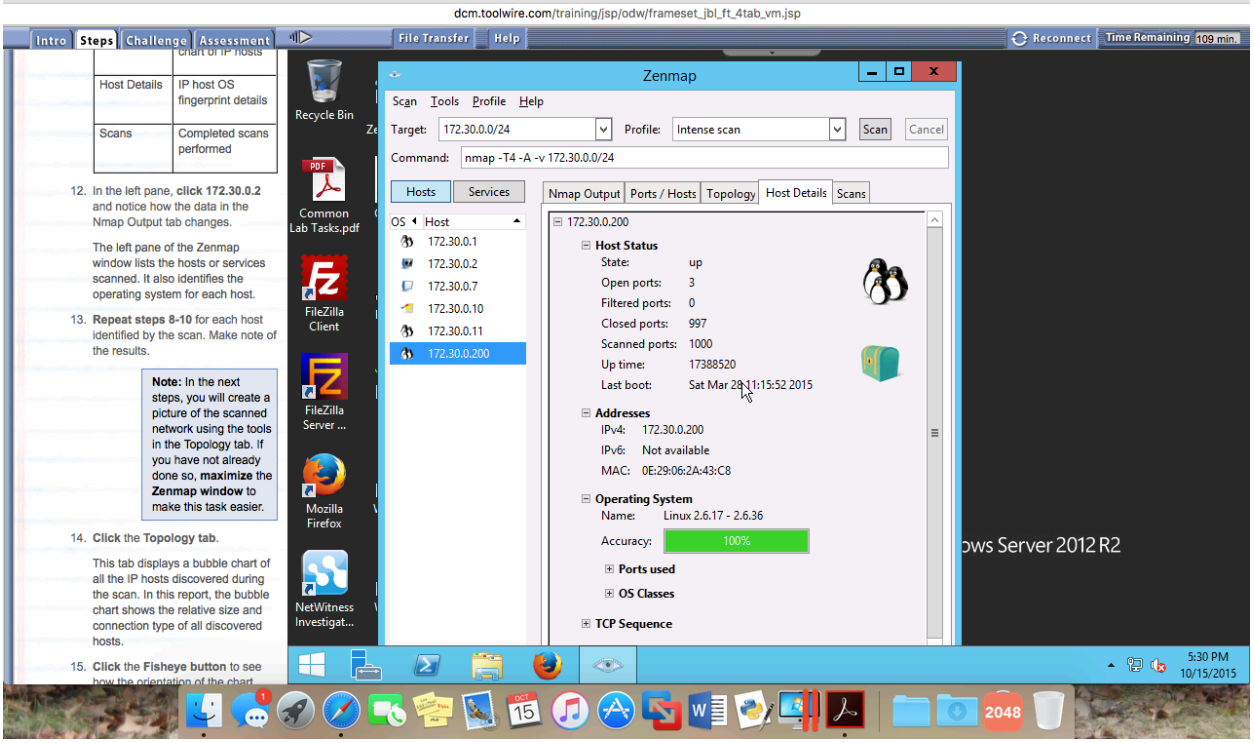

Safari File Edit View History Bookmarks Develop Window Help
100% Thu 7:45 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 110 min.
The Intense scan is actually a collection of several individual tests. The Nmap Output tab shows the raw output, including the name of each scan and its results (for example, the first scan in the report, the ARP Ping Scan, found 255 hosts on the subnet.) Review the output to identify each test performed by Zenmap.
Figure 20 Intense Scan
10. Click the Ports/Hosts tab and review the data, being sure to look for the information described in the following table. Make note of the results; you will use this data to complete the deliverables for this lab.
11. Repeat step 9 for each of the tabs on the Zenmap scan.
Tab | Data 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
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 997
Scanned ports: 1000
Up time: 17248853
Last boot: Mon Mar 30 02:03:39 2015
Addresses
IPv4: 172.30.0.1
IPv6: Not available
MAC: 0E:29:06:2A:43:C8
Operating System
Name: Linux 2.6.17 - 2.6.36
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
ows Server 2012 R2
5:29 PM 10/15/2015

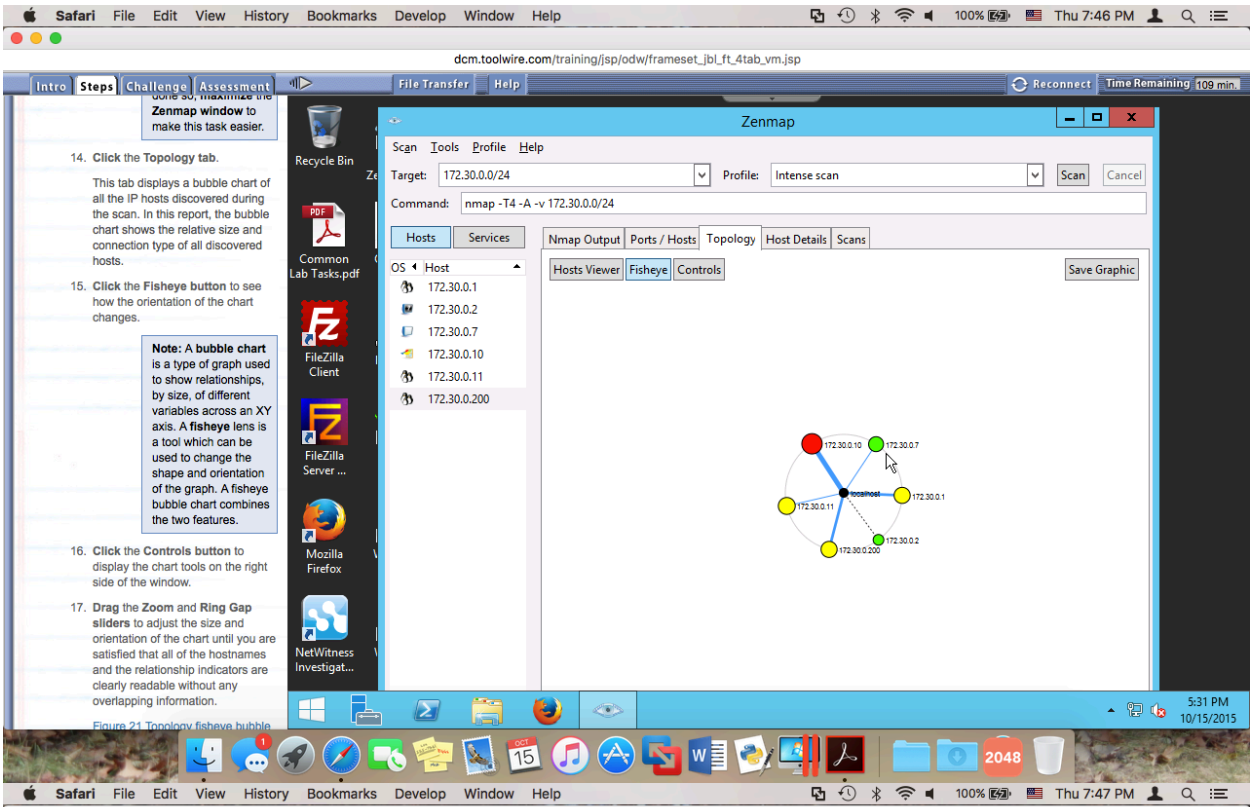
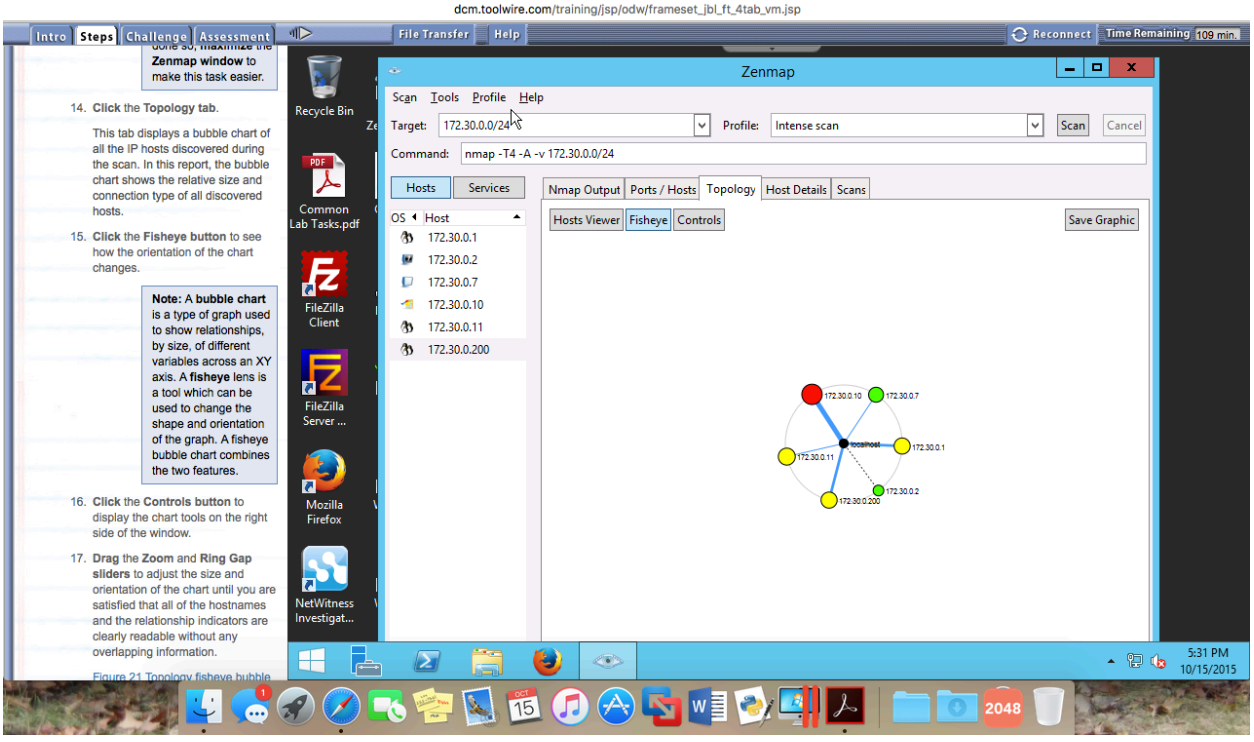

Safari File Edit View History Bookmarks Develop Window Help
100% Thu 7:46 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 110 min.
Host Details | IP host OS fingerprint details
Scans | Completed scans performed
12. In the left pane, click 172.30.0.2 and notice how the data in the Nmap Output tab changes.
The left pane of the Zenmap window lists the hosts or services scanned. It also identifies the operating system for each host.
13. Repeat steps 8-10 for each host identified by the scan. Make note of the results.
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.
14. 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.
15. Click the Fisheye button to see
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
172.30.0.2
Host Status
State: up
Open ports: 0
Filtered ports: 0
Closed ports: 0
Scanned ports: 1000
Up time: Not available
Last boot: Not available
Addresses
IPv4: 172.30.0.2
IPv6: Not available
MAC: Not available
Comments
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
ows Server 2012 R2
5:30 PM 10/15/2015

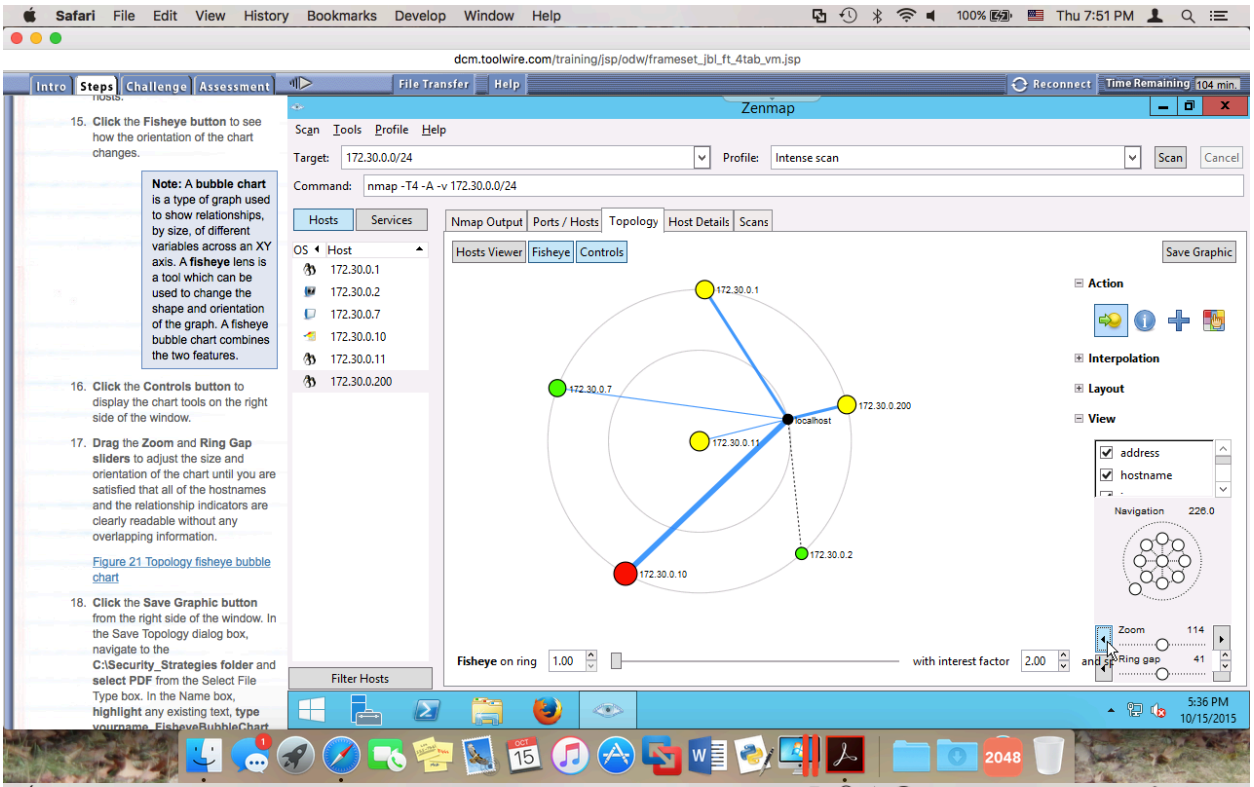

Safari File Edit View History Bookmarks Develop Window Help
Thu 7:46 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 110 min.
Host Details IP host OS fingerprint details
Scans Completed scans performed
12. In the left pane, click 172.30.0.2 and notice how the data in the Nmap Output tab changes.
The left pane of the Zenmap window lists the hosts or services scanned. It also identifies the operating system for each host.
13. Repeat steps 8-10 for each host identified by the scan. Make note of the results.
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.
14. 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.
15. Click the Fisheye button to see
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
172.30.0.7
Host Status
State: up
Open ports: 2
Filtered ports: 0
Closed ports: 998
Scanned ports: 1000
Up time: 17248860
Last boot: Mon Mar 30 02:03:32 2015
Addresses
IPv4: 172.30.0.7
IPv6: Not available
MAC: 92:9C:8F:35:E1:ED
Operating System
Name: Netgear DG834G WAP or Western Digital WD TV m
Accuracy: 96%
Ports used
OS Classes
TCP Sequence
ows Server 2012 R2
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
5:30 PM
10/15/2015

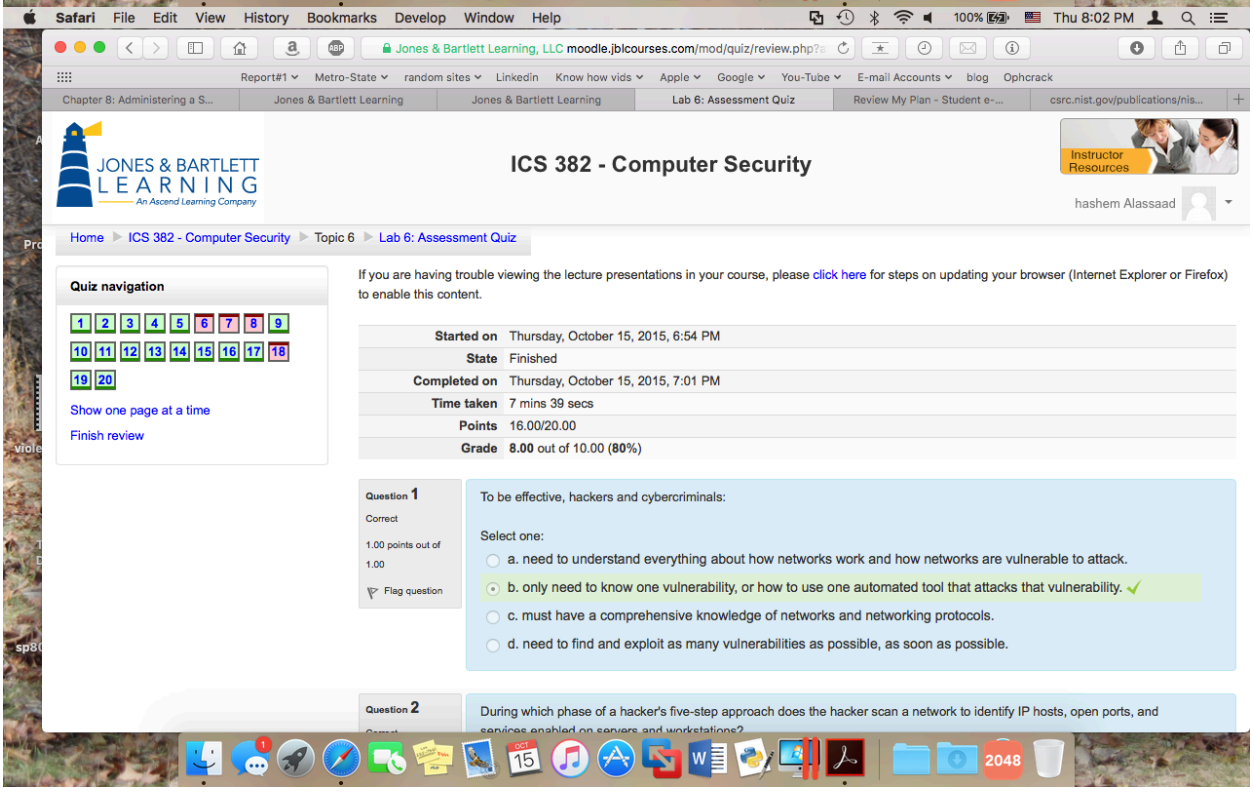

Safari File Edit View History Bookmarks Develop Window Help
Thu 7:46 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 110 min.
Host Details IP host OS fingerprint details
Scans Completed scans performed
12. In the left pane, click 172.30.0.2 and notice how the data in the Nmap Output tab changes.
The left pane of the Zenmap window lists the hosts or services scanned. It also identifies the operating system for each host.
13. Repeat steps 8-10 for each host identified by the scan. Make note of the results.
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.
14. 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.
15. Click the Fisheye button to see
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
172.30.0.10
Host Status
State: up
Open ports: 11
Filtered ports: 0
Closed ports: 989
Scanned ports: 1000
Up time: 258
Last boot: Thu Oct 15 17:20:14 2015
Addresses
IPv4: 172.30.0.10
IPv6: Not available
MAC: DE:8A:12:F1:39:43
Operating System
Name: Microsoft Windows 7 or Windows Server 2012
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
ows Server 2012 R2
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
5:30 PM
10/15/2015


Safari File Edit View History Bookmarks Develop Window Help
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 110 min.
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
172.30.0.11
Host Status
State: up
Open ports: 4
Filtered ports: 0
Closed ports: 996
Scanned ports: 1000
Up time: 17530421
Last boot: Thu Mar 26 19:50:51 2015
Addresses
IPv4: 172.30.0.11
IPv6: Not available
MAC: 12:34:CB:56:78:37
Operating System
Name: Linux 2.6.32 - 3.9
Accuracy: 98%
Ports used
OS Classes
TCP Sequence
Host Details IP host OS fingerprint details
Scans Completed scans performed
12. In the left pane, click 172.30.0.2 and notice how the data in the Nmap Output tab changes.
The left pane of the Zenmap window lists the hosts or services scanned. It also identifies the operating system for each host.
13. Repeat steps 8-10 for each host identified by the scan. Make note of the results.
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.
14. 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.
15. Click the Fisheye button to see
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
ows Server 2012 R2
5:30 PM
10/15/2015


Safari File Edit View History Bookmarks Develop Window Help
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 109 min.
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
172.30.0.200
Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 997
Scanned ports: 1000
Up time: 17388520
Last boot: Sat Mar 28 11:15:52 2015
Addresses
IPv4: 172.30.0.200
IPv6: Not available
MAC: 0E:29:06:2A:43:C8
Operating System
Name: Linux 2.6.17 - 2.6.36
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
Host Details IP host OS fingerprint details
Scans Completed scans performed
12. In the left pane, click 172.30.0.2 and notice how the data in the Nmap Output tab changes.
The left pane of the Zenmap window lists the hosts or services scanned. It also identifies the operating system for each host.
13. Repeat steps 8-10 for each host identified by the scan. Make note of the results.
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.
14. 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.
15. Click the Fisheye button to see
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
ows Server 2012 R2
5:30 PM
10/15/2015


Safari File Edit View History Bookmarks Develop Window Help
Thu 7:46 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 109 min.
Zenmap window to make this task easier.
14. 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.
15. Click the Fisheye button to see how the orientation of the chart changes.
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.
16. Click the Controls button to display the chart tools on the right side of the window.
17. 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.
Figure 21 Topology fisheye bubble
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Save Graphic
localhost
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
5:31 PM
10/15/2015
Safari File Edit View History Bookmarks Develop Window Help
Thu 7:47 PM
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp

Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 109 min.
Zenmap window to make this task easier.
14. 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.
15. Click the Fisheye button to see how the orientation of the chart changes.
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.
16. Click the Controls button to display the chart tools on the right side of the window.
17. 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.
Figure 21 Topology fisheye bubble
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Save Graphic
localhost
Recycle Bin
Common Lab Tasks.pdf
FileZilla Client
FileZilla Server ...
Mozilla Firefox
NetWitness Investigat...
5:31 PM
10/15/2015


Safari File Edit View History Bookmarks Develop Window Help
dcm.toolwire.com/training/jsp/odw/frameset_jbl_ft_4tab_vm.jsp
Intro Steps Challenge Assessment
File Transfer Help
Reconnect Time Remaining 104 min
15. Click the Fisheye button to see how the orientation of the chart changes.
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.
16. Click the Controls button to display the chart tools on the right side of the window.
17. 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.
Figure 21 Topology fisheye bubble chart
18. Click the Save Graphic button from the right side of the window. In the Save Topology dialog box, navigate to the C:\Security_Strategies folder and select PDF from the Select File Type box. In the Name box, highlight any existing text, type
Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 172.30.0.0/24
Hosts Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Save Graphic
Action
Interpolation
Layout
View
address
hostname
Navigation 226.0
Zoom 114
Ring gap 41
Fisheye on ring 1.00
with interest factor 2.00
5:36 PM
10/15/2015


Safari File Edit View History Bookmarks Develop Window Help
Thu 8:02 PM
Jones & Bartlett Learning, LLC moodle.jblcourses.com/mod/quiz/review.php?
Chapter 8: Administering a S...
Jones & Bartlett Learning
Jones & Bartlett Learning
Lab 6: Assessment Quiz
Review My Plan - Student e-...
csrc.nist.gov/publications/nis...
JONES & BARTLETT LEARNING
An Ascend Learning Company
ICS 382 - Computer Security
Instructor Resources
hashem Alassaad
Home ▶ ICS 382 - Computer Security ▶ Topic 6 ▶ Lab 6: Assessment Quiz
Quiz navigation
1 2 3 4 5 6 7 8 9
10 11 12 13 14 15 16 17 18
19 20
Show one page at a time
Finish review
If you are having trouble viewing the lecture presentations in your course, please click here for steps on updating your browser (Internet Explorer or Firefox) to enable this content.
Started on Thursday, October 15, 2015, 6:54 PM
State Finished
Completed on Thursday, October 15, 2015, 7:01 PM
Time taken 7 mins 39 secs
Points 16.00/20.00
Grade 8.00 out of 10.00 (80%)
Question 1
Correct
1.00 points out of 1.00
Flag question
To be effective, hackers and cybercriminals:
Select one:
a. need to understand everything about how networks work and how networks are vulnerable to attack.
b. only need to know one vulnerability, or how to use one automated tool that attacks that vulnerability.
c. must have a comprehensive knowledge of networks and networking protocols.
d. need to find and exploit as many vulnerabilities as possible, as soon as possible.
Question 2
During which phase of a hacker's five-step approach does the hacker scan a network to identify IP hosts, open ports, and