

Implementing Security Policies on Windows and Linux

OBJECTIVE:

CompTIA Security+ Domain:

Domain 2: Compliance and Operational Security

CompTIA Security+ Objective Mapping:

Objective 2.2: Summarize the security implications of integrating systems and data with third parties.

Objective 2.3: Given a scenario, implement appropriate risk mitigation strategies.

Objective 2.8: Summarize risk management best practices.

OVERVIEW:

In this lab, you will secure operating systems running Microsoft Windows and Linux. Security holes in operating systems can lead to attackers compromising your system.

Key Term Description

netplwiza command in Windows that will allow you to set logon parametersgpedit.mscopens the Group Policy Management Console on a Microsoft Windows operating systemEvent Viewercontains log files that contain information about activities on the computertelnetallows remote administration of Linux and Windows systems through the command lineuseradda command to add a user on a Linux/Unix system

Reading Assignment

Introduction

In this lab, you will secure operating systems running Microsoft Windows and Linux. You will learn how to secure the logon process and also use the highly vulnerable Metasploitable machine (from Rapid7) to do some basic security hardening on Linux.



FIGURE 1 - LAB TOPOLOGY FOR IMPLEMENTING SECURITY POLICIES ON WINDOWS AND LINUX

A system administrator's job can include administering, monitoring, configuring, as well as protecting an organization's network. A big part of the job today is to protect systems from unwanted attackers. For that reason, system administrators need to be skilled in how different operating systems work, and they need to patch, update, and monitor computers with various operating systems. It is also critical that they monitor networks for unwanted and unneeded traffic. There are a lot of tools, open-source and commercial tools, available to system administrators today to help them monitor networks, patch, and update systems.

System administrators must address security holes and vulnerabilities. Security holes in operating systems can lead to attackers compromising your system. There are many areas of weakness and security holes in unsecured operating systems that you need to mitigate to keep your systems safe from attacks. You will learn how to require users to log on to Windows with a username and password. The logon process is the first line of defense in securing operating systems.

Also, behind the scenes, Windows and Linux are monitoring and reporting different events into different logs. A log is a file that tracks significant events that occur when using an operating system. In some cases, Windows and Linux will track unsuccessful logons. Event Viewer is a Windows tool that allows you to review different logs that are created by Windows to track significant events that occur on a system. The three main event logs for the Windows Event Viewer are the Application, Security, and System logs, although other relevant logs may exist depending on the roles and applications in use.

Securing Windows Logon

The logon process is an area of weakness on most operating systems. A computer should not be configured to bypass the logon process. Requiring users to log on with a username and password will keep a system more secure. You can think of the logon process as the first line of defense in cybersecurity.

In this lab, you will force users to logon to Windows with a username and password. Also, you will enable an initial warning message stating that unauthorized use is prohibited. Organizations use this message to outline some acceptable use policies of an organization. These warning messages can also prevent users from claiming they were unaware of such policies.

Using Logs and the Event Viewer

Monitoring different events of an operating system is an important task of a system administrator. So, logs are set up to track different kinds of events such a logon success and failures as one example. One event is unsuccessful logons. You will learn to set up Windows to track unsuccessful logons. You will use the event viewer to review the events of the logs. Reviewing logs is an important task of a system administrator. A large number of unsuccessful logons can indicate that nefarious activity may be taking place on the system or network.

Securing a Linux system

When you install Linux for the first time, unnecessary ports can be open, and services that may not be needed could be running. Your job as a system administrator is to harden your operating system to minimize the attack vectors which is a path that hackers use to compromise a system.

This lab uses Metasploitable, an intentionally insecure virtual machine that is used to conduct security training as well as test different security monitoring and penetration testing tools.

Recall, the Transmission Control Protocol/Internet Protocol (TCP/IP) networking model consists of four layers: application, transport, network, and data link. Figure 2 shows the different TCP/IP layers. Services run at the application layer and interact with the transport layer using ports. Port numbers are assigned to different services on the operation system. Services, such as file transfer protocol (FTP), telnet, hypertext transport protocol (HTTP), and others use unique port numbers assigned to them by the operating system. FTP has a port number of 21. HTTP has a port number of 80. Telnet uses the port number of 23. These port numbers are how TCP/IP knows how to communicate from the transport layer to the application layer. TCP/IP was not initially designed with security in mind, so these applications are configured by default to send traffic over the network in plaintext. There are newer services that are used in place of the insecure services.

Application (FTP, telnet, HTTP, etc)
Transport (TCP/UDP)
Network (IP)
Data Link

FIGURE 2 - TCP/IP NETWORKING MODEL

One of the most insecure services that run in Linux is called telnet. Telnet is a service that allows you to logon to systems on the network for administration. Telnet communicates over the network in an insecure manner in which usernames and passwords are sent in clear text. With a simple protocol sniffer, you can capture the username and password from a telnet session. Secure Shell (SSH) is the preferred secure way to logon to remote systems for administration.

There is a GUI tool called Zenmap which is a graphical user interface to nmap. Nmap is an open-source tool to allow you to scan your network open ports and their corresponding services as well as for some

types of vulnerabilities. Zenmap and nmap also can be used to discover hosts on a network as well as the open ports and available services for the corresponding hosts.

So, if you want to prevent unencrypted data from transmitting on the network, then you need to configure the firewall to block these unsecure protocols (FTP, Telnet, etc.) and only allow the secure protocols (SSH, etc.) access to the network. You would set up firewall rules to configure your firewall. A part of a system administrator's job is to make sure that you close (block) unnecessary ports from accessing your network. If you leave these ports open, your systems are more likely to be vulnerable, allowing attackers to compromise your network.



FIGURE 3 - FIREWALL

The firewall can setup rules at different levels of the TCP/IP protocol stack.

The iptables command is a special utility that allows you to create IP packet filter rules for the Linux kernel firewall. You will use iptables to block all open ports on a system except port 80 which runs a protocol called http (hypertext transfer protocol) for your web browser.

CONCLUSION:

In this lab, you will learn to secure Windows logon and services on Linux. You will use tools such as zenmap/nmap, metasploitable, and iptables.

Securing the Windows Logon Process

1. Click on the internal Windows 10 icon on the topology. **Right-click** on the Windows key, **click** Shut down or sign out, and **select** Sign out.



2. Try to log on as student by **clicking** the arrow. Logging on as student fails because the password has not been entered correctly into the password box. **Click** OK.

Note: If anytime during this lab, the desktop displays a screen with the time, **click** on the screen.





FAILED LOG ON

3. **Click** the Power button icon in the right-hand corner of the screen and **click** Restart.



RESTART

4. When the machine reboots, it automatically logs back into Windows.



- AUTO LOGON
 - 5. **Right-click** on the cmd Shortcut and **select** Run as administrator.



RUN AS ADMINISTRATOR

6. **Type** the following command and **press** Enter to launch the User Accounts login configuration.

C:\Windows\system32>Netplwiz.exe

Indows\system3.	2 Netplwiz.exe	
Accounts		
s Advanced		
Use the list below and to change part Users must enter a user i	to grant or deny users access to swords and other settings. name and password to use this	o your computer,
lser Name	Group	
Administrator	Administrators Administrators; Us	ers
student	Administrators Administrators; Us	ers
student	Administrators Administrators; Us A <u>d</u> d <u>R</u> emove	ers Pr <u>o</u> pertie

NETPLWIZ.EXE

7. Place a check in the box that states "Users must enter a user name and password to use this computer." **Click** OK.

User Accounts		5	×
Users Advanced			
Use the list below and to change pa	to grant or deny sswords and oth	/ users access to yo er settings.	our computer,
Users must <u>e</u>nter a user	name and passv	vord to use this cor	mputer.
Users for this computer:			
User Name	Gro	up	
Sector Administrator	Adr	ninistrators	
🔩 student	Adr	ninistrators; Users	
	A <u>d</u> d	<u>R</u> emove	Pr <u>o</u> perties
-Password for Administrat	tor		
To change the	password for Ad	ministrator, click R	eset Password.
		Reset <u>P</u>	assword
	⇔⊑	OK Cance	el <u>A</u> pply

NETPWLIZ

8. **Right-click** on the Windows key, **click** Shut down or sign out, and **select** Restart to restart the Windows 10 machine.



9. After the machine reboots and comes back to the logon screen, **type** password for the password and **click** the arrow to log in.



10. **Right-click** on the cmd - Shortcut and select Run as administrator.



RUN AS ADMINISTRATOR

11. **Type** the following command and **press** Enter to launch the Group Policy Management Console.

C:\Windows\system32>gpedit.msc



12. Click the arrow to expand Computer Configuration.

Click the arrow to expand Windows Settings. Click the arrow to expand Security Settings. Click the arrow to expand Local Policies. Click on Security Options.

Local Group Policy Editor		- 0	\times
File Action View Help			
🗢 🔿 🔁 📷 🔒 🛛 🖬			
Local Computer Policy	^	Policy	Se ^
Computer Configuration		💹 Accounts: Administrator account status	Di
> Software Settings		Accounts: Block Microsoft accounts	Ne
Name Resolution Policy		💹 Accounts: Guest account status	Di
Scripts (Startup/Shutdown)		Accounts: Limit local account use of blank passwords to co	En
> En Deployed Printers		💹 Accounts: Rename administrator account	Ac
Security Settings		💯 Accounts: Rename guest account	Gι
> Account Policies		Audit: Audit the access of global system objects	Di
V 🔀 Local Policies		Audit: Audit the use of Backup and Restore privilege	En
> 🔀 Audit Policy		Audit: Force audit policy subcategory settings (Windows Vis	Nc
User Rights Assignment		Audit: Shut down system immediately if unable to log secur	Di
Security Options		DCOM: Machine Access Restrictions in Security Descriptor D	Ne



13. **Scroll down** using the arrow until you find the Interactive logon section.

File Action View Help <p< th=""><th>Local Group Policy Editor</th><th></th><th></th><th>-</th><th></th><th>×</th></p<>	Local Group Policy Editor			-		×
 Local Computer Policy Security Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Security Settings	File Action View Help					
 Local Computer Policy Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Security Settings Security Settings Security Settings Deployed Printers Security Settings Security Policies Security Options Se	🗢 🔿 🔯 🗟 🔒 🛛 🖬					
	 Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Epoloyed Printers Security Settings Account Policies Local Policies Local Policies Security Options Windows Firewall with Advanced Security Network List Manager Policies Public Key Policies 	< >	Policy Policy Domain member: Digitally encrypt or sign secure channel d Domain member: Digitally encrypt secure channel data (wh Domain member: Digitally sign secure channel data (when Domain member: Disable machine account password chan Domain member: Maximum machine account password age Domain member: Require strong (Windows 2000 or later) se Interactive logon: Display user information when the session Interactive logon: Do not display last user name Interactive logon: Do not require CTRL+ALT+DEL Interactive logon: Machine account lockout threshold Interactive logon: Machine inactivity limit Interactive logon: Message text for users attempting to log on Interactive logon: Message title for users attempting to log on	Security Set Enabled Enabled Disabled 30 days Enabled Not Defined Not Defined Not Defined	d d d	~

SECURITY OPTIONS

14. **Double-click** Interactive logon: Message text for users attempting to log on.



MESSAGE TEXT

15. In the message box, type Unauthorized use is prohibited. Click OK.



MESSAGE TEXT

16. Double-click Interactive logon: Message title for users attempting to log on.



MESSAGE TITLE

17. In the message box, **type** Warning! Click OK.

Interactive logon: Message title for users attempting to lo	?	×
Local Security Setting Explain		
Interactive logon: Message title for users attempting to I	og on	
Waming!		1
OK Cancel	Aţ	oply

MESSAGE TITLE

18. Right-click on the Windows key, click Shut down or sign out, and select Sign out.



SIGN OUT

19. Click on the screen. The Warning! message title and text will be displayed prior to logon. Click OK.



Auditing Logon Failures

1. **Type** 123 for the password and **click** the arrow to log in. (Note: This will fail!)



2. You will receive the message "The password is incorrect. Try again." Click OK.



PASSWORD INCORRECT

3. **Type** password for the password and **click** the arrow to log in.





4. **Right-click** on the Windows key and **select** Computer Management.



COMPUTER MANAGEMENT

5. **Expand** System Tools.

Expand Event Viewer.

Expand Windows Logs. Then **click** on Security.



EVENT VIEWER

6. **Click** View from the menu, and then **select** Add/Remove Columns.

🛃 Computer Management		
File Action View Help		
🗢 🔿 👔 Show Analytic and Debug Logs		
Computer V Preview Pane	Date and Time	Source ^
V 👔 System Sort By	9/15/2016 7:24:31 PM	Micro
> 🕒 lask Group By >	9/15/2016 7:24:31 PM	Micro
Add/Remove Columns	9/15/2016 7:24:31 PM	Micro
Curtomiza	9/15/2016 7:24:31 PM	Micro
	9/15/2016 7:24:31 PM	Micro
Security	9/15/2016 7·24·30 PM	Micros *
Setup		>
System Event 5059, Microsoft Windo	ows security auditing.	×
Forwarded Event		
> 💾 Applications and Se		
Subscriptions		
> 👸 Shared Folders	•	<u>^</u>
> 👰 Local Users and Groups Subject:		
> 📎 Performance Security ID:	SYSTEM	
🚔 Device Manager 🛛 🔹 Account Name	CONCORD\$	
V 🔄 Storage Account Doma	in: WORKGROUP	
Disk Management	UX3E7	
Services and Applications Cryptographic Parameter	rs:	
Provider Name	Microsoft Software Key Storage Provider	

ADD/REMOVE COLUMNS

7. From the Available columns choices, **scroll down** and **select** Event Source Name. **Click** the Add button, and then **click** OK.

🚂 Computer Management		
File Action View Help		
💠 🏟 🖄 🖬 🚺 🖬		
Computer Management (Local V V System Tools) D Task Scheduler V Event Viewer) Custom Views V Mindows Logs Application Security	Level Date and Time Information 9/15/2016 7:44:31 PM Add/Remove Columns 000000000000000000000000000000000000	Source A Micro: Micro: Micro: Micro: Micro: X
Setup Setup System Forwarded Event Applications and Se Subscriptions Subscriptions Shared Folders Service Manager Storage Storage Storage Services and Applications	Ev Available columns: Displayed columns: Operational Code Operational Code Operational Code Log Operational Code Operational Code Processor ID Add -> Event ID Session ID C- Remove Mov Verent Time Verent Correlation Id Mov Processor Time Correlation Id Restore Defaults Restore Defaults Verent Source Name Verent Source Name	ve Up re Down
	Log Name: Security Source: Microsoft Windows security Logged: 9/15/2016 7:44:31 PM	ancel

ADD EVENT SOURCE NAME

8. **Notice** that there are Audit Success logs but no Audit Failure logs listed. To confirm this, **click** on the Keywords Column to sort the keywords alphabetically.



9. Select File from the Computer Management menu and then select Exit.



EXIT

10. Right-click on the cmd - Shortcut and select Run as administrator.



RUN AS ADMINISTRATOR

11. **Type** the following command and **press** Enter to launch the Group Policy Management Console.

C:\Windows\system32>gpedit.msc





12. Click the arrow to expand Computer Configuration.

Click the arrow to expand Windows Settings.Click the arrow to expand Security Settings.Click the arrow to expand Local Policies.Click on Audit Policy and then double-click on Audit account logon events.



SECURITY OPTIONS

13. Check the box that says Failure and then click the OK button.

Audit account logon events Prope	rties	?	×
Local Security Setting Explain			
Audit account logon even	nts		
Audit these attempts:			
Success			
Failure			
This setting might not be e override category level aud for more information, see	nforced if other policy is con at policy. Audit account logon events.	figured to (Q921468)	
	OK Cancel	Арр	y

AUDIT FAILURES

14. **Right-click** on the Windows key, **select** Shut down or sign out, and **click** Sign out.



- SIGN OUT
 - 15. Click on the screen. The Warning! message will be displayed prior to logon. Click OK.

is prohibited	Warning! Unauthorized us
4	ОК
	ОК

MESSAGE TITLE AND TEXT

16. **Type** 123 for the password and **click** the arrow to log in. (Note: This will fail!)



17. You will receive the message "The password is incorrect. Try again." Click OK.



PASSWORD INCORRECT

18. **Type** password for the password and **click** the arrow to log in.





19. **Right-click** on the Windows key and **select** Computer Management.



COMPUTER MANAGEMENT

20. **Expand** System Tools.

Expand Event Viewer. **Expand** Windows Logs. Then **click** on Security.



EVENT VIEWER

21. Click View from the menu, and then select Add/Remove Columns.



ADD/REMOVE COLUMNS

22. From the Available columns choices, **scroll down** and **select** Event Source Name. **Click** the Add button, and then **click OK**.

🚂 Computer Management		
File Action View Help		
🗢 🄿 🖄 🖬 🚺 🖬		
Computer Management (Local System Tools Task Scheduler Event Viewer Sign Custom Views Sign Custom Views Application	Level Date and Time Information 9/15/2016 7:44:31 PM Information 9/15/2016 7:44:31 PM	Source A Micro: Micro: Micro: Micro: Micro: Micro:
Setup Setup Setup Forwarded Event Subscriptions	Add/Remove Columns Add/Remove Columns Available columns: Operational Code Log Computer Process ID Thread ID Processor ID Session ID Kemel Time User Time Processor Time Correlation Id Relative Correlation Id Event Source Name Restore Defaults	Move Up Move Down
	Log Name: Security Source: Microsoft Windows security Logged: 9/15/2016 7:44:31 P	Cancel

ADD EVENT SOURCE NAME

23. **Search** for Audit Failure logs listed. **Click** on the Keywords column to sort the keywords alphabetically. Then **click** on the Audit Failure event to view it.

🕌 Computer Management						
File Action View Help						
🔶 🄿 🞽 📰 🚺						
Computer Management (Local	Keywords	Date and Time		So	urce	^
V IS System Tools	🔒 Audit Failure	9/15/2016 11:44:38 AM		Mi	icrosoft Windows s	-
S Task Scrieduler	K Audit Success	9/15/2016 11:04:52 AM	1	Mi	icrosoft Windows se	e
Custom Views	Audit Success	9/15/2016 11:04:51 AM	4	Mi	icrosoft Windows se	e
Vindows Logs	Audit Success	9/15/2016 11:04:51 AM	4	Mi	icrosoft Windows se	e
Application	Audit Success	9/15/2016 11:04:52 AM	4	Mi	icrosoft Windows se	e
Security	Q Δudit Success	9/15/2016 11·04·57 ΔM	4	Mi	icrosoft Windows s	• ¥
Setup	<				~	
🛃 System	Event 4776, Microsoft	Windows security auditing.				×
Forwarded Event	General Details					
Subscriptions						
> Shared Folders	The computer atte	mpted to validate the credent	tials for an accou	nt.		
> 👰 Local Users and Groups	Authentication Da			CKACE VI O		
> 🔊 Performance	Logon Account:	student	INTICATION_PAG	LKAGE_VI_U		
👜 Device Manager	Source Workstatio	n: CONCORD				
✓ 🚰 Storage	Error Code:	0xC00006A				
Disk Management						
Services and Applications						
	Log Name:	Security				
	Source	Microsoft Windows security	Logged	0/15/2016 11:44:29		
	Source:	windows security	Logged:	9/15/2010 11:44:50		
	Event ID:	4//0	Task Category:	Credential validati	ion	
	Level:	Information	Keywords:	Audit Failure		
	User:	N/A	Computer:	CONCORD		
	OpCode:	Info				
	More Information:	Event Log Online Help				
< >						

24. Select File from the Computer Management menu and then select Exit.



Securing Linux

1. **Right-click** on the cmd - Shortcut and **select** Run as administrator.



RUN AS ADMINISTRATOR

 Type the following command and press Enter, to open Zenmap. After Zenmap opens, type 192.168.1.30 in the Target box and then click the Scan button to launch an intense scan.

C:\Windows\system32>zenmap

Select Administrator: cmd - Shortcut						
Microsoft Windows [Version 10.0.10240] (c) 2015 Microsoft Corporation. All rights reserved.						
C:\Windows\system32>zenmap						
Zenmap	_		×			
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> elp						
Target: 192.168.1.30 Profile: Intense scan 	~	Scan				
Command: nmap -T4 -A -v 192.168.1.30						
ZENMAP						

Note: This scan may take up to 5 minutes to complete. The words Nmap done will then be displayed.

3. After the scan is complete, **click** the Ports / Hosts tab to view the open ports and corresponding banner messages that are displayed. **Notice** that telnet Port 23 is open.

👁 Zenmap — 🗆 X										
Sc <u>a</u> n <u>T</u> o	ols <u>P</u> rofile	<u>H</u> elp								
Target:	192.168.1.30			\sim	Profile:	Intense sc	an	~ S	can 🔇	cancel
Command	d: nmap -T4	-A -v	192.10	58.1.30						
Hosts	Services		Massa	o Outout	Ports / H	osts Ton		otails Scans		
110303			141110	Port 4	Protocol	State 4	Service 4	Version		
OS I Ho	st ·	•		21	tcn	open	ftn	version vsftpd 2.3.4		
(30) 192	2.168.1.30			22	tcp	open	ssh	OpenSSH 4.7p	1 Debiar	n 8ubu
				23	tcp	open	telnet			
				25	tcp	open	smtp	Postfix smtpd		
			•	53	tcp	open	domain	ISC BIND 9.4.2		
			•	80	tcp	open	http	Apache httpd	2.2.8 ((U	(buntu)
			•	111	tcp	open	rpcbind	2 (RPC #10000	0)	
			•	139	tcp	open	netbios-ssn	Samba smbd 3	3.X (worl	kgroup
			•	445	tcp	open	netbios-ssn	Samba smbd 3	3.X (worl	kgroup
			•	512	tcp	open	exec			
			۲	513	tcp	open	login			
			•	514	tcp	open	shell			
			•	1099	tcp	open	java-rmi	Java RMI Regis	stry	
			۲	1524	tcp	open	shell	Metasploitable	e root sh	ell
			•	2049	tcp	open	nfs	2-4 (RPC #100	003)	
			•	3306	tcp	open	mysql	MySQL 5.0.51a	-3ubun	tu5
			•	5432	tcp	open	postgresql	PostgreSQL DI	3 8.3.0 -	8.3.7
			•	6667	tcp	open	irc	Unreal ircd		
			•	8009	tcp	open	ajp13	Apache Jserv (Protoco	l v1.3)
			0	8180	tcp	open	http	Apache Tomo	at/Coyo	te JSP (
Filt	ter Hosts		<							>

PORTS OPEN

4. **Get** the information for below Challenge Flags from the Ports/Hosts tab.

Note: If you do not see the flag numbers next to the corresponding ports for the below Challenge Flags, close the Zenmap window by clicking the X in the top right corner, go back to the Command Prompt, type zenmap, and run the scan again. You might need to run the scan 2 or 3 times.

Challenge #

Challenge #

4. **Select** Scan from the menu bar and then **select** Quit to close Zenmap.



QUIT ZENMAP

5. When asked about Unsaved changes, click Close anyway.

	×
7	Unsaved changes The given scan has unsaved changes. What do you want to do?
	Close anyway <u>C</u> ancel

UNSAVED CHANGES

6. **Type** the following command and **press** Enter, to telnet to the Linux system. Then **press** Enter.

C:\Windows\system32>telnet 192.168.1.30

C:\Windows\system32>telnet 192.168.1.30

TELNET

 Notice that the username and the password are displayed in the banner message. Type msfadmin for the username and msfadmin for the password and click Enter.

NOTE: When typing the password. it will not be dispayed for security reasons.

Telnet 192.168.1.30



8. **Type** the following command and **press** Enter, to add a user to the system. **Type** msfadmin for the password.

mfadmin@metasploitable:~\$ sudo useradd super

msfadmin@metasploitable:~\$ sudo useradd super sudo: unable to resolve host metasploitable [sudo] password for msfadmin:

USERADD COMMAND

 Type the following command to verify that the user exists and determine their UID. Then press Enter.

mfadmin@metasploitable:~\$ id super

msfadmin@metasploitable:~\$ id super uid=1004(super)_gid=1004(super)_groups=1004(super) D_COMMAND

10. **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

Challenge #

Challenge #

Challenge

10. **Type** the following command and **press** Enter, to leave the telnet session.

mfadmin@metasploitable:~\$ exit



11. **Click** on the Metasploitable virtual machine in the topology diagram.



METASPLOITABLE MACHINE

12. Log in as Username: root.

ubuntu
Username:

USERNAME ROOT

13. **Type** msfadmin for the password.

Ubuntu	
Password: msfadmin	

PASSWORD

14. **Click** Continue at the warning message about running as a privileged user.

Running a session as a privileged user should be avoided for security reasons. If possible, you should log in as a normal user.
<u>C</u> ontinue 🍕 Quit

MESSAGE WARNING

15. After the machine takes a minute to fully boot, **open** the terminal by **double-clicking** the Terminal icon on the Metasploitable desktop.



LISTEN

16. **Type** the following command to view the user that was recently created. Then **press** Enter.

root@metasploitable:~# cat /var/log/auth.log | grep super

1	🗖 root@metasploitable: ~ 🗖	
	<u>File E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp	
	root@metasploitable:~# cat /var/log/auth.log grep super	
	Apr 17 15:17:26 metasploitable sudo: msfadmin : TTY=pts/0 ; PWD=/home/msfadmi	in ;
L	USER=root ; COMMAND=/usr/sbin/useradd super	
	Apr 17 15:17:26 metasploitable useradd[6120]: new group: name=super, GID=1004	4
	Apr 17 15:17:26 metasploitable useradd[6120]: new user: name=super, UID=1004	, GI
l	D=1004, home=/home/super, shell=/bin/sh	
/	VAR/LOG/AUTH.LOG	

17. **Type** the following command and **press** Enter, to disallow all traffic to this Linux host.

root@metasploitable:~# iptables -P INPUT DROP

root@metasploitable:~# iptables -P INPUT DROP

18. **Type** the following command to allow web traffic to this Linux host. Then **press** Enter.

root@metasploitable:~# iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

root@metasploitable:~# iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT IPTABLES COMMAND

19. Click on the internal Windows 10 icon on the topology. Then, **right-click** on the cmd - Shortcut and **select** Run as administrator.



WINDOWS 10 MACHINE



RUN AS ADMINISTRATOR

20. **Type** the following command and **press** Enter, to open Zenmap. After Zenmap opens, **type** 192.168.1.30 in the Target box and then **click** the Scan button to launch an intense scan.

C:\Windows\system32>zenmap

ī

Select Administrator: cmd - Shortcut					
Microsoft Windows [Version 10.0.10240] (c) 2015 Microsoft Corporation. All rights reserved.					
C:\Windows\system32>zenmap					
Zenmap	_		×		
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> elp					
Target: 192.168.1.30 V Profile: Intense scan	~	Scan	Ca tel		
Command: nmap -T4 -A -v 192.168.1.30					
ZENMAP					

Note: This scan may take a few minutes to complete. The words Nmap done will then be displayed.

21. After the scan is complete, **click** the Ports / Hosts tab to view the open ports and corresponding banner messages that are displayed. **Notice** that only Port 80 is open.

Zenmap	– 🗆 X
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> elp	
Target: 192.168.1.30 V Profile: Inter	nse scan 🗸 Scan Cancel
Command: nmap -T4 -A -v 192.168.1.30	
Hosts Services Nmap Output Ports / Hosts Topology	Host Details Scans
OS Host Port Protocol State Serv	ce 🖣 Version 🔹 🧃
😚 192.168.1.30 😑 80 tcp open http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
PORT OPEN	

Note: **Press** the STOP button to complete the lab.

 $\ensuremath{\mathbb{C}}$ Infosec Learning, LLC. All rights reserved.