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
netplwiz	a command in Windows that will allow you to set logon parameters
gpedit.msc	opens the Group Policy Management Console on a Microsoft Windows operating system
Event Viewer	contains log files that contain information about activities on the computer
telnet	allows remote administration of Linux and Windows systems through the command line
useradd	a 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.

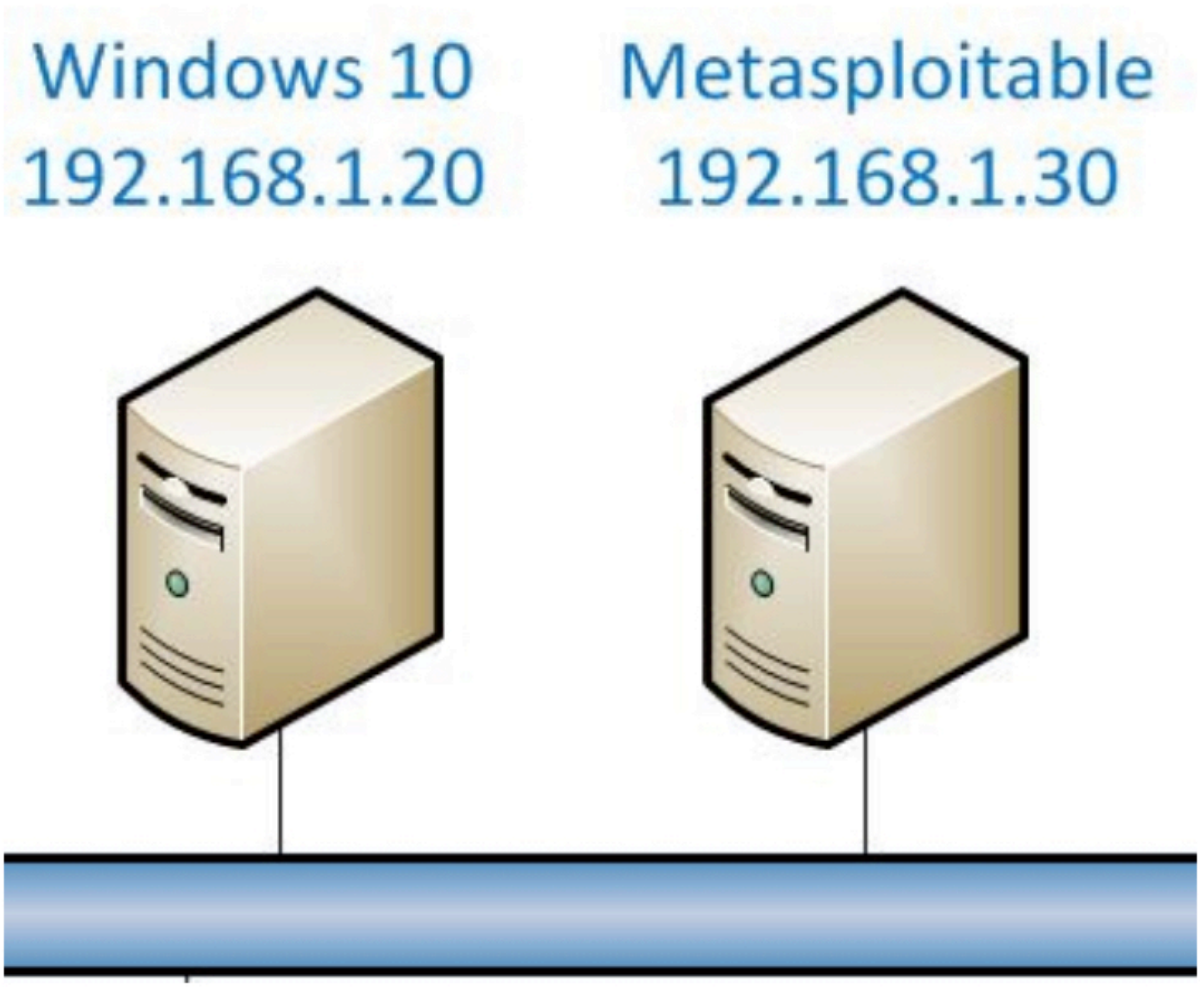


FIGURE 1 – LAB TOPOLOGY FOR IMPLEMENTING SECURITY POLICIES ON WINDOWS AND LINUX

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.

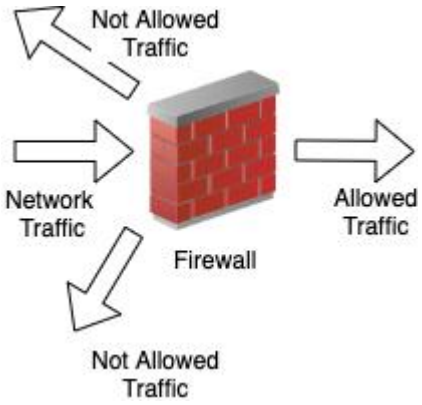


FIGURE 3 – FIREWALL

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

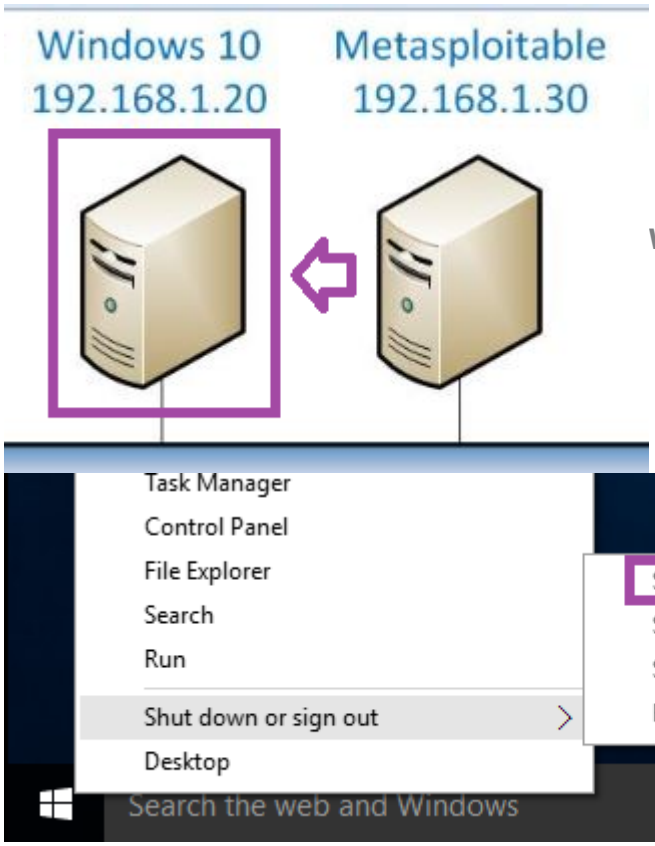
The iptables command is a special utility that allows you to create IP packet filter rules for the Linux kernel firewall. You will use iptables to block all open ports on a system except port 80 which runs a protocol called http (hypertext transfer protocol) for your web browser.

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.

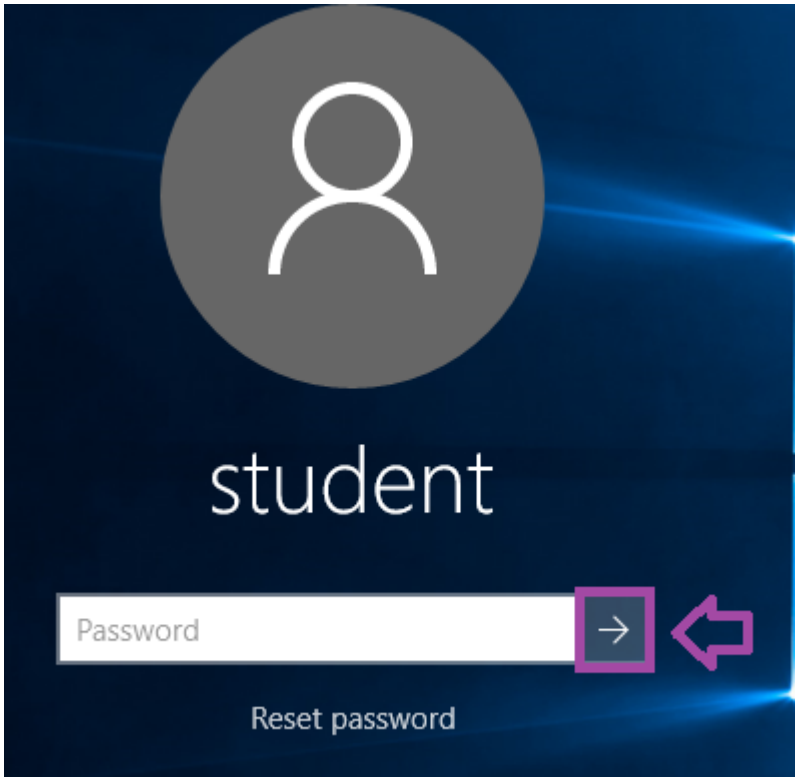


WINDOWS 10 MACHINE

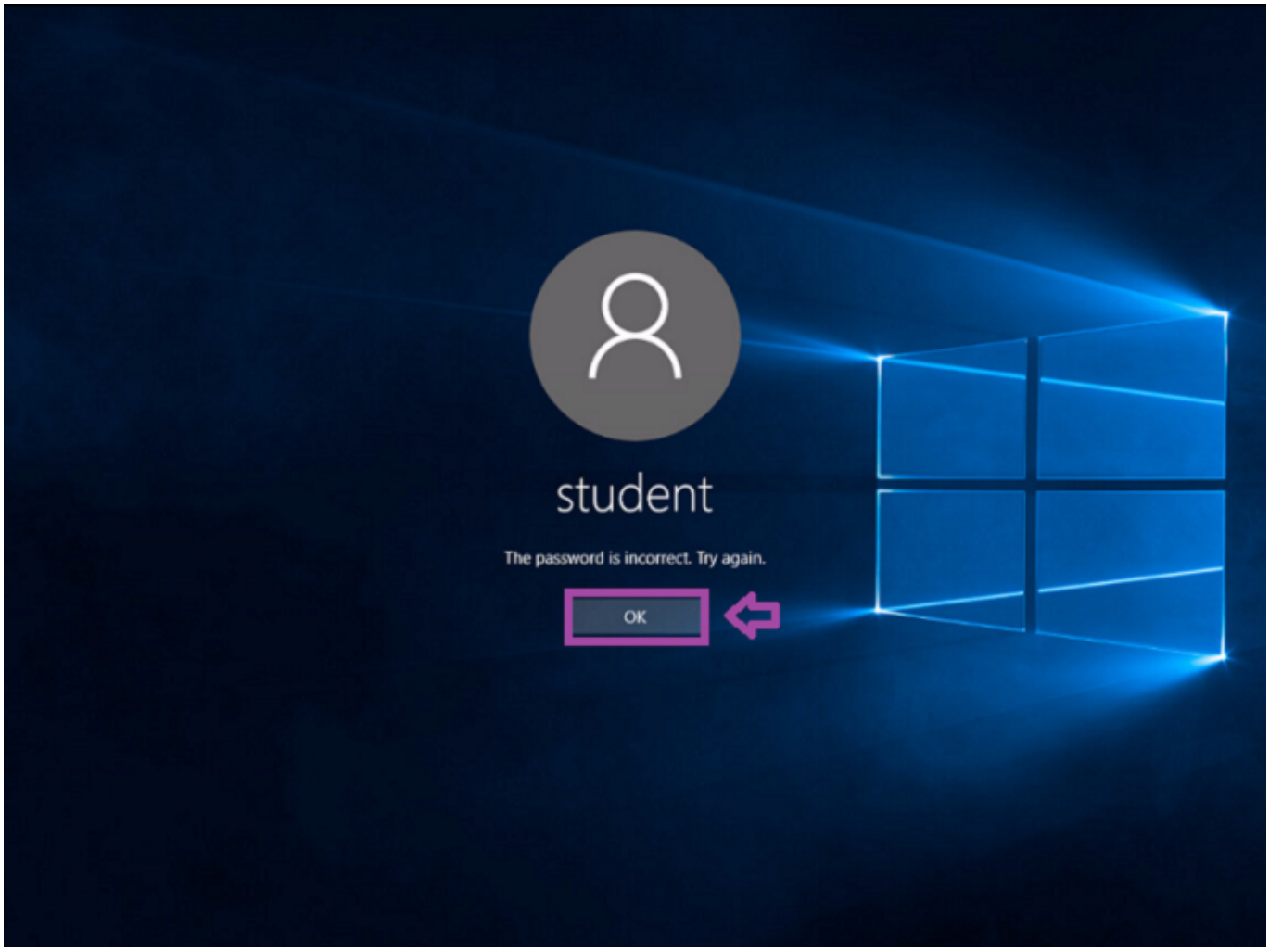
SIGN OUT

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.



LOG ON SCREEN



FAILED LOG ON

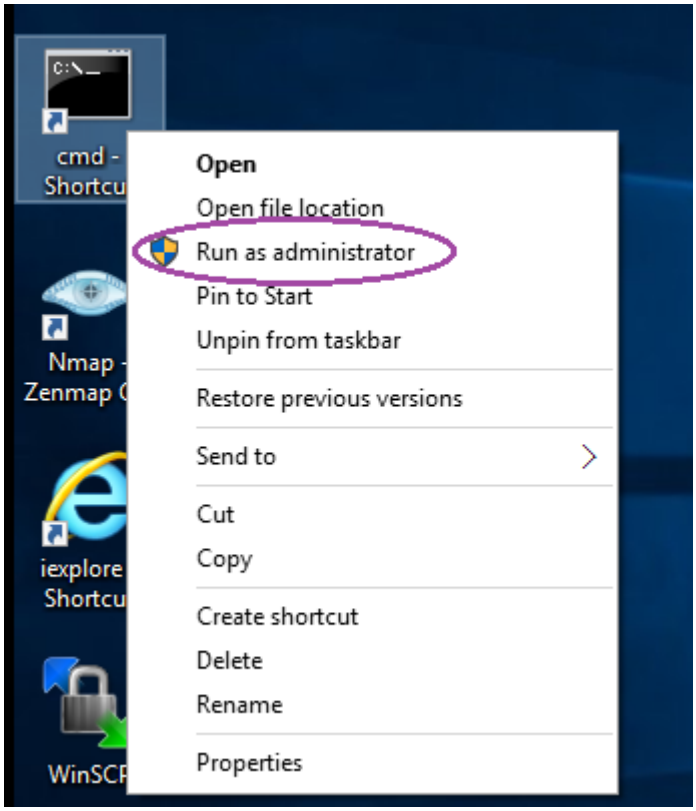
3. **Click** the Power button icon in the right-hand corner of the screen and **click** Restart.

RESTART

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

AUTO LOGON

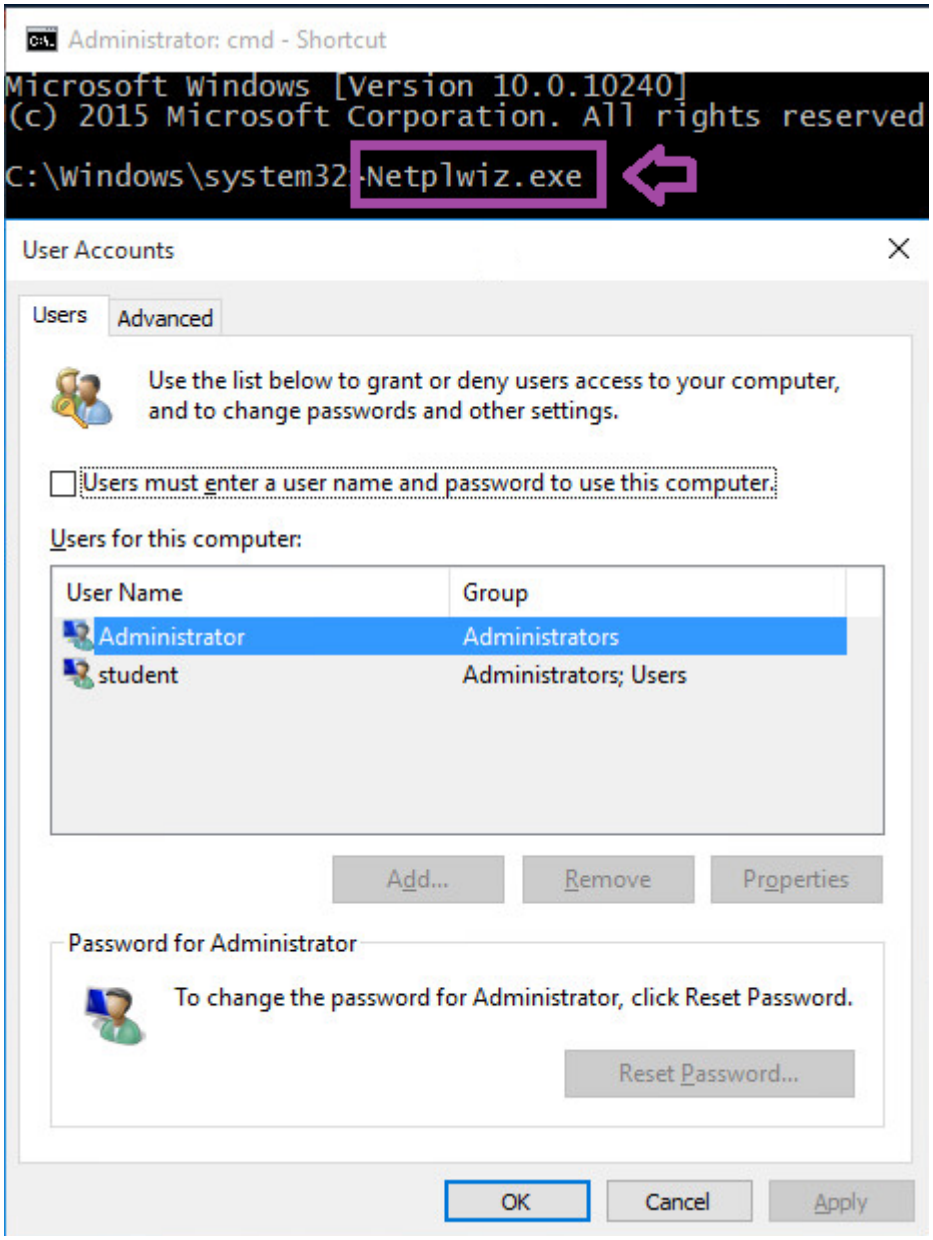
5. **Right-click** on the cmd - Shortcut and **select** Run as administrator.



RUN AS ADMINISTRATOR

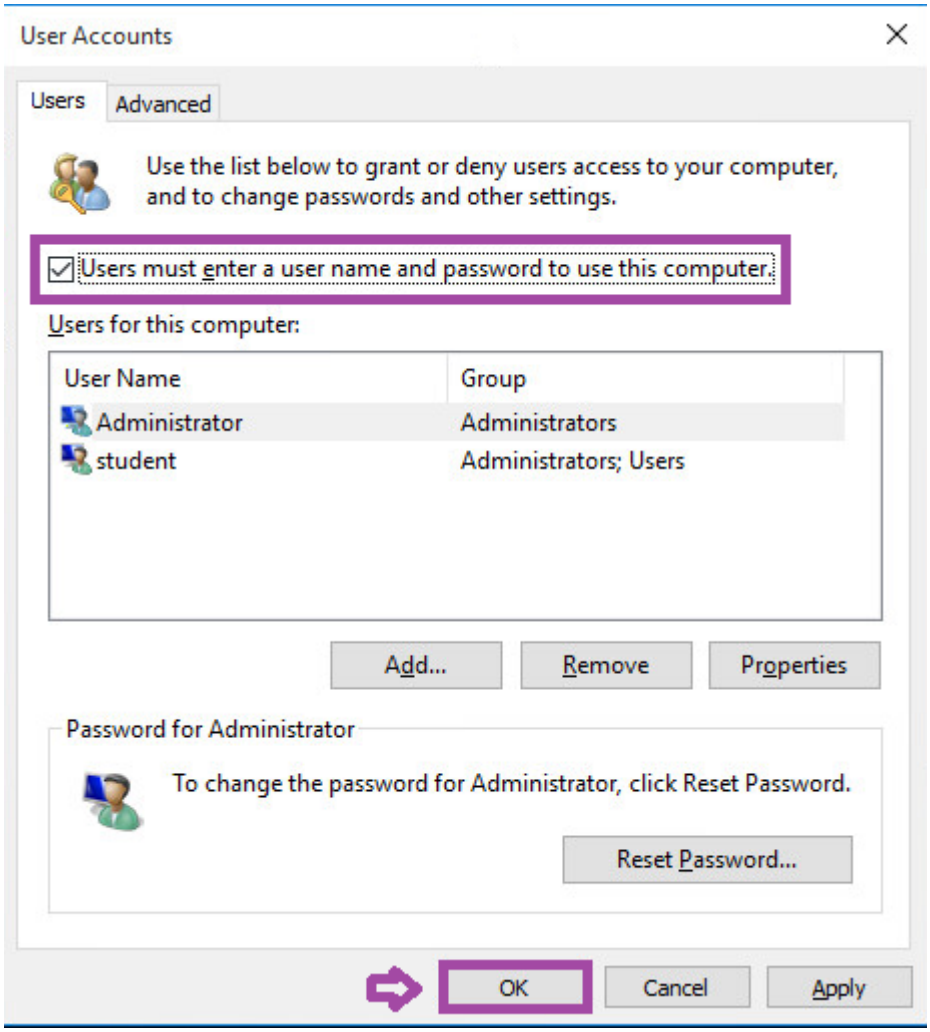
6. **Type** the following command and **press** Enter to launch the User Accounts login configuration.

C:\Windows\system32>`Netplwiz.exe`



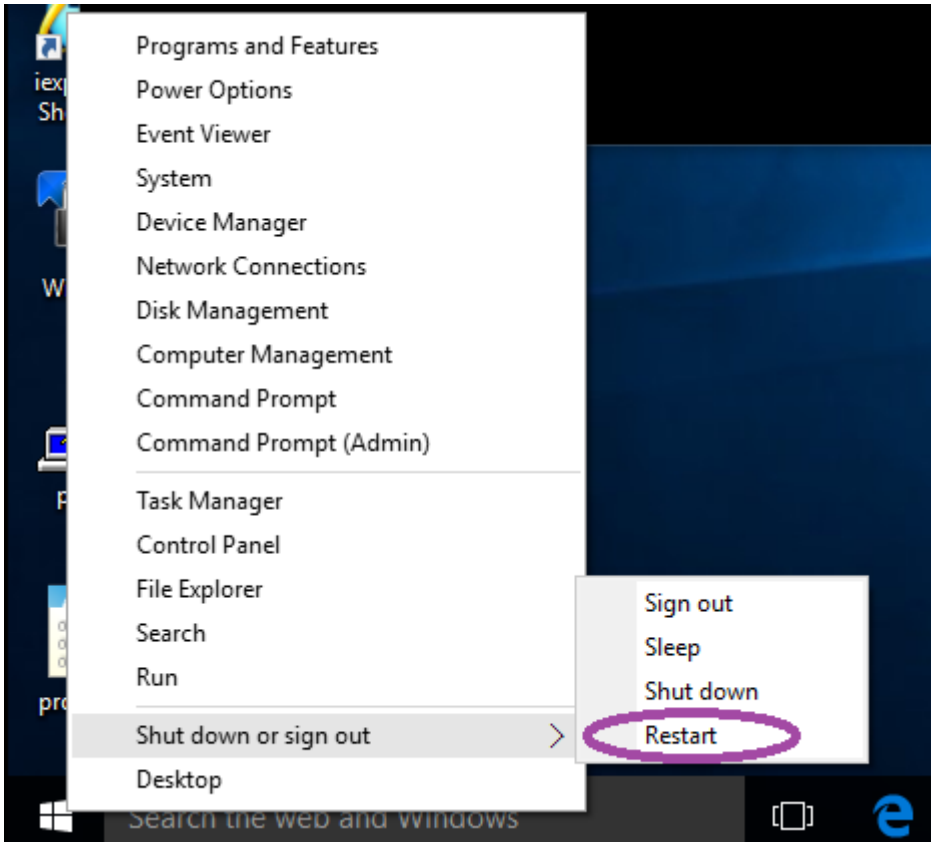
NETPLWIZ.EXE

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



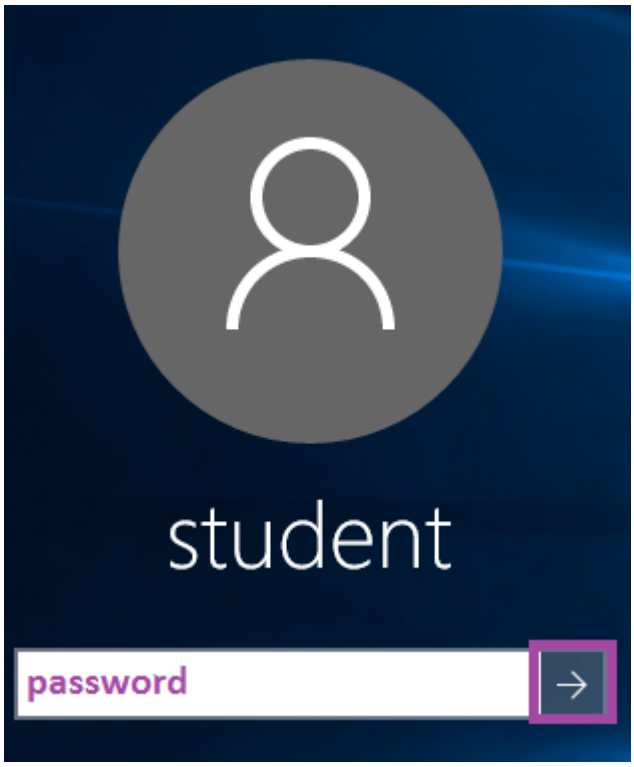
NETPWLIZ

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



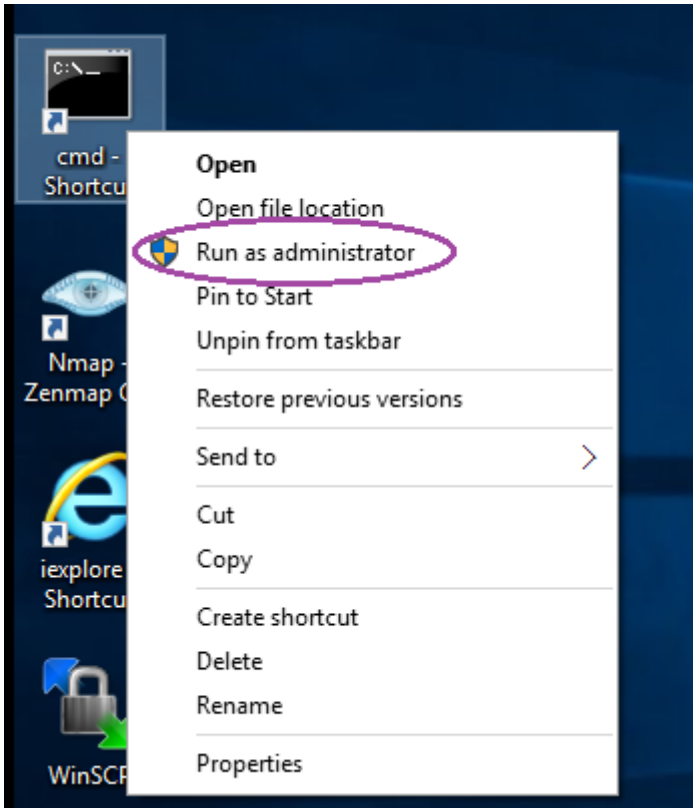
RESTART

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



LOG IN

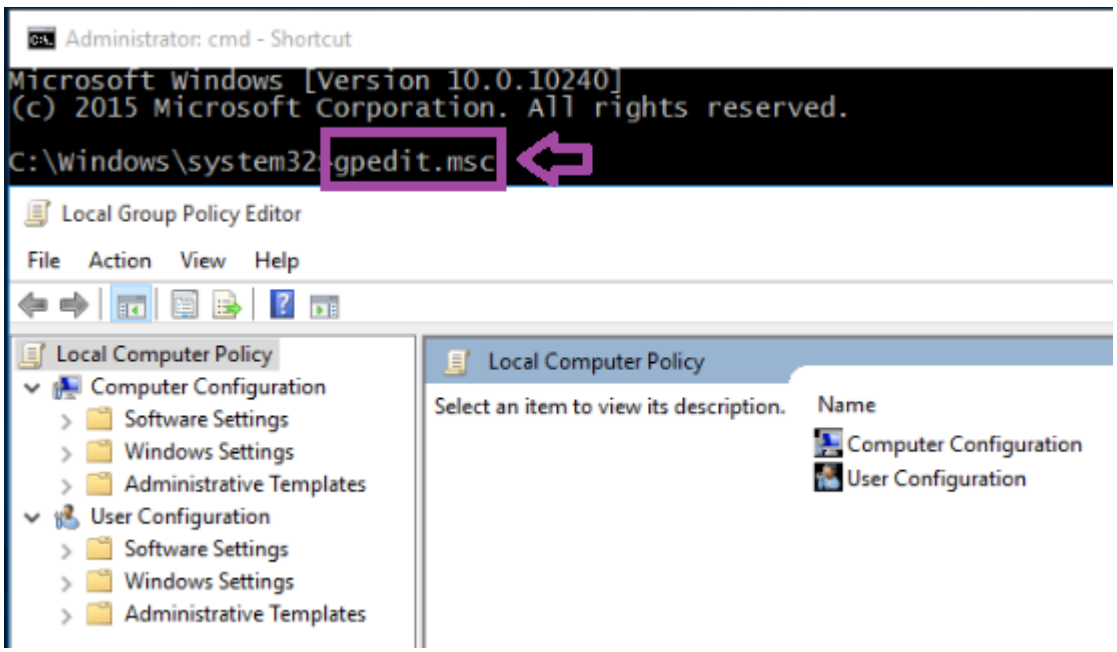
10. **Right-click** on the cmd - Shortcut and **select** Run as administrator.



RUN AS ADMINISTRATOR

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

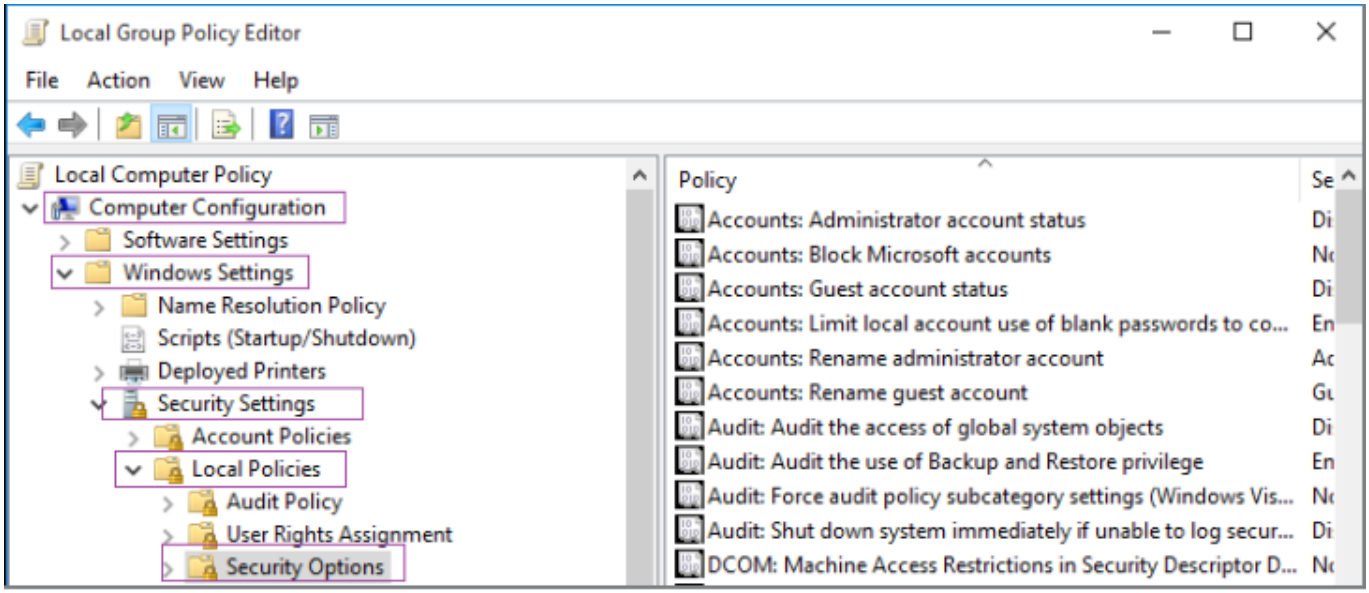
C:\Windows\system32>`gpedit.msc`



GPEDIT.MSC

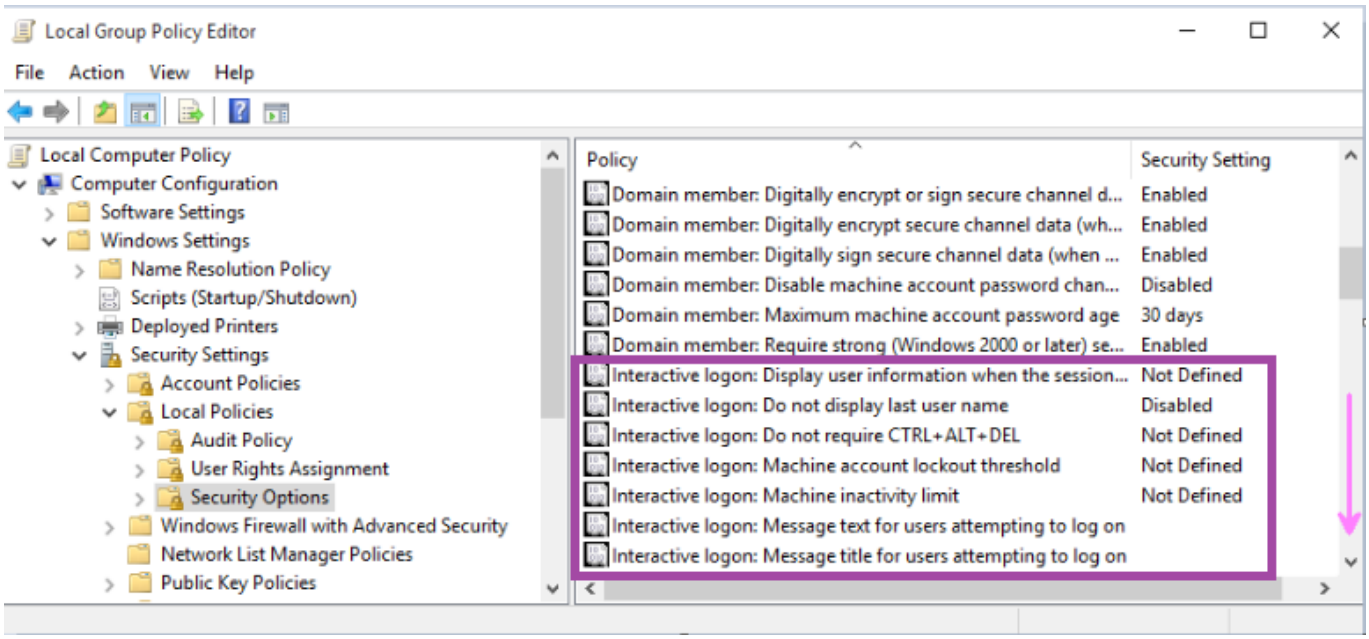
12. **Click** the arrow to expand Computer Configuration.

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.



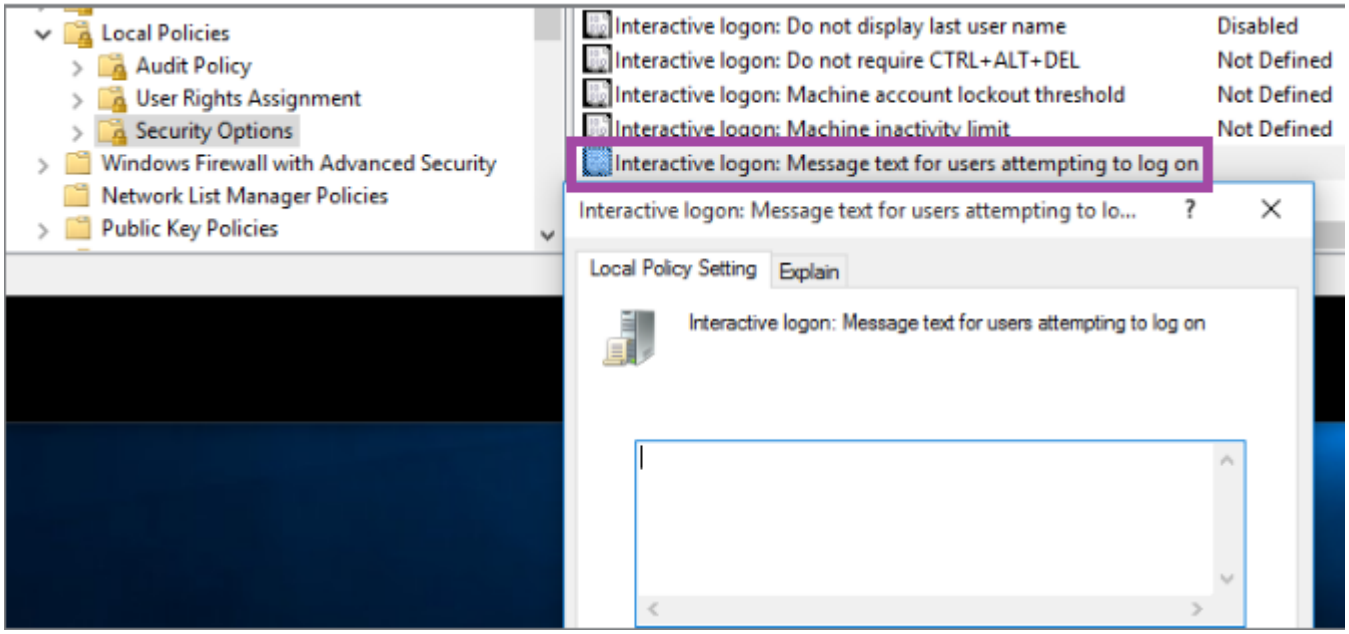
SECURITY OPTIONS

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



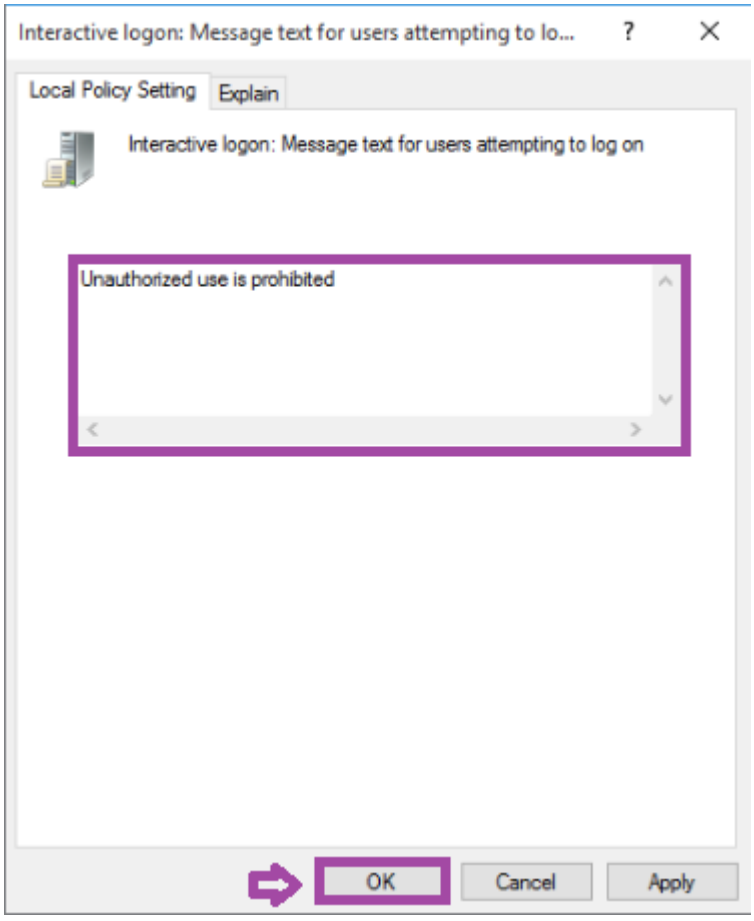
SECURITY OPTIONS

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



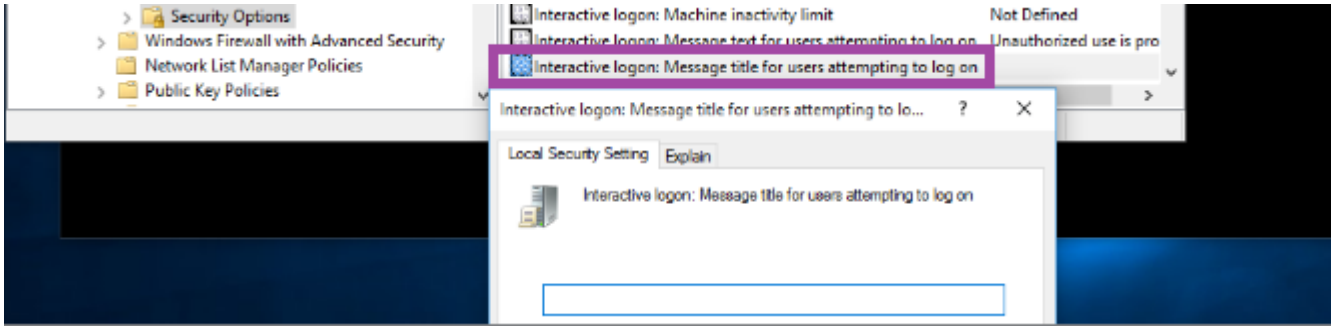
MESSAGE TEXT

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



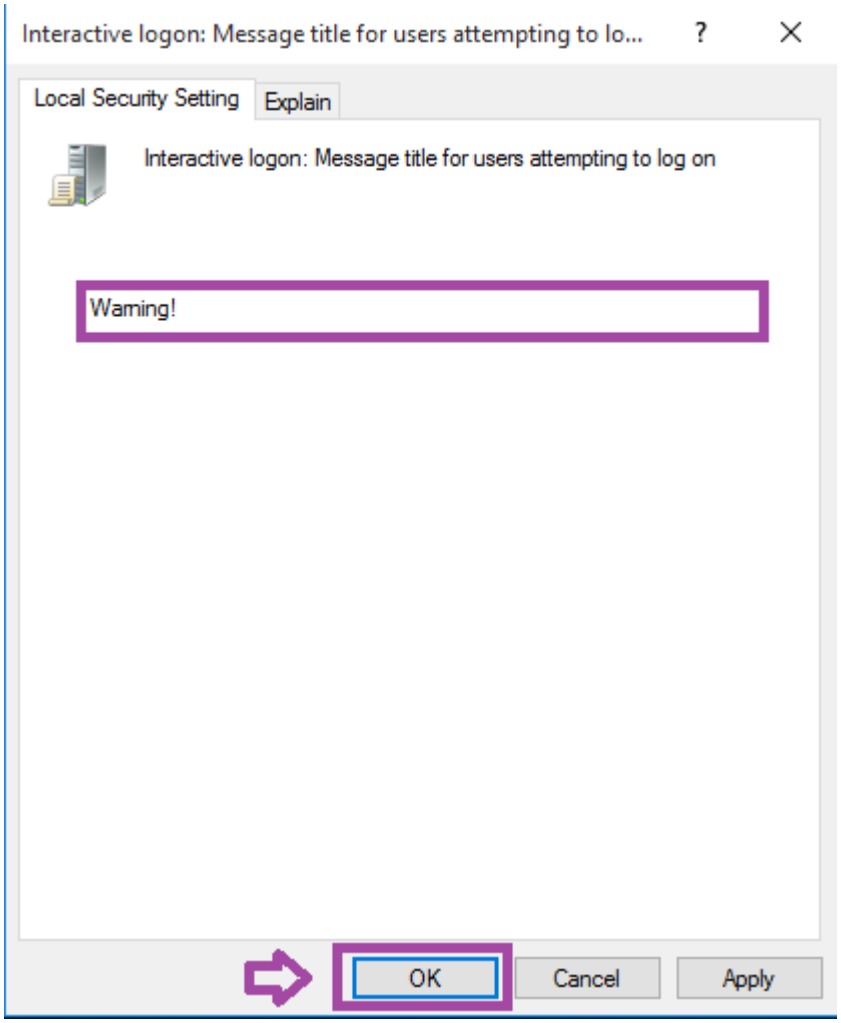
MESSAGE TEXT

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



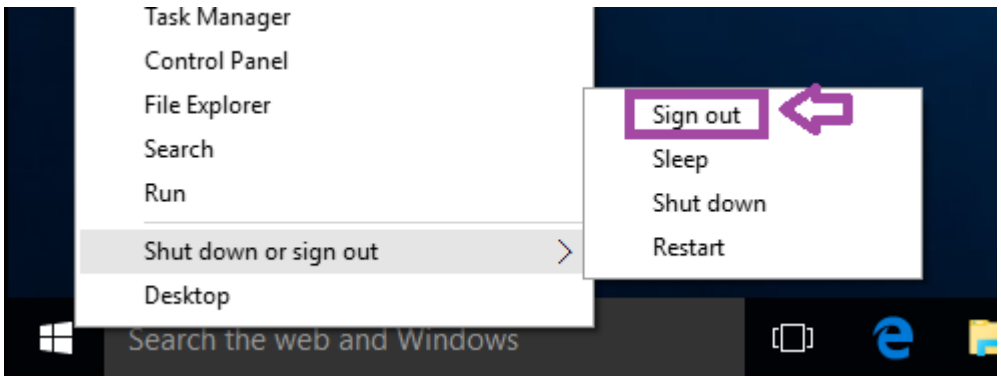
MESSAGE TITLE

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



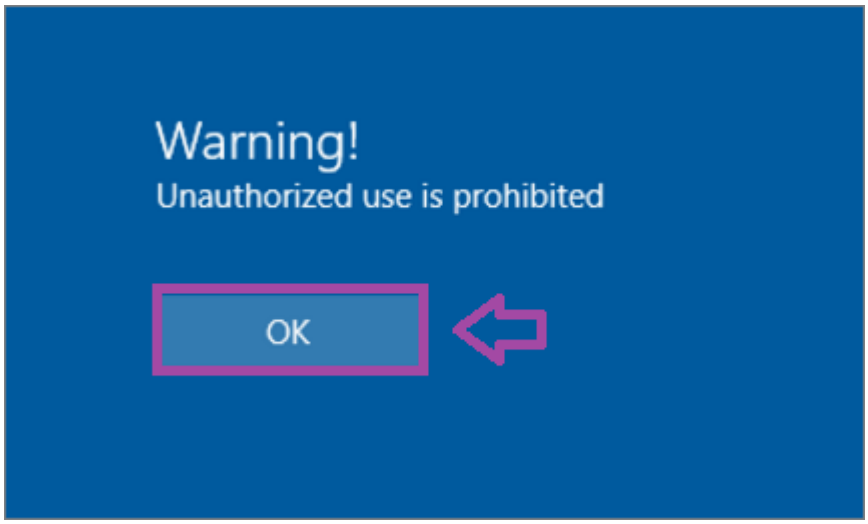
MESSAGE TITLE

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



SIGN OUT

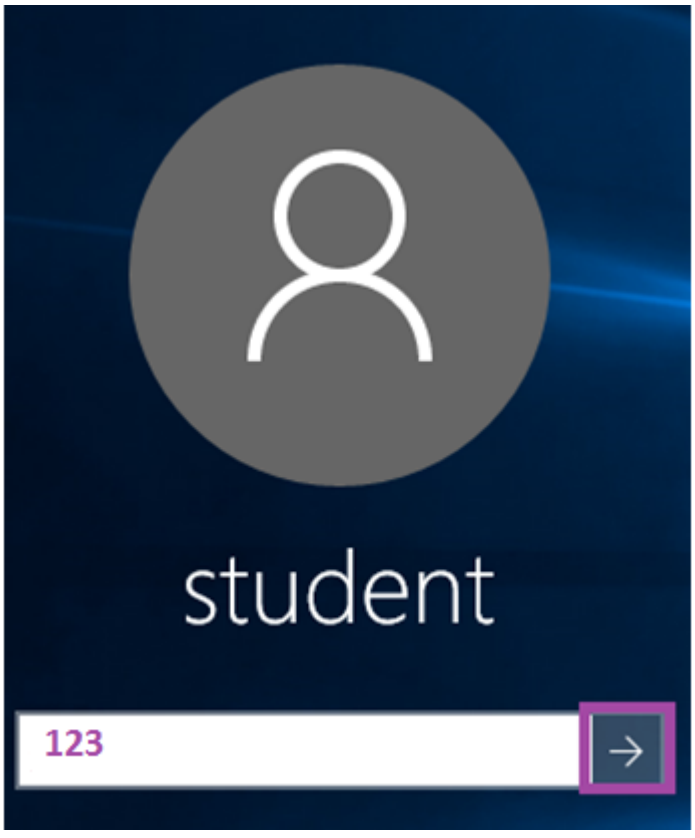
19. **Click** on the screen. The Warning! message title and text will be displayed prior to logon. **Click** OK.



MESSAGE TITLE AND TEXT

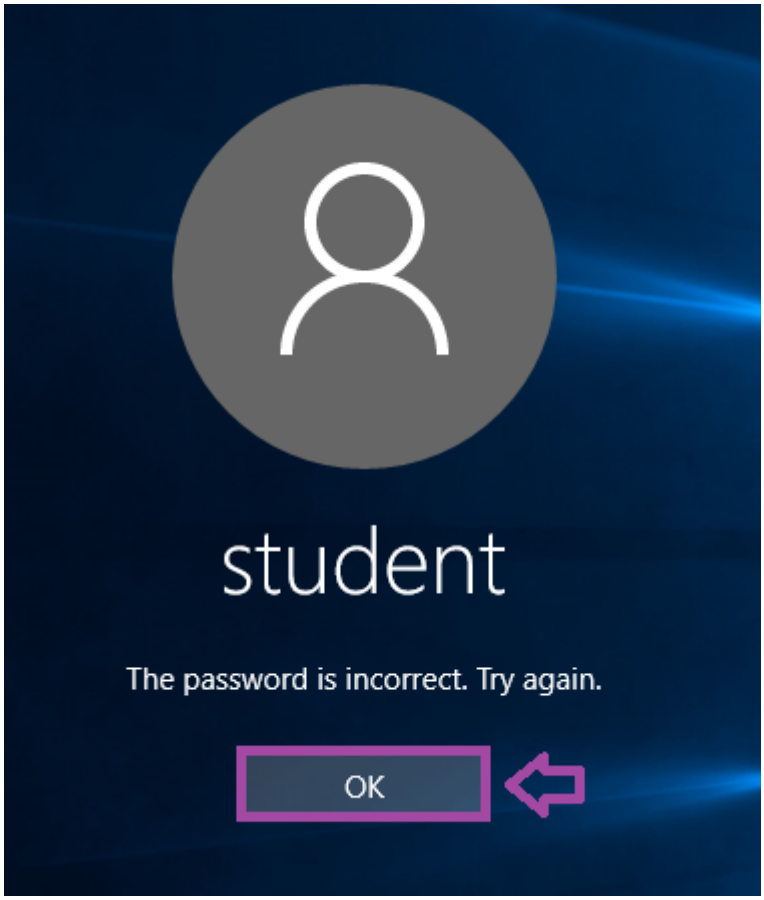
Auditing Logon Failures

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



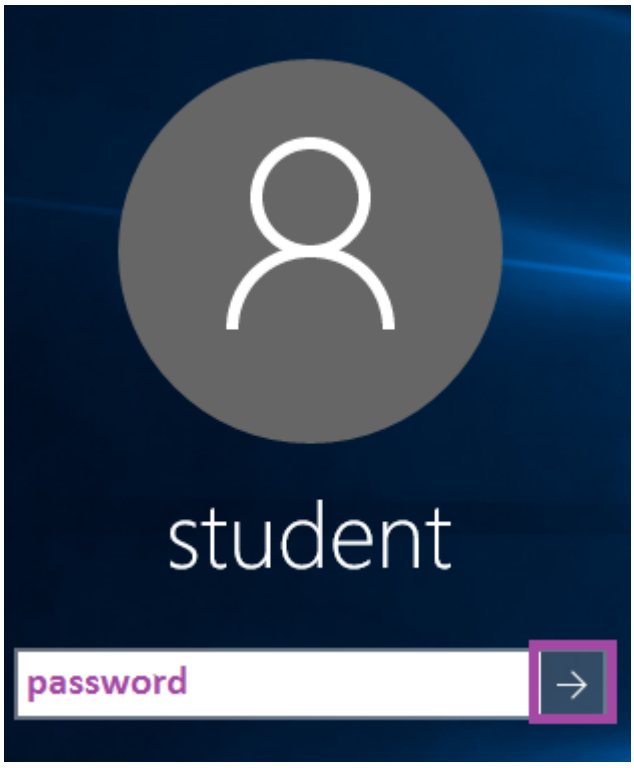
LOG IN

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



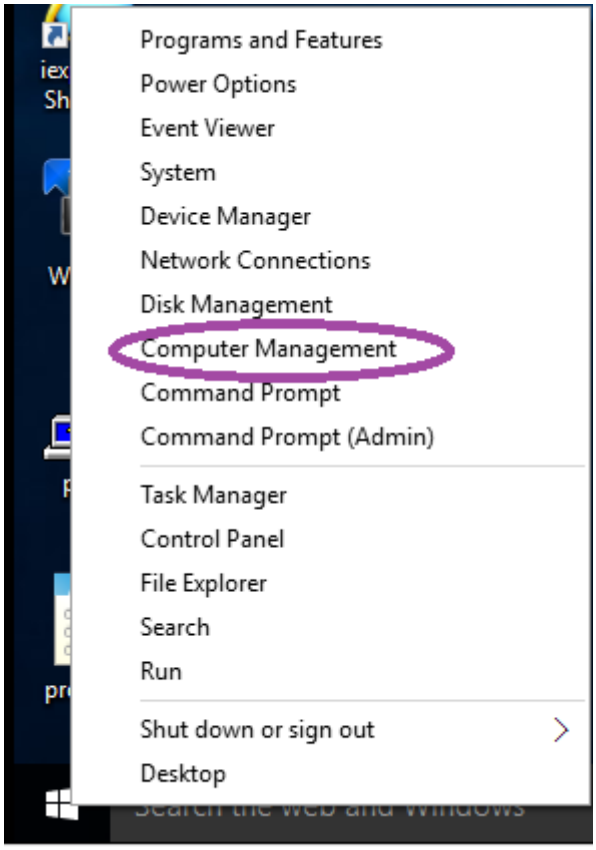
PASSWORD INCORRECT

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



LOG IN

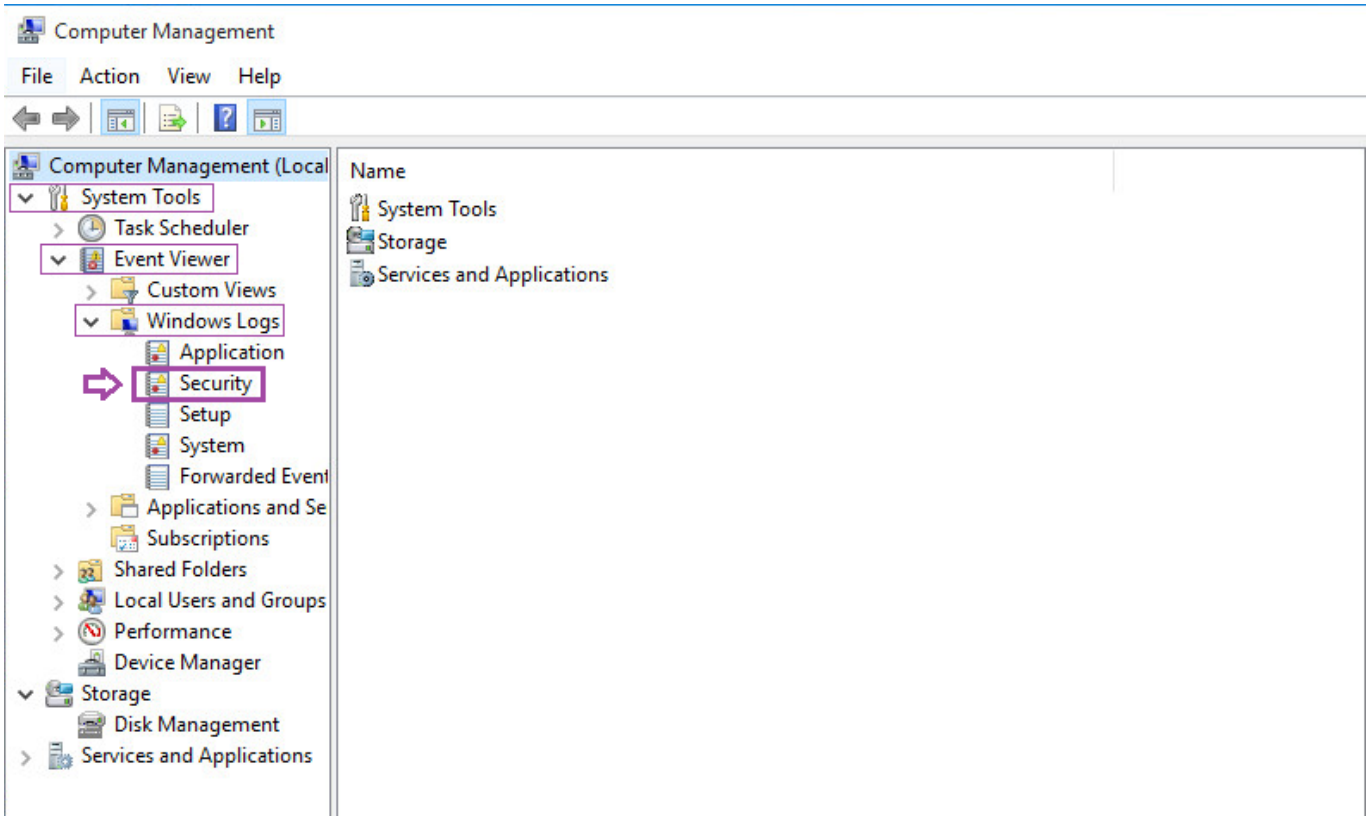
4. **Right-click** on the Windows key and **select** Computer Management.



COMPUTER MANAGEMENT

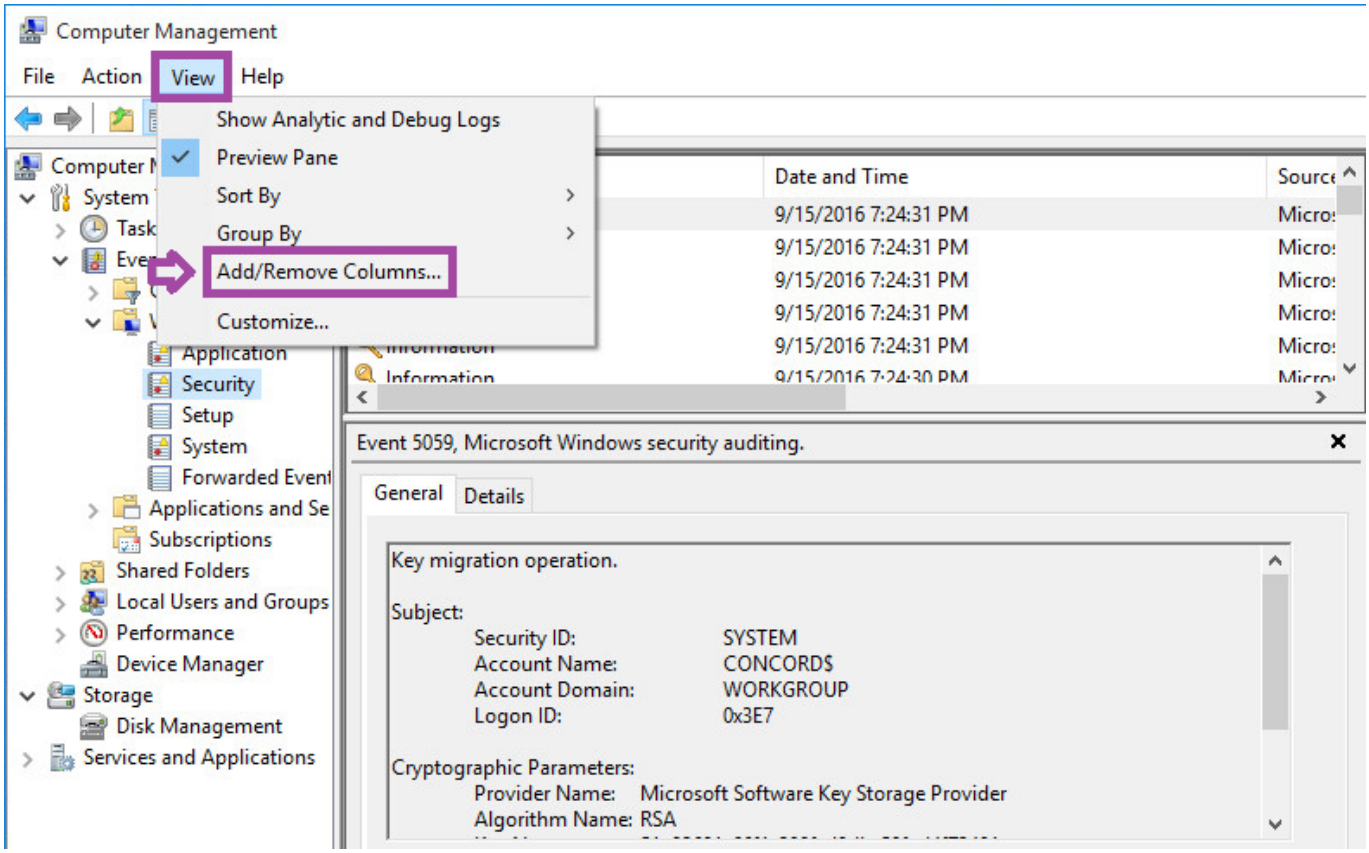
5. **Expand** System Tools.

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



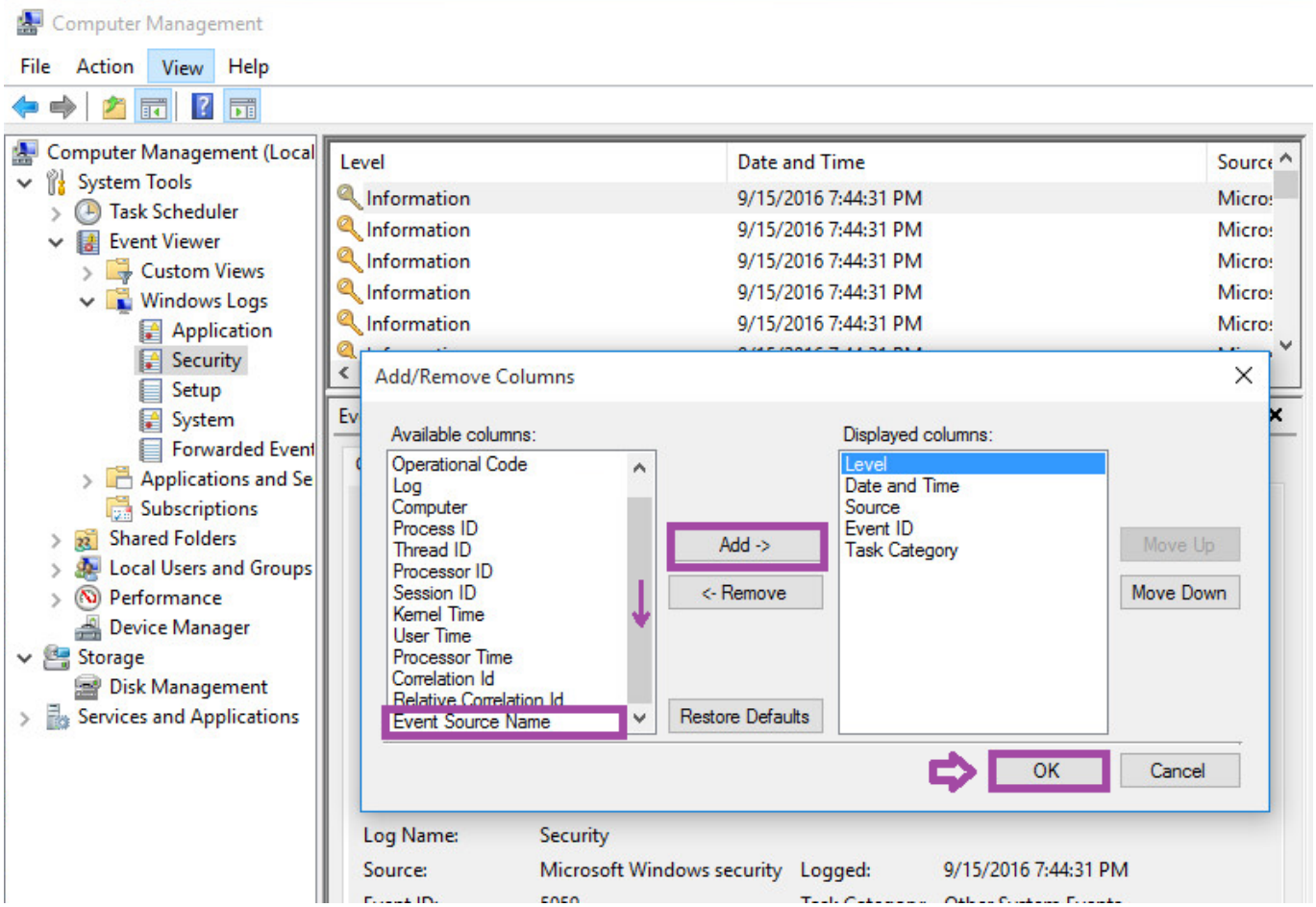
EVENT VIEWER

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



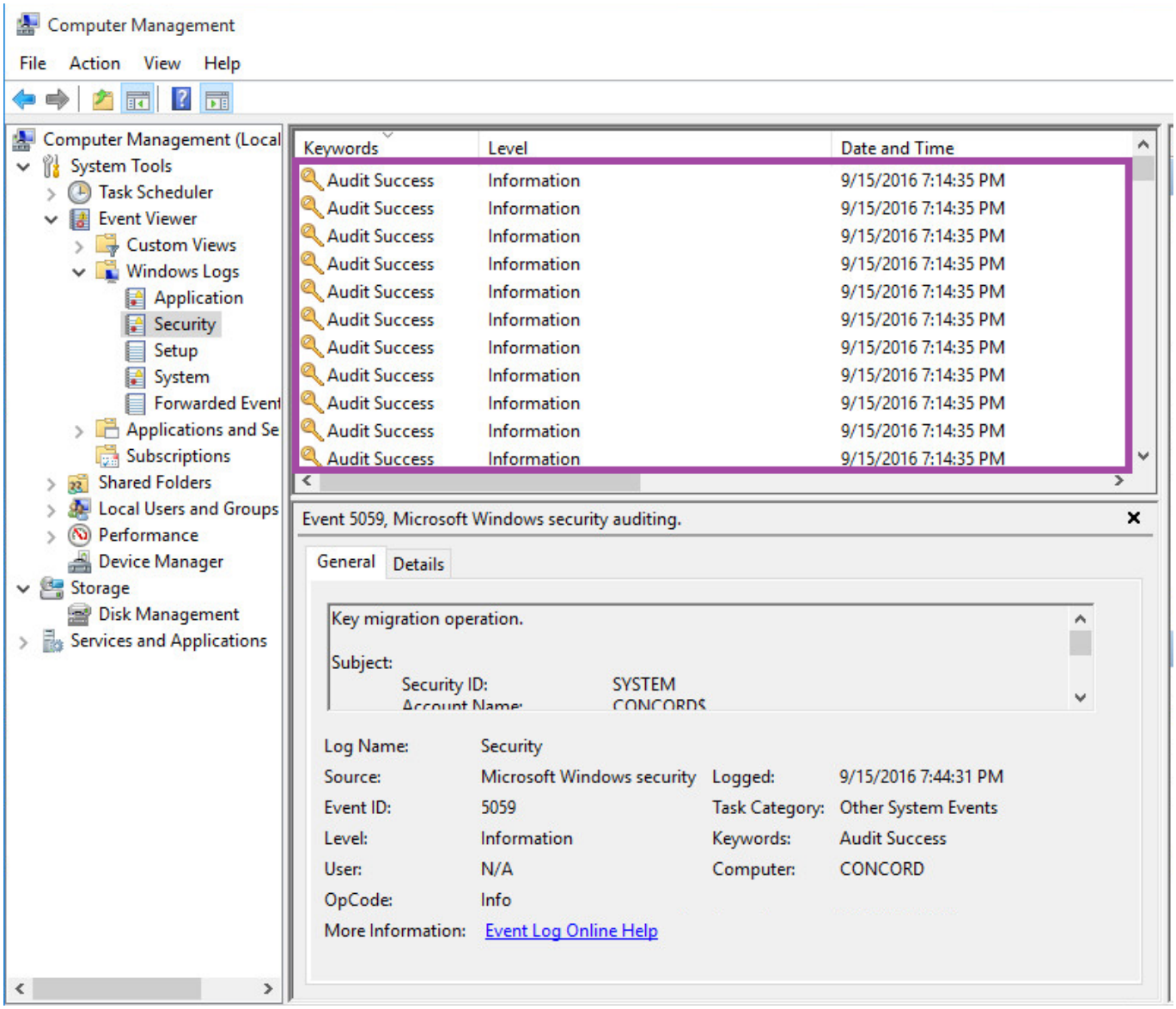
ADD/REMOVE COLUMNS

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

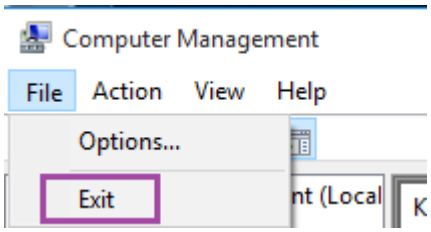


ADD EVENT SOURCE NAME

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.

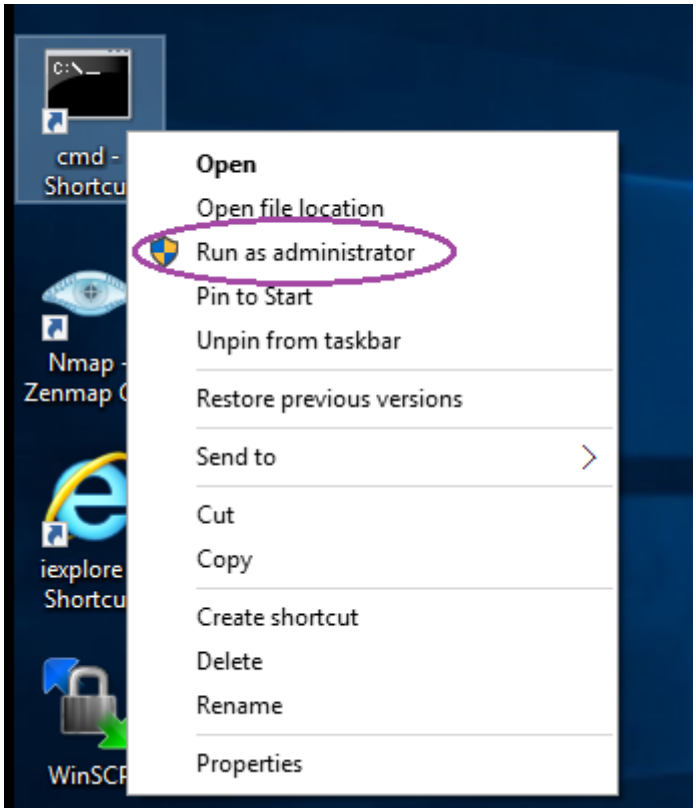


9. **Select** File from the Computer Management menu and then **select** Exit.



EXIT

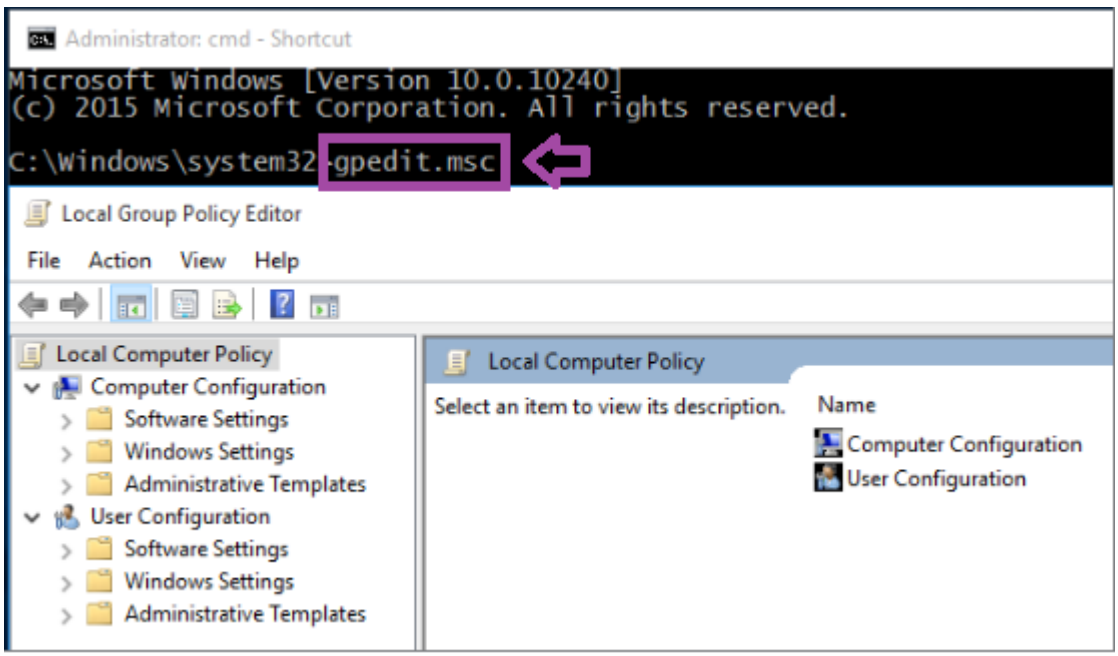
10. **Right-click** on the cmd - Shortcut and **select** Run as administrator.



RUN AS ADMINISTRATOR

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

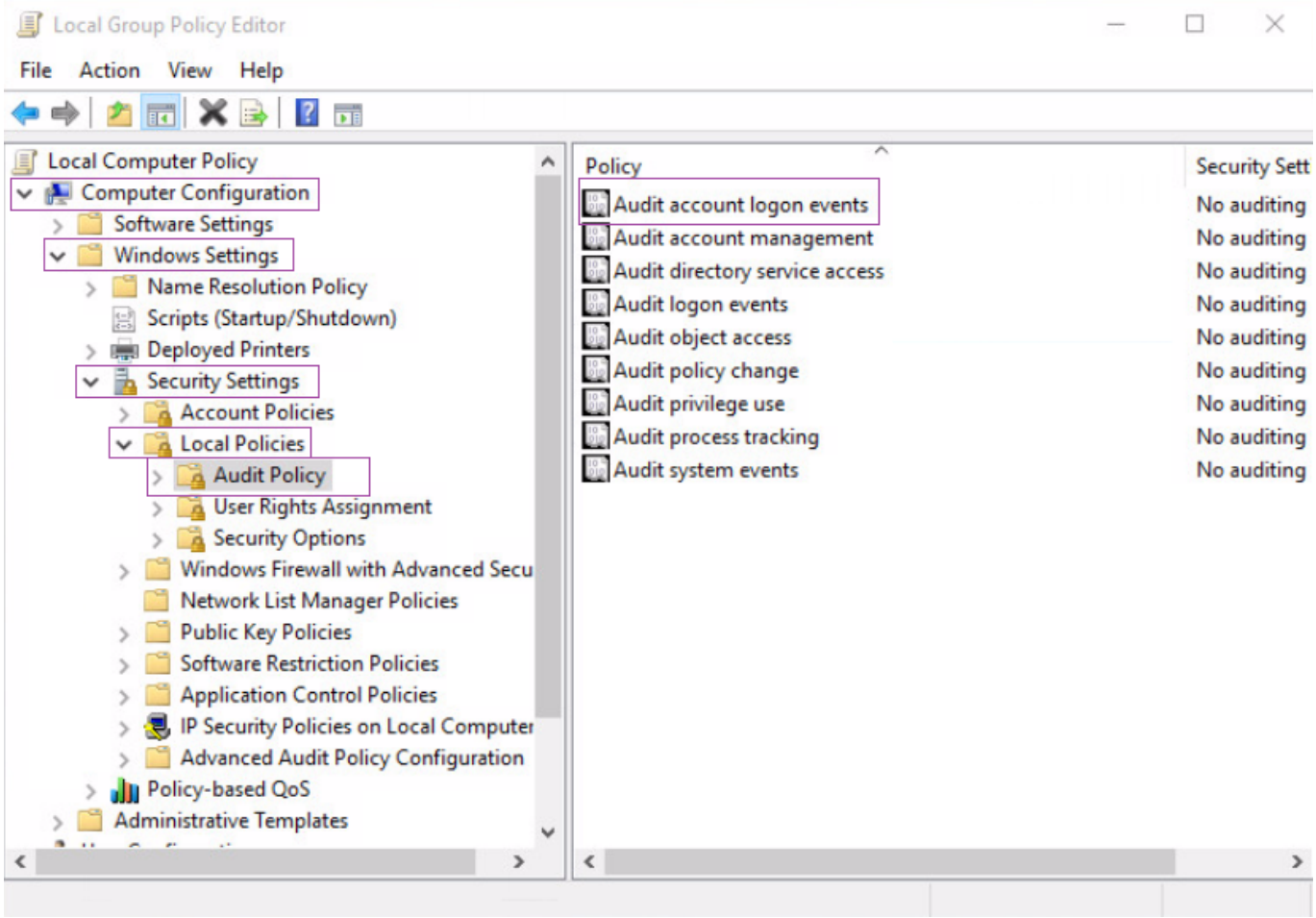
C:\Windows\system32>`gpedit.msc`



GPEDIT.MSC

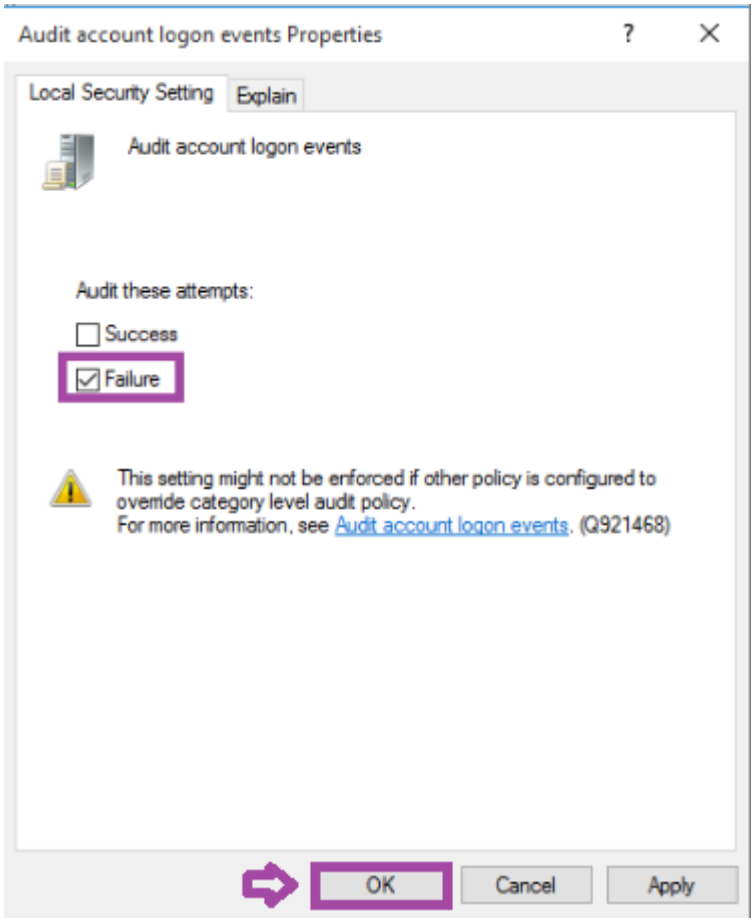
12. **Click** the arrow to expand Computer Configuration.

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.



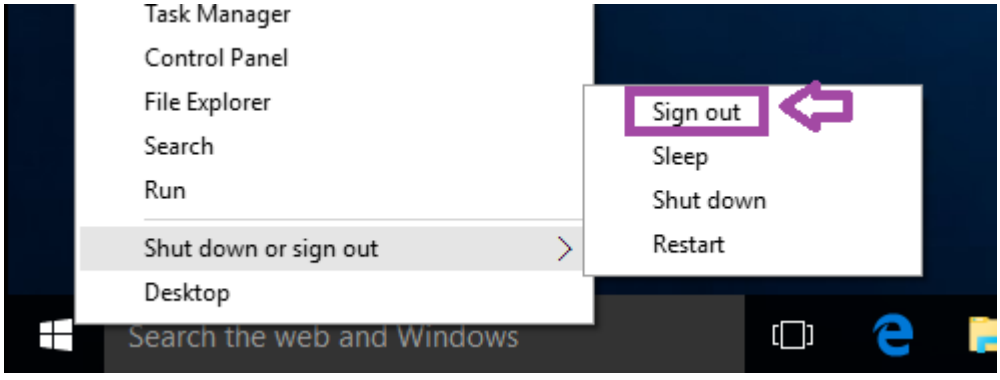
SECURITY OPTIONS

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



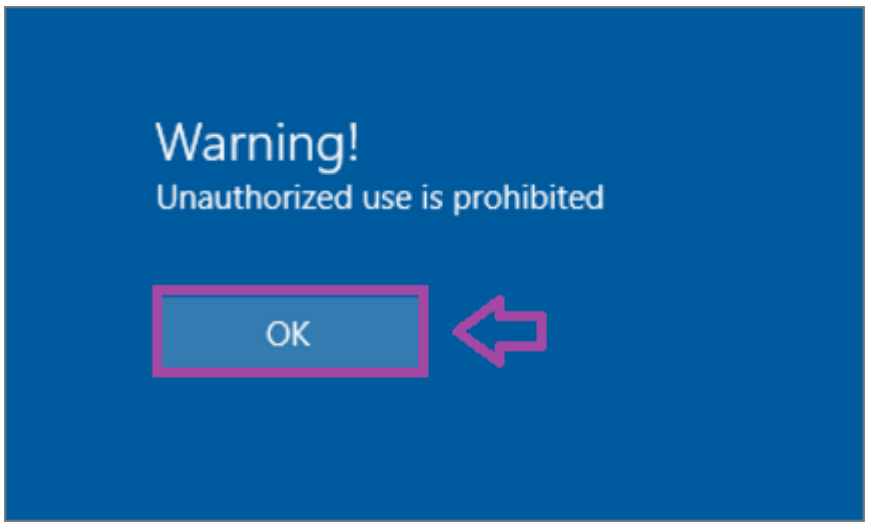
AUDIT FAILURES

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



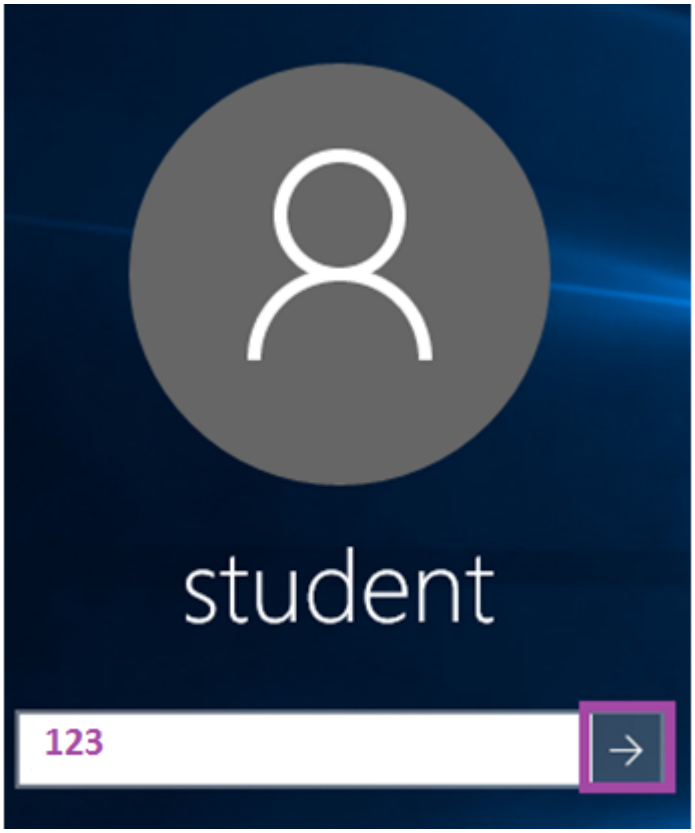
SIGN OUT

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



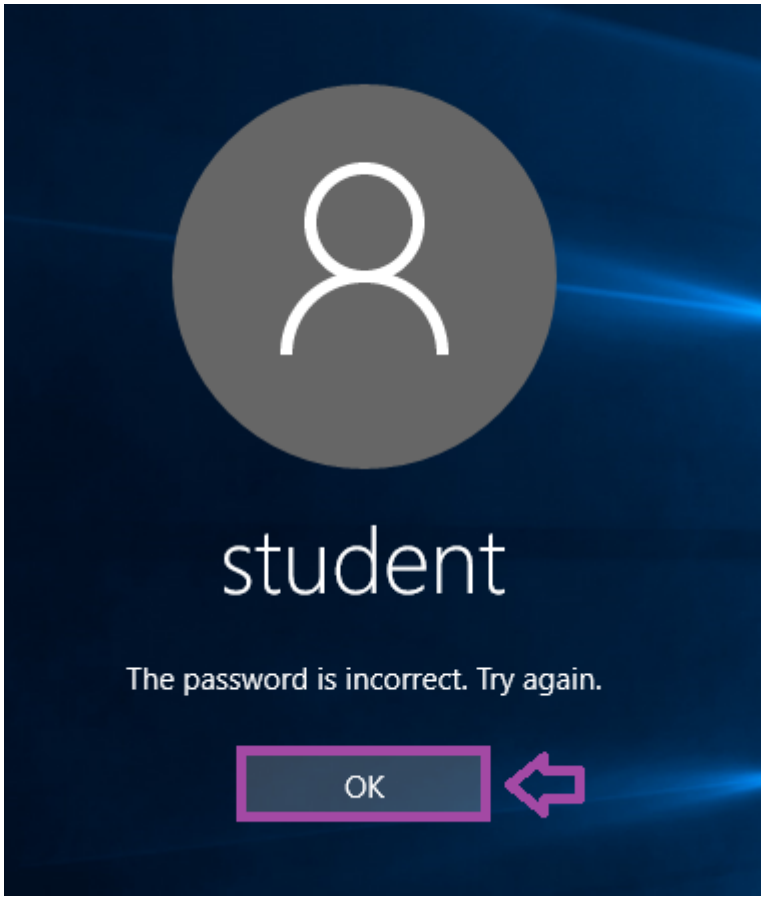
MESSAGE TITLE AND TEXT

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



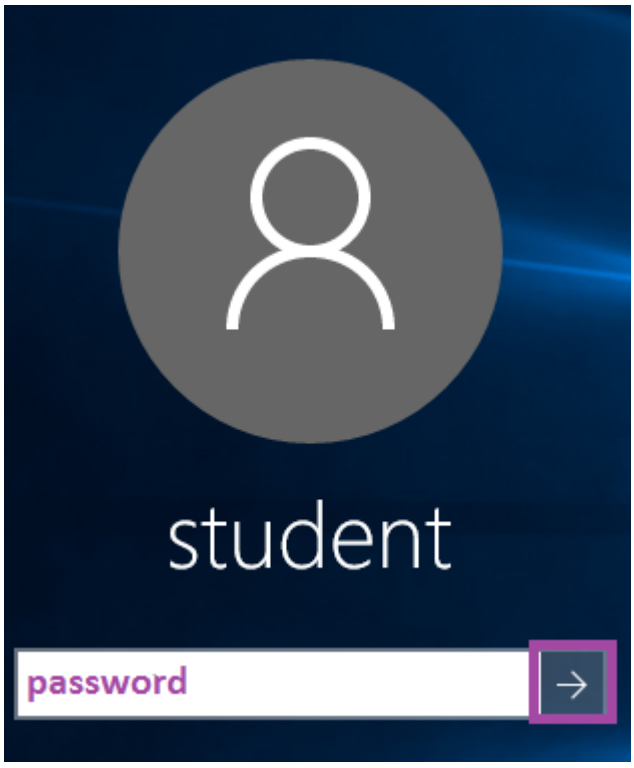
LOG IN

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



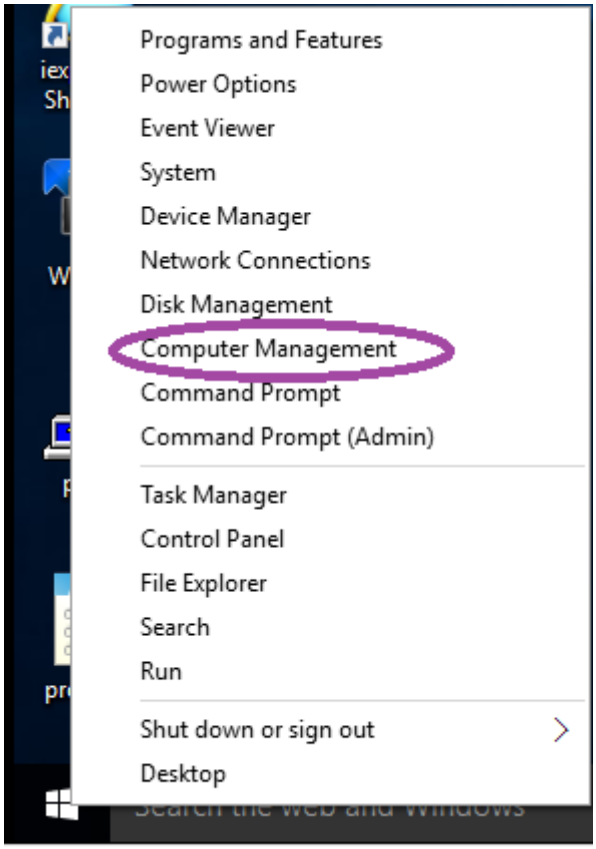
PASSWORD INCORRECT

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



LOG IN

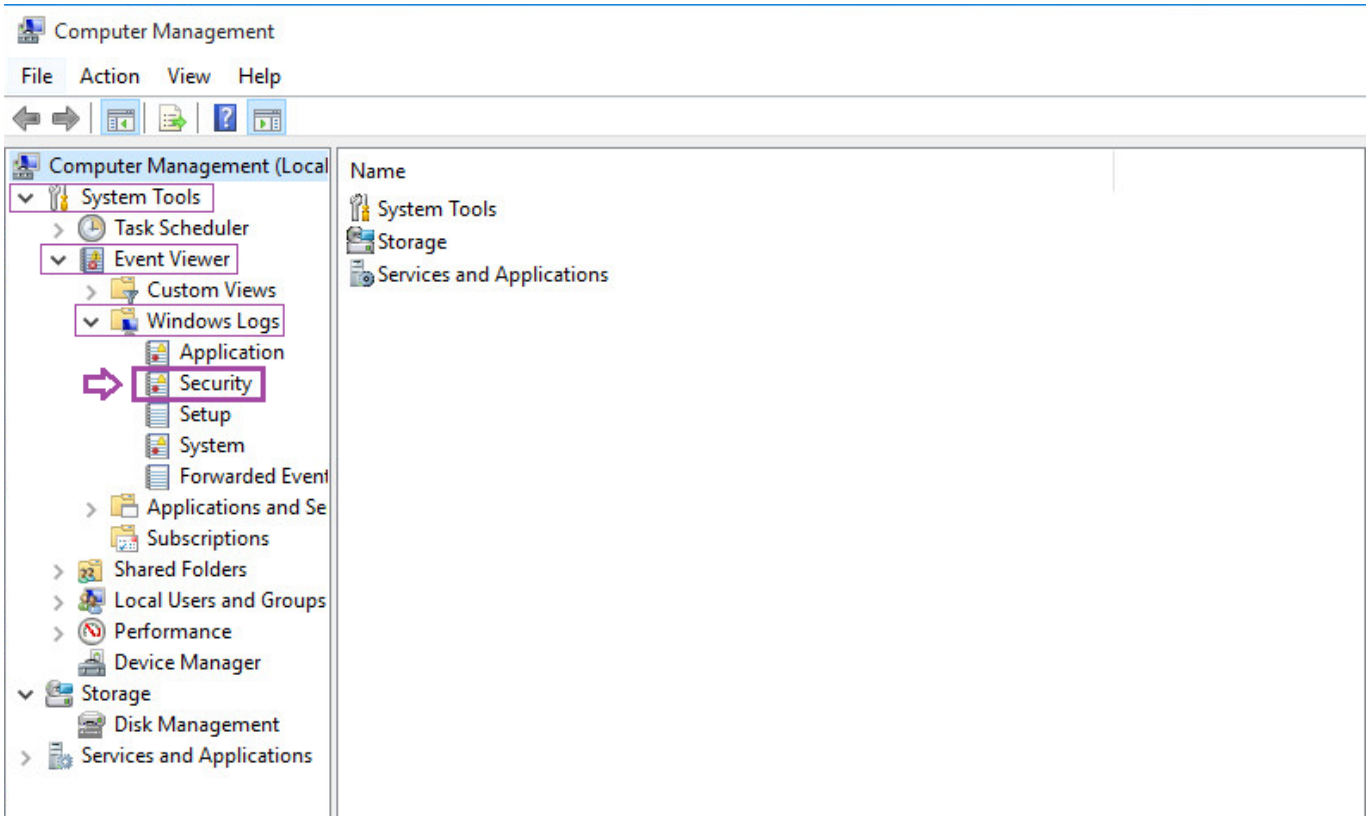
19. **Right-click** on the Windows key and **select** Computer Management.



COMPUTER MANAGEMENT

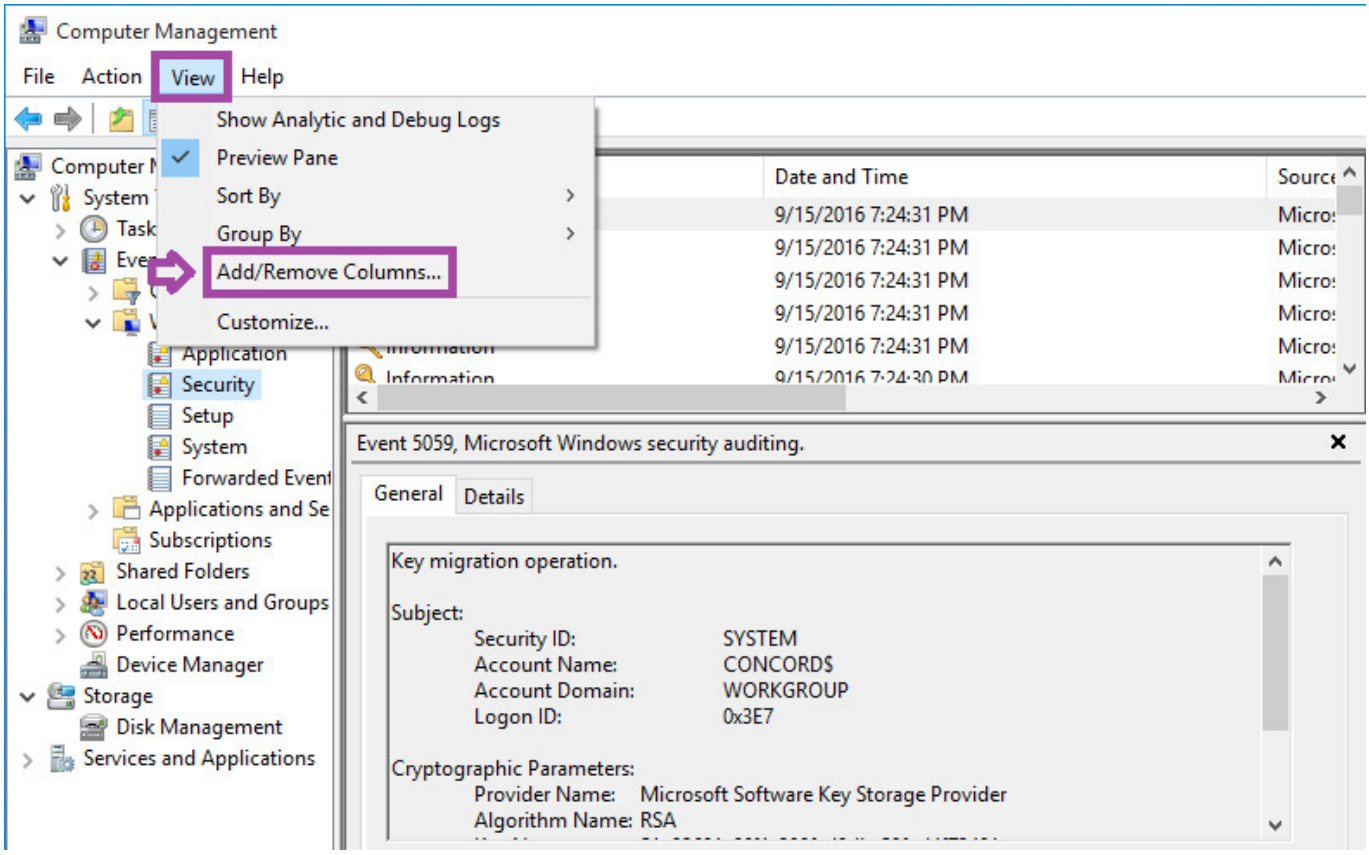
20. **Expand** System Tools.

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



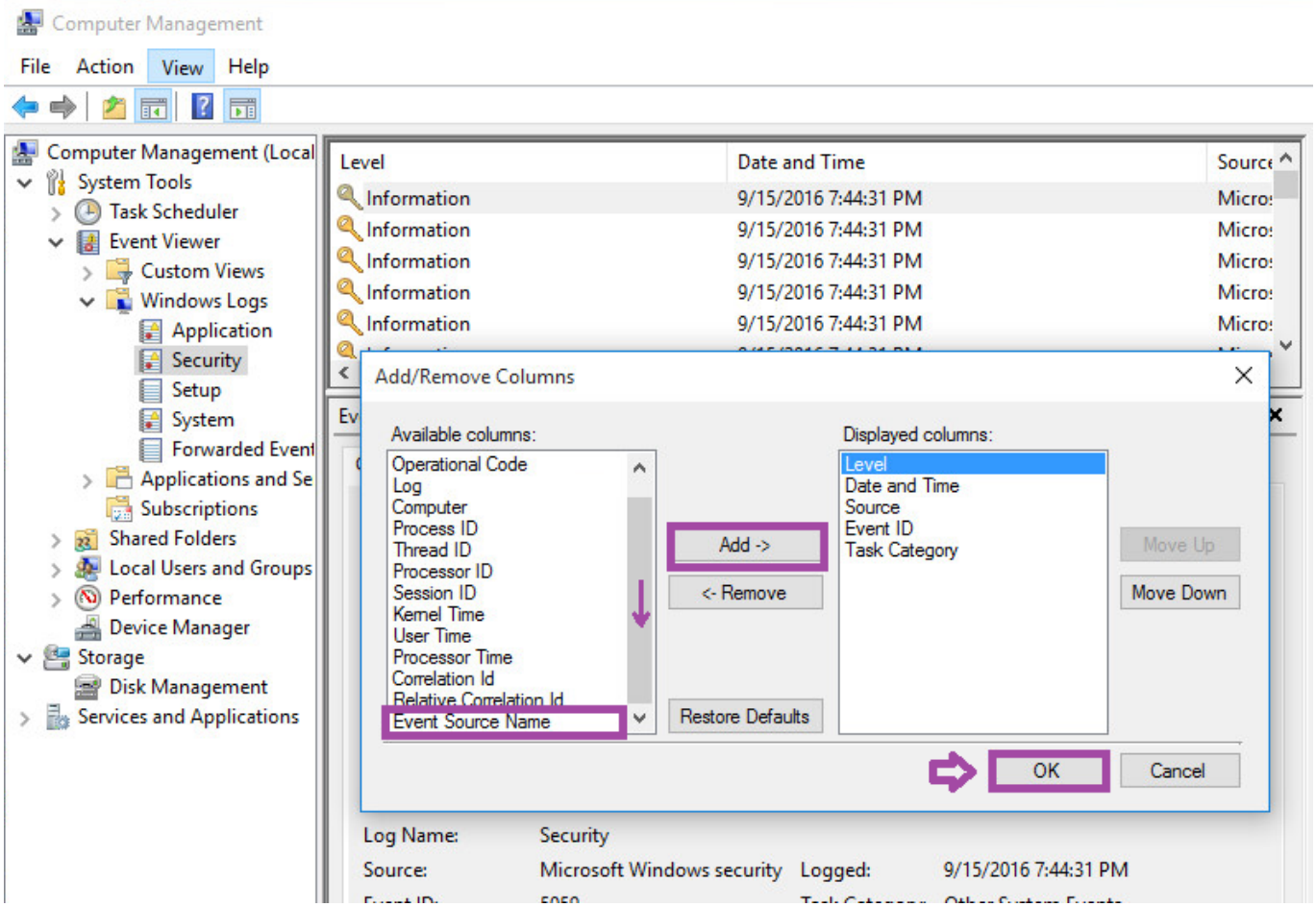
EVENT VIEWER

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



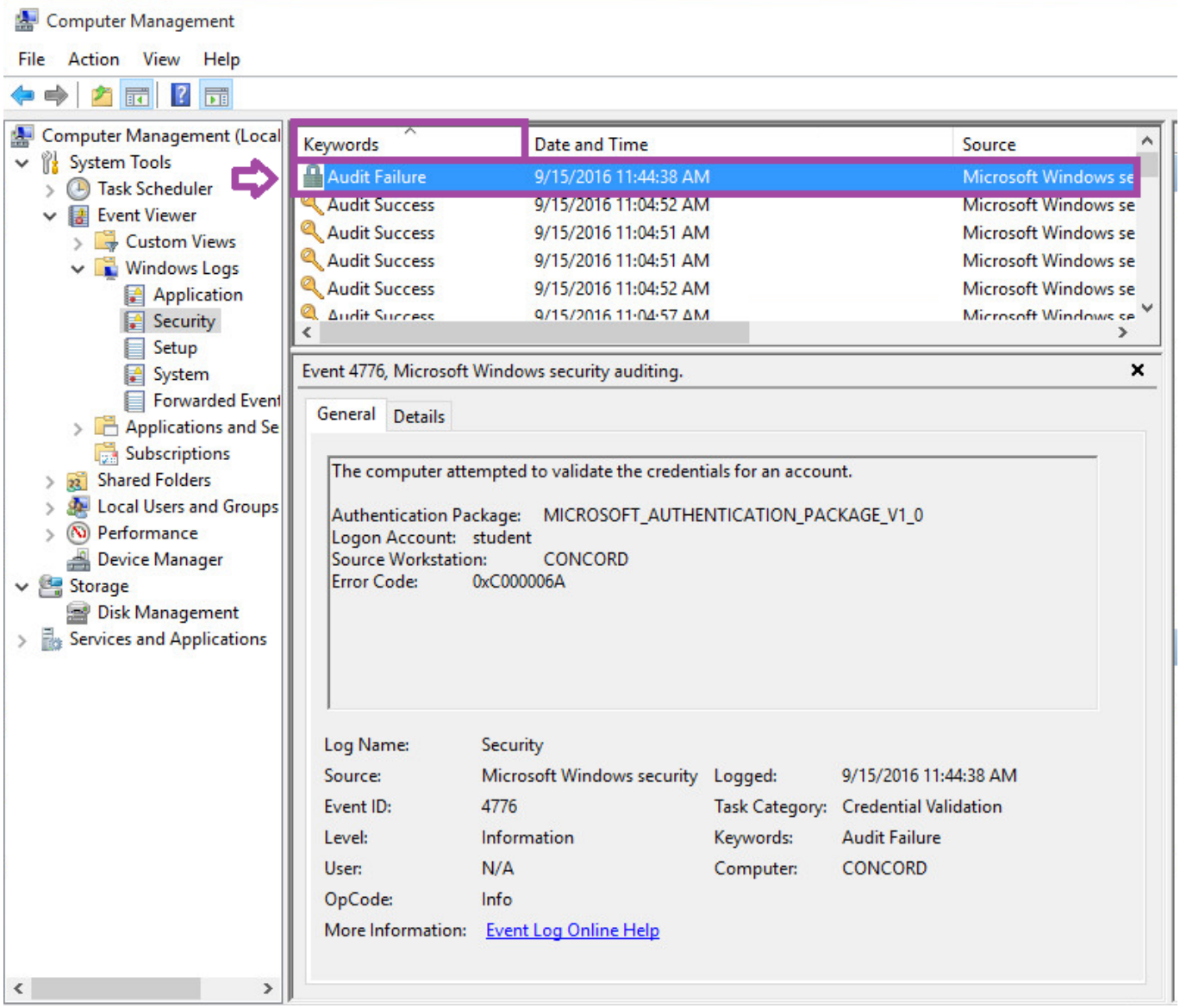
ADD/REMOVE COLUMNS

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

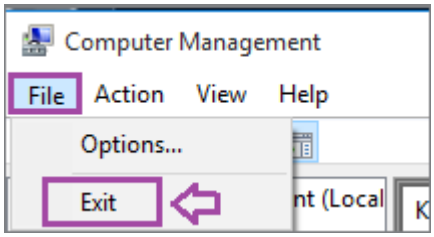


ADD EVENT SOURCE NAME

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.



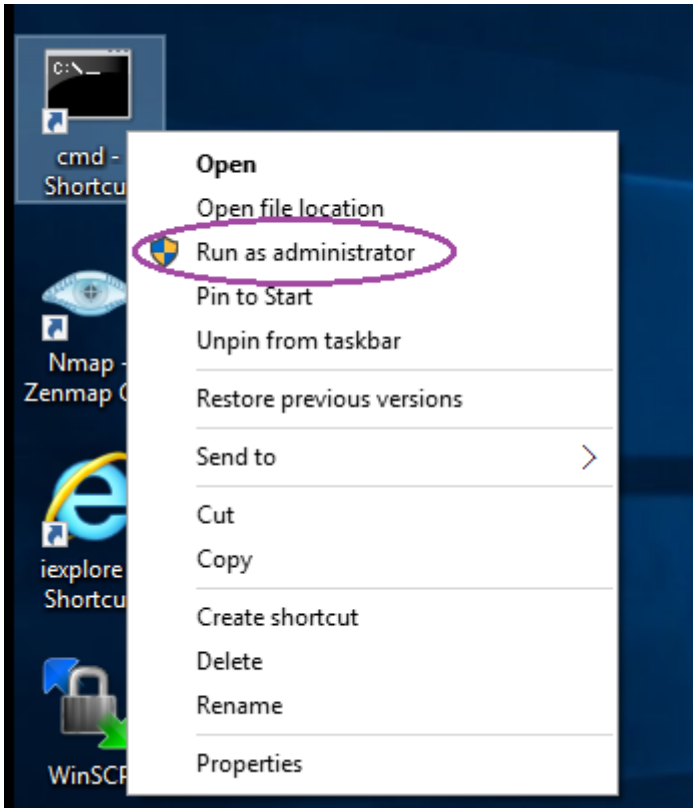
24. **Select** File from the Computer Management menu and then **select** Exit.



EXIT

Securing Linux

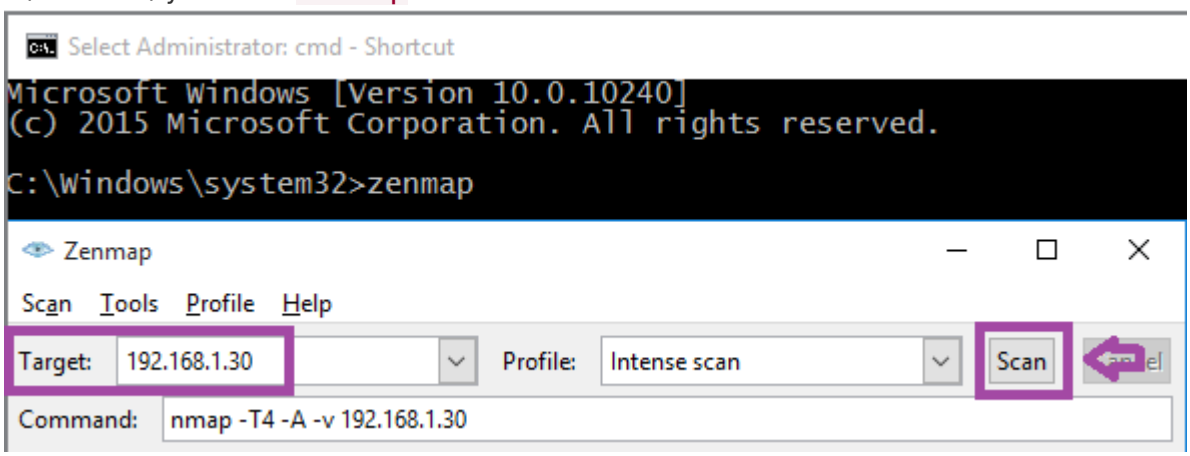
1. **Right-click** on the cmd - Shortcut and **select** Run as administrator.



RUN AS ADMINISTRATOR

2. **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.

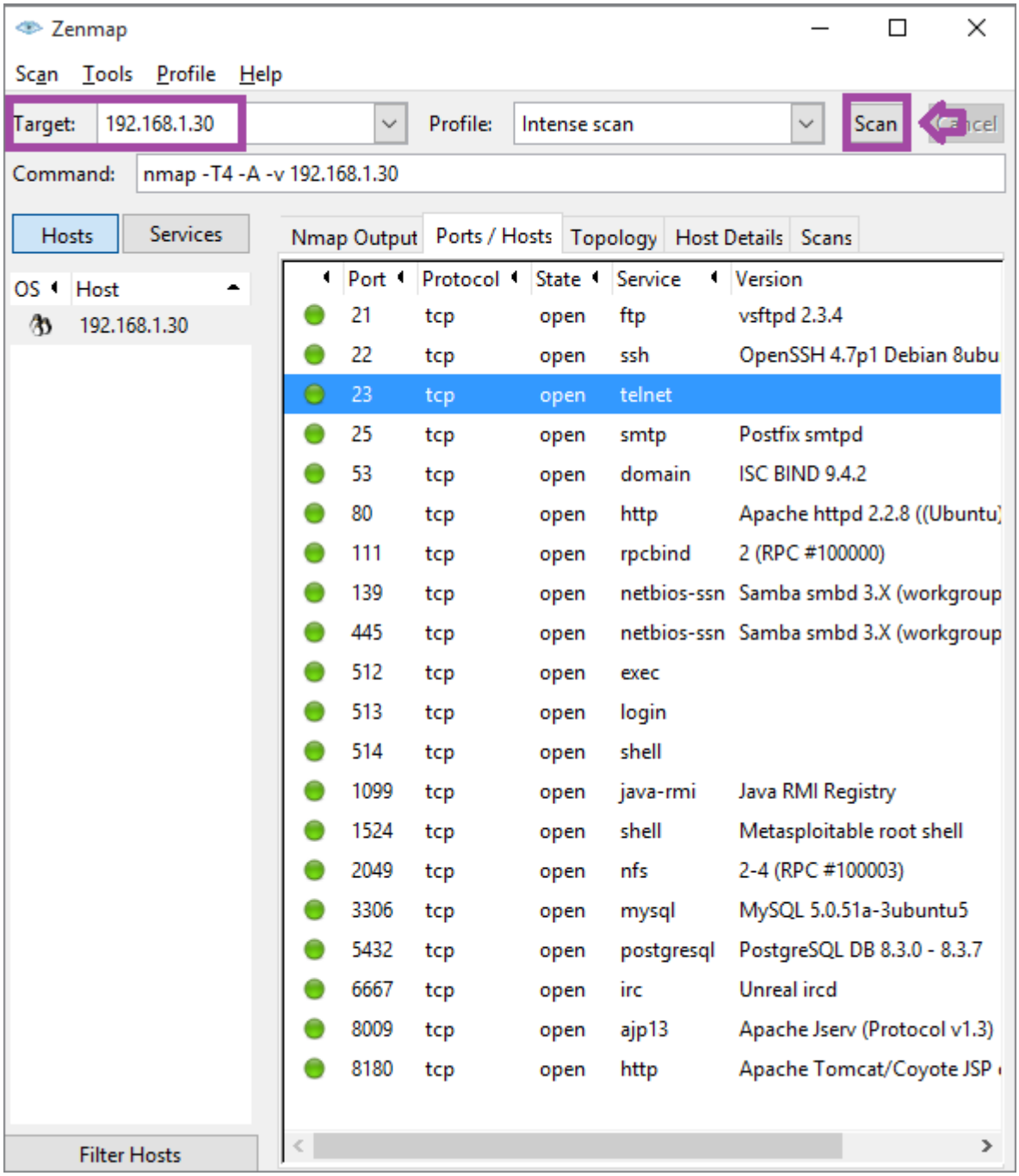
C:\Windows\system32>`zenmap`



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.



PORTS OPEN

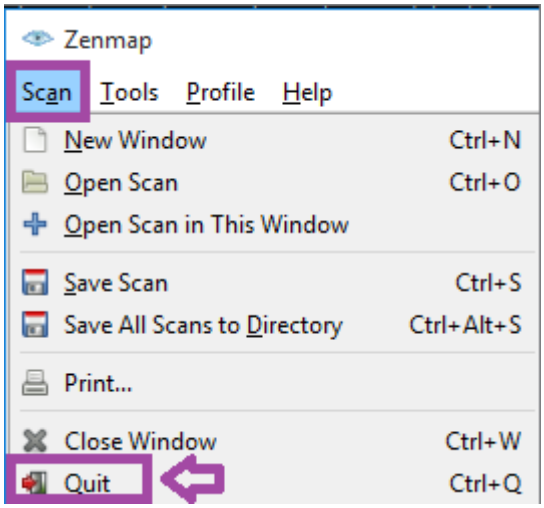
4. **Get** the information for below Challenge Flags from the Ports/Hosts tab.

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 #

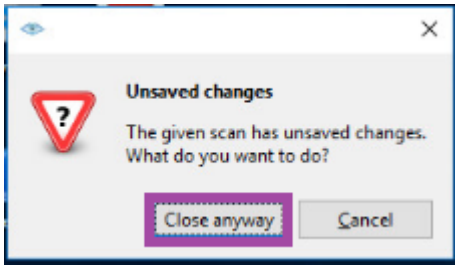
Challenge #

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



QUIT ZENMAP

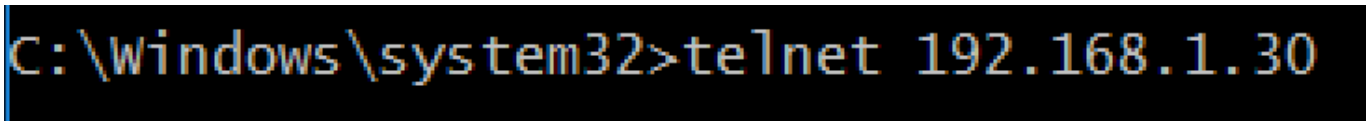
5. When asked about `Unsaved changes`, **click** Close anyway.



UNSAVED CHANGES

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

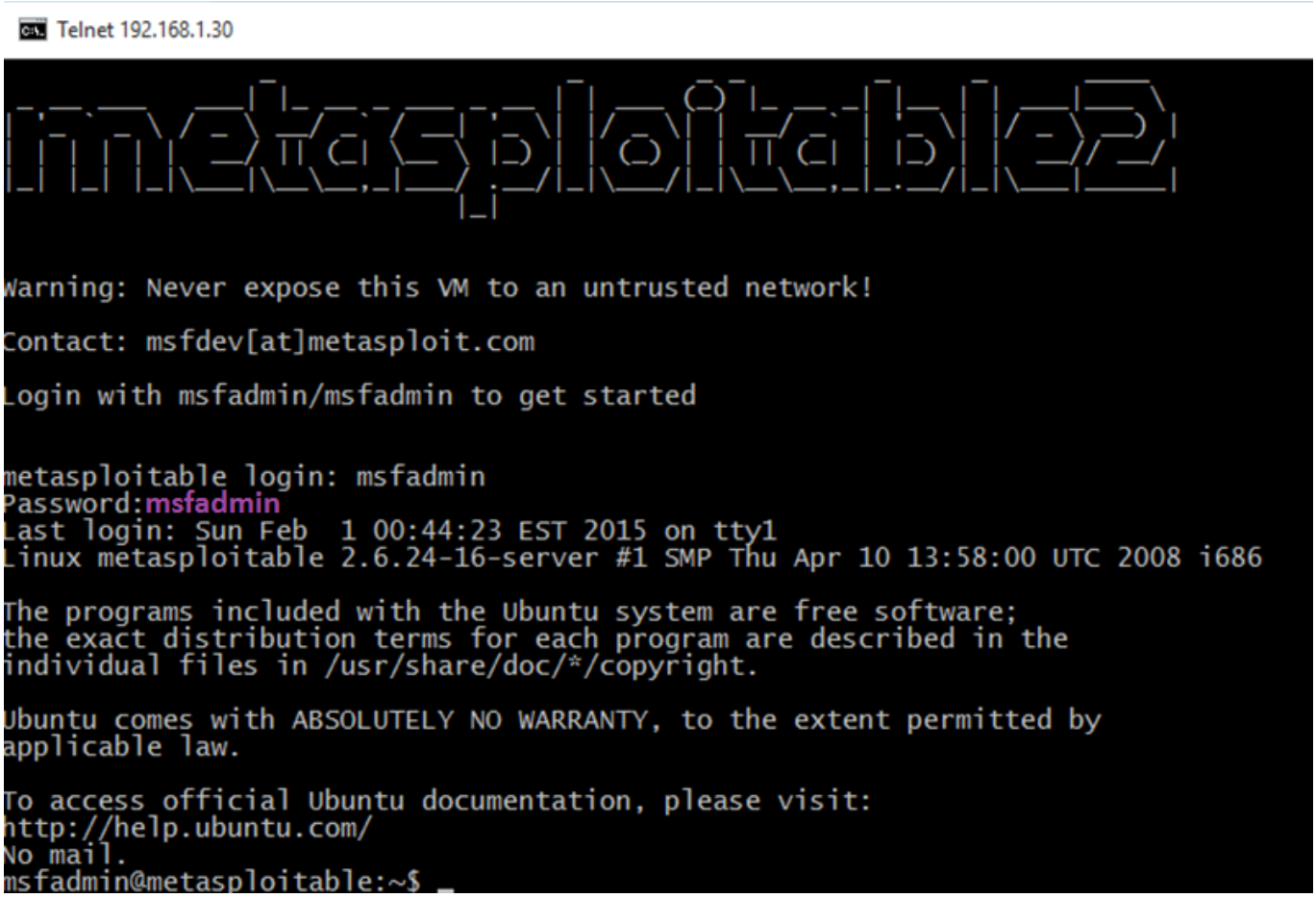
C:\Windows\system32>`telnet 192.168.1.30`



TELNET

7. **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.

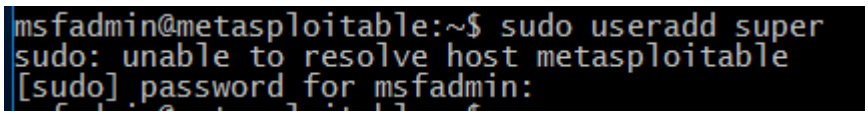
NOTE: When typing the password. it will not be dispayed for security reasons.



METASPLOITABLE2

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

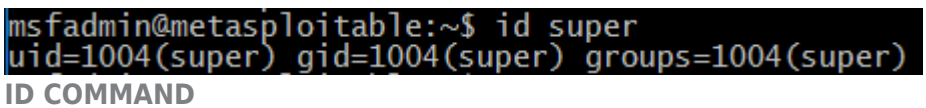
mfadmin@metasploitable:~$ `sudo useradd super`



USERADD COMMAND

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

mfadmin@metasploitable:~$ `id super`



ID COMMAND

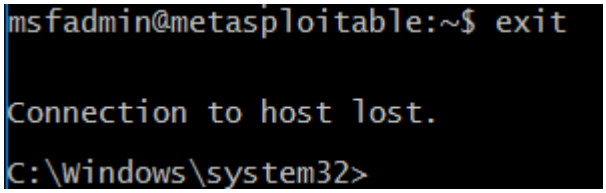
10. **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

Challenge #

Challenge #

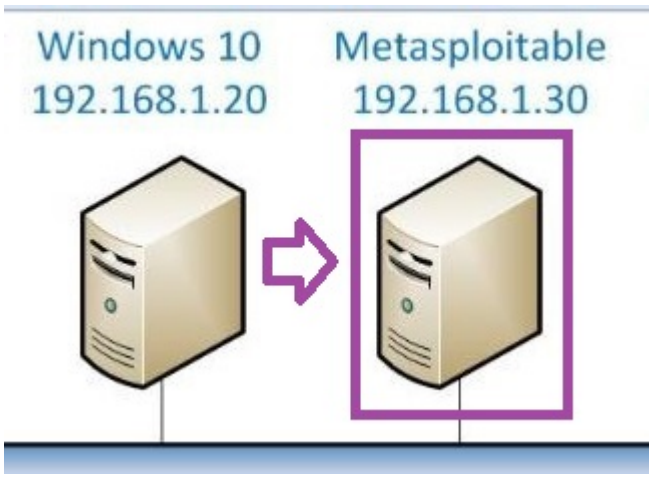
10. **Type** the following command and **press** Enter, to leave the telnet session.

mfadmin@metasploitable:~$ `exit`



ID COMMAND

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



METASPLOITABLE MACHINE

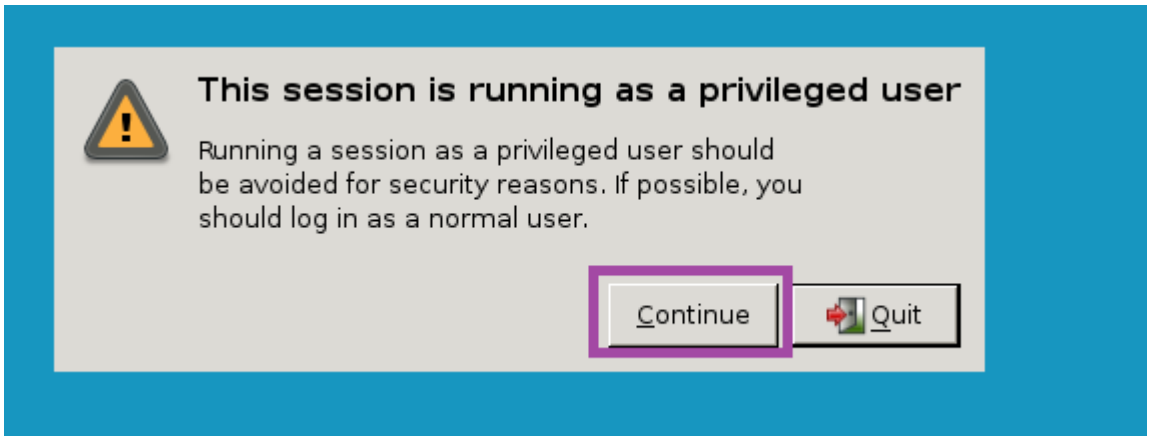
12. **Log in** as Username: `root`.

USERNAME ROOT

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

PASSWORD

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



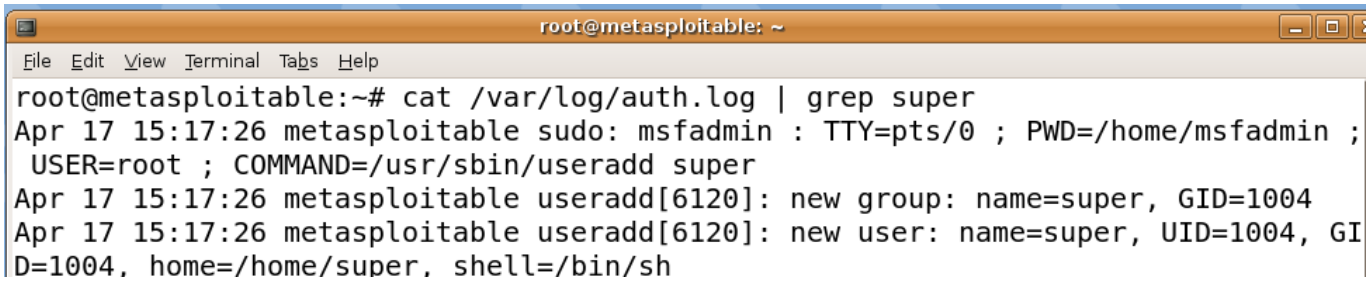
MESSAGE WARNING

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`



/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`

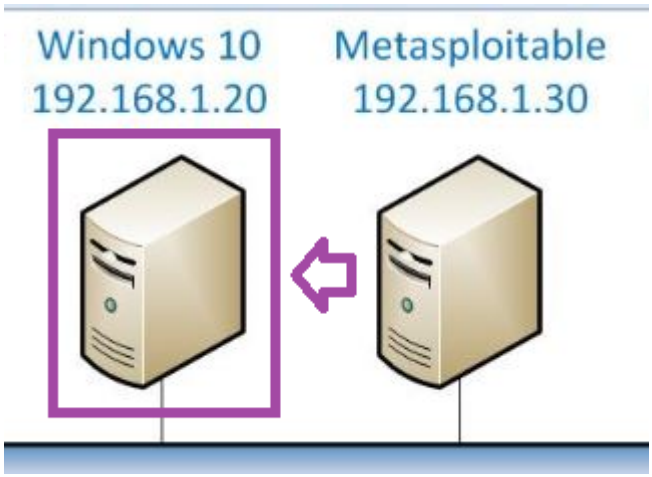
```
root@metasploitable:~# iptables -P INPUT DROP
```
IPTABLES COMMAND

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

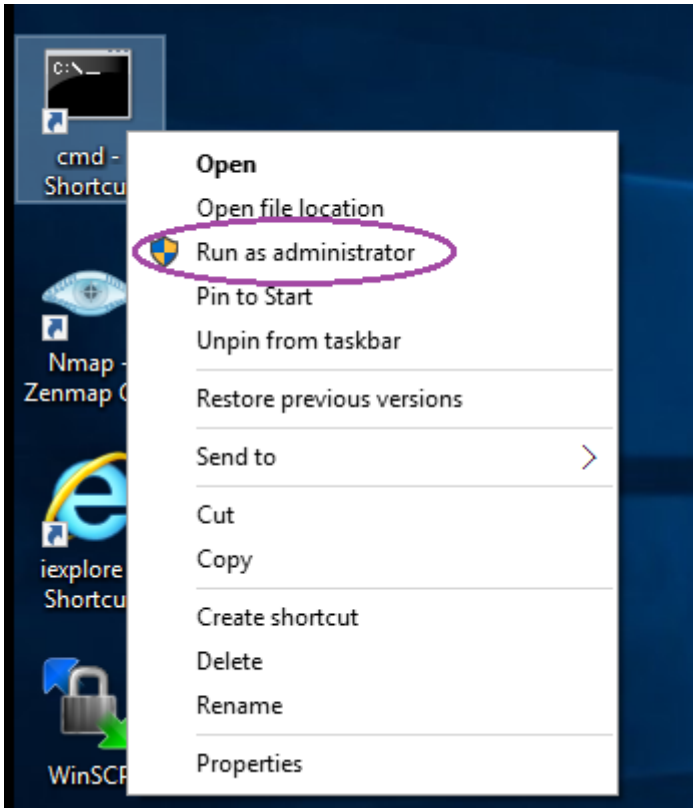
root@metasploitable:~# `iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT`

```
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.



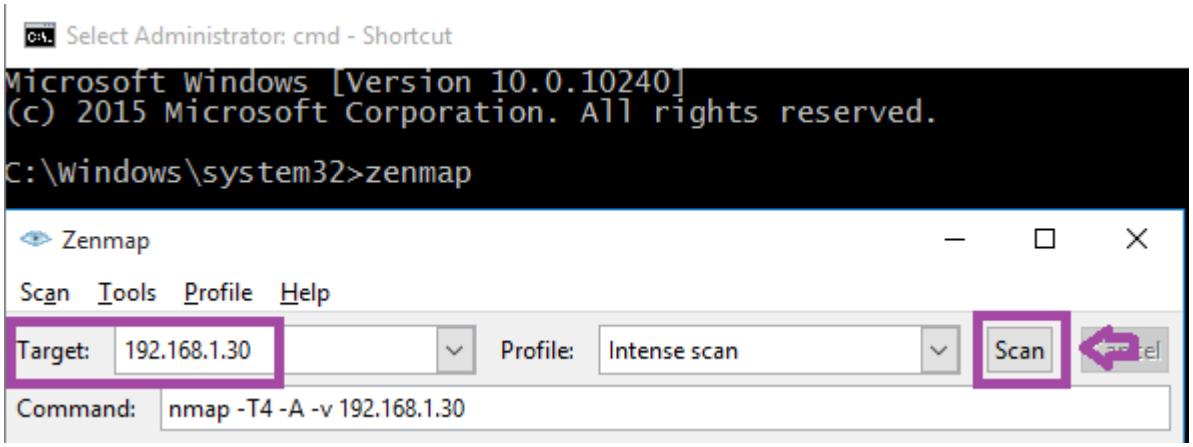
WINDOWS 10 MACHINE



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.

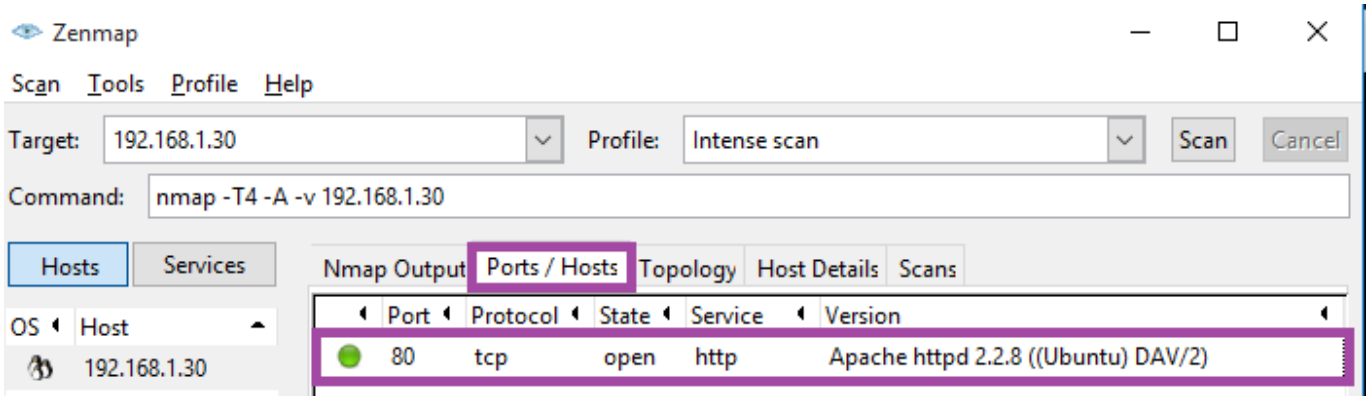
C:\Windows\system32>`zenmap`



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.



PORT OPEN

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