

CMP5329 Cyber Security

Cyber Security Coursework

Name: Kacper Popis

ID: 23161791

Contents

Module 7: Windows Labs.....	5
7.2.11 Lab - Exploring Processes, Threads, Handles, and Windows Registry	5
Part 1.....	5
Step 1	5
Step 2	6
Step 3	9
Part 2.....	12
Step 1	12
Step 2	14
Part 3.....	15
7.3.10 Lab - Create User Accounts	19
Part 1.....	19
Step 1	19
Step 2	21
Part 2.....	30
Part 3.....	34
Step 1	34
Step 2	39
7.3.11 Lab - Using Windows PowerShell	40
Part 1.....	40
Step 1	40
Part 2.....	43
Part 3.....	45
Part 4.....	46
Part 5.....	51
7.3.12 Lab - Windows Task Manager.....	53
Part 1.....	53
Part 2.....	63
Part 3.....	64
Module 8: Linux Labs.....	68
8.2.6 Lab – Working with Text Files in the CLI.....	68
Part 1.....	68
Step 1	68
Step 2	74
Part 2.....	75

Part 3.....	77
Step 1	77
Step 2	79
Step 3	83
8.2.7 Lab – Getting Familiar with the Linux Shell.....	84
Part 1.....	85
Step 1	85
Step 2	86
Step 3	89
Step 4	91
Step 5	93
Step 6	94
Part 2.....	96
Step 1	96
Step 2	97
Step 3	98
8.5.4 Lab - Navigating the Linux Filesystem and Permission Settings.....	99
Part 1.....	99
Step 1	99
Step 2	100
Step 3	102
Part 2.....	103
Step 1	103
Step 2	105
Part 3.....	106
Step 1	106
Module 18: Cryptography	109
18.1.11 Lab - Use Classic and Modern Encryption Algorithms	109
Part 1.....	109
Step 1	109
Step 2	109
Step 3	110
Step 4	111
Step 5	112
Part 2.....	113
Step 1	113

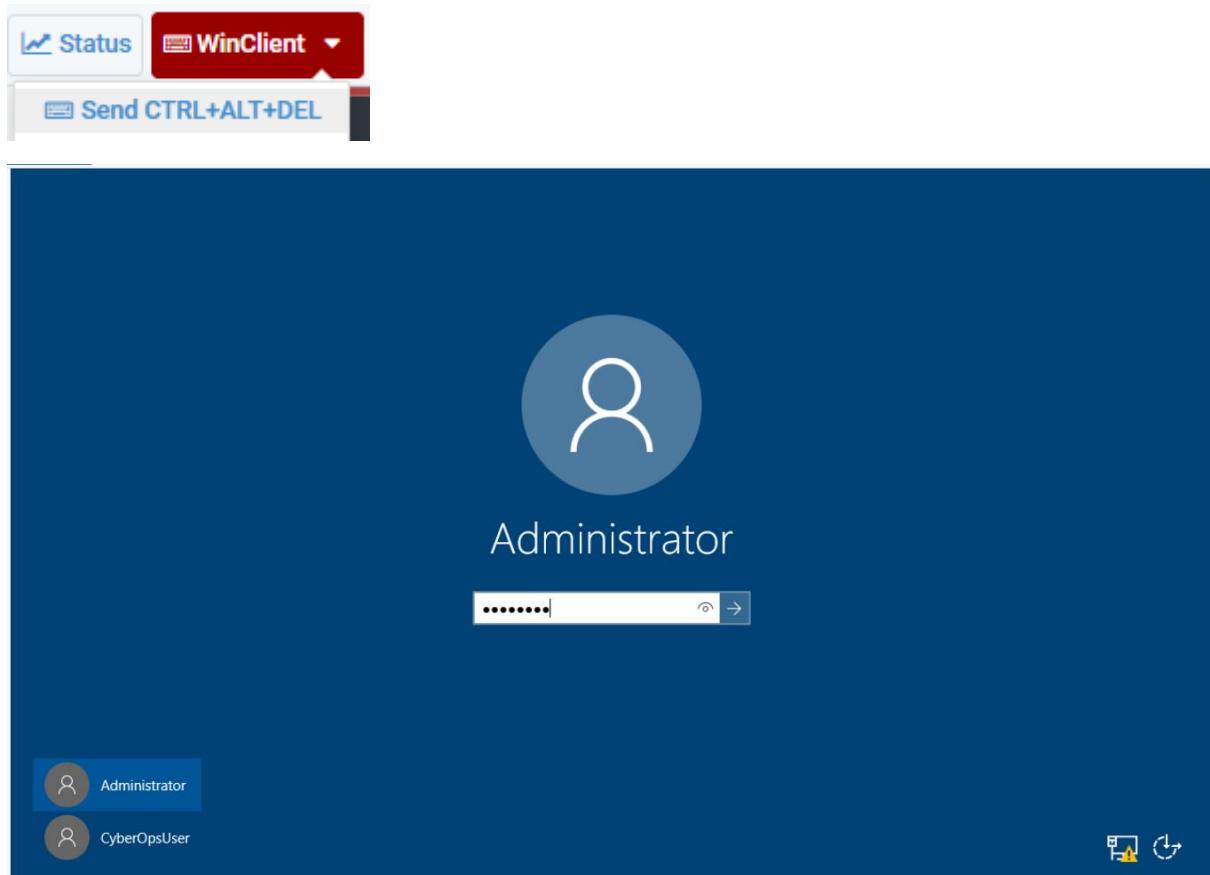
Step 2	114
Part 3.....	115
Step 1	115
Step 2	117
18.4.10 Lab – Hashing Things Out.....	118
Part 1.....	118
Part 2.....	120
18.5.5 Lab - Generate and Use a Digital Signature	121
Part 1.....	121
Part 2.....	121
Part 3.....	123
Part 4.....	123
Part 5.....	123
Part 6.....	124
Part 7.....	124
Part 8.....	124
Module 19: Technologies and Protocols (ACL)	125
19.1.7 Check Your Understanding - Identify the Monitored Protocol	126
19.2.6 Check Your Understanding - Identify the Impact of the Technology on Security and Monitoring	127
Reflective Report (cryptography and access control)	128

Module 7: Windows Labs

7.2.11 Lab - Exploring Processes, Threads, Handles, and Windows Registry

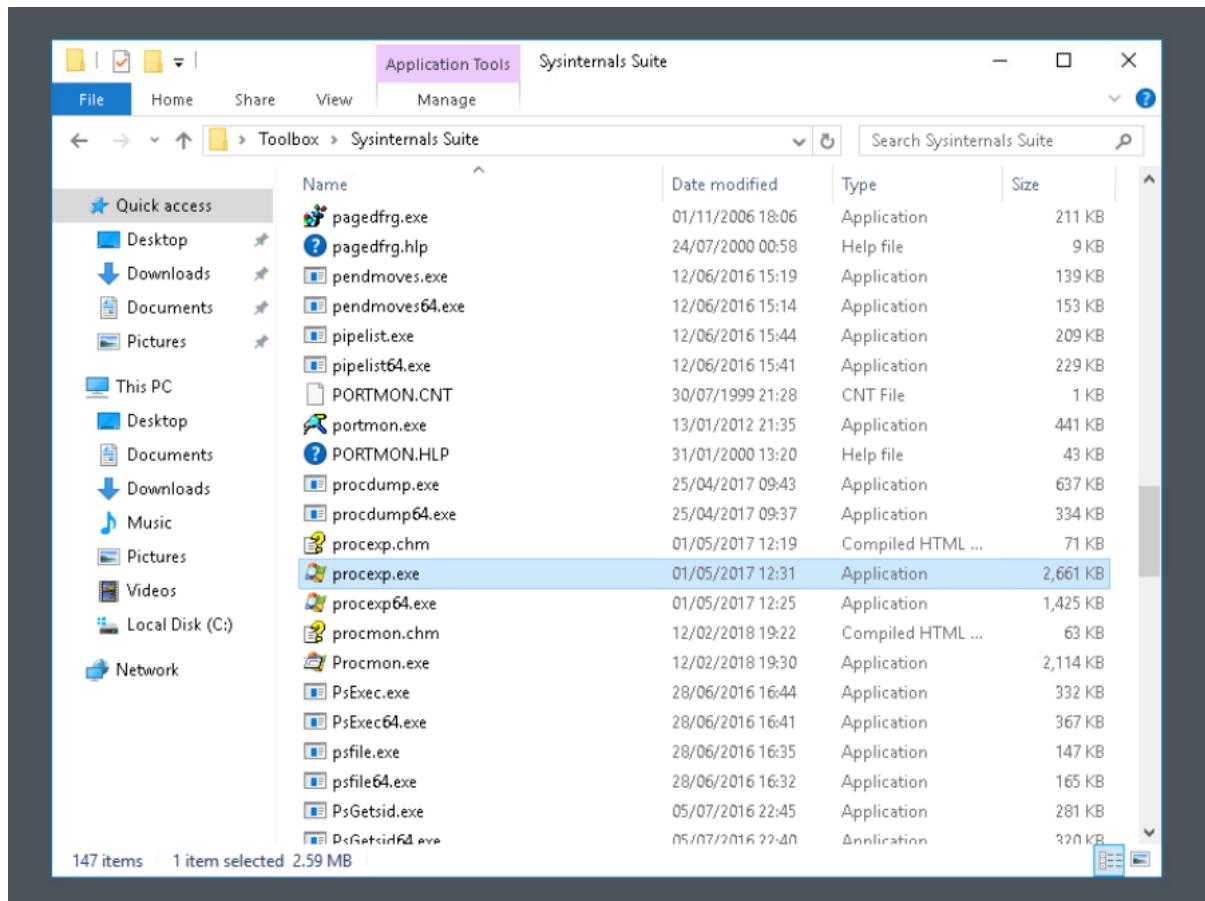
Part 1

Step 1

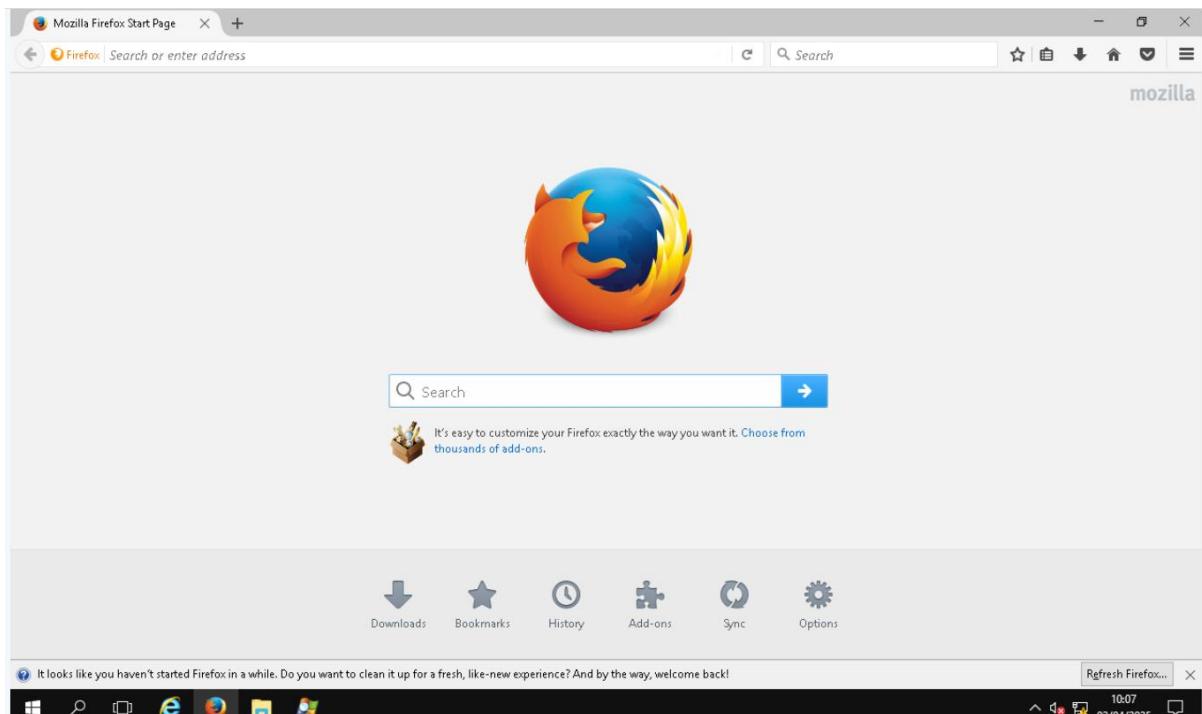


Accessing the VM on netlab.

Step 2



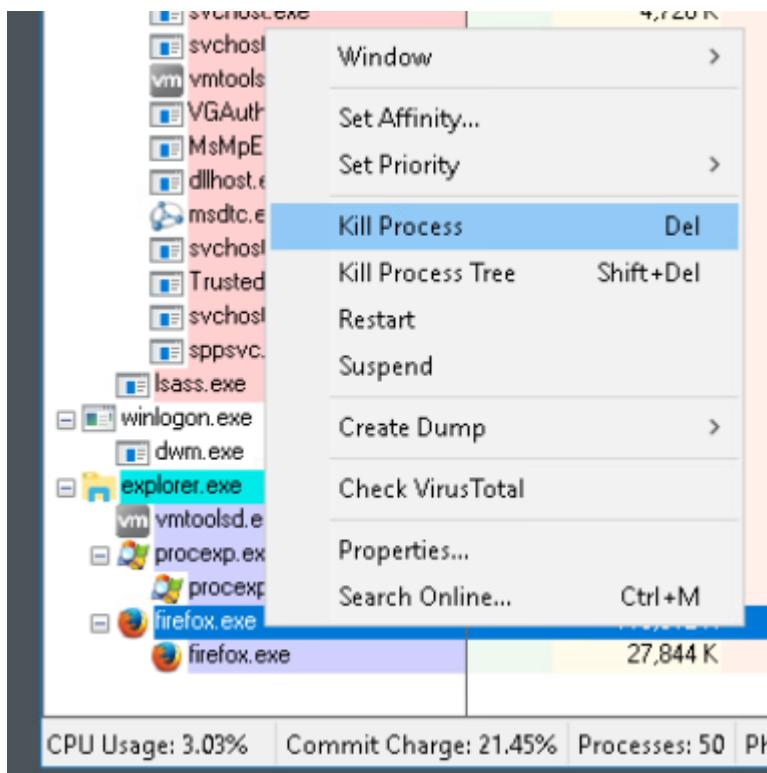
Finding and locating the **Sysinternals Suite** folder on the desktop and locating the **procexp.exe** inside of the folder and starting it, then accepting the licence agreement to be able to use it.



Opening **Firefox** browser to be used in this task.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	0.06	13,188 K	21,636 K	912	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.02	6,952 K	16,980 K	292	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.02	10,248 K	16,336 K	384	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	1,944 K	7,372 K	320	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.20	7,644 K	19,440 K	336	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	3,692 K	11,272 K	1236	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,484 K	6,884 K	1408	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		5,908 K	16,012 K	1472	Spooler SubSystem App	Microsoft Corporation
svchost.exe		2,092 K	8,380 K	1624	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,668 K	16,152 K	1648	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,960 K	19,220 K	1692	Host Process for Windows S...	Microsoft Corporation
vm vmtoolsd.exe	0.02	9,548 K	22,536 K	1700	VMware Tools Core Service	VMware, Inc.
VGAuthService.exe		5,444 K	12,588 K	1720	VMware Guest Authenticatio...	VMware, Inc.
MsmPEng.exe		117,572 K	71,352 K	1764	Antimalware Service Execut...	Microsoft Corporation
dllhost.exe		3,792 K	12,836 K	2196	COM Surrogate	Microsoft Corporation
dllhost.exe	0.01	3,980 K	13,036 K	2332	COM Surrogate	Microsoft Corporation
msdtc.exe	0.01	2,764 K	10,084 K	2484	Microsoft Distributed Transa...	Microsoft Corporation
VSSVC.exe		1,688 K	8,140 K	3032	Microsoft® Volume Shadow ...	Microsoft Corporation
svchost.exe		3,616 K	14,244 K	636	Host Process for Windows S...	Microsoft Corporation
lsass.exe	0.02	4,272 K	12,236 K	572	Local Security Authority Proc...	Microsoft Corporation
winlogon.exe		1,928 K	8,988 K	492	Windows Logon Application	Microsoft Corporation
dwm.exe	0.14	27,292 K	48,640 K	808	Desktop Window Manager	Microsoft Corporation
explorer.exe	0.11	24,652 K	70,088 K	920	Windows Explorer	Microsoft Corporation
vm vmtoolsd.exe	0.05	3,880 K	14,556 K	3480	VMware Tools Core Service	VMware, Inc.
proexp.exe		3,092 K	10,604 K	3664	Sysinternals Process Explorer	Sysinternals - www.sysinter...
proexp64.exe	1.20	14,220 K	37,920 K	3692	Sysinternals Process Explorer	Sysinternals - www.sysinter...
firefox.exe	3.22	111,256 K	158,048 K	3808	Firefox	Mozilla Corporation
firefox.exe	0.34	28,284 K	61,492 K	3996	Firefox	Mozilla Corporation

Using the **Find Window's Processes** (inside process explorer) by drag and dropping it onto the **Firefox** icon in the taskbar, it will locate the process inside of the process list



Right clicking the **firefox.exe** process will open a menu where the process can be terminated.

lsass.exe	0.04	4,284 K	12,252 K	572 Local Security Authority Proc...	Microsoft Corporation
winlogon.exe		1,928 K	8,988 K	492 Windows Logon Application	Microsoft Corporation
dwm.exe	0.84	27,260 K	48,356 K	808 Desktop Window Manager	Microsoft Corporation
explorer.exe	0.59	26,356 K	71,096 K	920 Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.04	3,852 K	14,548 K	3480 VMware Tools Core Service	VMware, Inc.
firefox.exe	105,164 K	149,364 K	3608 Firefox	Mozilla Corporation	
firefox.exe	4.09	28,208 K	61,596 K	3012 Firefox	Mozilla Corporation
firefox.exe	Susp...	2,548 K	44 K	4028 Firefox	Mozilla Corporation
WerFault.exe	8.36	2,992 K	12,028 K	4008 Windows Problem Reporting	Microsoft Corporation
proexp.exe		3,240 K	10,464 K	3892 Sysinternals Process Explorer	Sysinternals - www.sysinter...

After killing the process, the executable gets suspended, progressively stops using processing power (CPU usage as an example) and eventually turns red before disappearing from the process list.

Step 3



Opening **Command Prompt** application from search bar.

任务	CPU	内存	磁盘 I/O	线程数	状态	启动方式	公司
explorer.exe	0.13	24,608 K	73,852 K	920	Windows Explorer	Microsoft Corporation	
vmtoolsd.exe	0.06	3,852 K	14,548 K	3480	VMware Tools Core Service	VMware, Inc.	
procexp.exe		3,096 K	10,412 K	3892	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	3.28	13,036 K	35,712 K	3848	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		1,572 K	2,844 K	1972	Windows Command Processor	Microsoft Corporation	
conhost.exe	0.01	5,836 K	15,328 K	3856	Console Window Host	Microsoft Corporation	

Using the **Find Window's Processes** (inside process explorer) by drag and dropping it onto the **Command Prompt** icon in the taskbar, it will locate the process inside of the process list

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

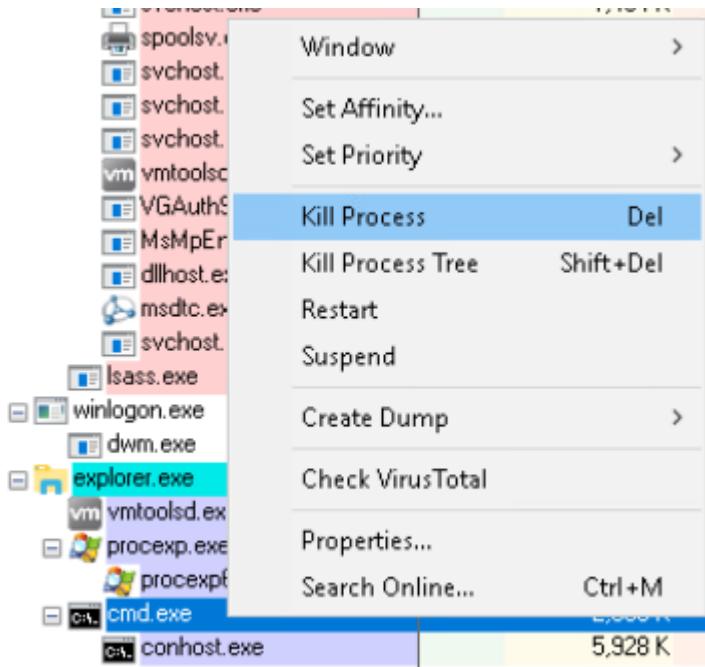
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.12: Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Administrator>
```

explorer.exe	0.25	22,944 K	72,576 K	920 Windows Explorer	Microsoft Corporation	
vmtoolsd.exe	0.06	3,852 K	14,548 K	3480 VMware Tools Core Service	VMware, Inc.	
procesp.exe		3,096 K	10,412 K	3892 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procesp64.exe	4.14	13,336 K	34,200 K	3848 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		1,596 K	2,980 K	1972 Windows Command Processor	Microsoft Corporation	
conhost.exe	0.24	5,808 K	17,396 K	3856 Console Window Host	Microsoft Corporation	
PING.EXE	0.72	772 K	3,412 K	1136 TCP/IP Ping Command	Microsoft Corporation	

After typing the **ping** command with an appropriate IP address (in this case its **192.168.0.1**) in **cmd** your device will send a total of 4 packets to the desired IP address and will give a breakdown of how many packets were sent, received and lost. Additionally when executing the **ping** command, in the **Process Explorer** a child process will appear called **PING.EXE**.

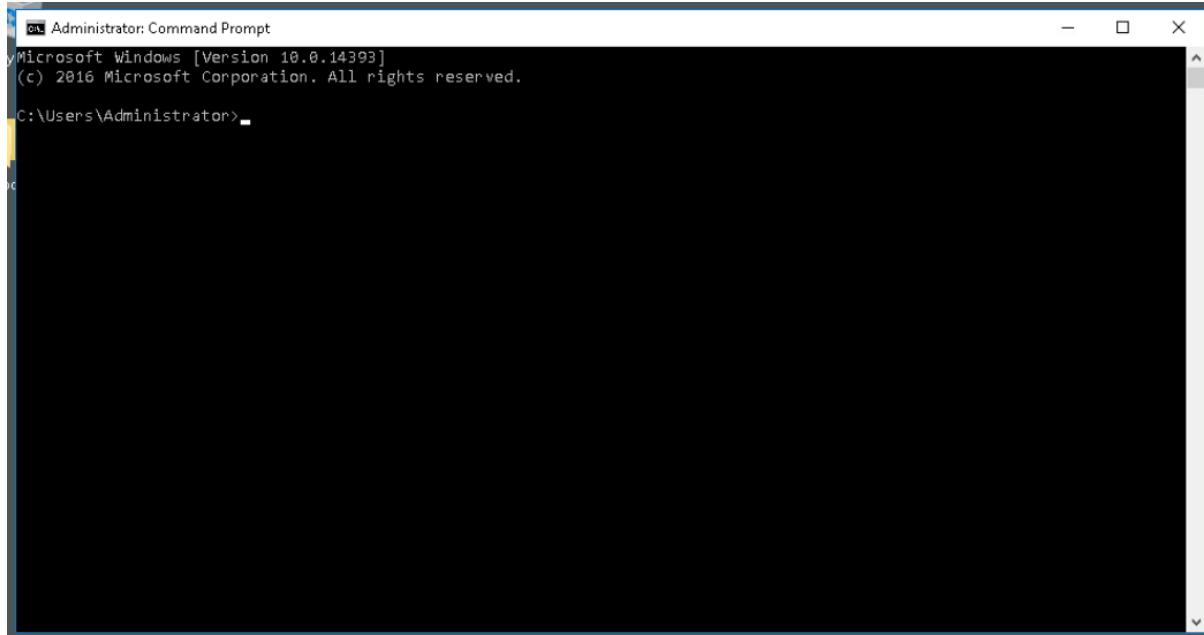


explorer.exe	1.44	23,132 K	72,560 K	920 Windows Explorer	Microsoft Corporation	
vmtoolsd.exe	0.05	3,884 K	14,656 K	3480 VMware Tools Core Service	VMware, Inc.	
procexp.exe		3,096 K	10,412 K	3892 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	3.54	13,380 K	34,236 K	3848 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		1,596 K	2,980 K	1972 Windows Command Processor	Microsoft Corporation	
conhost.exe		5,808 K	17,404 K	3856 Console Window Host	Microsoft Corporation	

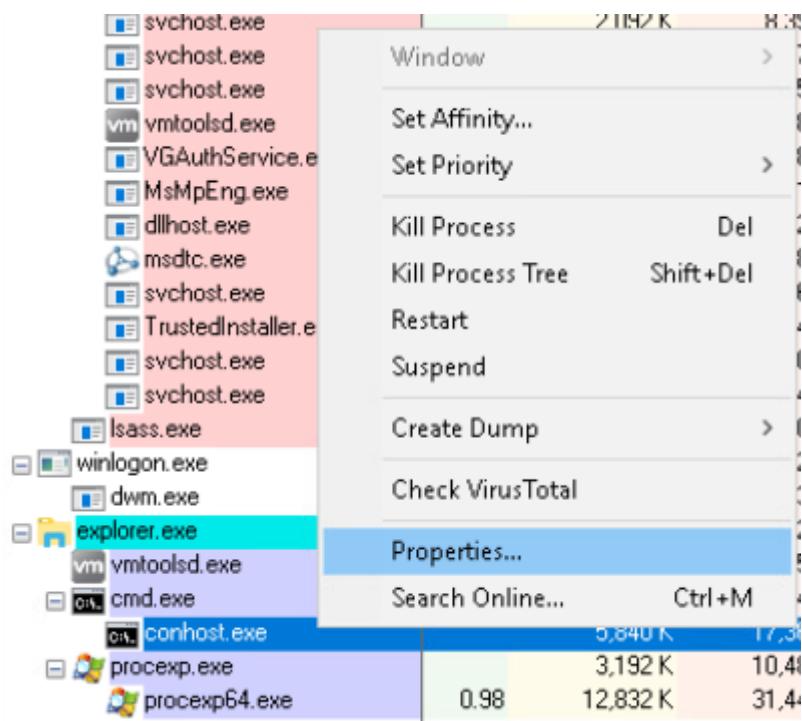
After killing the process, the executable progressively stops using processing power (CPU usage as an example) and eventually turns red before disappearing from the process list as it has been terminated.

Part 2

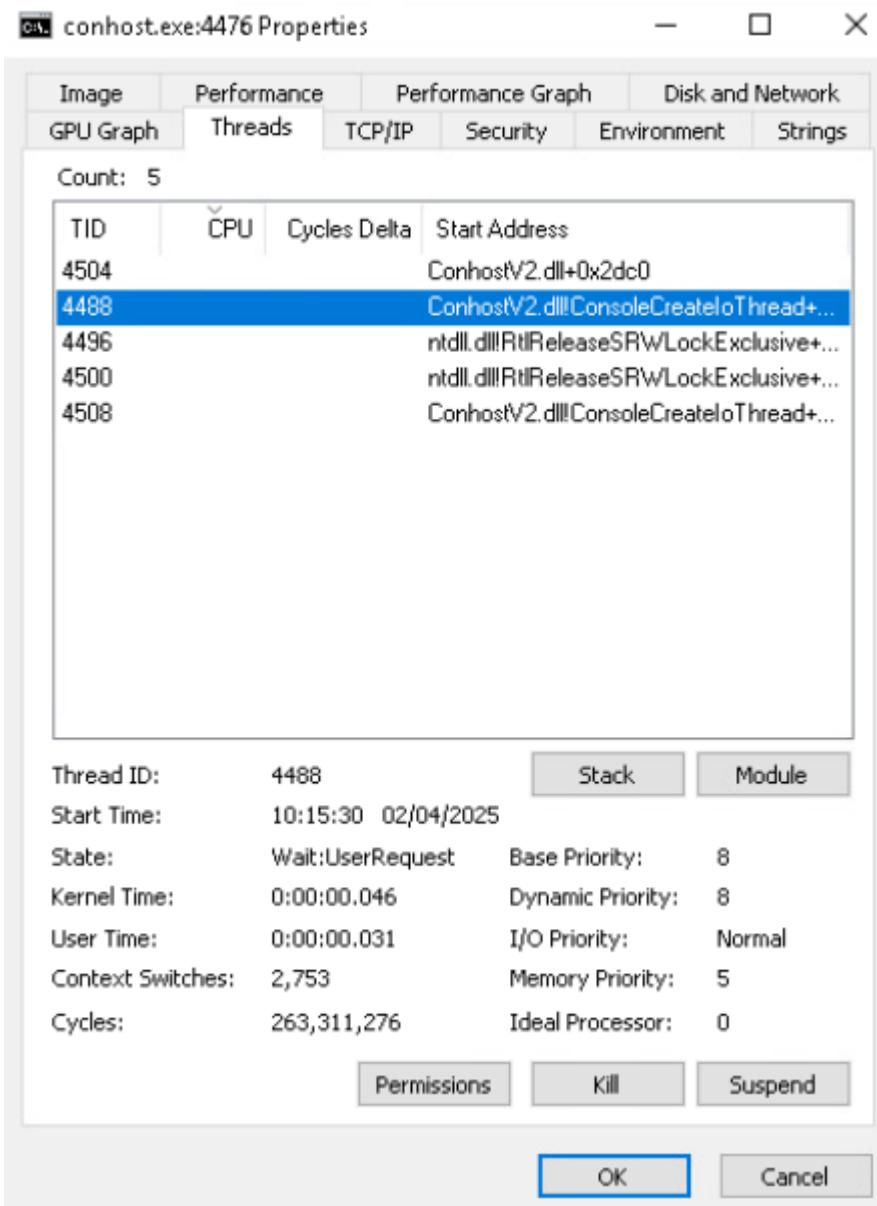
Step 1



Opening a fresh **Command Prompt**



Tabbing back into the **Process Explorer**, finding the **cmd** process using the **Find Window's Processes** tool and expanding it to be able to see **conhost.exe** process. After right clicking it and clicking on properties a property window will open.



Thread ID:	4496	Stack	Module
Start Time:	10:15:31 02/04/2025		
State:	Wait:WrQueue	Base Priority:	8
Kernel Time:	0:00:00.000	Dynamic Priority:	8
User Time:	0:00:00.000	I/O Priority:	Normal
Context Switches:	6	Memory Priority:	5
Cycles:	3,801,298	Ideal Processor:	0

Permissions Kill Suspend

Inside the **Thread** tab each thread is selectable and once selected it will different information about each one (like memory priority and state)

Step 2

Process Explorer - Sysinternals: www.sysinternals.com [WINCLIENT\Administrator]

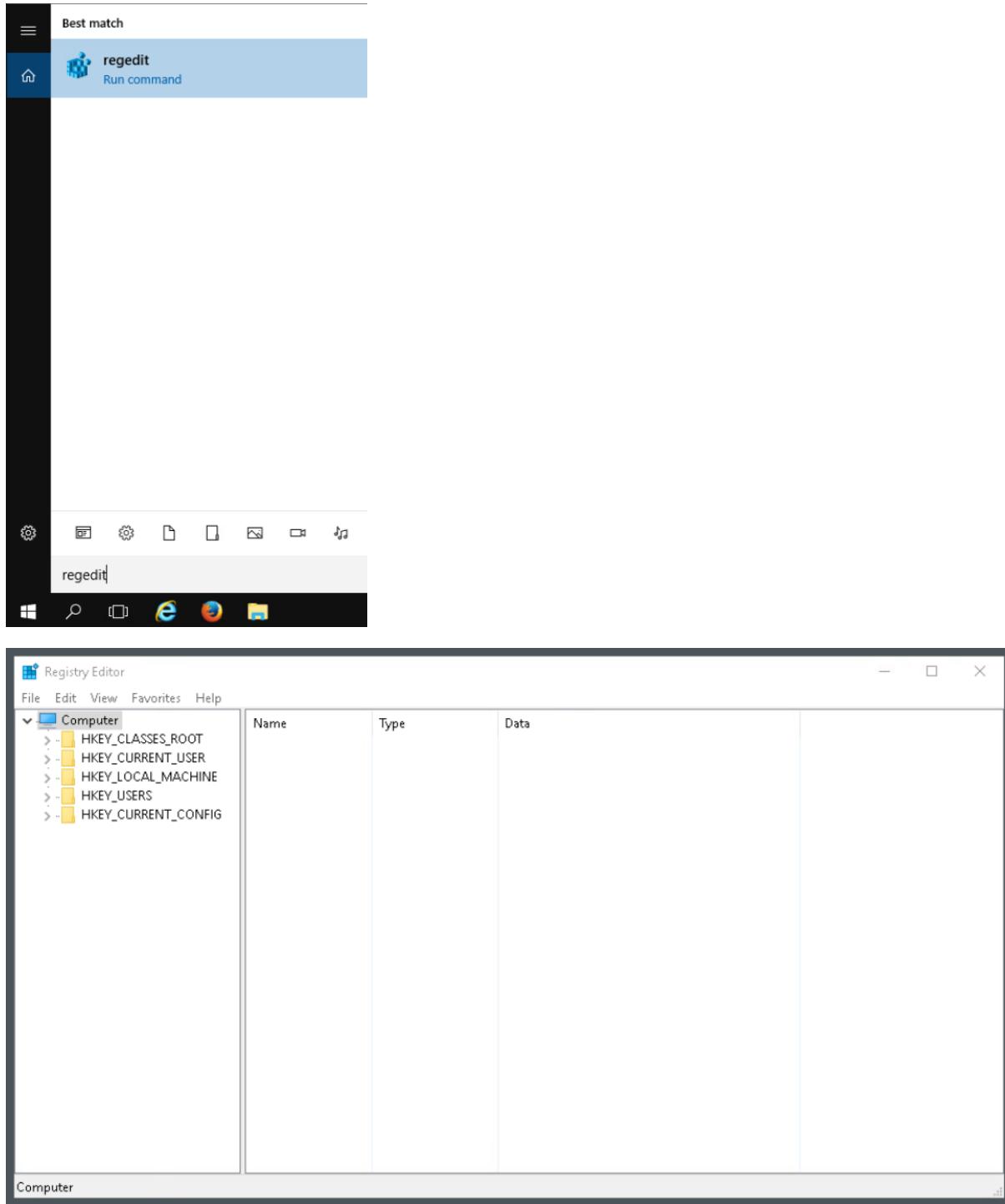
The screenshot shows the Windows Task Manager interface. The 'View' menu is open, and the 'Handles' option is highlighted with a blue selection bar. The main pane displays a list of handles, which are essentially file descriptors or pointers used by processes. The columns are 'Type' and 'Name'. The list includes various system objects like registry keys and files.

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	\Device\CNG
File	\Device\DeviceApi
File	C:\Windows\Registration\R00000000000c.cib
File	C:\Windows\System32\en-US\user32.dll.mui
File	C:\Windows\System32\en-US\ConhostV2.dll.mui
File	C:\Windows\WinSxS\land64_microsoft.windows.common-controls_6595b64144ccf1df_6.0....
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

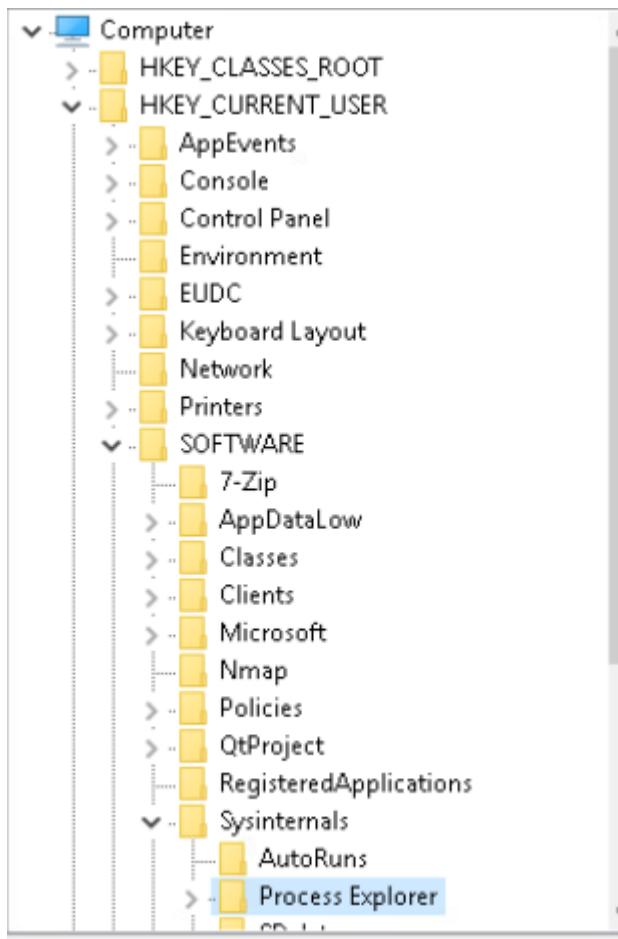
CPU Usage: 4.02% | Commit Charge: 20.54% | Processes: 47 | Physical Usage: 27.40%

Opening the **Handles** panel allows to see all associated files that are used on the process (in this example its for **cmd**).

Part 3



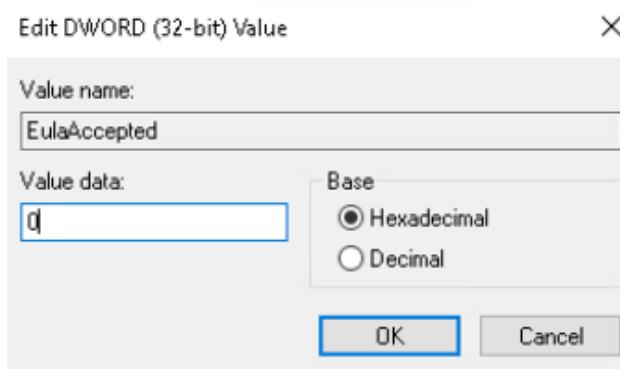
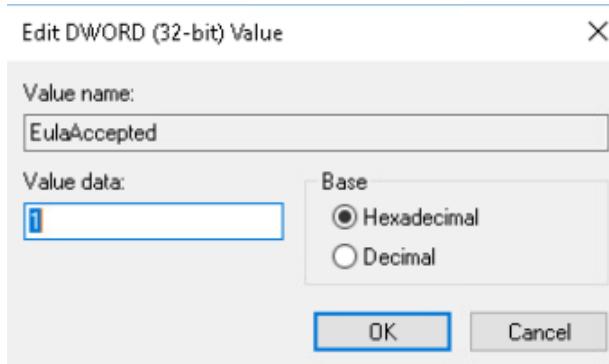
Opening **Registry Editor**



Following and expanding the hierarchy to locate the **Process Explorer's** configuration

Name	Type	Data
ETWStandardUs...	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000001 (1)
FindWindowpla...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
FormatIoBytes	REG_DWORD	0x00000001 (1)
GpuNodeUsage...	REG_DWORD	0x00000001 (1)
HandleColumn...	REG_DWORD	0x00000002 (2)
HandleSortColu...	REG_DWORD	0x00000000 (0)
HandleSortDire...	REG_DWORD	0x00000001 (1)
HideWhenMinim...	REG_DWORD	0x00000000 (0)
HighlightDelProc	REG_DWORD	0x00000001 (1)
HighlightDurati...	REG_DWORD	0x000003e8 (1000)
HighlightImmer...	REG_DWORD	0x00000001 (1)
HighlightJobs	REG_DWORD	0x00000000 (0)
HighlightNetPr...	REG_DWORD	0x00000000 (0)
HighlightNewPr...	REG_DWORD	0x00000001 (1)
HighlightOwnP...	REG_DWORD	0x00000001 (1)
HighlightPacked	REG_DWORD	0x00000001 (1)
HighlightProtec...	REG_DWORD	0x00000000 (0)
HighlightReloca...	REG_DWORD	0x00000000 (0)
HighlightServices	REG_DWORD	0x00000001 (1)
HighlightSuspe...	REG_DWORD	0x00000001 (1)
NumColumnSets	REG_DWORD	0x00000000 (0)

Highlighted is the **key** value behind the condition of "**EulaAccepted**", and the value is 0x00000001 (1) - this prevents from the EULA window opening every time when opening the application



Name	Type	Data
ETWstandardUs...	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000000 (0)

This key's value can be edited, and for this task it will be changed to the value **0**, and saved by pressing **OK**. Once this is done the value of the **Data column** for this key will change to **0x00000000 (0)**, showing that the value has been changed.

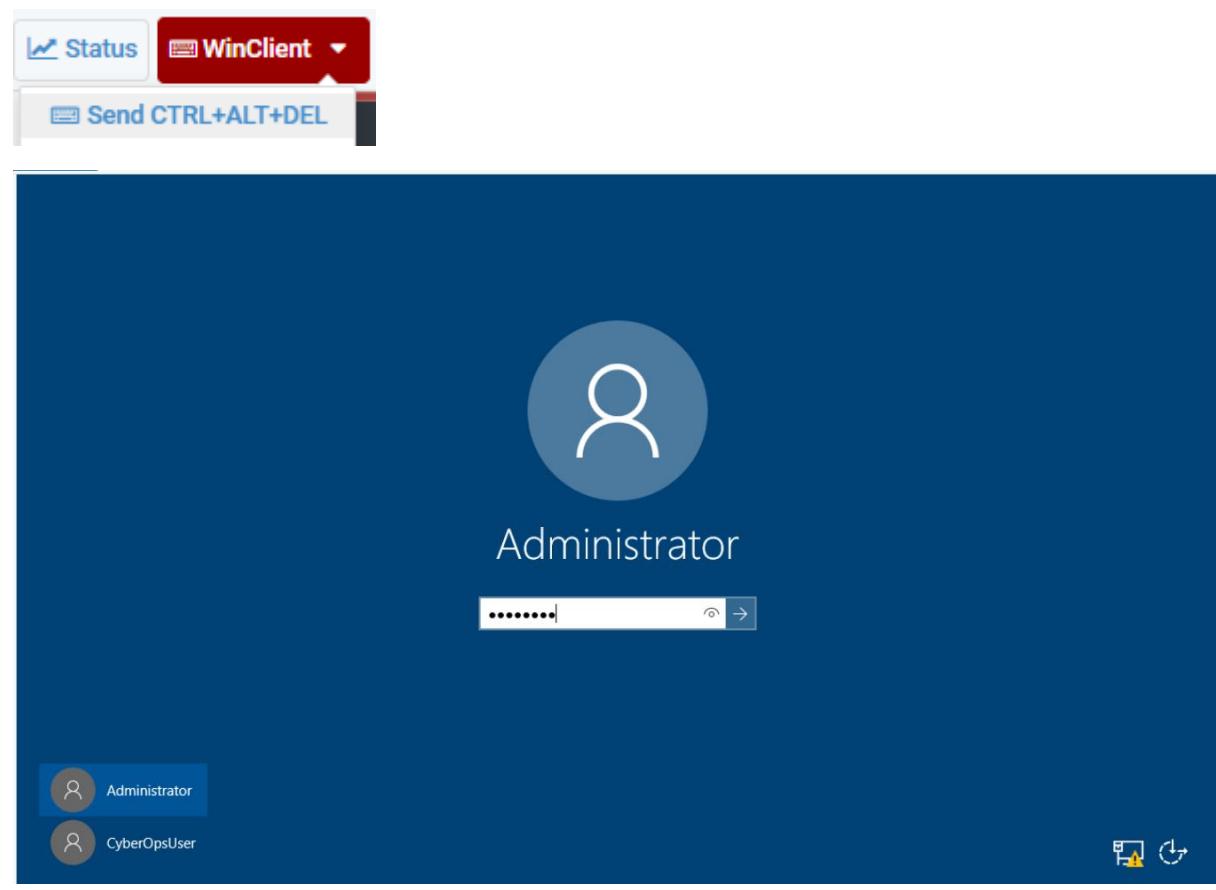


When opening the **Process Explorer** application again, the EULA window will open and will prompt the user to accept it before using the app.

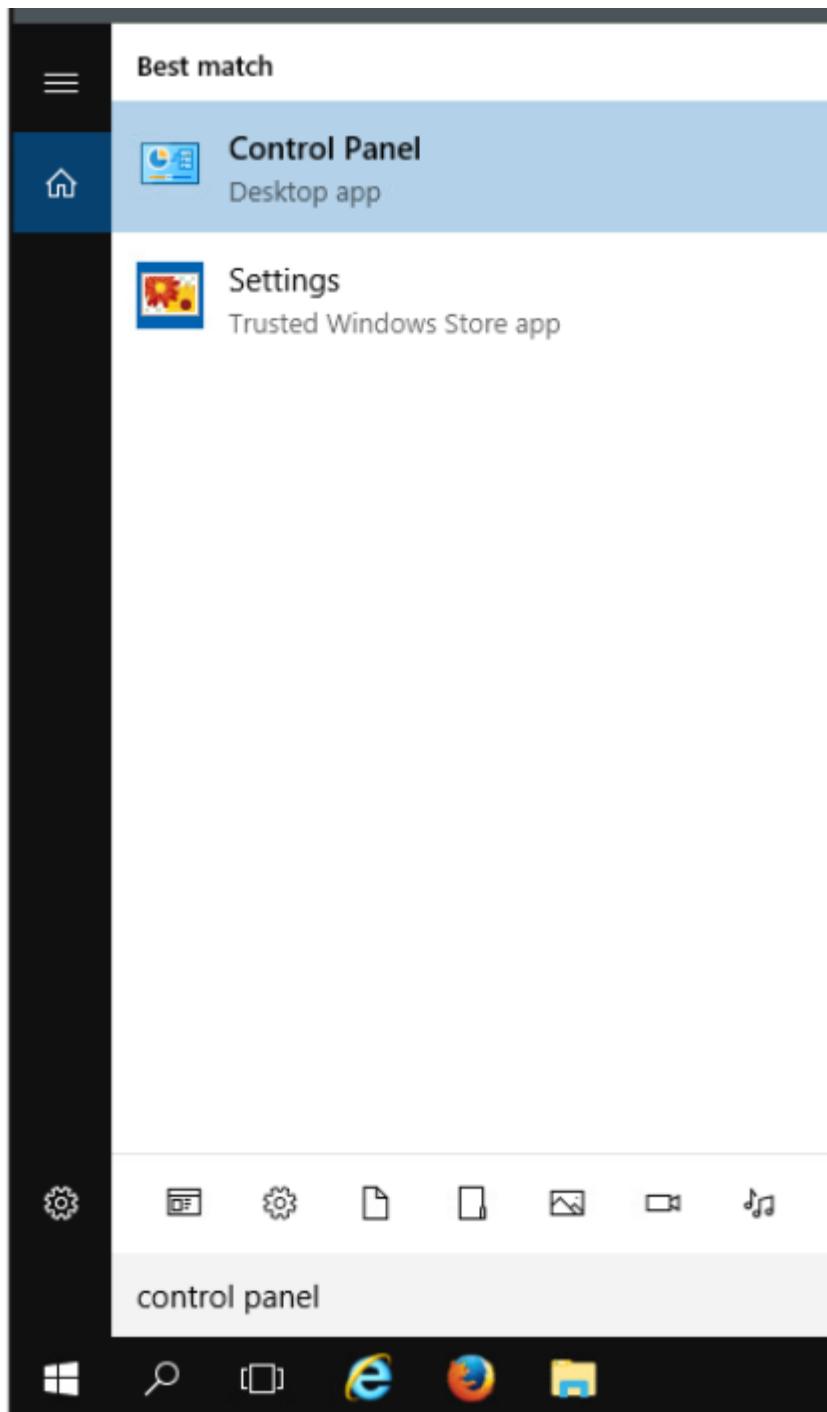
7.3.10 Lab - Create User Accounts

Part 1

Step 1

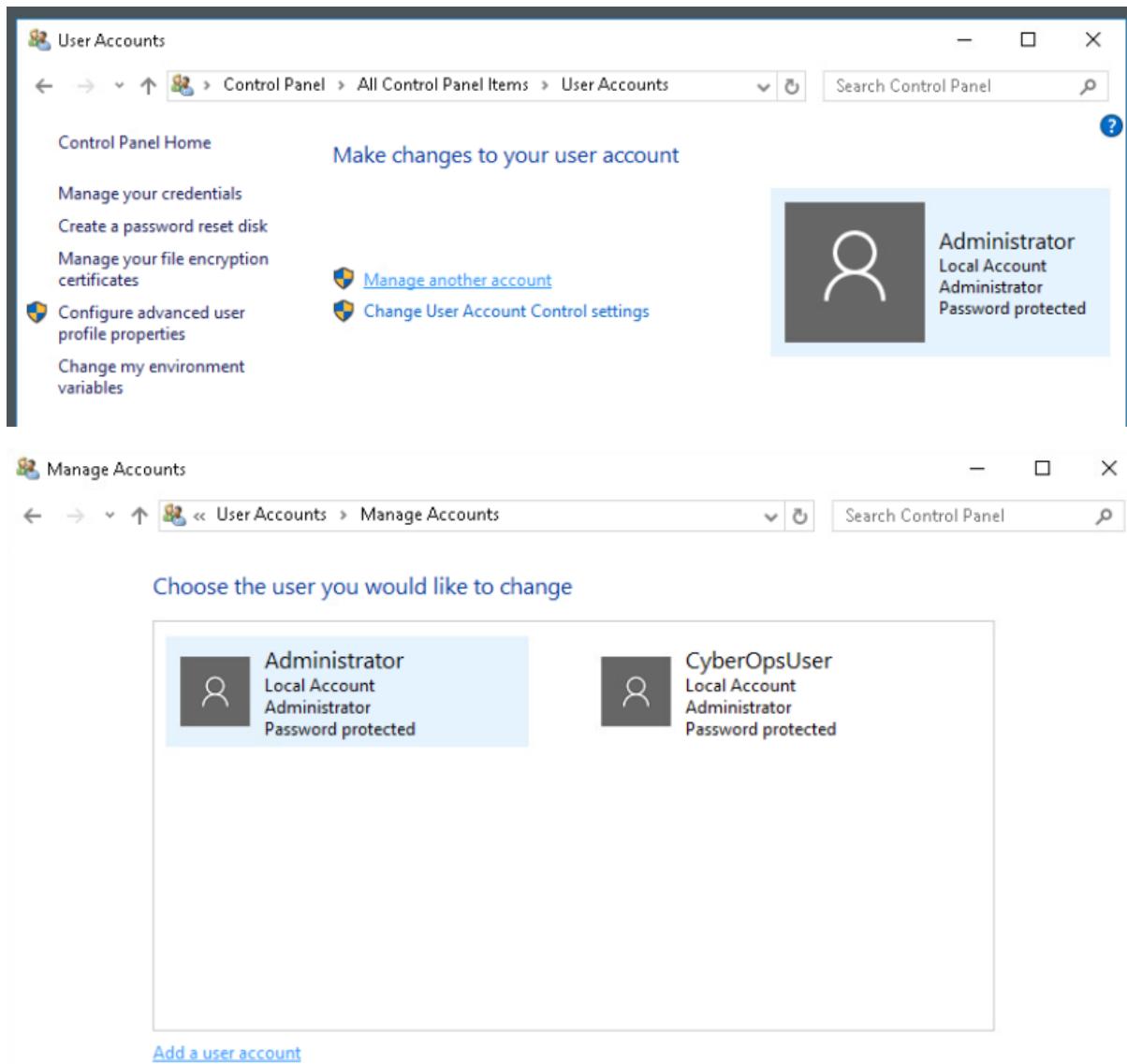


Accessing the VM on netlab



Opening **Control Panel**

Step 2



Accessing the **User Accounts** window and selecting “**Manage another account**” > “**Add a user account**”

Add a user

Choose a password that will be easy for you to remember but hard for others to guess. If you forget, we'll show the hint.

Windows can't connect to the Internet right now. Check your Internet connection and try again later if you want to add a Microsoft account.

User name	User1
Password	*****
Reenter password	*****
Password hint	User1 Password X

Your password hint cannot contain your password.

Add a user

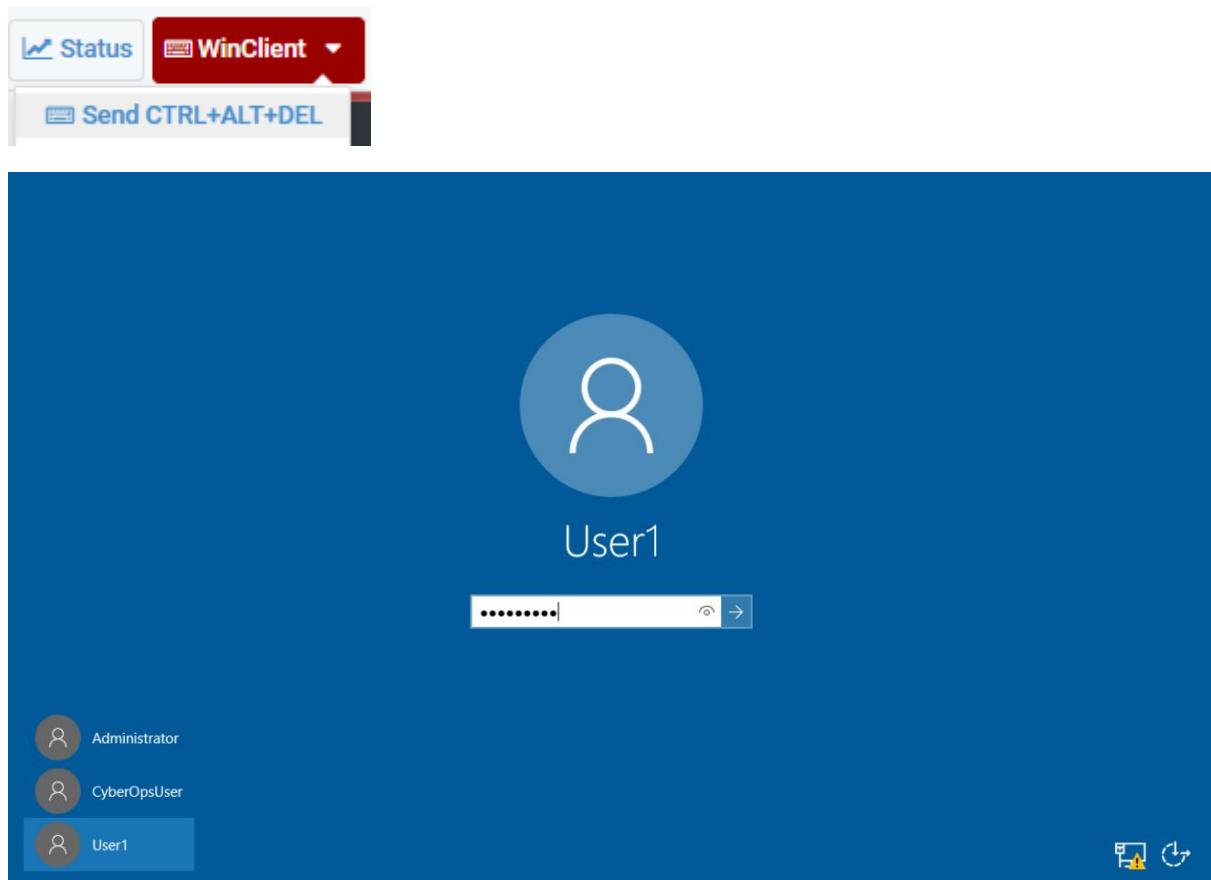
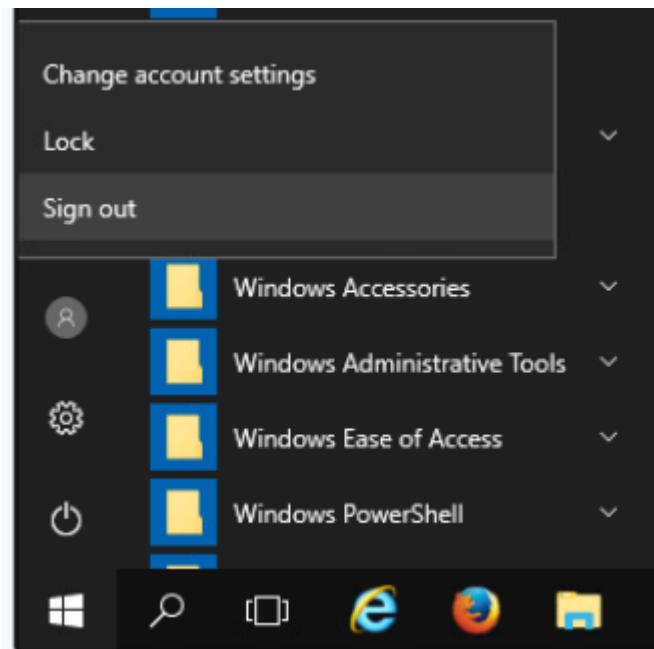
The following user will be able to sign in to this PC.



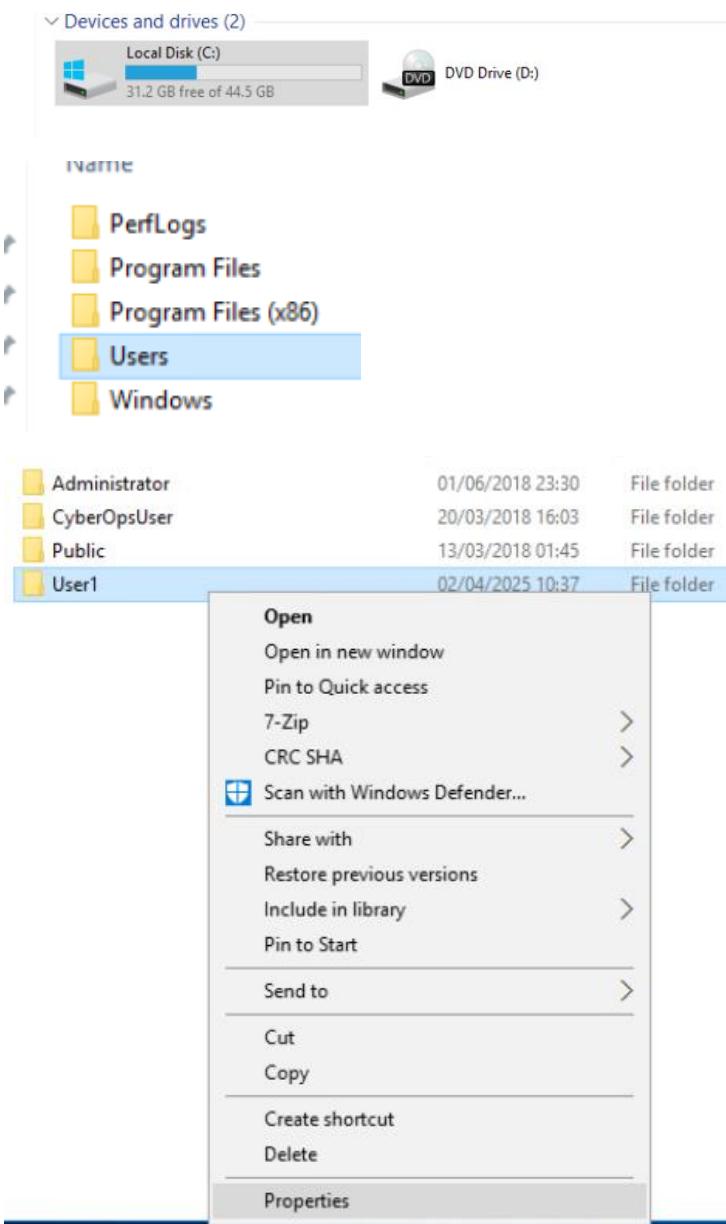
User1
Local account

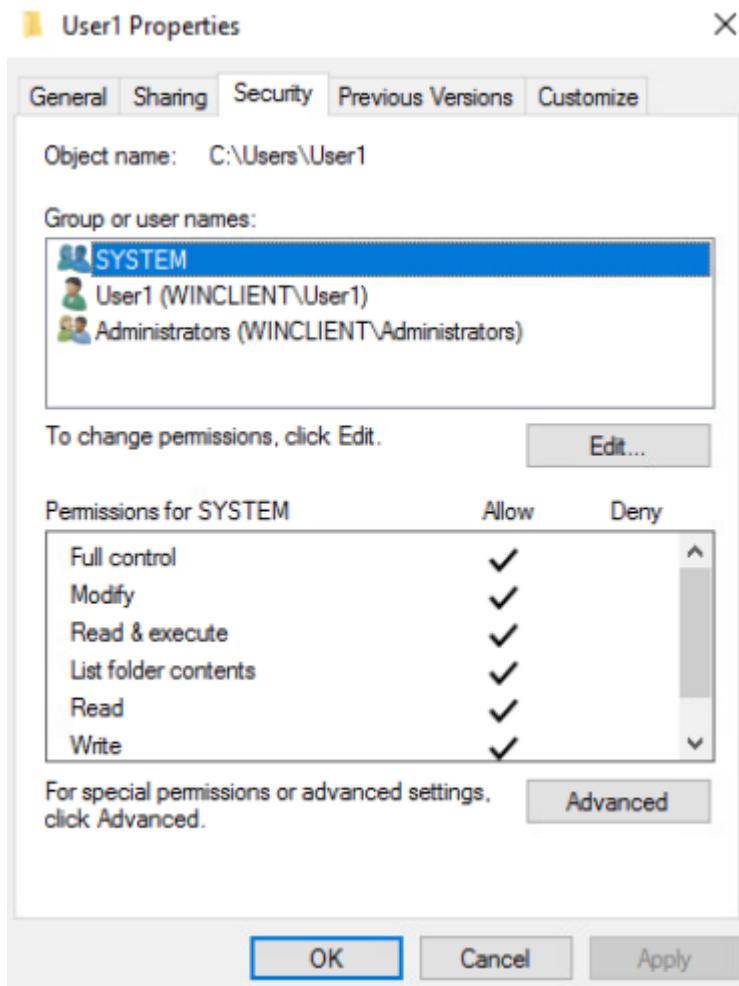
Finish

Creating a **new** user with mentioned parameters then selecting "**Next**" > "**Finish**"

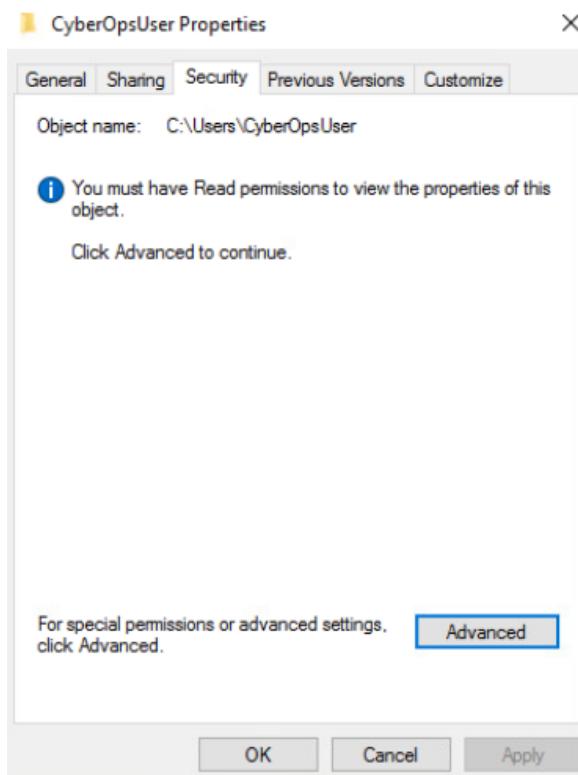
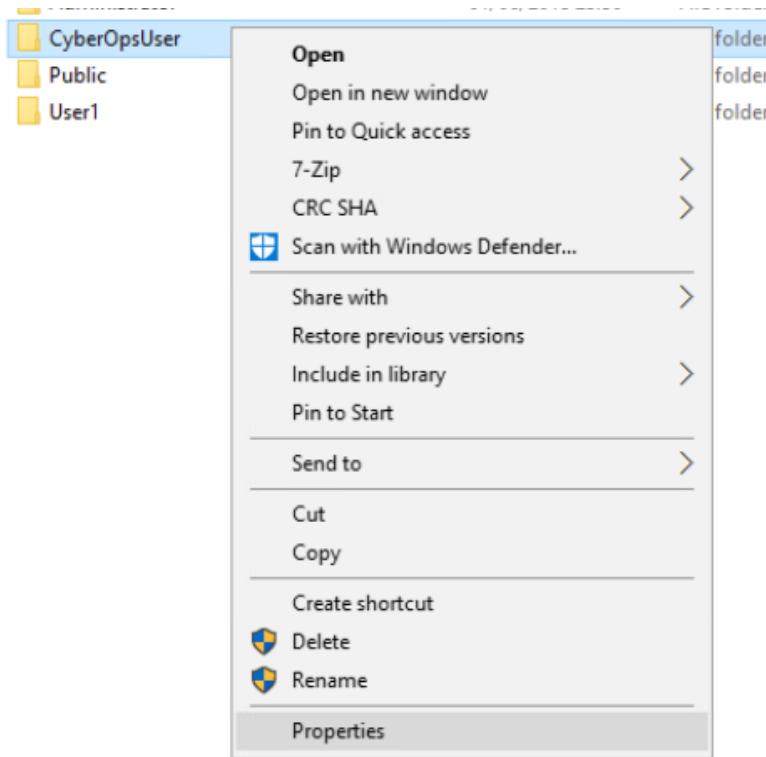


Logging out of the current account and logging into the new **User1** account

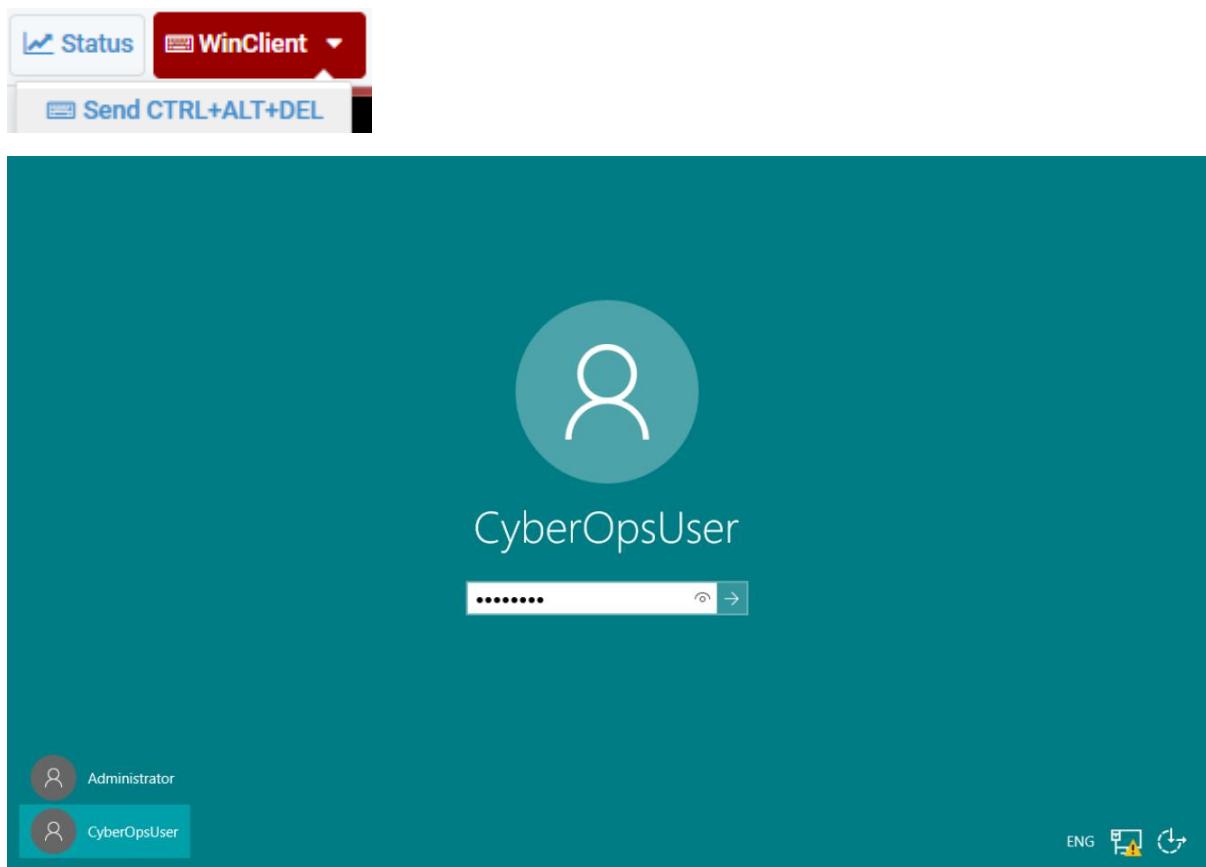
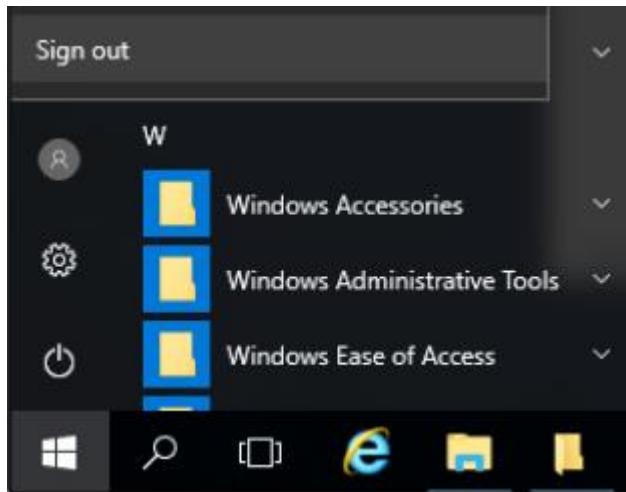




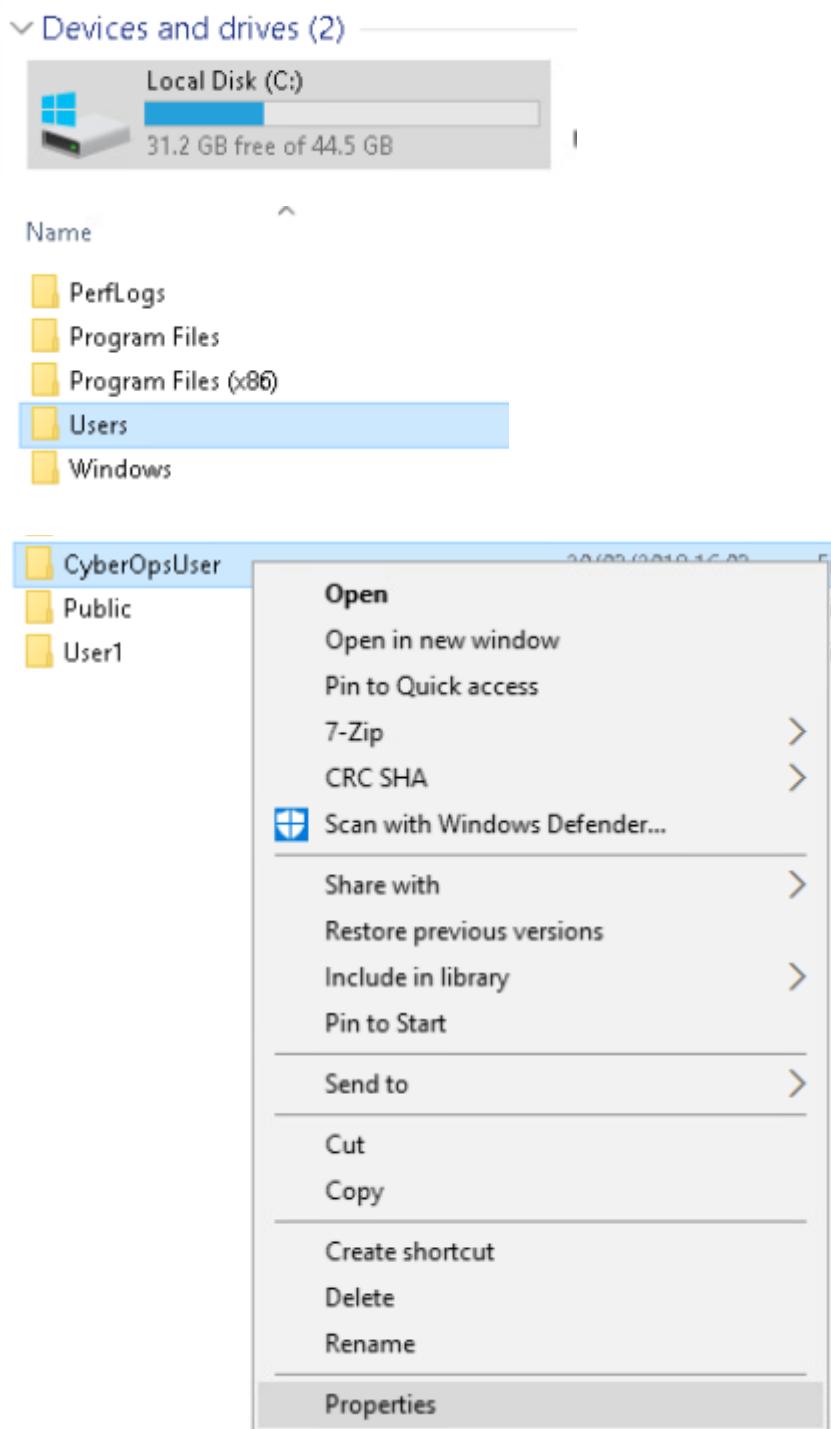
Navigating “C:” > “Users” > “User1” > “Properties” > “Security” will show the groups & users and the amount of access they have to the folder – in this case the groups **System** & **Administrators** have full access to the folder

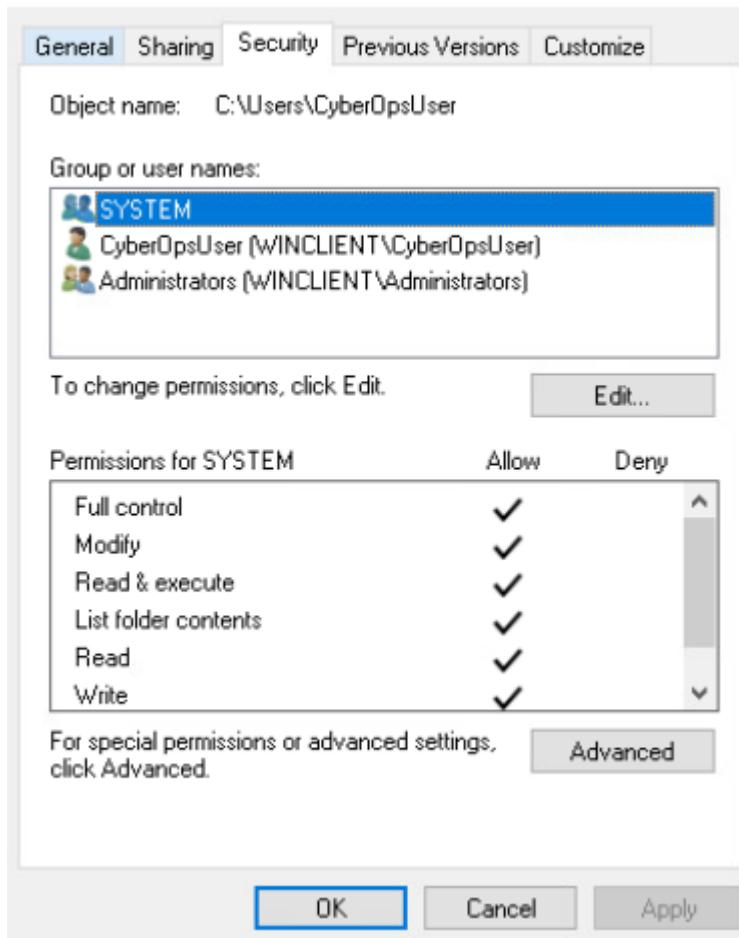


While logged in as **User1** and attempting to look at the **Security** tab of the **CyberOpsUser** folder, you will be denied access to view that data as you do not have the permission for that



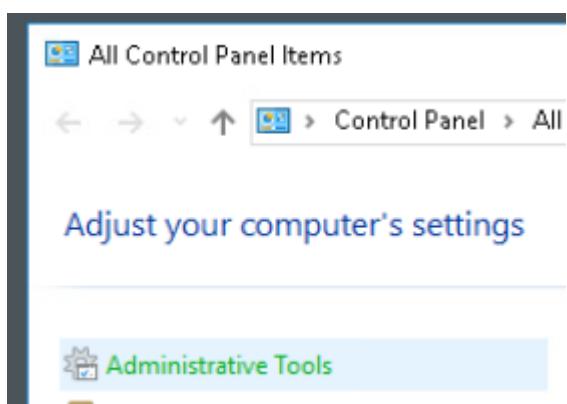
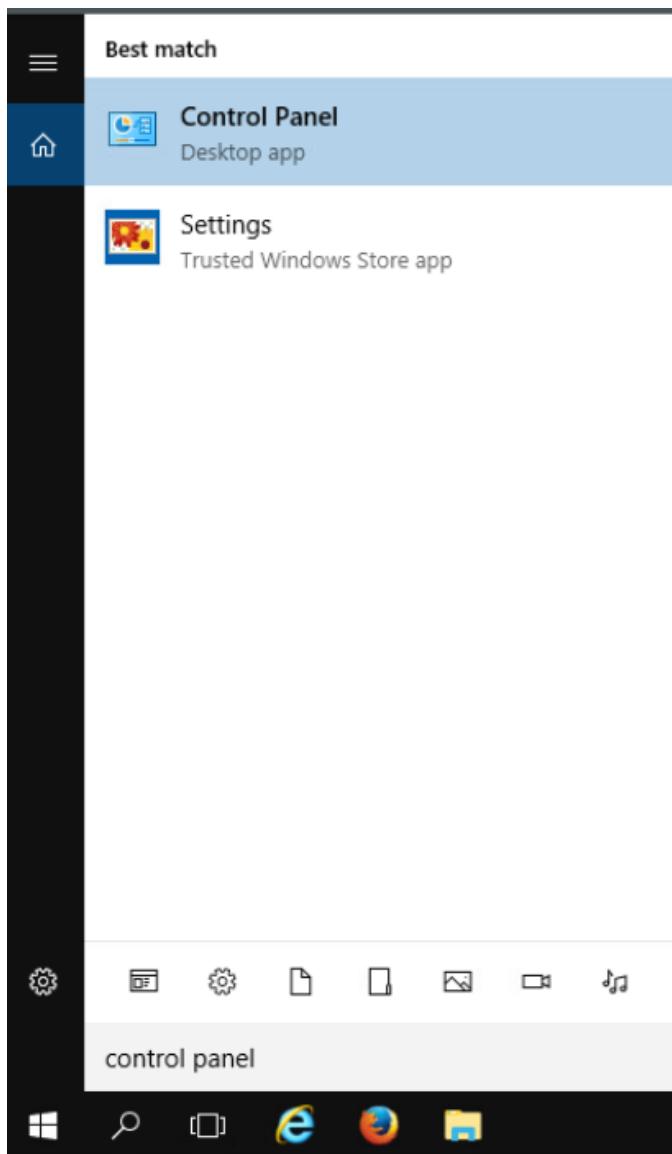
Logging in as **CyberOpsUser**

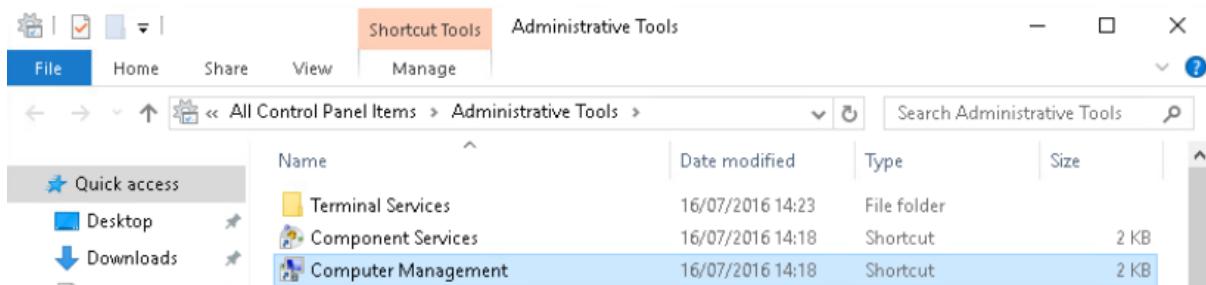




Navigating to the folder “**C:\Users**” and checking the **Security** tab of that folder will show that the system and administrator groups have full control over it

Part 2

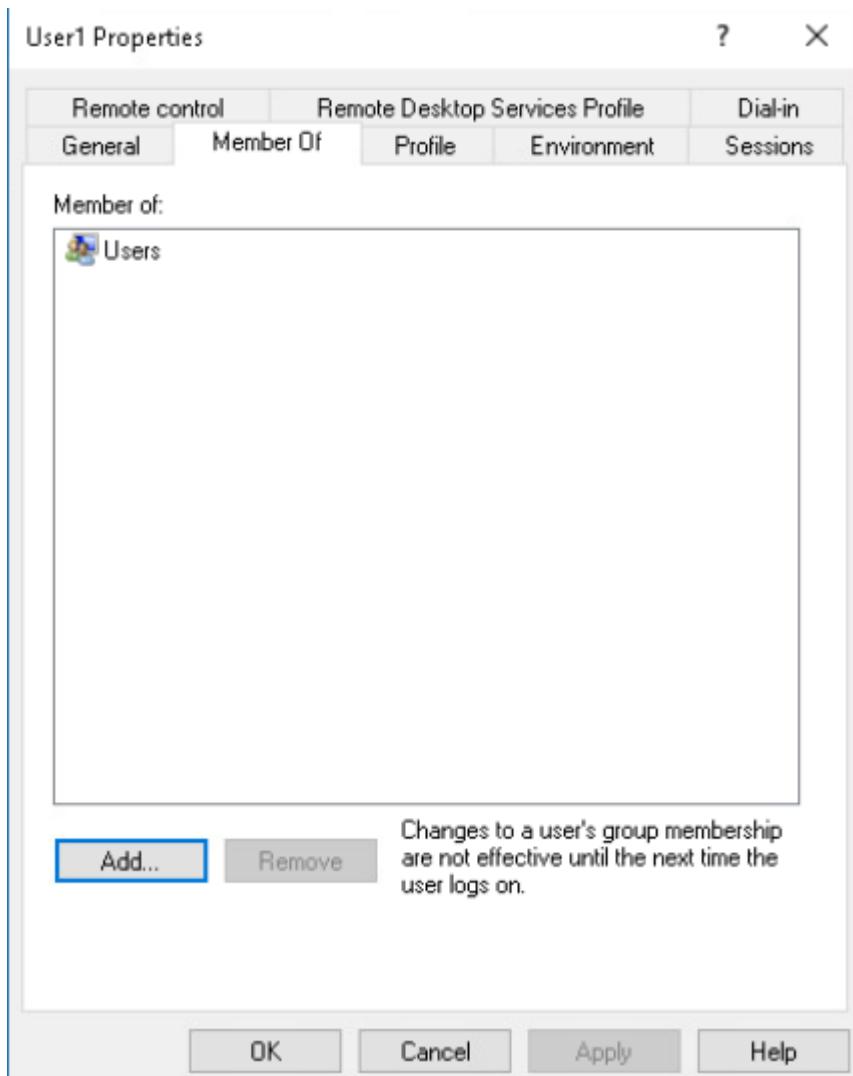




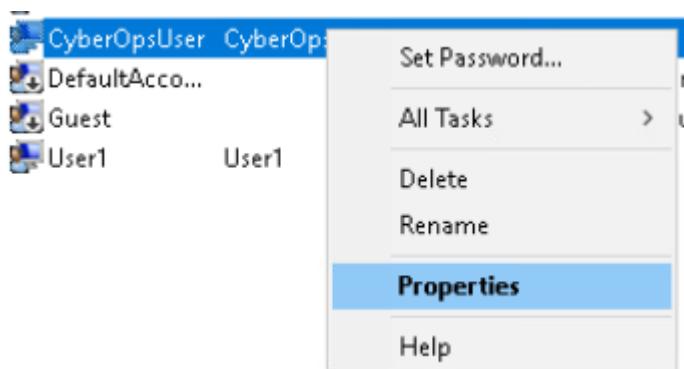
Opening and navigating: "Control Panel" > "Administrative Tools" > "Computer Management"

The screenshots illustrate the navigation and configuration process within the Computer Management tool. The top window shows the overall structure of the management tools, while the bottom window focuses on managing user accounts.

Navigating: "Local Users and Groups" > "Users" > "Right click on User1" > "Properties"



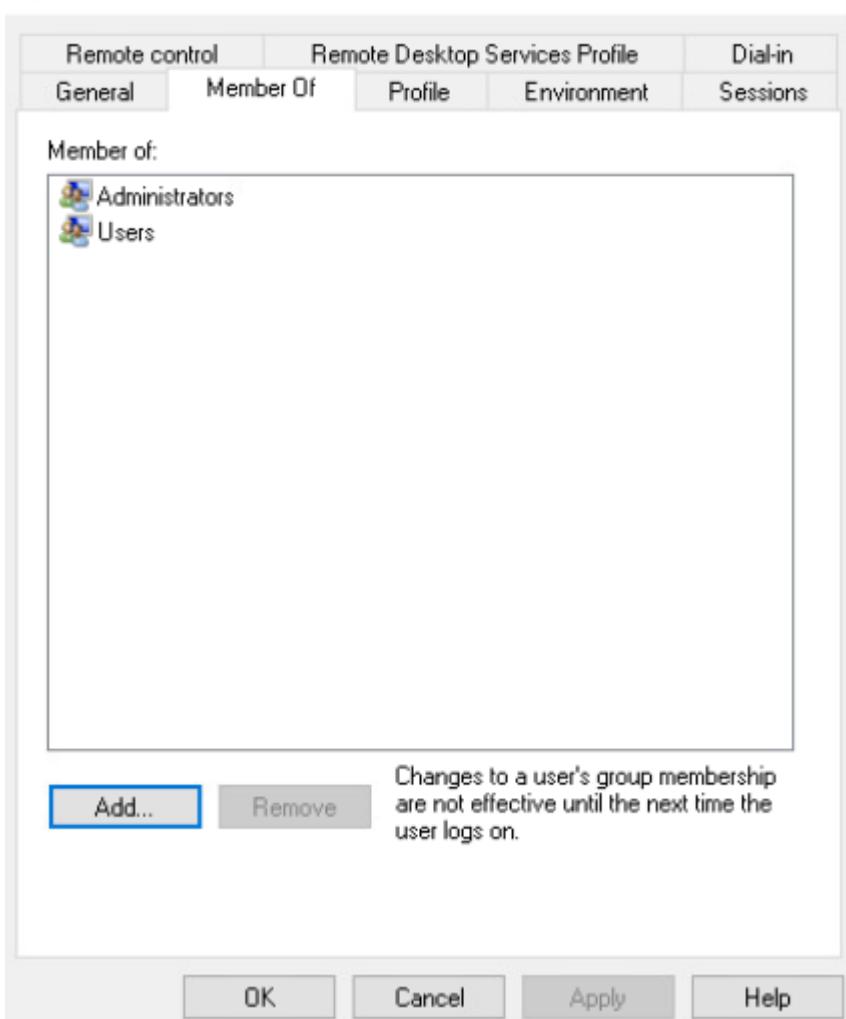
User1 is a member of the group “Users”



CyberOpsUser Properties

?

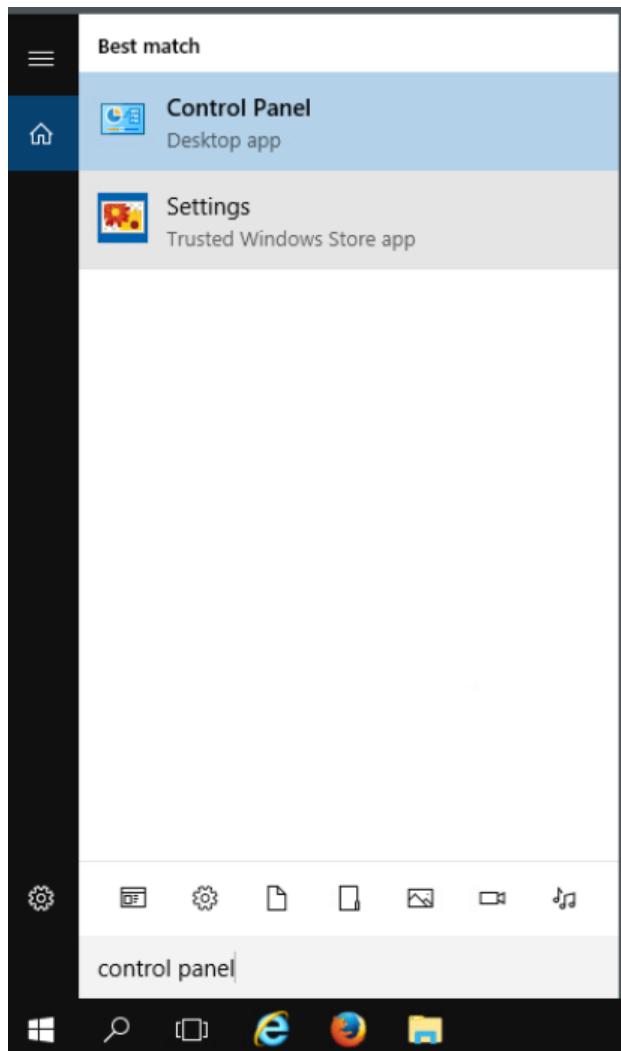
X

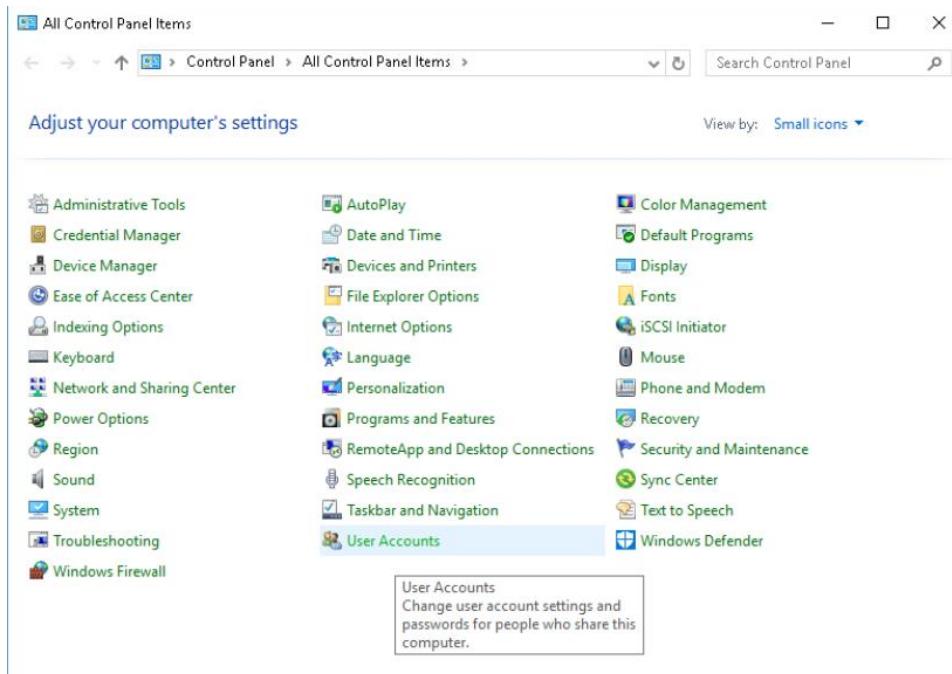


CyberOpsUser is a member of the groups “**Administrators**” and “**Users**”

Part 3

Step 1





Make changes to your user account

Manage another account

Change an Account

User Accounts > Manage Accounts > Change an Account

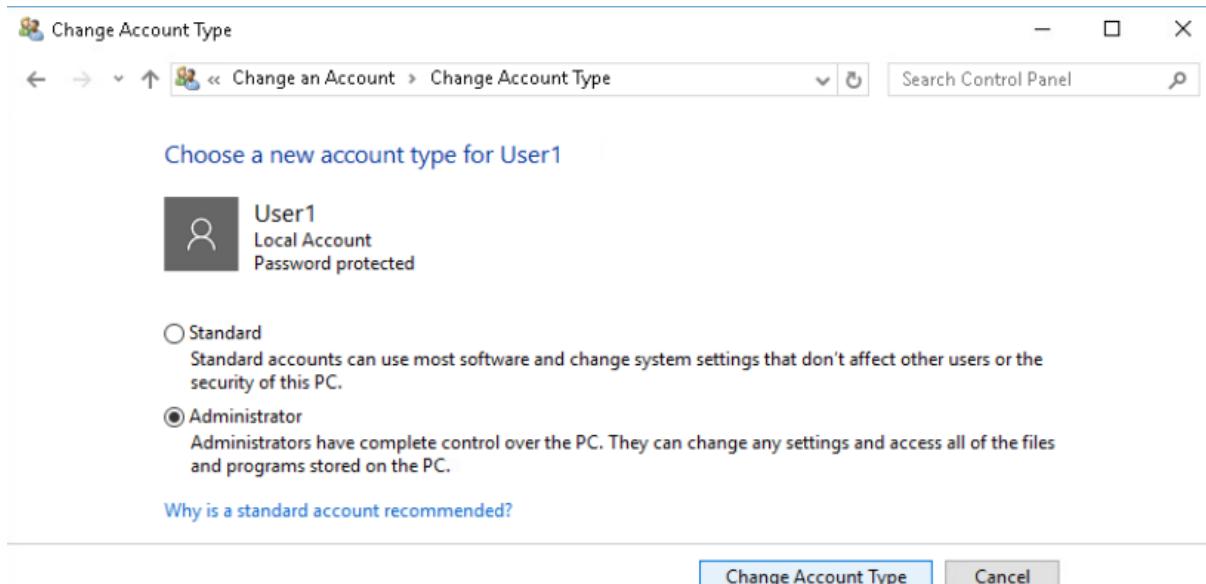
Search Control Panel

Make changes to User1's account

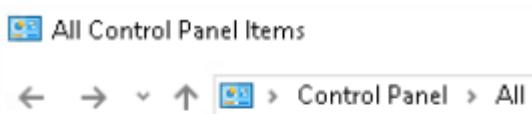
Change the account name
Change the password
Change the account type
Delete the account
Manage another account

User1
Local Account
Password protected

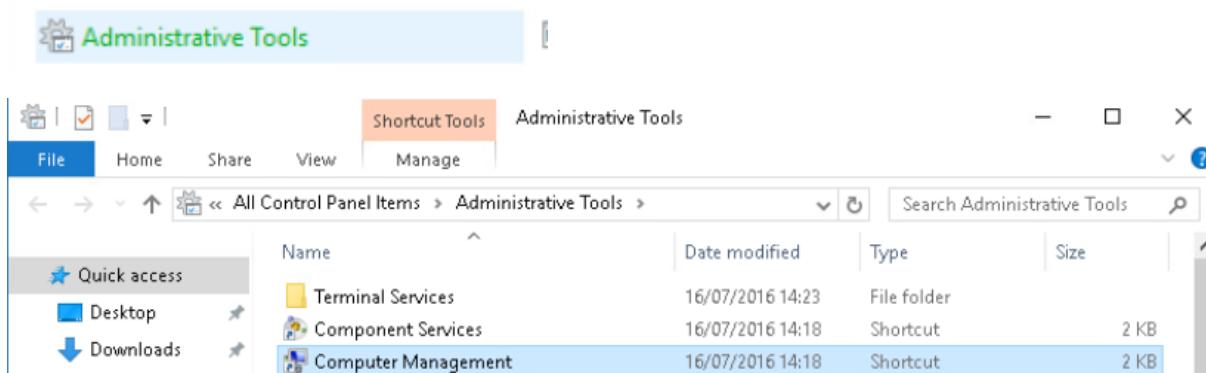
Opening and navigating: **"Control Panel"** > **"User Accounts"** > **"Manage another account"** > **"Change the account type"**



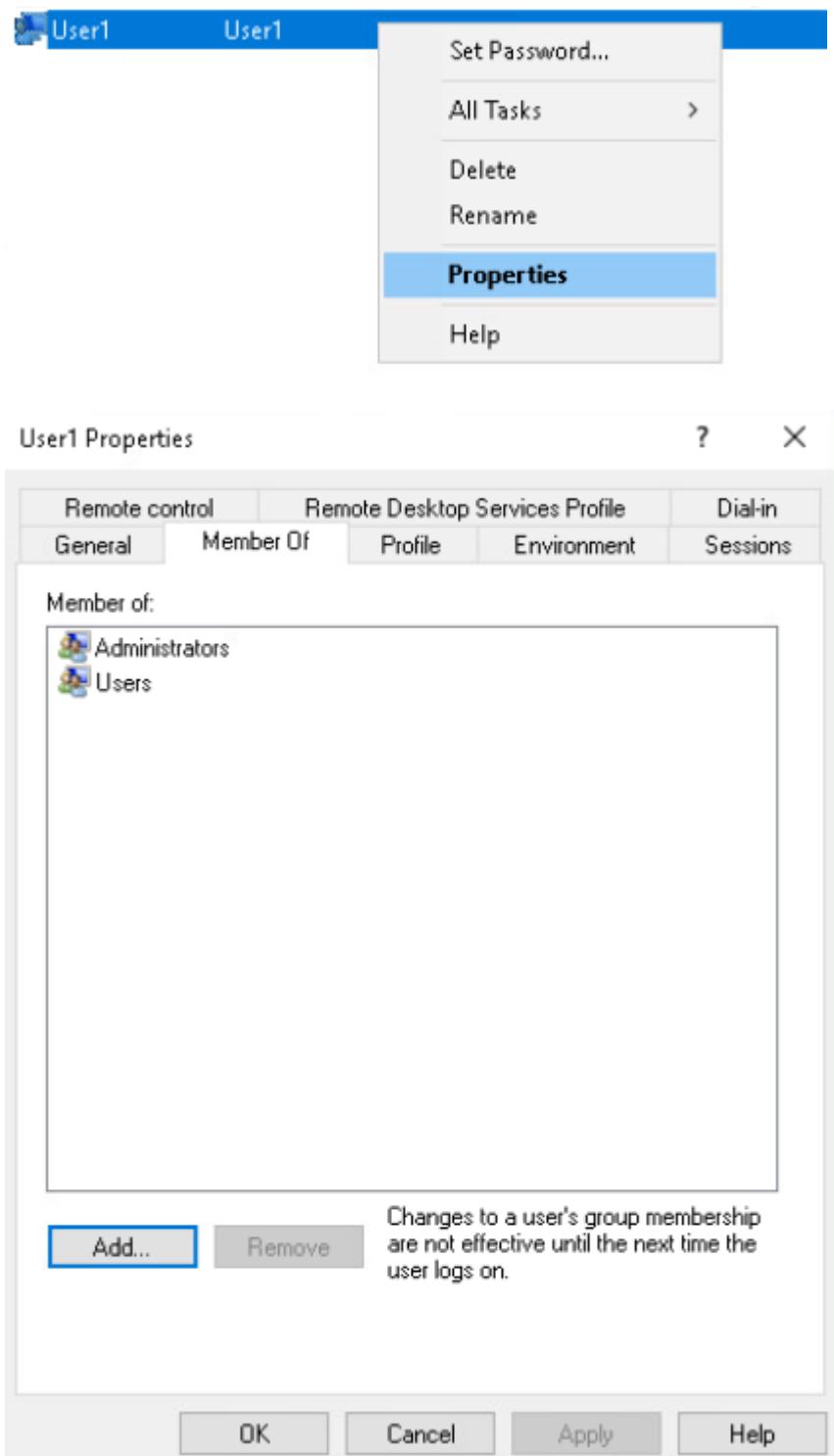
Selecting the **"Administrator"** radio button and pressing **"Change Account Type"** button will give User1 **administrative rights**.



Adjust your computer's settings



Navigating: **"Control Panel"** > **"Administrative Tools"** > **"Computer Management"**



Navigating: “Right click User1” > “Properties” > “Member Of” will show that **User1** is a part of **Administrators** group

User1 Properties

Remote control Remote Desktop Services Profile Dial-in

General	Member Of	Profile	Environment	Sessions
---------	-----------	---------	-------------	----------

Member of:

 Administrators
 Users

Add... Remove

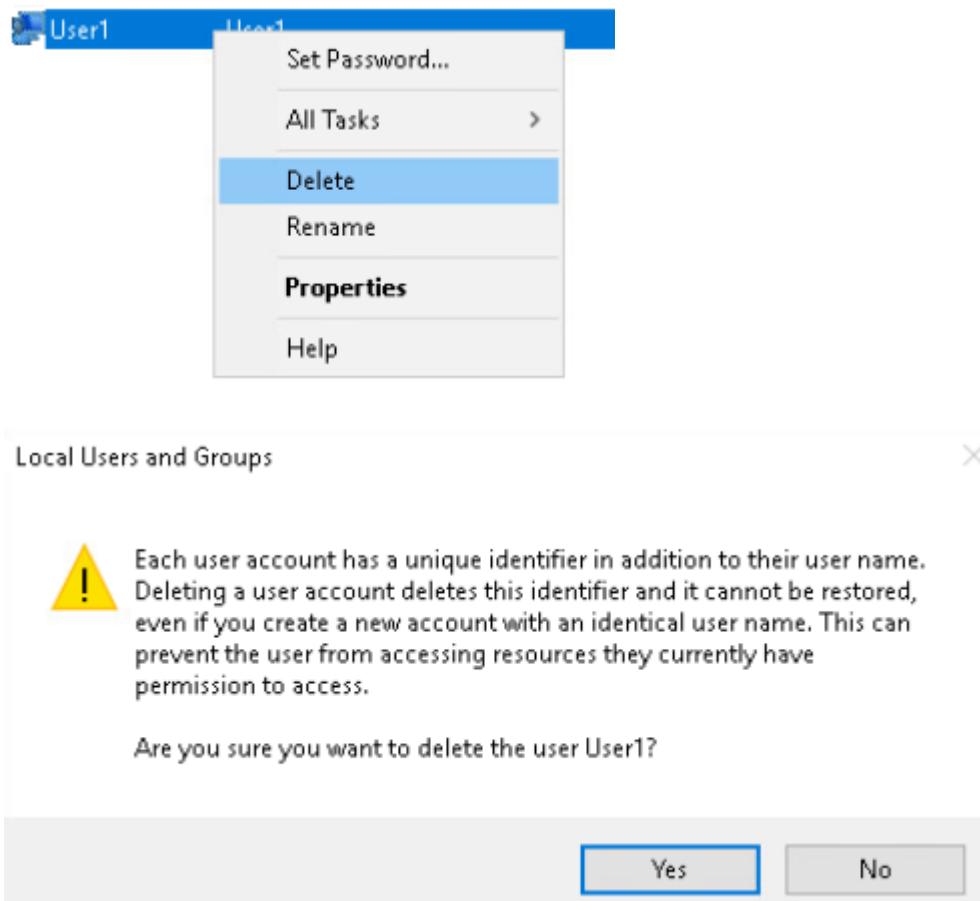
Changes to a user's group membership are not effective until the next time the user logs on

Member of:

 Users

Navigating: “**Click Administrators**” > “**Remove**” > “**OK**” will remove **User1** from the group **Administrators**

Step 2

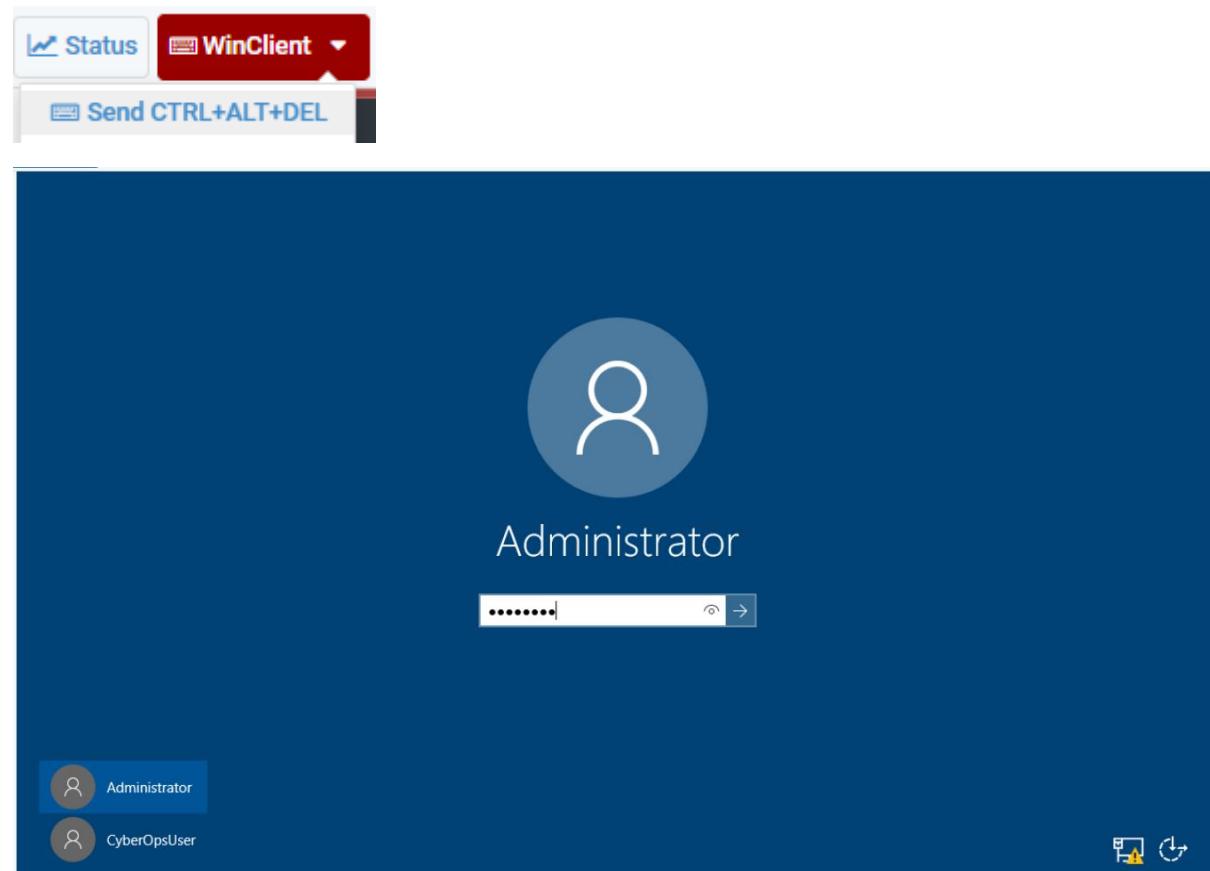


Navigate: “Right click on User1” > “Delete” > “OK” > “Yes” will delete the account from the device. Another way to delete a user account would be doing so via the Settings app

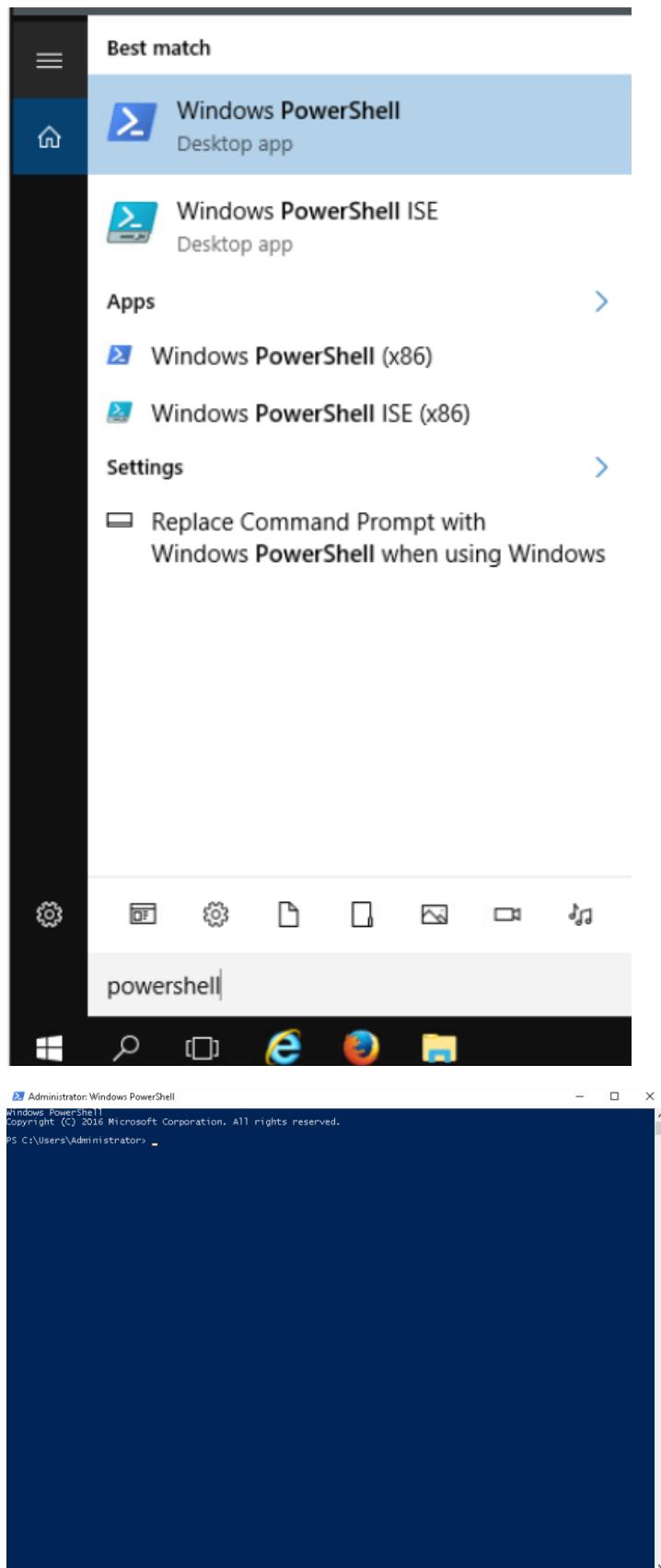
7.3.11 Lab - Using Windows PowerShell

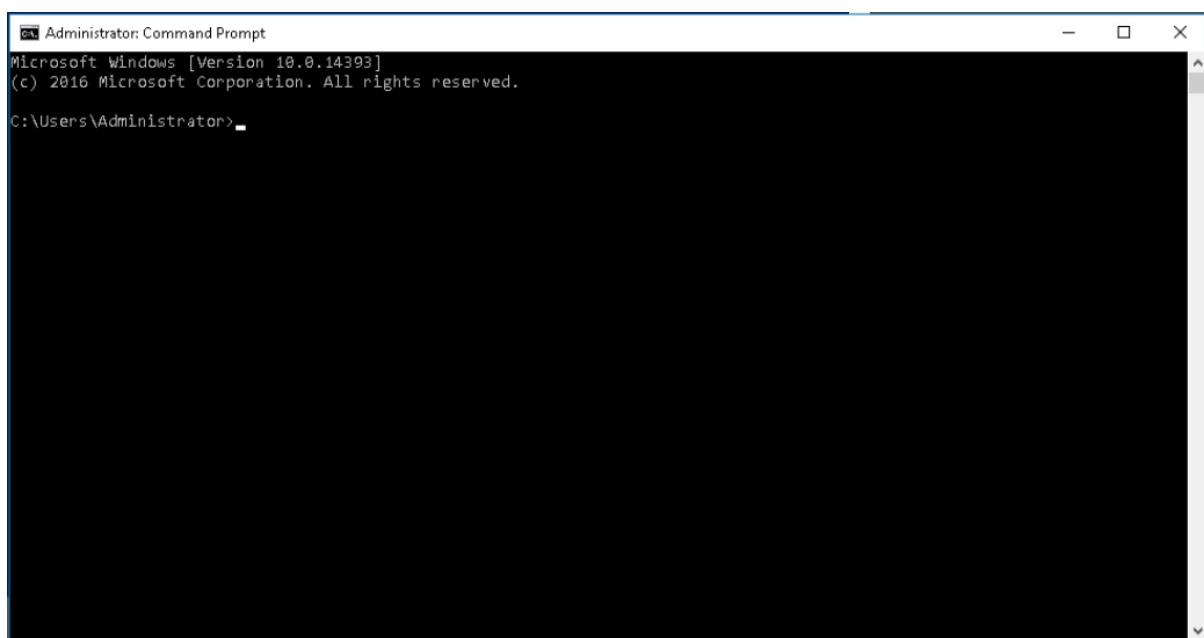
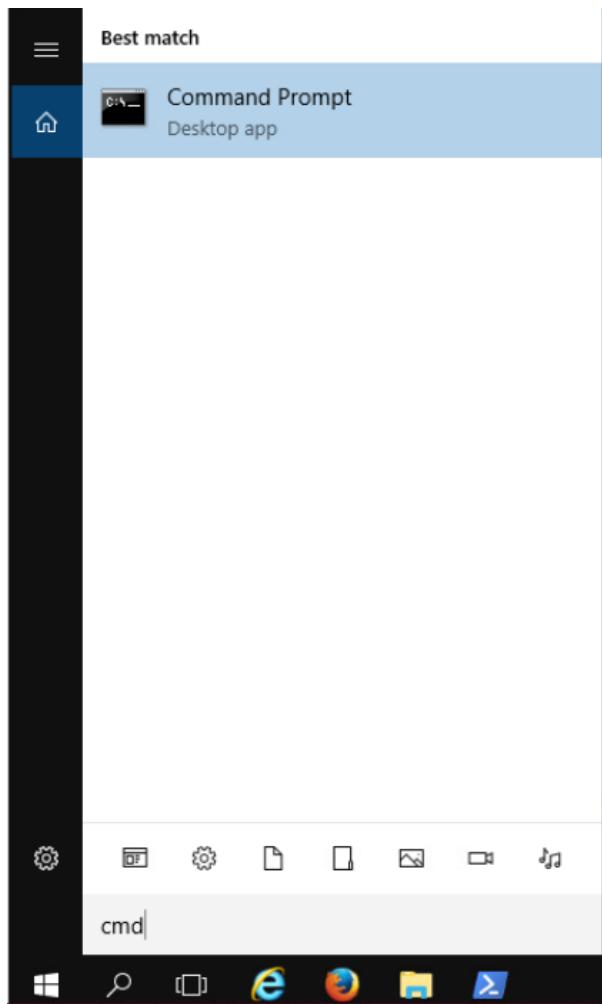
Part 1

Step 1



Accessing the VM on netlab





Administrator: Command Prompt

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

C:\Users\Administrator>
```

Opening **Windows PowerShell** and **Command Prompt** via windows search bar

Part 2

```
PS C:\Users\Administrator> dir
```

```
Directory: C:\Users\Administrator
```

Mode	LastWriteTime	Length	Name
d-r---	11/08/2020 19:50		Contacts
d-r---	11/08/2020 19:50		Desktop
d-r---	11/08/2020 19:50		Documents
d-r---	11/08/2020 19:50		Downloads
d-r---	11/08/2020 19:50		Favorites
d-r---	11/08/2020 19:50		Links
d-r---	11/08/2020 19:50		Music
d-r---	11/08/2020 19:50		Pictures
d-r---	11/08/2020 19:50		Saved Games
d-r---	11/08/2020 19:50		Searches
d-r---	11/08/2020 19:50		Videos

```
PS C:\Users\Administrator>
```

```
C:\Users\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is 224B-75F9
```

```
Directory of C:\Users\Administrator
```

01/06/2018 23:30 <DIR>	.
01/06/2018 23:30 <DIR>	..
11/08/2020 19:50 <DIR>	Contacts
11/08/2020 19:50 <DIR>	Desktop
11/08/2020 19:50 <DIR>	Documents
11/08/2020 19:50 <DIR>	Downloads
11/08/2020 19:50 <DIR>	Favorites
11/08/2020 19:50 <DIR>	Links
11/08/2020 19:50 <DIR>	Music
11/08/2020 19:50 <DIR>	Pictures
11/08/2020 19:50 <DIR>	Saved Games
11/08/2020 19:50 <DIR>	Searches
11/08/2020 19:50 <DIR>	Videos
	0 File(s) 0 bytes
	13 Dir(s) 33,589,452,800 bytes free

```
C:\Users\Administrator>■
```

Using **dir** command on **PowerShell** provides a similar output to the output of **cmd** but with headers. But the **cmd** output contains data like the current directory “.” and the previous directory “..”, alongside the amount of data free on the drive.

```
PS C:\Users\Administrator> ping 192.168.0.12
Pinging 192.168.0.12 with 32 bytes of data:
Reply from 192.168.0.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> _
```

```
C:\Users\Administrator>ping 192.168.0.12
C:\Users\Administrator>
Pinging 192.168.0.12 with 32 bytes of data:
Reply from 192.168.0.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Administrator> _
```

Using the **ping** command provides the same output both on **PowerShell** and **cmd**

Part 3

```
PS C:\Users\Administrator> Get-Alias dir
 CommandType      Name          Version      Source
-----      ----
 Alias        dir -> Get-ChildItem

PS C:\Users\Administrator> 

PS C:\Users\Administrator> Get-ChildItem

 Directory: C:\Users\Administrator

 Mode          LastWriteTime    Length Name
 ----          -----          ---- 
 d-r--- 11/08/2020 19:50          Contacts
 d-r--- 11/08/2020 19:50          Desktop
 d-r--- 11/08/2020 19:50          Documents
 d-r--- 11/08/2020 19:50          Downloads
 d-r--- 11/08/2020 19:50          Favorites
 d-r--- 11/08/2020 19:50          Links
 d-r--- 11/08/2020 19:50          Music
 d-r--- 11/08/2020 19:50          Pictures
 d-r--- 11/08/2020 19:50          Saved Games
 d-r--- 11/08/2020 19:50          Searches
 d-r--- 11/08/2020 19:50          Videos

PS C:\Users\Administrator>
```

The PowerShell command equivalent of **dir** is **Get-ChildItem**

As shown when executing it, it gives the same output as the **dir** command

Part 4

```
PS C:\Users\Administrator> netstat -h
Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables host
           multiple independent components, and in these cases the
           sequence of components involved in creating the connection
           or listening port is displayed. In this case the executable
           name is in [] at the bottom, on top is the component it called,
           and so forth until TCP/IP was reached. Note that this option
           can be time-consuming and will fail unless you have sufficient
           permissions.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
           be associated with an active connection.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
           the -p option may be used to specify a subset of the default.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
           endpoints.
-y          Displays the TCP connection template for all connections.
           Cannot be combined with the other options.
interval   Redisplays selected statistics, pausing interval seconds
           between each display. Press CTRL+C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.
```

PS C:\Users\Administrator>

```

PS C:\Users\Administrator> netstat -r
=====
Interface List
 4...00 50 56 82 da 48 .....vmxnet3 Ethernet Adapter
 6...02 00 4c 4f 4f 50 .....Npcap Loopback Adapter
 1..... Software Loopback Interface 1
 2...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 8...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway        Interface Metric
          127.0.0.0      255.0.0.0    On-link       127.0.0.1     331
          127.0.0.1      255.255.255.255  On-link       127.0.0.1     331
 127.255.255.255  255.255.255.255  On-link       127.0.0.1     331
          169.254.0.0      255.255.0.0    On-link      169.254.12.163   281
 169.254.12.163  255.255.255.255  On-link      169.254.12.163   281
 169.254.255.255  255.255.255.255  On-link      169.254.12.163   281
          192.168.0.0      255.255.255.0    On-link      192.168.0.12    271
          192.168.0.12      255.255.255.255  On-link      192.168.0.12    271
 192.168.0.255  255.255.255.255  On-link      192.168.0.12    271
          224.0.0.0      240.0.0.0    On-link       127.0.0.1     331
          224.0.0.0      240.0.0.0    On-link      169.254.12.163   281
          224.0.0.0      240.0.0.0    On-link      192.168.0.12    271
 255.255.255.255  255.255.255.255  On-link       127.0.0.1     331
 255.255.255.255  255.255.255.255  On-link      169.254.12.163   281
 255.255.255.255  255.255.255.255  On-link      192.168.0.12    271
=====
Persistent Routes:
  None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
 1    331 ::1/128        On-link
 6    281 fe80::/64        On-link
 4    271 fe80::/64        On-link
 6    281 fe80::563:b673:a53:ca3/128
                                On-link
 4    271 fe80::a5b9:4eb7:1d5:818a/128
                                On-link
 1    331 ff00::/8         On-link
 6    281 ff00::/8         On-link
 4    271 ff00::/8         On-link
=====
Persistent Routes:
  None
PS C:\Users\Administrator>

```

The IPv4 gateway would be 192.168.1.1

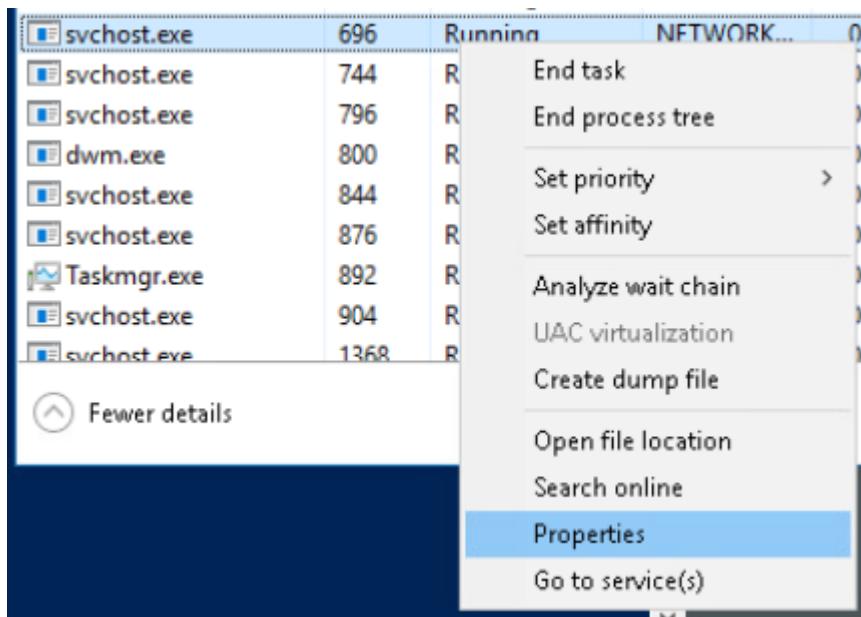
```

PS C:\Users\Administrator> netstat -abno

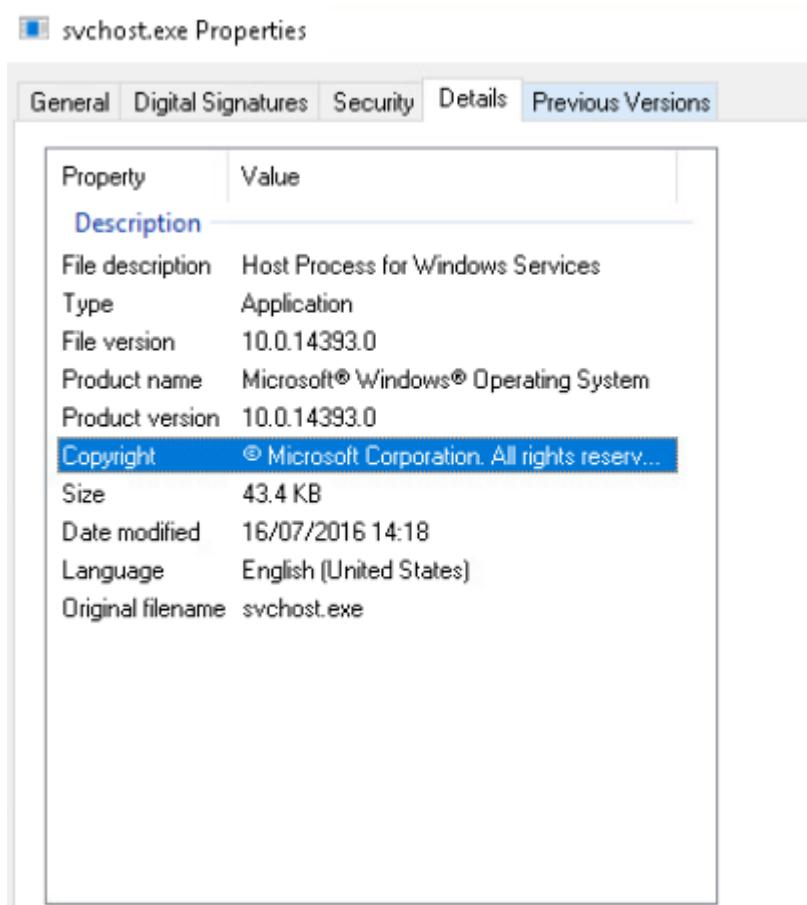
Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    0.0.0.0:135           0.0.0.0:0           LISTENING   696
  RpcSs [svchost.exe]
  TCP    0.0.0.0:445           0.0.0.0:0           LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:1536          0.0.0.0:0           LISTENING   444
  Can not obtain ownership information
  TCP    0.0.0.0:1537          0.0.0.0:0           LISTENING   904
  EventLog
  [svchost.exe]
  TCP    0.0.0.0:1538          0.0.0.0:0           LISTENING   844
  Schedule
  [svchost.exe]
  TCP    0.0.0.0:1539          0.0.0.0:0           LISTENING   1444
  [spoolsv.exe]
  TCP    0.0.0.0:1540          0.0.0.0:0           LISTENING   1368
  PolicyAgent
  [svchost.exe]
  TCP    0.0.0.0:1541          0.0.0.0:0           LISTENING   560
  Can not obtain ownership information
  TCP    0.0.0.0:1542          0.0.0.0:0           LISTENING   576
  [lsass.exe]
  TCP    0.0.0.0:5985          0.0.0.0:0           LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:47001         0.0.0.0:0           LISTENING   4
  Can not obtain ownership information
  TCP    169.254.12.163:139    0.0.0.0:0           LISTENING   4
  Can not obtain ownership information
  TCP    192.168.0.12:139     0.0.0.0:0           LISTENING   4
  Can not obtain ownership information
  TCP    [::]:135              [::]:0             LISTENING   696
  RpcSs
  [svchost.exe]
  TCP    [::]:445              [::]:0             LISTENING   4
  Can not obtain ownership information
  TCP    [::]:1536              [::]:0             LISTENING   444
  Can not obtain ownership information
  TCP    [::]:1537              [::]:0             LISTENING   904
  EventLog
  [svchost.exe]
  TCP    [::]:1538              [::]:0             LISTENING   844
  Schedule
  [svchost.exe]
  - - -

```

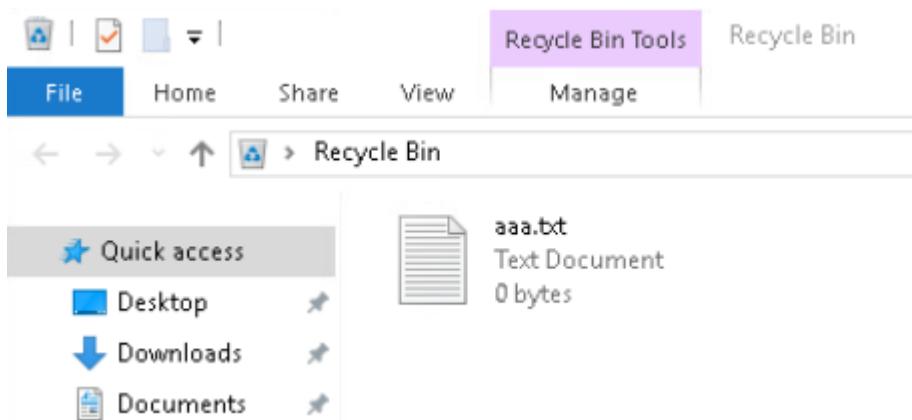
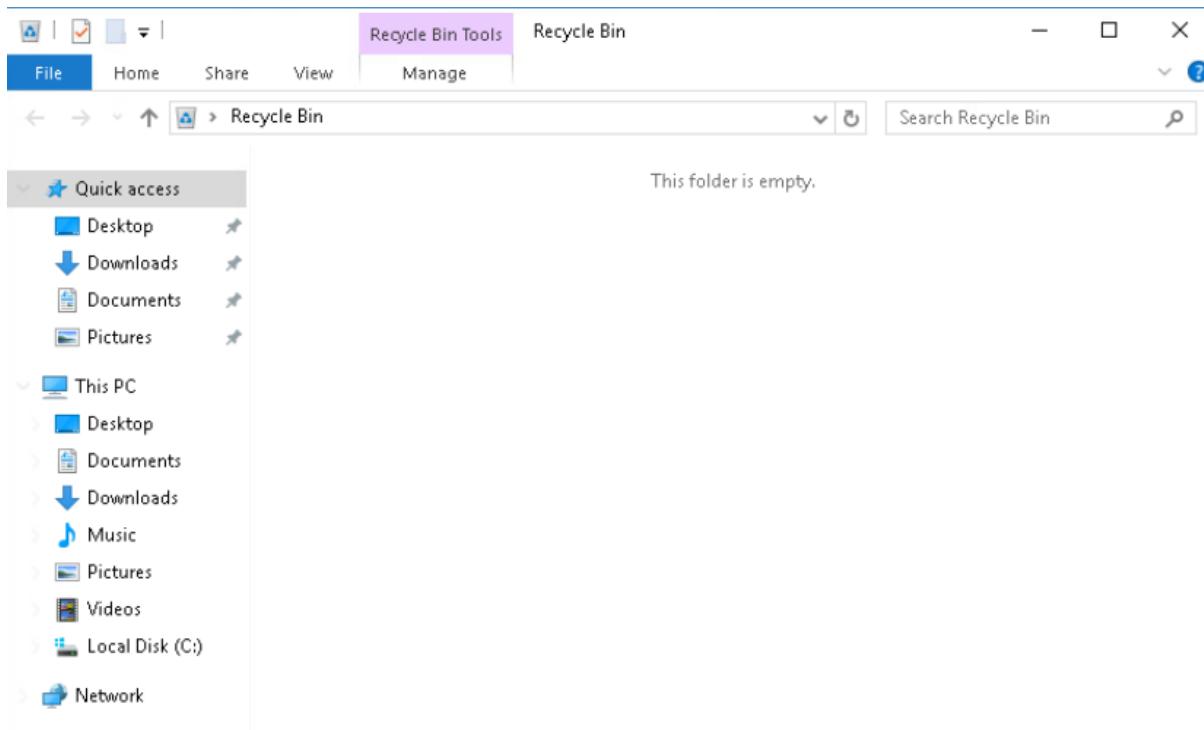


Navigating: “Task Manager” > “Details” > “Click on PID” and finding the PID value of 696 (for this task). Once found, Right click and open **Properties**.



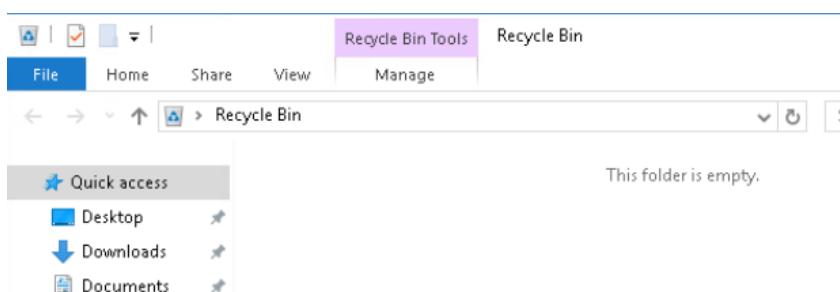
From the “**Details**” tab you can find details like size of the file, the type of file it is (in this case Application) and a description of the file

Part 5



Opening the **Recycle Bin** from desktop and creating a dummy text file and dropping it inside the bin

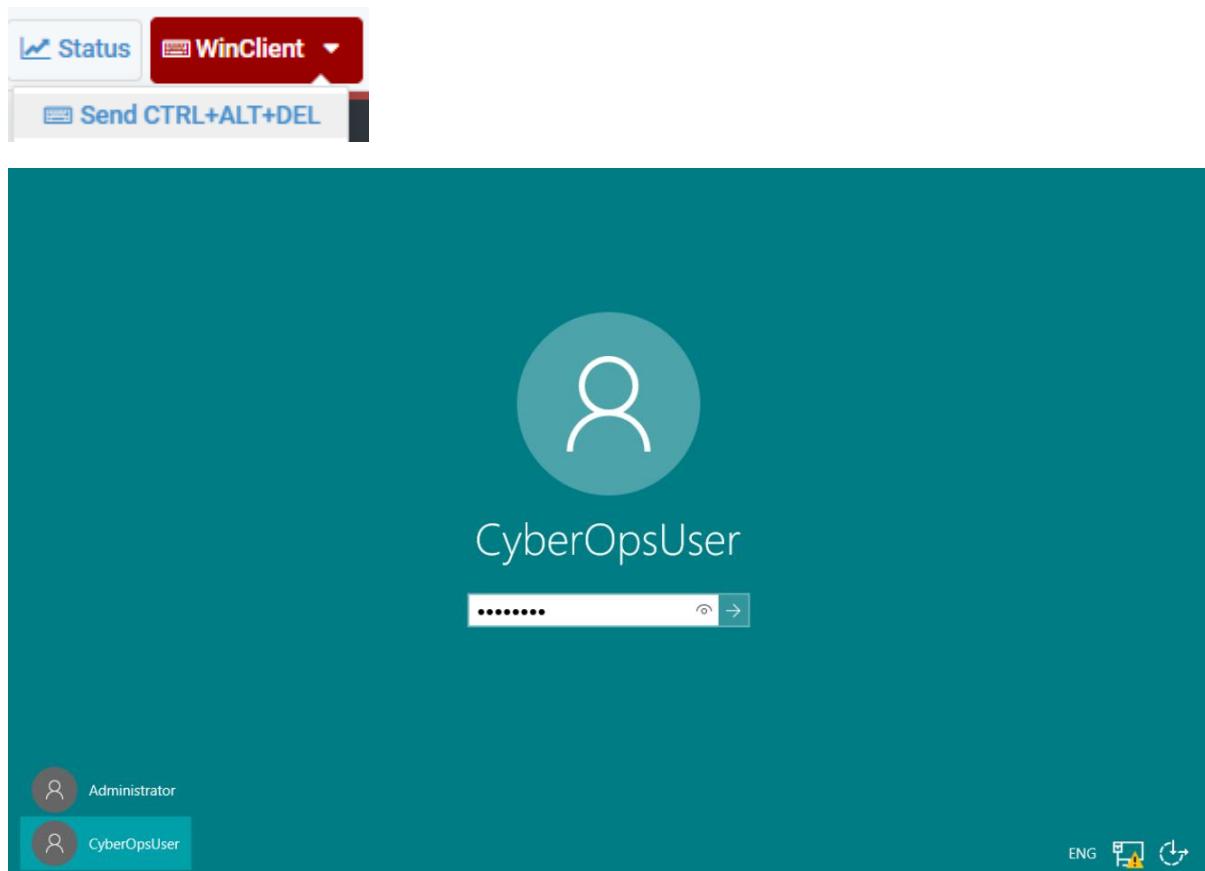
```
PS C:\Users\Administrator> clear-recyclebin
Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
PS C:\Users\Administrator>
```



Entering “**clear-recyclebin**” into PowerShell and confirming the execution will clear the bin’s contents.

7.3.12 Lab - Windows Task Manager

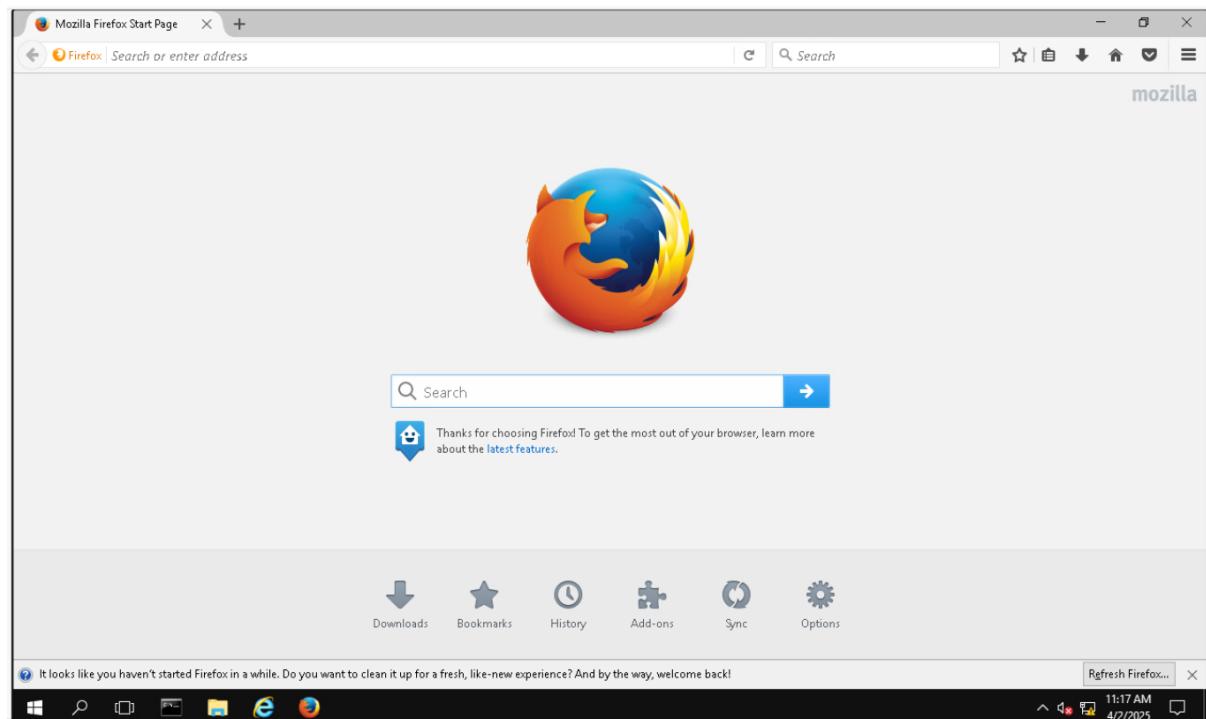
Part 1



Accessing the VM on netlab

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

C:\Users\CyberOpsUser>
```



Task Manager

File Options View

Processes Performance Users Details Services

Name	1% CPU	27% Memory
Apps (3)		
> Firefox	0%	101.1 MB
> Task Manager	0%	7.5 MB
> Windows Command Processor	0%	0.4 MB
Background processes (19)		
> Antimalware Service Executable	0%	49.3 MB
> COM Surrogate	0%	3.0 MB
Firefox	0%	24.5 MB
Host Process for Windows Tasks	0%	2.3 MB
Microsoft Compatibility Telemetry	0%	0.5 MB
> Microsoft Distributed Transaction Coordinator	0%	2.2 MB
Runtime Broker	0%	6.2 MB
Search	0%	8.8 MB
Search Background Task Host	0%	9.2 MB

Fewer details End task

Opening **Firefox**, **Command Prompt** and **Task Manager**

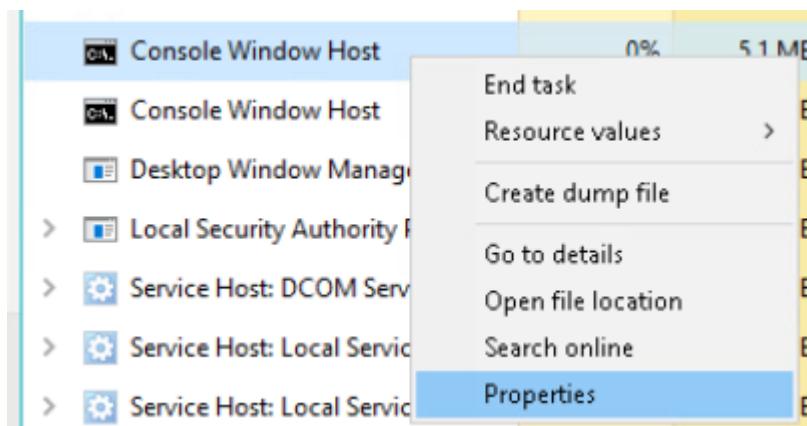
Task Manager

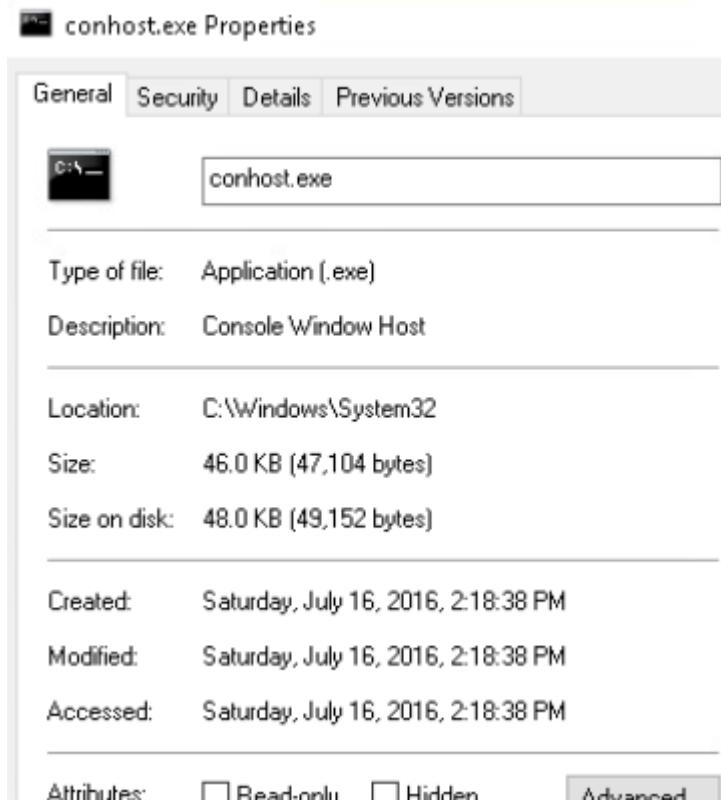
File Options View

Processes Performance Users Details Services

Name	8% CPU	24% Memory
Apps (3)		
> Firefox	1.8%	97.7 MB
> Task Manager	2.0%	7.7 MB
▼ Windows Command Processor	0%	0.4 MB
Command Prompt		

Locating the **Windows Command Processor** and expanding it (which contains **Command Prompt**)





Property	Value
Description	
File description	Console Window Host
Type	Application
File version	10.0.14393.0
Product name	Microsoft® Windows® Operating System
Product version	10.0.14393.0
Copyright	© Microsoft Corporation. All rights reserv...
Size	46.0 KB
Date modified	7/16/2016 2:18 PM
Language	English (United States)
Original filename	CONHOST.EXE

Locating **Console Window Host**, right clicking it and selecting properties will allow us to check the file name (which is found at the top-most entry field) and the location of the file – **C:\Windwos\System32**. The original file name of the file can be found in the **Details** tab.

Windows processes (27)			
>	appmodel (2)	0%	3.9 MB
	Client Server Runtime Process	0%	1.2 MB
	Client Server Runtime Process	0%	1.2 MB
>	Console Window Host	0%	0.6 MB
	Desktop Window Manager	11.2%	17.2 MB
>	Local Security Authority Proces...	0%	3.5 MB

After closing the **Command Prompt** window, it will disappear from task manager and one of the **Console Window Host** processes will disappear, resulting in a slight decrease of CPU and memory usage

Task Manager

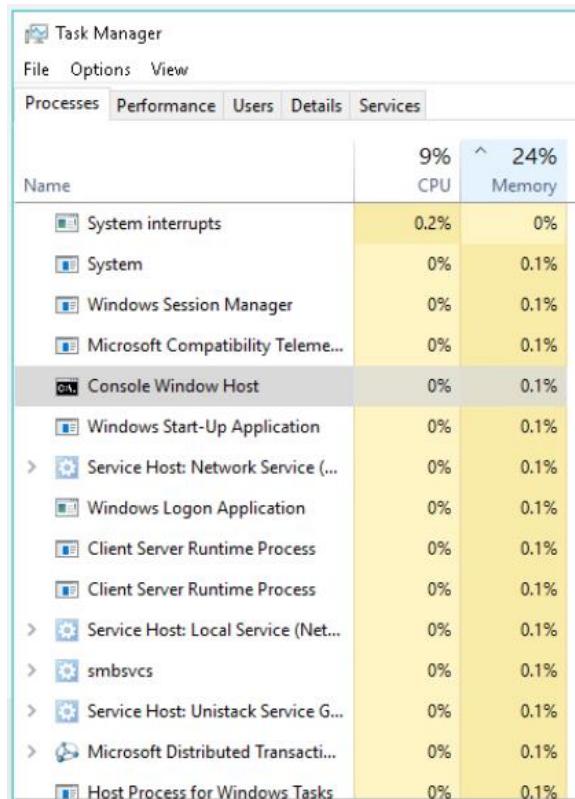
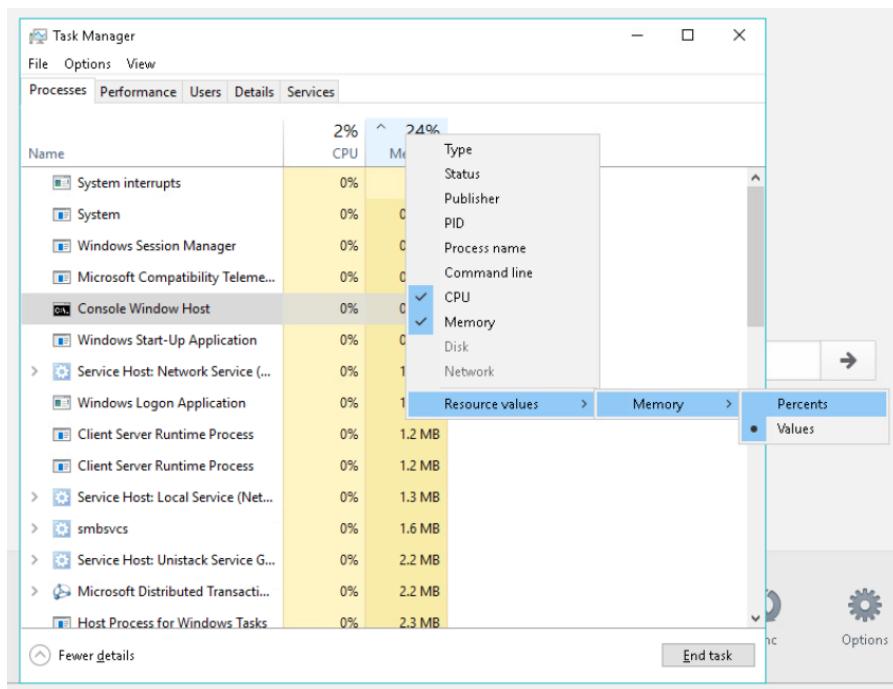
File Options View

Processes Performance Users Details Services

Name	1% CPU	^ 24% Memory
System interrupts	0%	0 MB
System	0%	0.1 MB
Windows Session Manager	0%	0.3 MB
Microsoft Compatibility Teleme...	0%	0.5 MB
Console Window Host	0%	0.6 MB
Windows Start-Up Application	0%	0.7 MB
Service Host: Network Service (...	0%	1.1 MB
Windows Logon Application	0%	1.1 MB
Client Server Runtime Process	0%	1.2 MB
Client Server Runtime Process	0%	1.2 MB
Service Host: Local Service (Net...	0%	1.3 MB
smbsvcs	0%	1.6 MB
Service Host: Unistack Service G...	0%	2.2 MB
Microsoft Distributed Transacti...	0%	2.2 MB
Host Process for Windows Tasks	0%	2.3 MB

(Fewer details)

Clicking on the **Memory** heading will sort all the processes in an **Descending** order, after another click on the header will sort all the processes in a **Ascending** order.



Changing the display of the resource values to **Percents** will show the percentage value of the process out of the total (in this case) memory used (in descending order)

This way the user is able to locate any potentially malicious processes that are using an unusual amount of processing power, be it **CPU, Memory or Disk Usage**

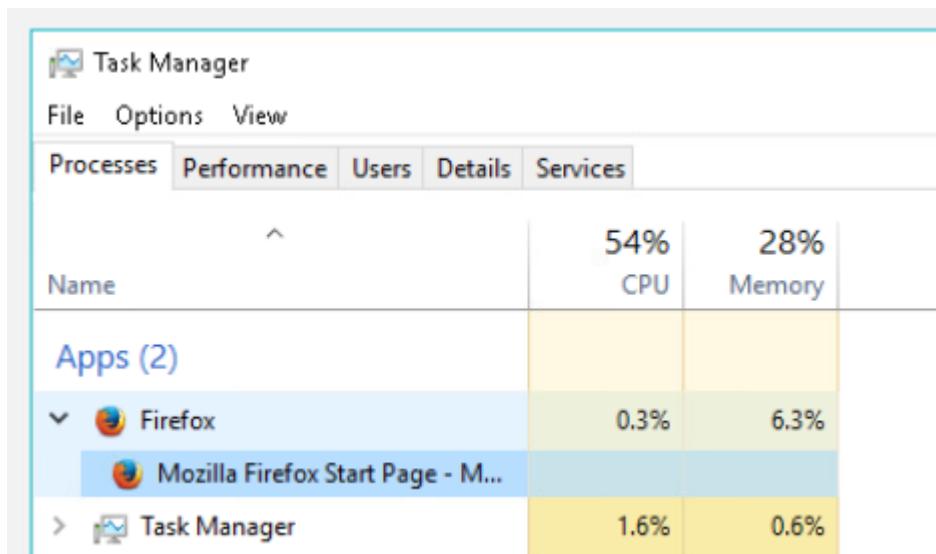
Task Manager

File Options View

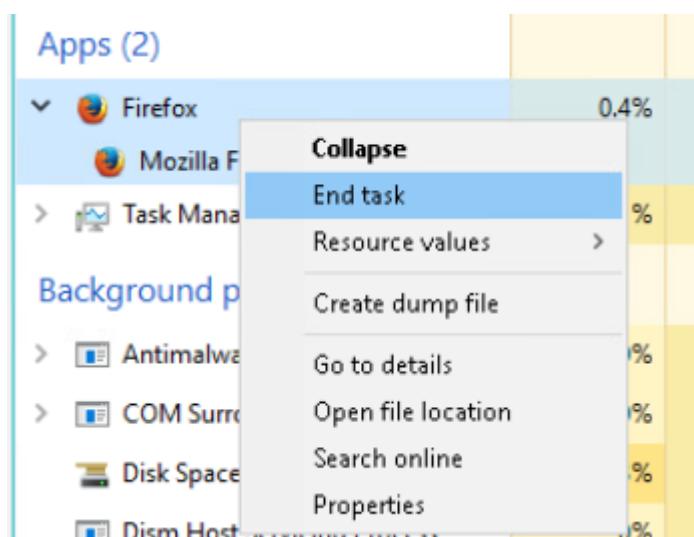
Processes Performance Users Details Services

Name	88%	28%
	CPU	Memory
Apps (2)		
> Firefox	0.8%	6.1%
> Task Manager	4.0%	0.5%
Background processes (29)		
> Antimalware Service Executable	30.8%	4.3%
COM Surrogate	0%	0.1%
> COM Surrogate	0%	0.2%
Disk Space Cleanup Manager fo...	0.3%	0.1%
Firefox	0%	1.5%
Host Process for Windows Tasks	0.6%	0.2%
Host Process for Windows Tasks	15.6%	0.2%
Host Process for Windows Tasks	0%	0.1%
Microsoft .NET Framework opti...	0%	0.1%
Microsoft Compatibility Teleme...	0%	0.1%

Clicking on the **Name** header will sort the processes into the 3 categories **Apps**, **Background Processes**, and **Windows Processes** – in descending alphabetical order

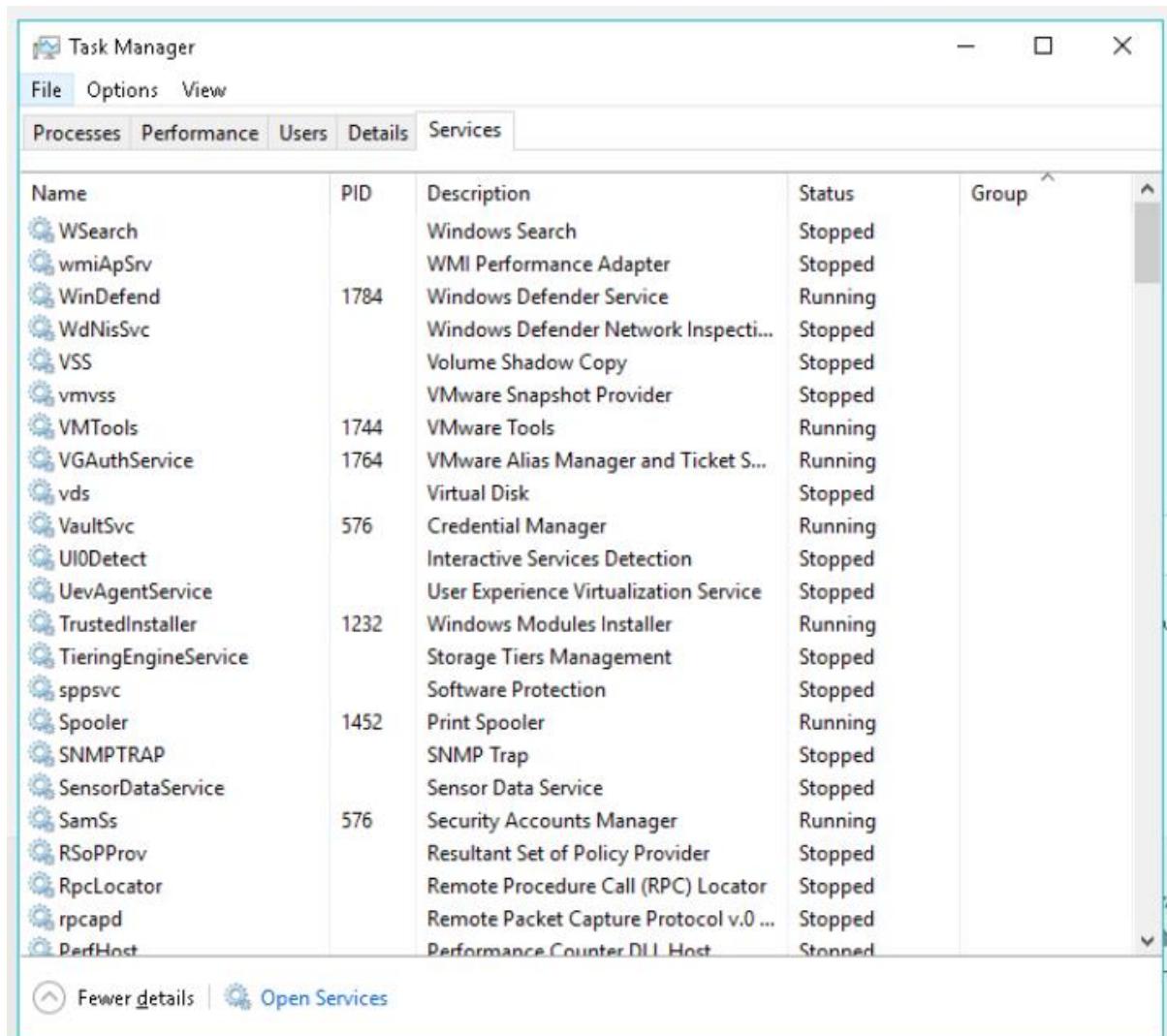


Double clicking the browser will expand the application and show all different processes that the application is using, and allow you to pinpoint which process is using what specific amount of resources



Ending the task on the browser will close the application

Part 2



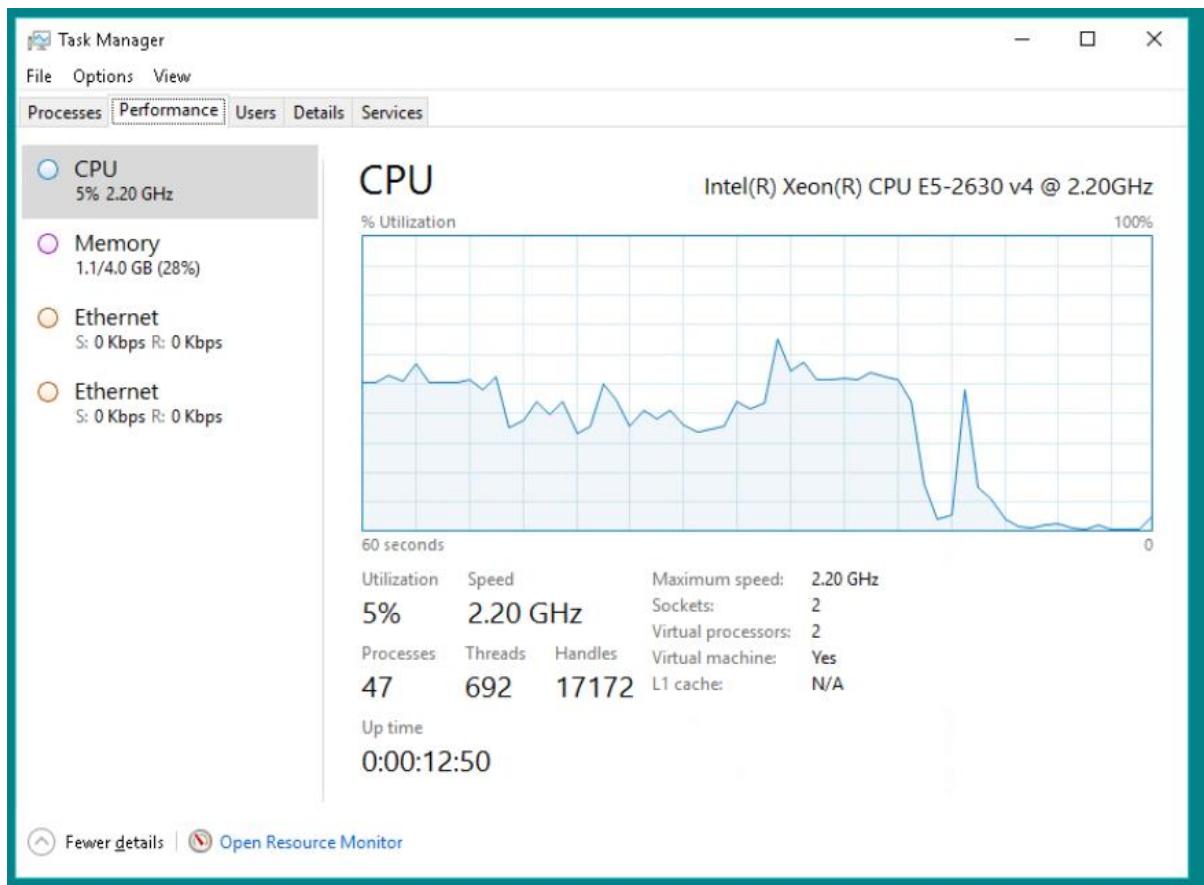
The screenshot shows the Windows Task Manager window with the 'Services' tab selected. The table lists various Windows services with their names, Process IDs (PID), descriptions, current status, and group information. Some services like WSearch, wmiApSrv, and WinDefend have a PID of 1784, while others like VSS, VMTools, and VGAAuthService have a PID of 1744. Most services are currently stopped, except for a few like WinDefend, VMTools, VGAAuthService, and several with PID 1744 which are running.

Name	PID	Description	Status	Group
WSearch		Windows Search	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	1784	Windows Defender Service	Running	
WdNisSvc		Windows Defender Network Inspecti...	Stopped	
VSS		Volume Shadow Copy	Stopped	
vmvss		VMware Snapshot Provider	Stopped	
VMTools	1744	VMware Tools	Running	
VGAAuthService	1764	VMware Alias Manager and Ticket S...	Running	
vds		Virtual Disk	Stopped	
VaultSvc	576	Credential Manager	Running	
UIODetect		Interactive Services Detection	Stopped	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller	1232	Windows Modules Installer	Running	
TieringEngineService		Storage Tiers Management	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	1452	Print Spooler	Running	
SNMPTRAP		SNMP Trap	Stopped	
SensorDataService		Sensor Data Service	Stopped	
SamSs	576	Security Accounts Manager	Running	
RSoPProv		Resultant Set of Policy Provider	Stopped	
RpcLocator		Remote Procedure Call (RPC) Locator	Stopped	
rpcapd		Remote Packet Capture Protocol v.0 ...	Stopped	
PerfHost		Performance Counter DLL Host	Stopped	

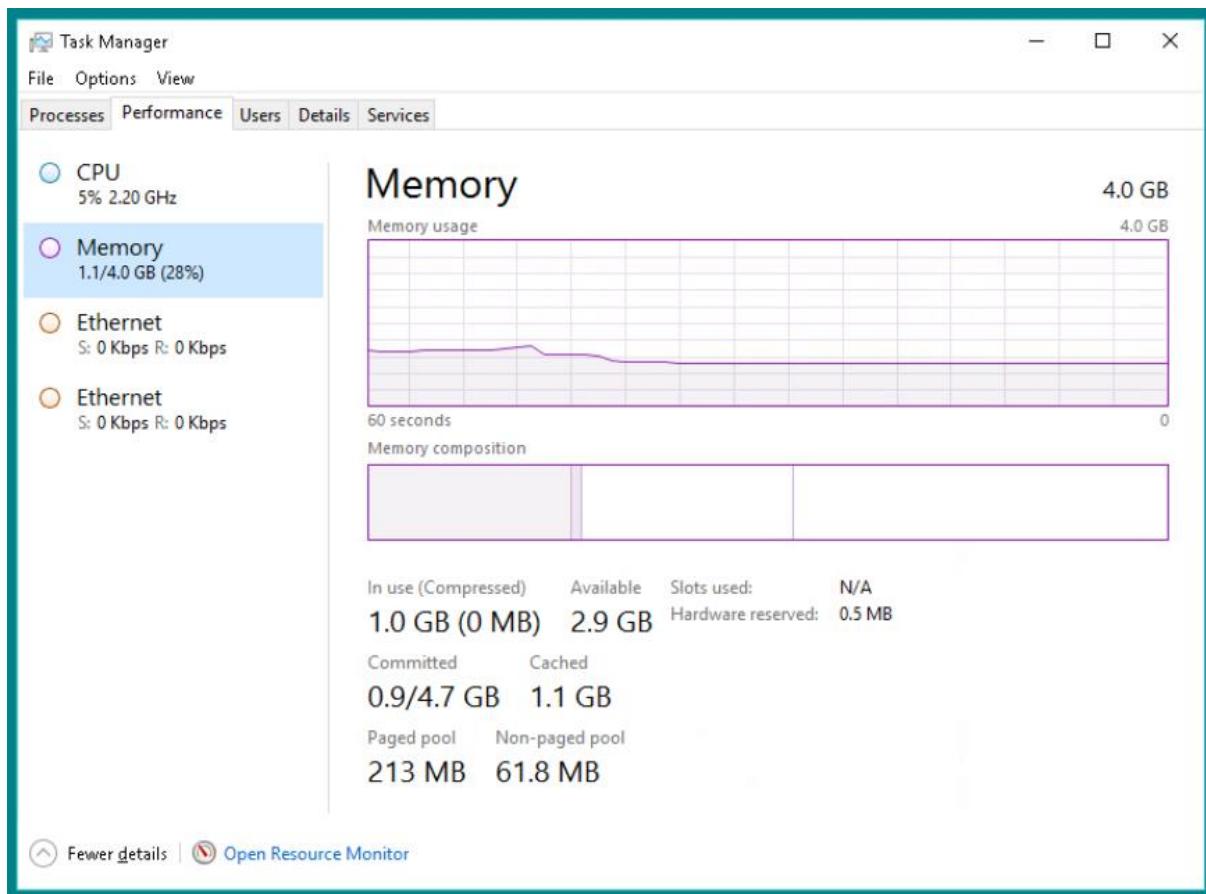
[Fewer details](#) | [Open Services](#)

The **Services** tab shows all the windows services that run in the background. Each service has a description that comes with it, a PID (if the service is running) and the status of each service.

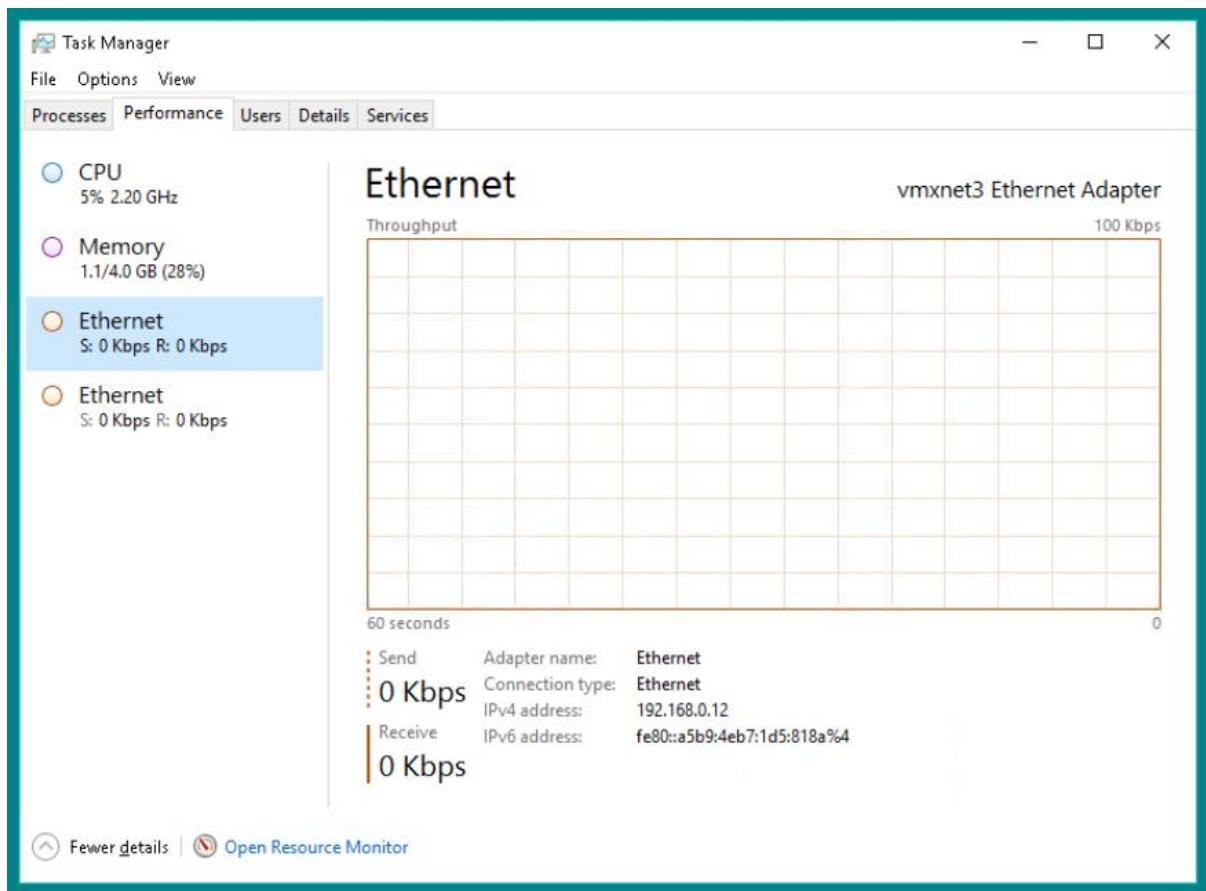
Part 3



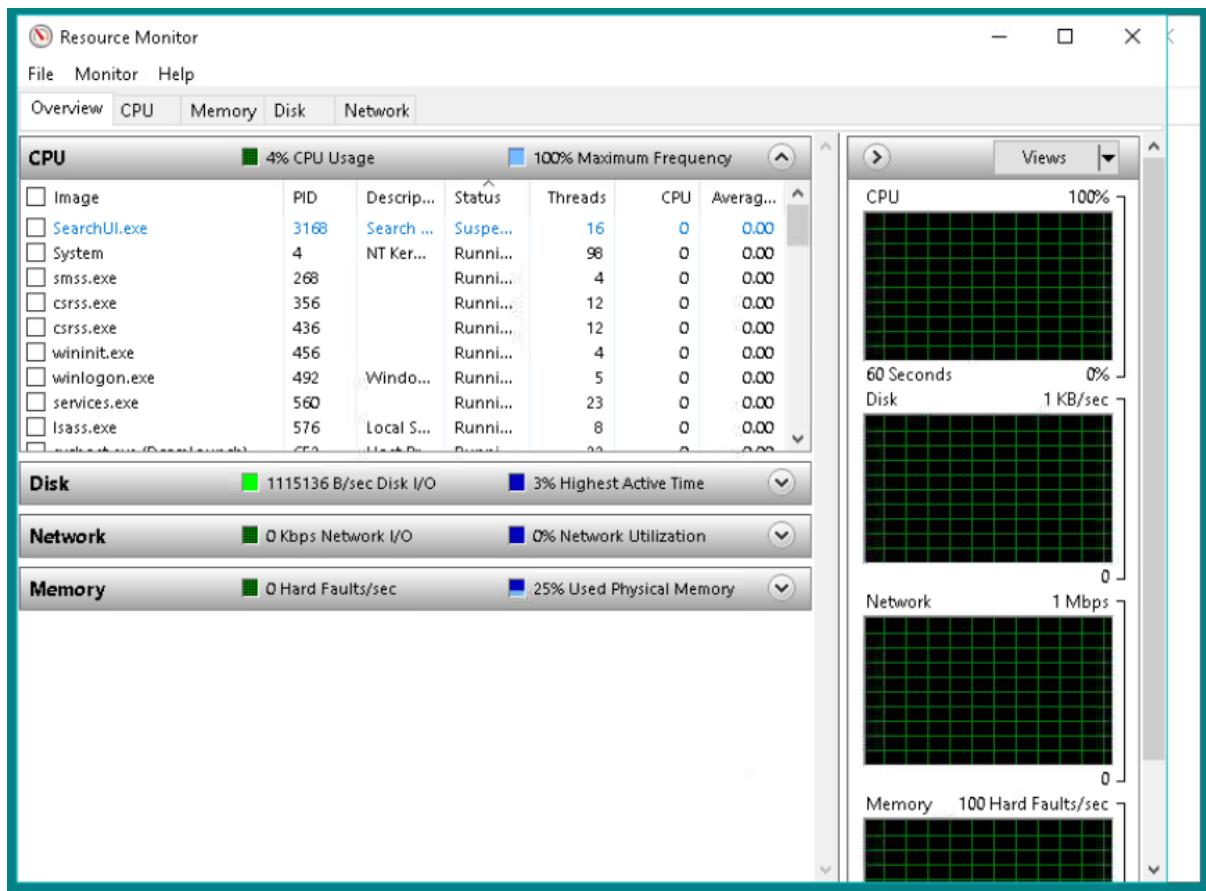
There are currently 692 in use and a total of 104 processes running



There is a total of 4.0 GB physical memory, 2.9 GB available physical memory and 1.0 GB memory in use.



The link speed is shown by the **Receive** section of ethernet section, in this instance its 0kbps as its the VM used on Netlab, and the IPv4 address of the VM is 192.168.0.12

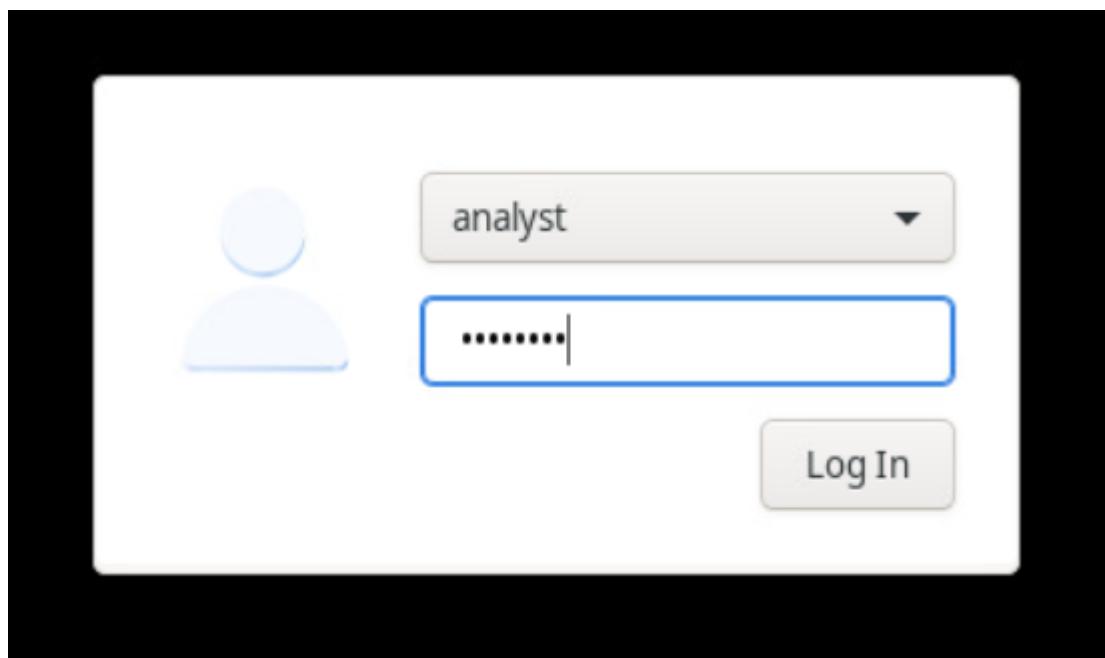


Module 8: Linux Labs

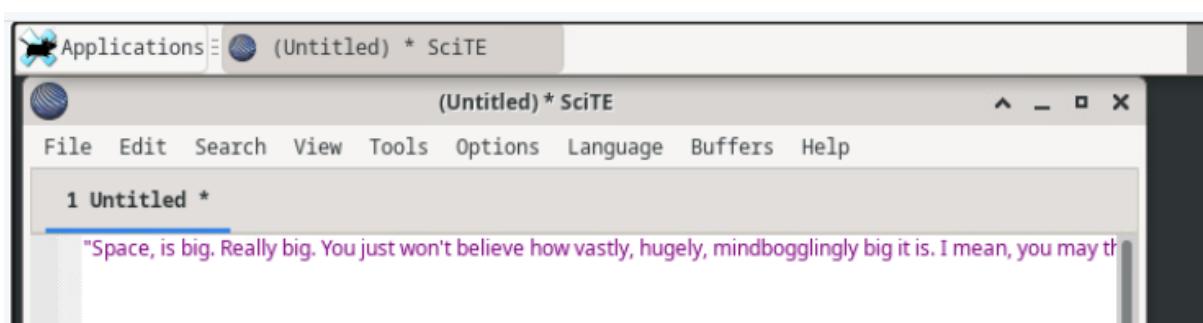
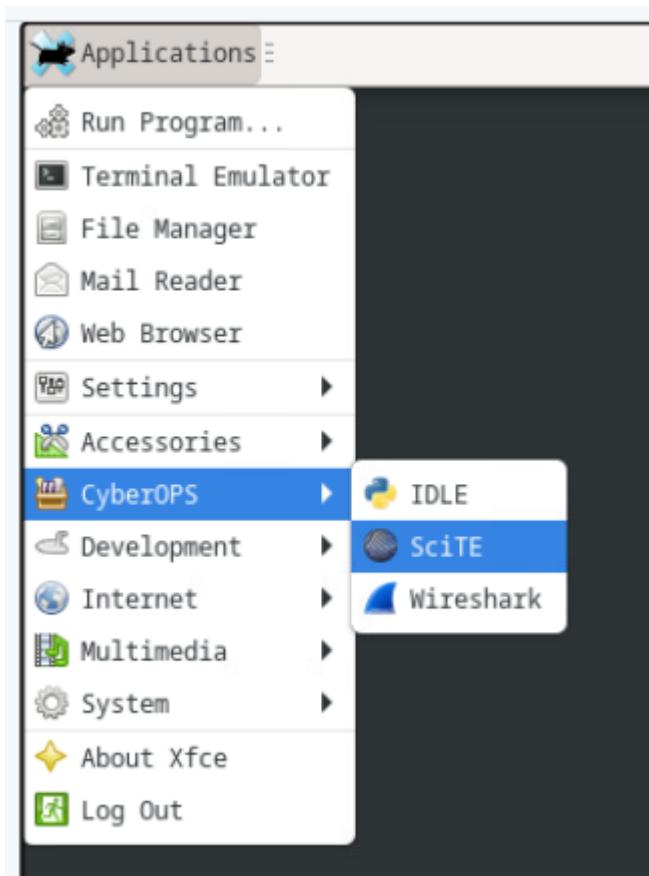
8.2.6 Lab – Working with Text Files in the CLI

Part 1

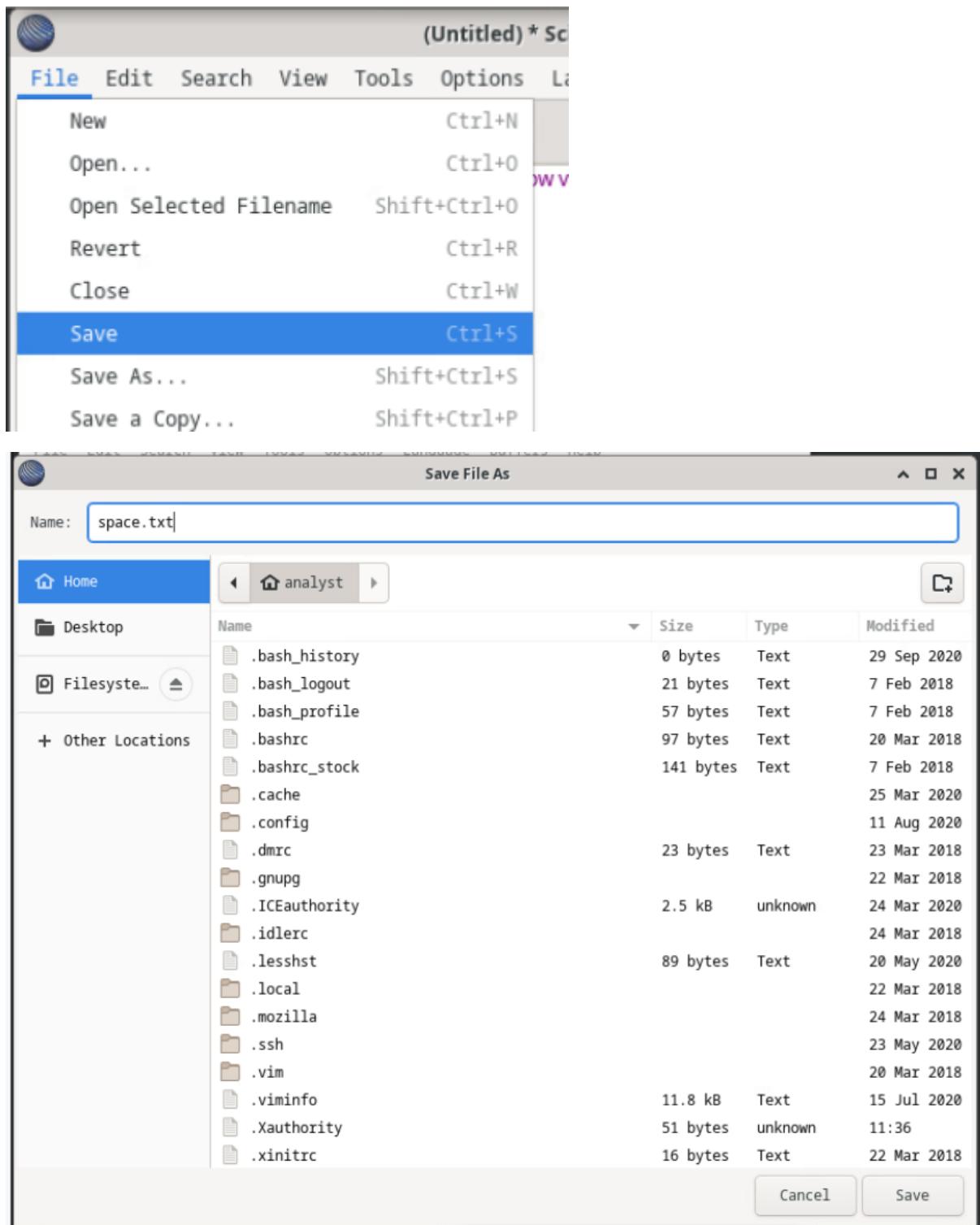
Step 1



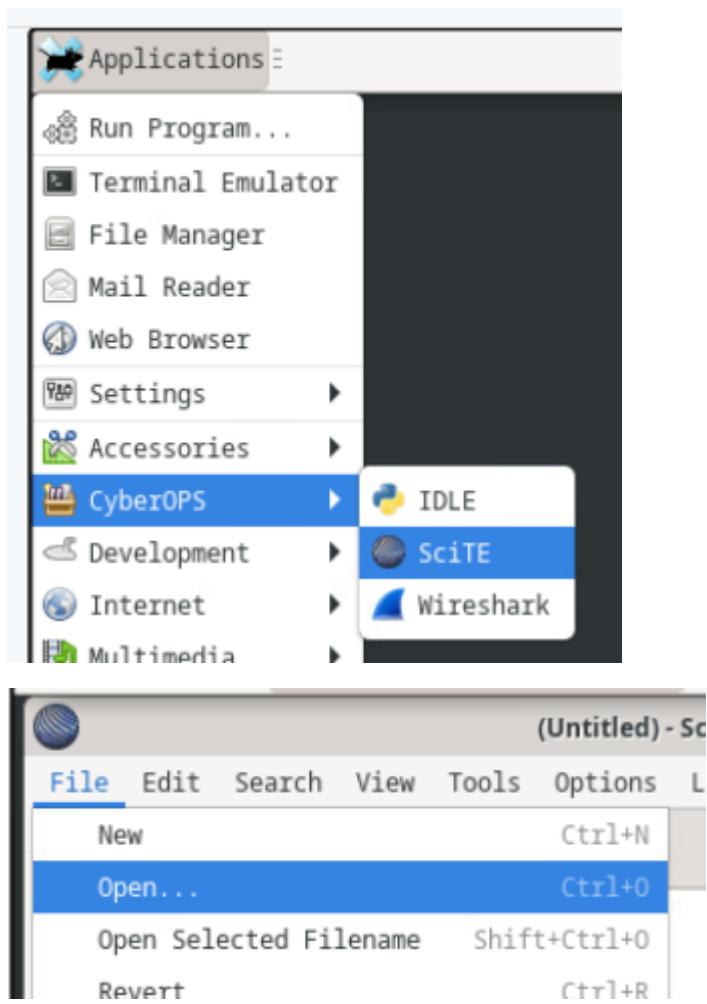
Logging into the VM



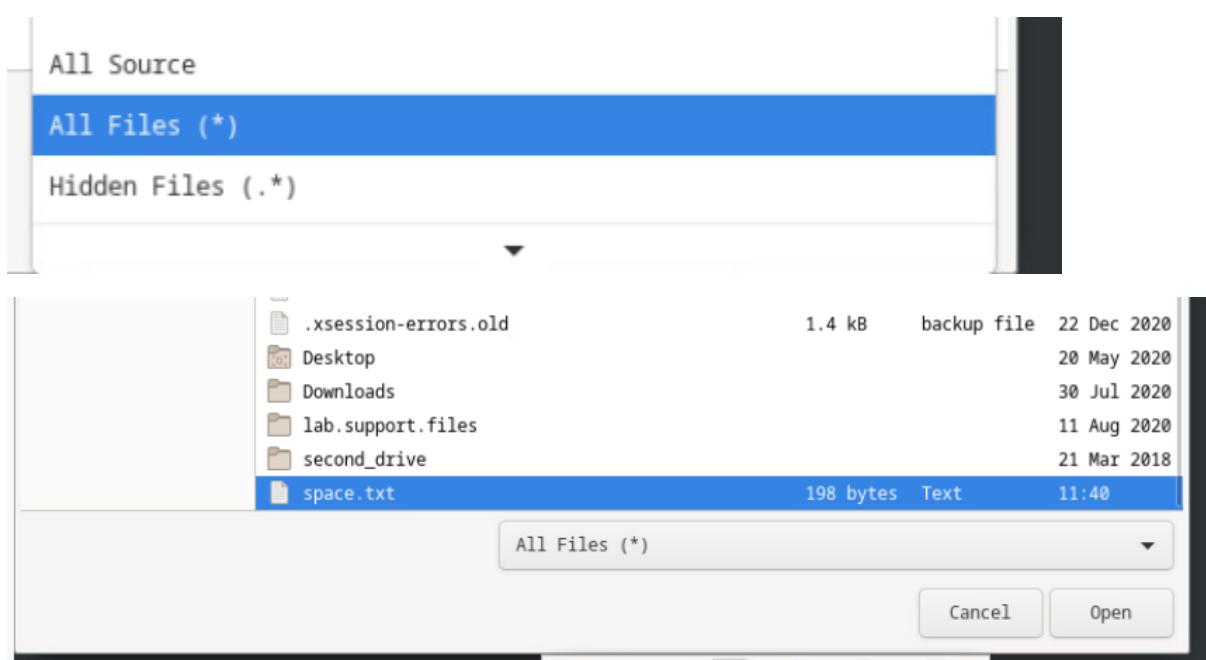
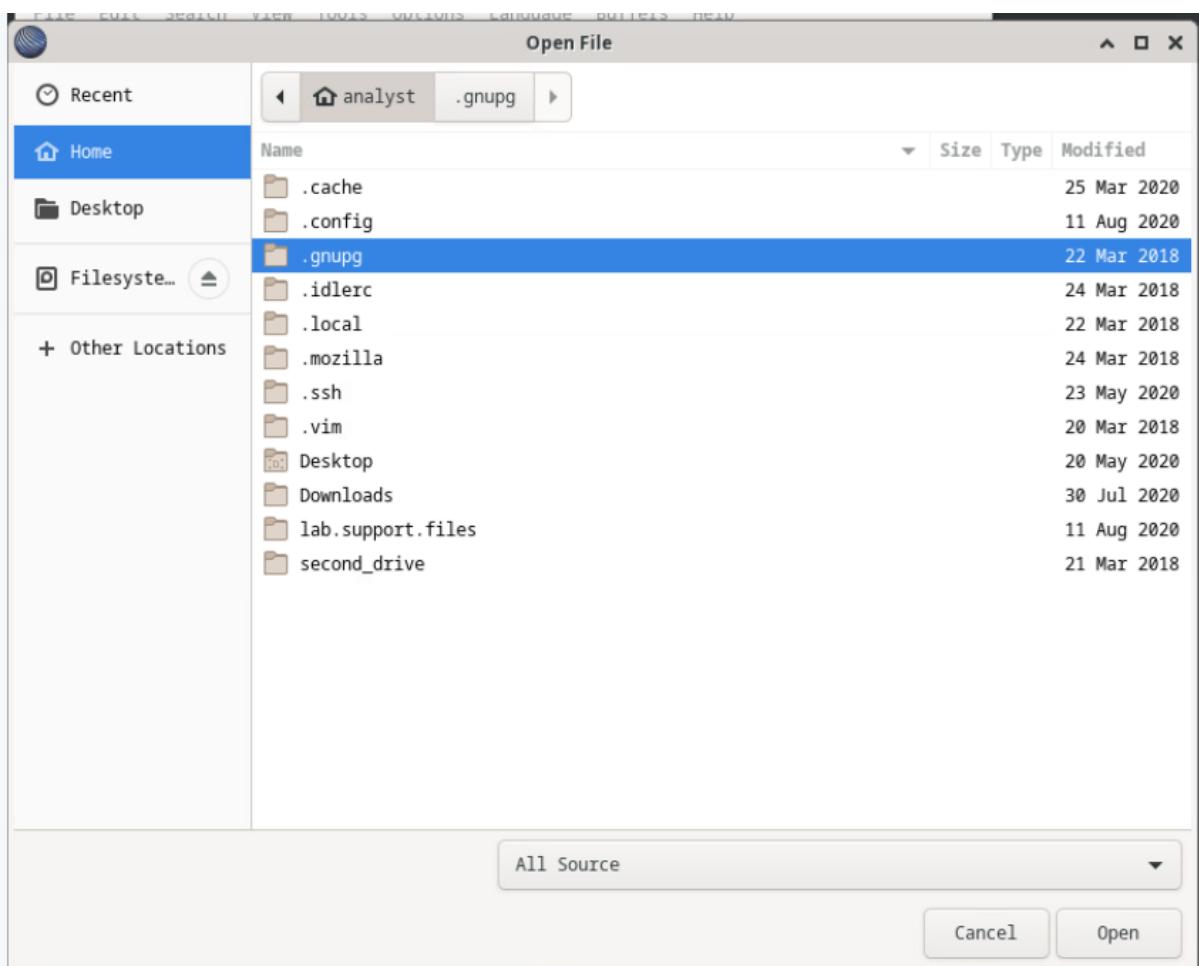
Opening the **SciTE** text editor and entering some text inside it



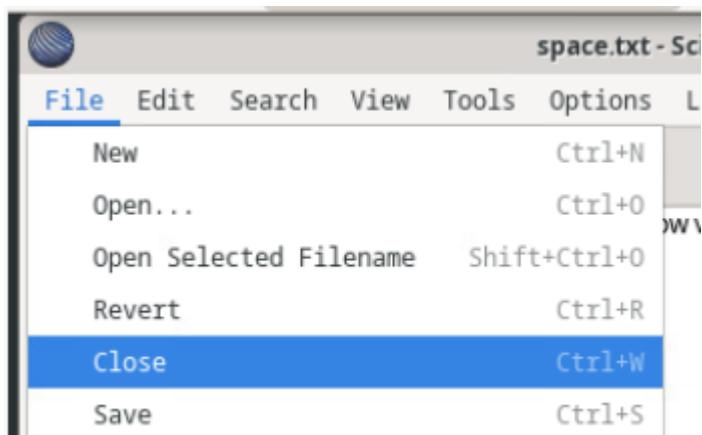
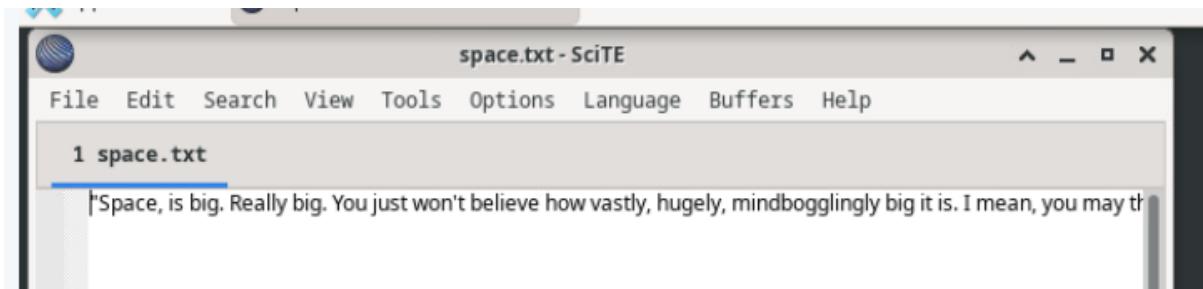
Saving the text file in the **home directory**



Re-opening the text editor and locating the text file

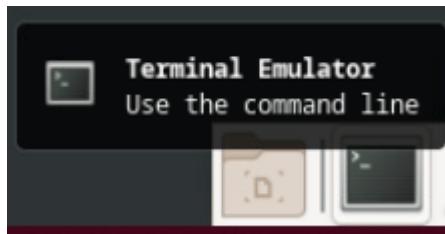


The text file is hidden due to the ".txt" file extension not classified as a "known extension" to the editor, as such you need to change visibility to **All Files (*)**



Closing the .txt file

Step 2



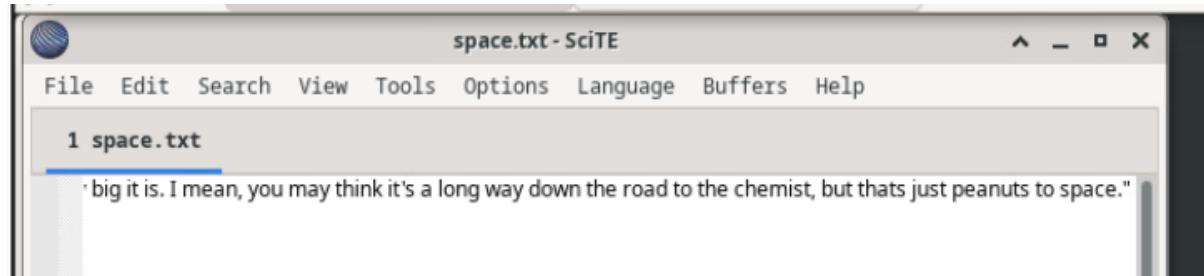
Opening terminal

```
[analyst@secOps ~]$ ls
Desktop Downloads lab.support.files second_drive space.txt
[analyst@secOps ~]$
```

```
[analyst@secOps ~]$ scite space.txt
```

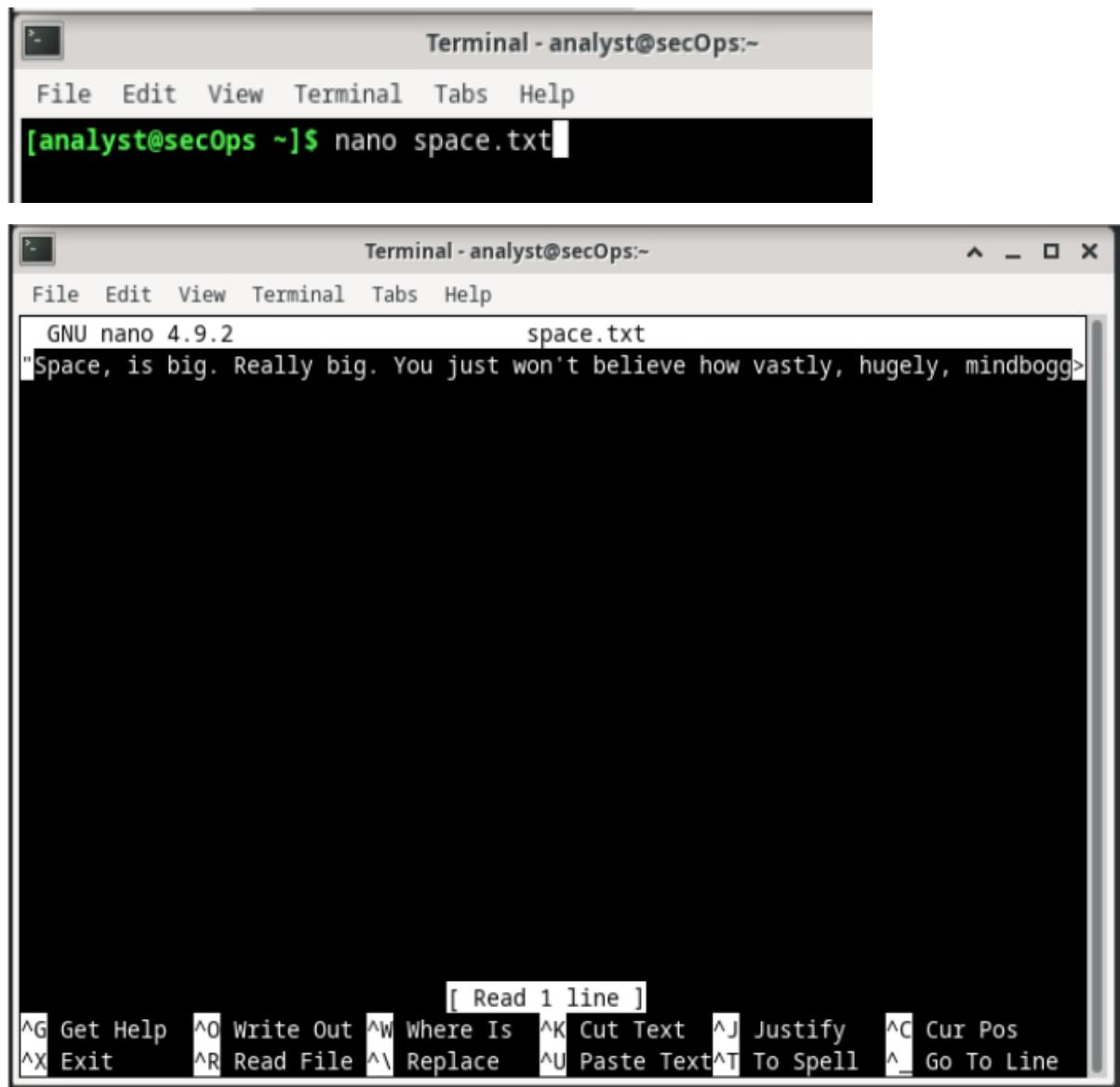
Opening the .txt file and loading it using the command “scite”

The next prompt doesn't show as the terminal currently has a process running – you need to interrupt the process to be able to enter another prompt



```
[analyst@secOps ~]$ scite space.txt
[analyst@secOps ~]$
```

Part 2



Terminal - analyst@secOps:~

File Edit View Terminal Tabs Help

[analyst@secOps ~]\$ nano space.txt

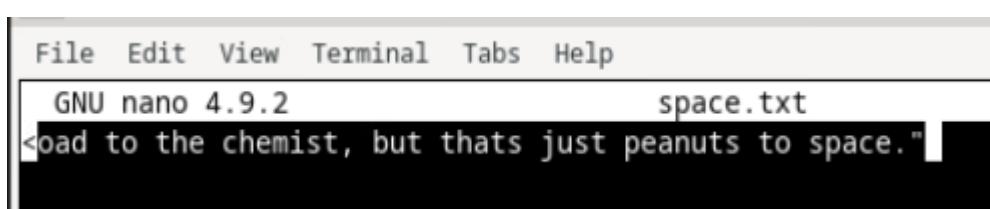
GNU nano 4.9.2 space.txt

"Space, is big. Really big. You just won't believe how vastly, hugely, mindbogg>

[Read 1 line]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^V Replace ^U Paste Text ^T To Spell ^_ Go To Line

Using the command **nano** followed by the **.txt** file, will display the contents of the file. The UI shows that there is more to a line using the **>** symbol found near the end of the border.



File Edit View Terminal Tabs Help

GNU nano 4.9.2 space.txt

<oad to the chemist, but thats just peanuts to space."

```
File Edit View Terminal Tabs Help
Main nano help text
The nano editor is designed to emulate the functionality and ease-of-use
of the UW Pico text editor. There are four main sections of the editor.
The top line shows the program version, the current filename being
edited, and whether or not the file has been modified. Next is the main
editor window showing the file being edited. The status line is the
third line from the bottom and shows important messages. The bottom two
lines show the most commonly used shortcuts in the editor.

Shortcuts are written as follows: Control-key sequences are notated with
a '^' and can be entered either by using the Ctrl key or pressing the Esc
key twice. Meta-key sequences are notated with 'M-' and can be entered
using either the Alt, Cmd, or Esc key, depending on your keyboard setup.
Also, pressing Esc twice and then typing a three-digit decimal number
from 000 to 255 will enter the character with the corresponding value.
The following keystrokes are available in the main editor window.
Alternative keys are shown in parentheses:

^G      (F1)      Display this help text
^X      (F2)      Close the current buffer / Exit from nano
^O      (F3)      Write the current buffer (or the marked region) to disk

^L Refresh    ^W Where Is  M-Q Previous  ^P Prev Line  ^Y Prev Page  M-\ First Line
^X Close     ^Q Where Was M-W Next    ^N Next Line   ^V Next Page  M-/ Last Line
```

Accessing the help screen of **nano** is done by pressing **CTRL + G**.

Part 3

Step 1

```
[analyst@secOps ~]$ ls -l
total 20
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst analyst   98 Apr  2 11:40 space.txt
[analyst@secOps ~]$ █
```

Using the **ls -l** command to list all the files in the home directory

```
[analyst@secOps ~]$ ls -la
total 124
drwx----- 14 analyst analyst 4096 Apr  2 11:40 .
drwxr-xr-x  3 root   root   4096 Mar 20  2018 ..
-rw-----  1 analyst analyst   67 Apr  2 11:49 .bash_history
-rw-r--r--  1 analyst analyst  21 Feb  7 2018 .bash_logout
-rw-r--r--  1 analyst analyst  57 Feb  7 2018 .bash_profile
-rw-r--r--  1 analyst analyst  97 Mar 20 2018 .bashrc
-rw-r--r--  1 analyst analyst 141 Feb  7 2018 .bashrc_stock
drwxr-xr-x  8 analyst analyst 4096 Mar 25 2020 .cache
drwxr-xr-x 10 analyst analyst 4096 Aug 11 2020 .config
drwxr-xr-x  2 analyst analyst 4096 May 20 2020 Desktop
-rw-r--r--  1 analyst analyst  23 Mar 23 2018 .dmrc
drwxr-xr-x  3 analyst analyst 4096 Jul 30 2020 Downloads
drwx-----  3 analyst analyst 4096 Mar 22 2018 .gnupg
-rw-----  1 analyst analyst 2520 Mar 24 2020 .ICEauthority
drwxr-xr-x  2 analyst analyst 4096 Mar 24 2018 .idlerc
drwxr-xr-x 11 analyst analyst 4096 Aug 11 2020 lab.support.files
-rw-----  1 analyst analyst  89 May 20 2020 .lessht
drwxr-xr-x  3 analyst analyst 4096 Mar 22 2018 .local
drwx-----  5 analyst analyst 4096 Mar 24 2018 .mozilla
drwxr-xr-x  2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r--  1 analyst analyst 198 Apr  2 11:40 space.txt
drwx-----  2 analyst analyst 4096 May 23 2020 .ssh
drwxr-xr-x  3 analyst analyst 4096 Mar 20 2018 .vim
-rw-----  1 analyst analyst 11848 Jul 15 2020 .viminfo
-rw-----  1 analyst analyst  51 Apr  2 11:36 .Xauthority
-rw-r--r--  1 analyst analyst  16 Mar 22 2018 .xinitrc
-rw-r--r--  1 analyst analyst  16 Mar 22 2018 .Xinitrc
-rw-----  1 analyst analyst 1177 Apr  2 11:36 .xsession-errors
-rw-----  1 analyst analyst 1413 Dec 22 2020 .xsession-errors.old
[analyst@secOps ~]$
```

Using the **ls -la** to show all the files in the home directory (including the hidden files)

```
[analyst@secOps ~]$ cat .bashrc
export EDITOR=vim

PS1='\[\e[1;32m\]\[\u@\h \w\]\$\[\e[0m\] '
alias ls="ls --color"
alias vi="vim"
[analyst@secOps ~]$
```

Using the **cat** command to display the contents of the **.bashrc** file

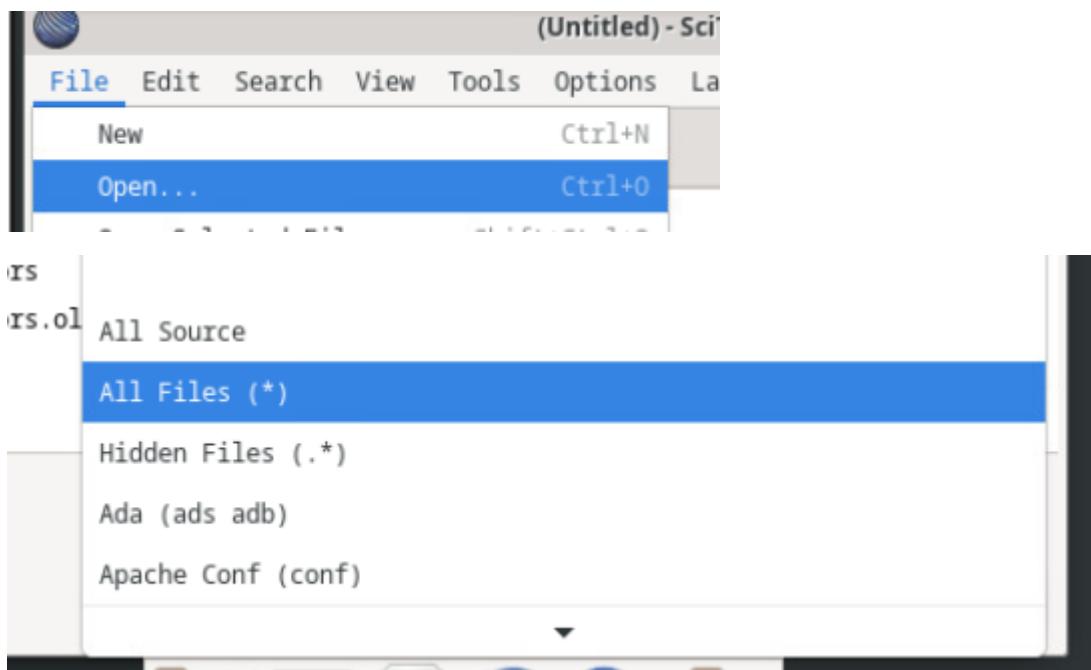
```
[analyst@secOps ~]$ ls /etc
adjtime           init.d          nanorc        services
apparmor.d       inputrc         netconfig     shadow
arch-release     iproute2        netctl        shadow-
audisp           iptables        nginx         shells
audit            issue          nscd.conf    skel
avahi            kernel          nsswitch.conf snort
bash.bash_logout krb5.conf     ntp.conf      ssh
bash.bashrc       ld.so.cache   openldap     ssl
bindresvport.blacklist ld.so.conf    openvswitch sudoers
binfmt.d         libaudit.conf  os-release   sudoers.d
ca-certificates  libnl          pacman.conf  sysctl.d
conf.d           libva.conf    pacman.conf.pacnew syslog-ng
crypttab         lightdm        pam.d        systemd
dconf             locale.conf   passwd       tmpfiles.d
default          locale.gen    passwd-      trusted-key.key
depmod.d         locale.gen.pacnew pcmcia     udev
dhpcd.conf       localtime      pkcs11       UPower
e2scrub.conf     login.defs    polkit-1    vbox
environment      logrotate.conf profile     vconsole.conf
ethertypes       logrotate.d   profile.d   vdpau_wrapper.cfg
fonts
```

Using the **ls** command to show the contents of the **/etc** directory

```
[analyst@secOps ~]$ cat /etc/bash.bashrc
#
# /etc/bash.bashrc
#
# If not running interactively, don't do anything
[[ $- != *i* ]] && return
[[ $DISPLAY ]] && shopt -s checkwinsize
PS1='[\u@\h \W]\$ '
case ${TERM} in
xterm*|rxvt*|Eterm|aterm|kterm|gnome*)
PROMPT_COMMAND=${PROMPT_COMMAND:+$PROMPT_COMMAND; }'printf "\033]0;%s@%s:%s\007" "${USER}"
"${HOSTNAME%.*}" "${PWD/#$HOME/\~}"'
;;
screen*)
PROMPT_COMMAND=${PROMPT_COMMAND:+$PROMPT_COMMAND; }'printf "\033_%s@%s:%s\033\\" "${USER}"
"${HOSTNAME%.*}" "${PWD/#$HOME/\~}"'
;;
esac
[ -r /usr/share/bash-completion/bash_completion ] && . /usr/share/bash-completion/bash_comple
tion
[analyst@secOps ~]$
```

Using the **cat** command to display the **bash.bashrc** file (from the **/etc** directory)

Step 2



Selecting **All Files (*)** to see the hidden files

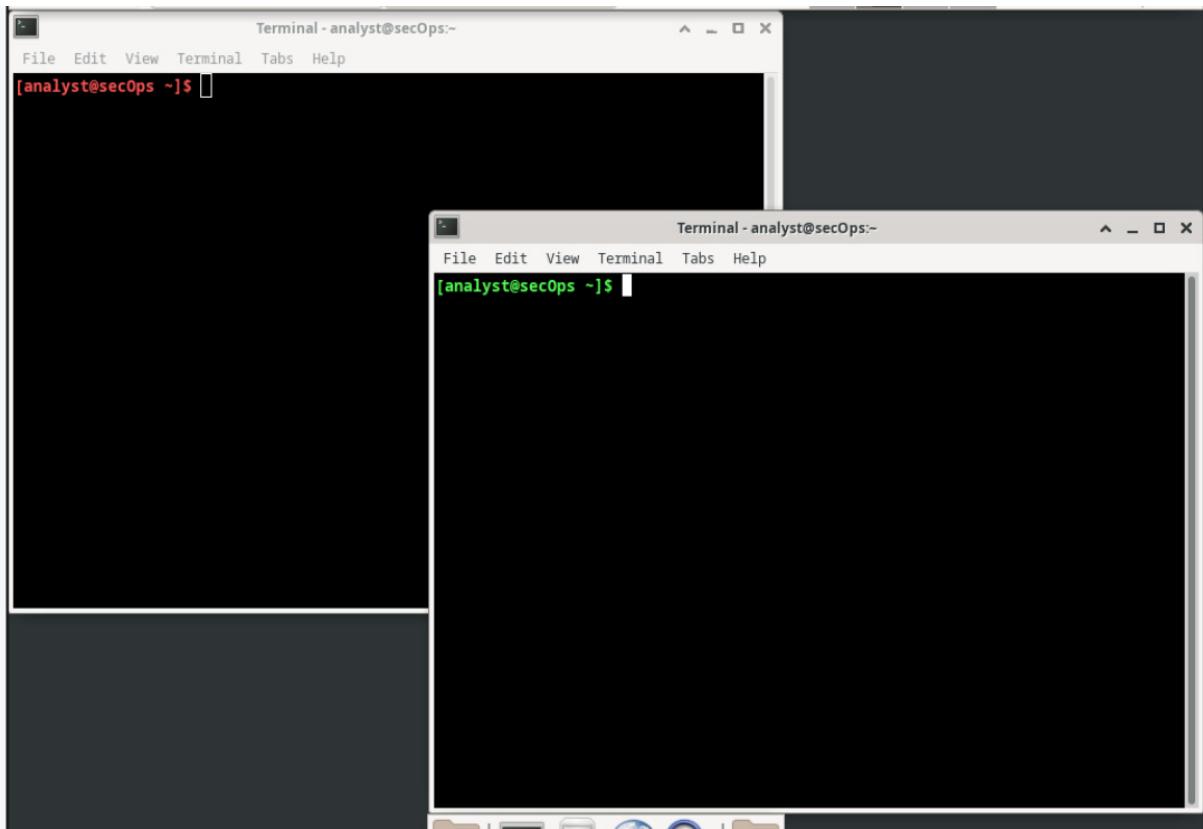
The screenshot shows two code editors side-by-side. Both display the same content: a file named **1 .bashrc**. The code contains:

```
export EDITOR=vim

PS1='\[\e[1;32m\]\u@\h \W\$\\[\e[0m\] '
alias ls="ls --color"
alias vi="vim"
```

The second editor window has a title bar that includes an asterisk (*) next to the file name, indicating it is a modified version.

Opening the **.bashrc** file and changing the colour code from 32 (green) to 31 (red)



After saving the file the terminal that is already open does not change colour to red, but if a new one is open then the colour of the new terminal is changed to red

```
[analyst@secOps ~]$ nano .bashrc
```

```
File Edit View Terminal Tabs Help
GNU nano 4.9.2 .bashrc
export EDITOR=vim

PS1='[\e[1;32m][\u@\h \w]\$[\e[0m] '
alias ls="ls --color"
alias vi="vim"
```

```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
GNU nano 4.9.2 .bashrc
export EDITOR=vim

PS1='[\e[1;33m][\u@\h \w]\$[\e[0m] '
alias ls="ls --color"
alias vi="vim"
```

Opening the **.bashrc** file using the **nano** command, and changing the colour code to 33 (yellow)

```
[analyst@secOps ~]$ nano .bashrc
[analyst@secOps ~]$ bash
[analyst@secOps ~]$ 
```

Using the command **bash** will reload the terminal and the colour of the text in the terminal will update.

Step 3

```
[analyst@secOps ~]$ sudo nano -l /etc/nginx/custom_server.conf  
[sudo] password for analyst:
```

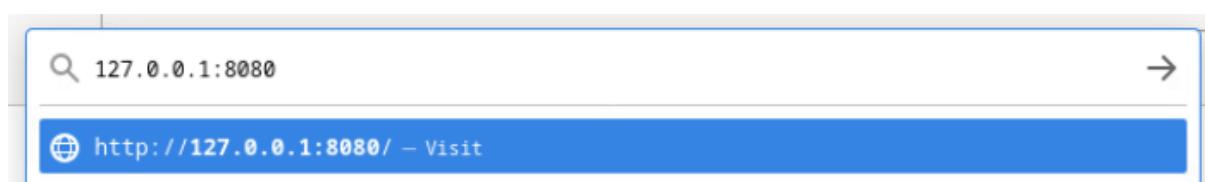
Using the **sudo nano -l** command to access the configuration file in the **/etc/nginx** directory

```
37      server {  
38          listen          8080;  
39          server_name    localhost;  
40          #charset koi8-r;  
41  
42          location / {  
43              root   /usr/share/nginx/html/text_ed_lab/;  
44              index  index.html index.htm;  
45          }  
46          #  
Save modified buffer?  
Y Yes  
N No          ^C Cancel
```

Changing the port number from **81** to **8080** and changing the root path from **/usr/share/nginx/html/** to **/usr/share/nginx/text_ed_lab/**

```
[analyst@secOps ~]$ sudo nginx -c custom_server.conf
```

Executing the new configuration



Accessing the website on the new port

The screenshot shows a web browser window with the URL `127.0.0.1:8080/`. The main content area displays the text "Congratulations!" in large, bold, black font. Below it, a smaller message reads: "As part of the Working with Text Files lab, you have successfully configured NGINX!". At the bottom of the browser window, there is a terminal-like interface showing a command-line session:

```
[analyst@secOps ~]$ 2025/04/02 12:06:06 [error] 2836#2836: *2 open() "/usr/share/nginx/html/text_ed_lab/favicon.ico" failed (2: No such file or directory), client: 127.0.0.1, server: localhost, request: "GET /favicon.ico HTTP/1.1", host: "127.0.0.1:8080"
```

The error message is coming up due to a missing file "**favicon.ico**"

The screenshot shows a terminal window with the command `sudo pkill nginx` entered and partially typed.

Using the **sudo pkill nginx** will terminate the website

The screenshot shows a Firefox browser window with the URL `127.0.0.1:8080`. The page title is "Problem loading page". The main content area displays the text "Unable to connect" and "Firefox can't establish a connection to the server at 127.0.0.1:8080.". Below this, there is a cartoon illustration of a blue, blob-like character with a sad expression. To the right of the character, there is a bulleted list of troubleshooting steps:

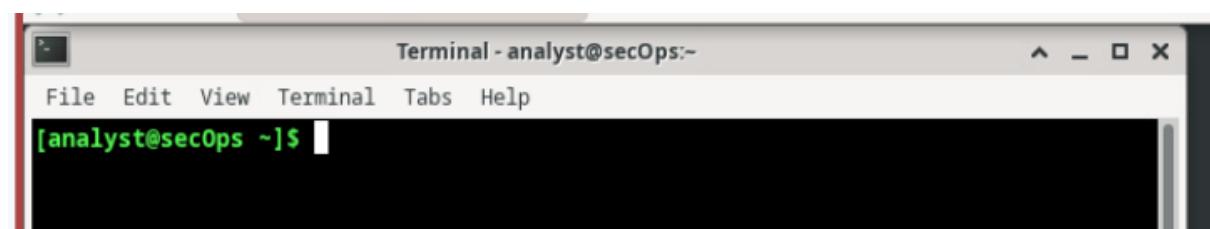
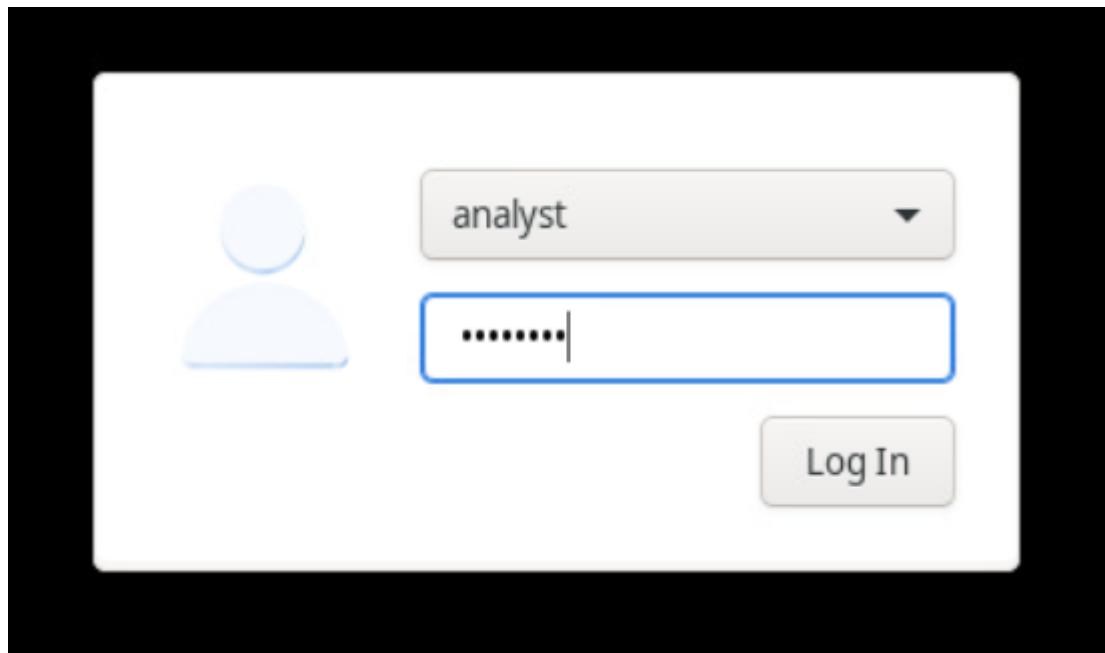
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

A blue "Try Again" button is located at the bottom right of the error page.

8.2.7 Lab – Getting Familiar with the Linux Shell

Part 1

Step 1



Logging into the VM on netlab and opening terminal

Step 2

The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The window contains the man(1) manual page for the "man" command. The page is divided into sections: NAME, SYNOPSIS, and DESCRIPTION. The SYNOPSIS section lists several command-line options for "man". The DESCRIPTION section provides a detailed explanation of what "man" does and how it finds manual pages. A message at the bottom indicates that the table below shows section numbers and types of pages.

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
MAN(1) Manual pager utils MAN(1)  
NAME  
man - an interface to the system reference manuals  
SYNOPSIS  
man [man options] [[section] page ...] ...  
man -k [apropos options] regexp ...  
man -K [man options] [section] term ...  
man -f [whatis options] page ...  
man -l [man options] file ...  
man -w|-W [man options] page ...  
DESCRIPTION  
man is the system's manual pager. Each page argument given to man is normally the name of a program, utility or function. The manual page associated with each of these arguments is then found and displayed. A section, if provided, will direct man to look only in that section of the manual. The default action is to search in all of the available sections following a pre-defined order (see DEFAULTS), and to show only the first page found, even if page exists in several sections.  
The table below shows the section numbers of the manual followed by the types of pages they contain.  
Manual page man(1) line 1 (press h for help or q to quit)
```

Opening the man (manual) page using **man man** in terminal

The table below shows the section numbers of the manual followed by the types of pages they contain.

1 Executable programs or shell commands
2 System calls (functions provided by the kernel)
3 Library calls (functions within program libraries)
4 Special files (usually found in <u>/dev</u>)
5 File formats and conventions, e.g. <u>/etc/passwd</u>
6 Games
7 Miscellaneous (including macro packages and conventions), e.g. <u>man(7)</u> , <u>groff(7)</u>
8 System administration commands (usually only for root)
9 Kernel routines [Non standard]

A manual page consists of several sections.

Conventional section names include **NAME**, **SYNOPSIS**, **CONFIGURATION**, **DESCRIPTION**, **OPTIONS**, **EXIT STATUS**, **RETURN VALUE**, **ERRORS**, **ENVIRONMENT**, **FILES**, **VERSIONS**, **CONFORMING TO**, **NOTES**, **BUGS**, **EXAMPLE**, **AUTHORS**, and **SEE ALSO**.

Some of the sections on this page are **Library calls**, **Special Files** and **Games**

```
File Edit View Terminal Tabs Help  
CP(1) User Commands CP(1)  
NAME  
cp - copy files and directories  
SYNOPSIS  
cp [OPTION]... [-T] SOURCE DEST  
cp [OPTION]... SOURCE... DIRECTORY  
cp [OPTION]... -t DIRECTORY SOURCE...  
DESCRIPTION  
Copy SOURCE to DEST, or multiple SOURCE(s) to DIRECTORY.  
Mandatory arguments to long options are mandatory for short options too.  
  
-a, --archive  
    same as -dR --preserve=all  
  
--attributes-only  
    don't copy the file data, just the attributes  
  
--backup[=CONTROL]  
Manual page cp(1) line 1 (press h for help or q to quit)
```

The **cp** command allows the user to copy files and directories

```
PWD(1) User Commands PWD(1)  
NAME  
pwd - print name of current/working directory  
SYNOPSIS  
pwd [OPTION]...  
DESCRIPTION  
Print the full filename of the current working directory.  
  
-L, --logical  
    use PWD from environment, even if it contains symlinks  
  
-P, --physical  
    avoid all symlinks  
  
--help display this help and exit  
  
--version  
    output version information and exit  
  
If no option is specified, -P is assumed.  
Manual page pwd(1) line 1 (press h for help or q to quit)
```

The command to learn about the **cp** command would be **man cp**

Step 3

```
[analyst@secOps ~]$ pwd  
/home/analyst
```

Using the **pwd** command the current directory is **/home/analyst**

```
[analyst@secOps ~]$ cd /home/analyst  
[analyst@secOps ~]$ ls -l  
total 16  
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop  
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads  
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files  
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive  
[analyst@secOps ~]$
```

Using **ls -l** showing all files in directory

```
[analyst@secOps ~]$ mkdir cyops_folder1  
[analyst@secOps ~]$ mkdir cyops_folder2  
[analyst@secOps ~]$ mkdir cyops_folder3  
[analyst@secOps ~]$ ls -l  
total 28  
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder1  
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder2  
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder3  
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop  
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads  
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files  
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive  
[analyst@secOps ~]$
```

Creating 3 new folders using the **mkdir** command

```
[analyst@secOps ~]$ cd /home/analyst/cyops_folder3  
[analyst@secOps cyops_folder3]$
```

Entering the **cyops_folder3** directory

```
[analyst@secOps cyops_folder3]$ cd ~  
[analyst@secOps ~]$
```

Going back to **/home/analyst** directory

```
[analyst@secOps ~]$ mkdir /home/analyst/cyops_folder3/cyops_folder4
[analyst@secOps ~]$ ls -l /home/analyst/cyops_folder3
total 4
drwxr-xr-x 2 analyst analyst 4096 Apr  2 12:31 cyops_folder4
[analyst@secOps ~]$
```

Creating a new folder **cyops_folder4** inside **cyops_folder3**

```
[analyst@secOps ~]$ ls -la /home/analyst/cyops_folder3
total 12
drwxr-xr-x 3 analyst analyst 4096 Apr  2 12:31 .
drwx----- 17 analyst analyst 4096 Apr  2 12:28 ..
drwxr-xr-x 2 analyst analyst 4096 Apr  2 12:31 cyops_folder4
[analyst@secOps ~]$
```

```
[analyst@secOps ~]$ cd /home/analyst/cyops_folder3
[analyst@secOps cyops_folder3]$ cd .
[analyst@secOps cyops_folder3]$ cd ..
[analyst@secOps ~]$
```

Changing directory to **cyops_folder3**

Using “**cd .**” doesn't switch the directory, but using “**cd ..**” returns you to the parent directory

```
[analyst@secOps ~]$ cd ..
[analyst@secOps home]$
```

```
[analyst@secOps home]$ cd ..
[analyst@secOps /]$
```

```
[analyst@secOps /]$ cd ..
[analyst@secOps /]$
```

Step 4

```
[analyst@secOps ~]$ cd /home/analyst  
[analyst@secOps ~]$ 
```

```
[analyst@secOps ~]$ echo This is a message echoed by the terminal  
This is a message echoed by the terminal  
[analyst@secOps ~]$ 
```

Using **echo** command to return a message in terminal

```
[analyst@secOps ~]$ echo This is a message echoed by the terminal > some_text_file.txt  
[analyst@secOps ~]$ 
```

Adding “> **some_text_file.txt**” to the previous line will save the text that was echo’d into a **.txt** file

```
[analyst@secOps ~]$ ls -l  
total 32  
drwxr-xr-x 2 analyst analyst 4096 Apr  2 12:28 cyops_folder1  
drwxr-xr-x 2 analyst analyst 4096 Apr  2 12:28 cyops_folder2  
drwxr-xr-x 3 analyst analyst 4096 Apr  2 12:31 cyops_folder3  
drwxr-xr-x 2 analyst analyst 4096 May 20 2020 Desktop  
drwxr-xr-x 3 analyst analyst 4096 Jul 30 2020 Downloads  
drwxr-xr-x 11 analyst analyst 4096 Aug 11 2020 lab.support.files  
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive  
-rw-r--r-- 1 analyst analyst    41 Apr  2 12:35 some_text_file.txt  
[analyst@secOps ~]$ 
```

```
[analyst@secOps ~]$ ls -l some_text_file.txt  
-rw-r--r-- 1 analyst analyst 41 Apr  2 12:35 some_text_file.txt  
[analyst@secOps ~]$ 
```

```
[analyst@secOps ~]$ cat some_text_file.txt  
This is a message echoed by the terminal  
[analyst@secOps ~]$ 
```

Using **cat** command to return the value of the **.txt** file

```
[analyst@secOps ~]$ echo This is a DIFFERENT message > some_text_file.txt  
[analyst@secOps ~]$ cat some_text_file.txt  
This is a DIFFERENT message  
[analyst@secOps ~]$ 
```

Changing the content of the file using the same command but different message

Step 5

```
[analyst@secOps ~]$ echo This is another line of text >> some_text_file.txt
[analyst@secOps ~]$ cat some_text_file.txt
This is a DIFFERENT message
This is another line of text
[analyst@secOps ~]$ █
```

Same command used but instead of using “>”, “>>” is used – this appends to a current .txt file

Step 6

```
[analyst@secOps ~]$ ls -l
total 32
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder1
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder2
drwxr-xr-x  3 analyst analyst 4096 Apr  2 12:31 cyops_folder3
drwxr-xr-x  2 analyst analyst 4096 May 20 2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30 2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11 2020 lab.support.files
drwxr-xr-x  2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r--  1 analyst analyst   57 Apr  2 12:38 some_text_file.txt
[analyst@secOps ~]$
```

Checking home directory

```
[analyst@secOps ~]$ ls -la
total 132
drwx----- 17 analyst analyst 4096 Apr  2 12:35 .
drwxr-xr-x  3 root    root    4096 Mar 20 2018 ..
-rw-------  1 analyst analyst     0 Sep 29 2020 .bash_history
-rw-r--r--  1 analyst analyst   21 Feb  7 2018 .bash_logout
-rw-r--r--  1 analyst analyst   57 Feb  7 2018 .bash_profile
-rw-r--r--  1 analyst analyst   97 Mar 20 2018 .bashrc
-rw-r--r--  1 analyst analyst  141 Feb  7 2018 .bashrc_stock
drwxr-xr-x  8 analyst analyst 4096 Mar 25 2020 .cache
drwxr-xr-x 10 analyst analyst 4096 Aug 11 2020 .config
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder1
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder2
drwxr-xr-x  3 analyst analyst 4096 Apr  2 12:31 cyops_folder3
drwxr-xr-x  2 analyst analyst 4096 May 20 2020 Desktop
-rw-r--r--  1 analyst analyst   23 Mar 23 2018 .dmrc
drwxr-xr-x  3 analyst analyst 4096 Jul 30 2020 Downloads
drwx-----  3 analyst analyst 4096 Mar 22 2018 .gnupg
-rw-------  1 analyst analyst 2520 Mar 24 2020 .ICEauthority
drwxr-xr-x  2 analyst analyst 4096 Mar 24 2018 .idlerc
drwxr-xr-x 11 analyst analyst 4096 Aug 11 2020 lab.support.files
-rw-------  1 analyst analyst   89 May 20 2020 .lesshtst
```

Checking home directory (with hidden files)

```
[analyst@secOps ~]$ man ls
[analyst@secOps ~]$
```

LS(1)

User Commands

LS(1)

NAME

ls - list directory contents

SYNOPSIS

ls [OPTION]... [FILE]...

DESCRIPTION

List information about the FILEs (the current directory by default). Sort entries alphabetically if none of **-cftuvSUX** nor **--sort** is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all
do not ignore entries starting with .

-A, --almost-all
do not list implied . and ..

--author

Manual page ls(1) line 1 (press h for help or q to quit)

Part 2

Step 1

```
[analyst@secOps ~]$ cp some_text_file.txt cyops_folder2/
[analyst@secOps ~]$ ls cyops_folder2/
some_text_file.txt
[analyst@secOps ~]$
```

The command **cp** | file to copy | directory to paste into

```
[analyst@secOps ~]$ ls -l
total 32
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder1
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:41 cyops_folder2
drwxr-xr-x  3 analyst analyst 4096 Apr  2 12:31 cyops_folder3
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst analyst    57 Apr  2 12:38 some_text_file.txt
[analyst@secOps ~]$
```

Checking both **home** directory and **cyops_folder2**

Step 2

```
[analyst@secOps ~]$ rm some_text_file.txt
[analyst@secOps ~]$ ls -l
total 28
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:28 cyops_folder1
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:41 cyops_folder2
drwxr-xr-x  3 analyst analyst 4096 Apr  2 12:31 cyops_folder3
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive
[analyst@secOps ~]$
```

Deleting the **some_text_file.txt** using the **rm** command and checking if the file has been deleted

```
[analyst@secOps ~]$ rm -r cyops_folder1
[analyst@secOps ~]$ ls -l
total 24
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:41 cyops_folder2
drwxr-xr-x  3 analyst analyst 4096 Apr  2 12:31 cyops_folder3
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive
[analyst@secOps ~]$
```

Deleting the folder **cyops_folder1** using the **rm -r** command and checking if it has been deleted

Step 3

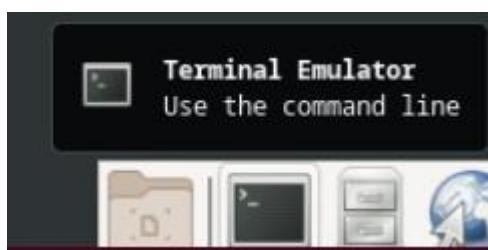
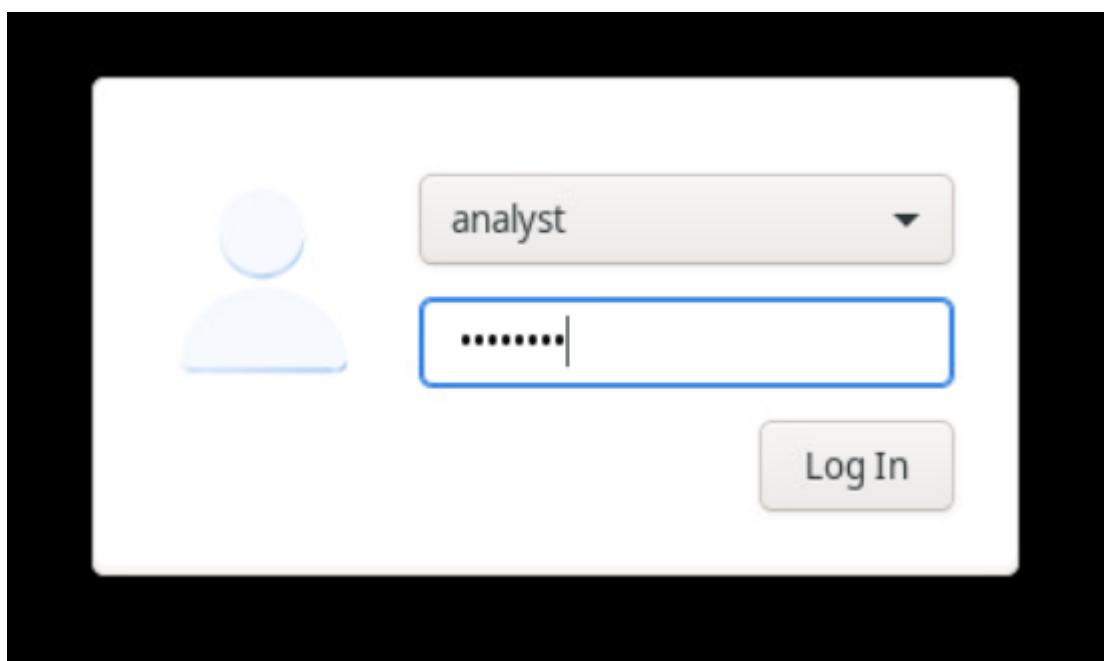
```
[analyst@secOps ~]$ mv cyops_folder2/some_text_file.txt .
[analyst@secOps ~]$ ls -l cyops_folder2/
total 0
[analyst@secOps ~]$ ls -l /home/analyst
total 28
drwxr-xr-x  2 analyst analyst 4096 Apr  2 12:43 cyops_folder2
drwxr-xr-x  3 analyst analyst 4096 Apr  2 12:31 cyops_folder3
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst analyst    57 Apr  2 12:41 some_text_file.txt
[analyst@secOps ~]$
```

Using the **mv** command followed by the file (with directory) followed by the destination will move the desired file to the location mention (in this case to the **/home/analyst/** directory as that is the directory we are in

8.5.4 Lab - Navigating the Linux Filesystem and Permission Settings

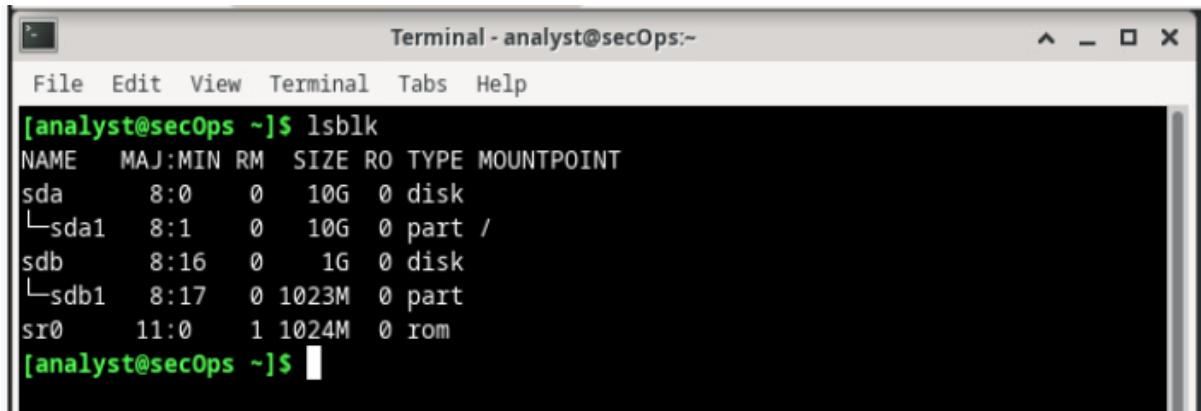
Part 1

Step 1



Accessing the VM on netlab and opening terminal

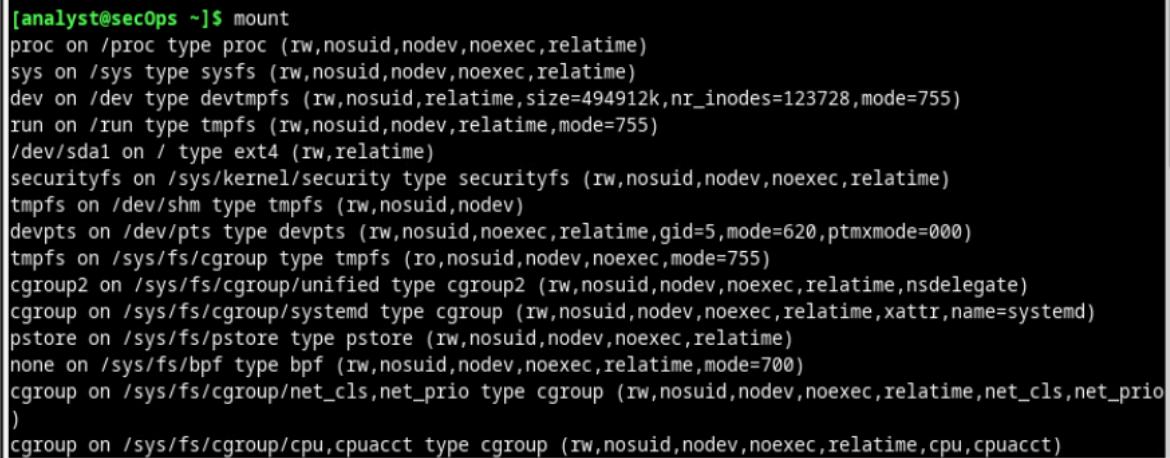
Step 2



A terminal window titled "Terminal - analyst@secOps:-" showing the output of the lsblk command. The output lists block devices and their details:

```
[analyst@secOps ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   10G  0 disk 
└─sda1   8:1    0   10G  0 part /
sdb      8:16   0    1G  0 disk 
└─sdb1   8:17   0 1023M 0 part 
sr0     11:0    1 1024M 0 rom
```

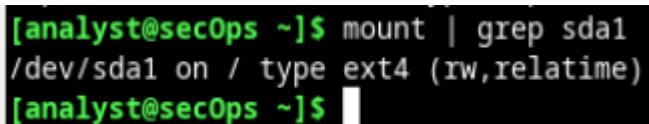
Using the **lsblk** command to check the block devices



A terminal window showing the output of the mount command. It lists all currently mounted filesystems:

```
[analyst@secOps ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=494912k,nr_inodes=123728,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
```

Using the **mount** command to check the currently mounted filesystems



A terminal window showing the output of the command "mount | grep sda1", which filters the mount command output to show only the entry for the root filesystem:

```
[analyst@secOps ~]$ mount | grep sda1
/dev/sda1 on / type ext4 (rw,relatime)
[analyst@secOps ~]$
```

Filtering the output of the **mount** command to the root filesystem

```
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx  1 root root    7 Nov 13  2019 bin  -> usr/bin
drwxr-xr-x  3 root root  4096 Apr 10  2020 boot
drwxr-xr-x 18 root root  3260 Apr   2 18:20 dev
drwxr-xr-x 63 root root  4096 Dec 22  2020 etc
drwxr-xr-x  3 root root  4096 Mar 20  2018 home
lrwxrwxrwx  1 root root    7 Nov 13  2019 lib  -> usr/lib
lrwxrwxrwx  1 root root    7 Nov 13  2019 lib64 -> usr/lib
drwx----- 2 root root 16384 Mar 20  2018 lost+found
drwxr-xr-x  2 root root  4096 Jan  5  2018 mnt
drwxr-xr-x  2 root root  4096 Jan  5  2018 opt
dr-xr-xr-x 288 root root     0 Apr   2 18:20 proc
drwxr-x---  8 root root  4096 Sep 29  2020 root
drwxr-xr-x 19 root root   580 Apr   2 18:20 run
lrwxrwxrwx  1 root root    7 Nov 13  2019 sbin -> usr/bin
drwxr-xr-x  6 root root  4096 Mar 24  2018 srv
dr-xr-xr-x 13 root root     0 Apr   2 18:20 sys
drwxrwxrwt 12 root root   300 Apr   2 18:20 tmp
drwxr-xr-x  9 root root  4096 Jun  8  2020 usr
drwxr-xr-x 12 root root  4096 Jun  8  2020 var
[analyst@secOps /]$
```

Switching the directory to **/home** and checking the visible files & directories on it

Sdb1 isn't visible as it isn't mounted

Step 3

```
[analyst@secOps ~]$ cd ~  
[analyst@secOps ~]$ ls -l  
total 16  
drwxr-xr-x 2 analyst analyst 4096 May 20 2020 Desktop  
drwxr-xr-x 3 analyst analyst 4096 Jul 30 2020 Downloads  
drwxr-xr-x 11 analyst analyst 4096 Aug 11 2020 lab.support.files  
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive  
[analyst@secOps ~]$
```

Checking if “second_drive” directory is present

```
[analyst@secOps ~]$ ls -l second_drive/  
total 0  
[analyst@secOps ~]$
```

Checking contents of the directory

```
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/  
[sudo] password for analyst:  
[analyst@secOps ~]$
```

Mounting sdb1

```
[analyst@secOps ~]$ ls -l second_drive/  
total 20  
drwx----- 2 root      root 16384 Mar 26 2018 lost+found  
-rw-rw-r-x 1 analyst    root   188 May 19 2020 myFile.txt  
[analyst@secOps ~]$
```

Checking if it has been mounted successfully

```
[analyst@secOps ~]$ mount | grep /dev/sd  
/dev/sda1 on / type ext4 (rw,relatime)  
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime)  
[analyst@secOps ~]$
```

Checking partition details

```
[analyst@secOps ~]$ sudo umount /dev/sdb1  
[analyst@secOps ~]$ ls -l second_drive/  
total 0  
[analyst@secOps ~]$
```

Unmounting sdb1

Part 2

Step 1

```
[analyst@secOps ~]$ cd lab.support.files/scripts/
[analyst@secOps scripts]$ ls -l
total 60
-rwxr-xr-x 1 analyst analyst 952 Mar 21 2018 configure_as_dhcp.sh
-rwxr-xr-x 1 analyst analyst 1153 Mar 21 2018 configure_as_static.sh
-rwxr-xr-x 1 analyst analyst 3459 Mar 21 2018 cyberops_extended_topo_no_fw.py
-rwxr-xr-x 1 analyst analyst 4062 Mar 21 2018 cyberops_extended_topo.py
-rwxr-xr-x 1 analyst analyst 3669 Mar 21 2018 cyberops_topo.py
-rw-r--r-- 1 analyst analyst 2871 Mar 21 2018 cyops.mn
-rwxr-xr-x 1 analyst analyst 458 Mar 21 2018 fw_rules
-rwxr-xr-x 1 analyst analyst 70 Mar 21 2018 mal_server_start.sh
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 net_configuration_files
-rwxr-xr-x 1 analyst analyst 65 Mar 21 2018 reg_server_start.sh
-rwxr-xr-x 1 analyst analyst 189 Mar 21 2018 start_ELK.sh
-rwxr-xr-x 1 analyst analyst 85 Mar 21 2018 start_miniedit.sh
-rwxr-xr-x 1 analyst analyst 76 Mar 21 2018 start_pox.sh
-rwxr-xr-x 1 analyst analyst 106 Mar 21 2018 start_snort.sh
-rwxr-xr-x 1 analyst analyst 61 Mar 21 2018 start_tftpd.sh
[analyst@secOps scripts]$
```

Changing directory to **lab.support.files/scripts** and checking file permissions

```
[analyst@secOps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@secOps scripts]$
```

Attempting to use the **touch** command

```
[analyst@secOps scripts]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan  5 2018 /mnt
[analyst@secOps scripts]$
```

Checking the permissions of parent directory

```
[analyst@secOps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
[analyst@secOps scripts]$
```

Changing permissions of a directory using the **chmod** command

```
[analyst@secOps scripts]$ cd ~/second_drive/
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root 16384 Mar 26 2018 lost+found
-rw-rw-r-x 1 analyst    root   188 May 19 2020 myFile.txt
[analyst@secOps second_drive]$
```

Changing directory to `/~/second_drive`

`myFile.txt` has read and write permission for owner, read permissions for group owner of the file and read permissions for all other users

```
[analyst@secOps second_drive]$ sudo chmod 665 myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root 16384 Mar 26  2018 lost+found
-rw-rw-r-x  1 analyst   root   188 May 19  2020 myFile.txt
[analyst@secOps second_drive]$
```

Changing permission of `myFile.txt` so that group owners can read and write

`chmod 777` would give `-rwxrwxrwx` permissions

```
[analyst@secOps second_drive]$ sudo chown analyst myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root 16384 Mar 26  2018 lost+found
-rw-rw-r-x  1 analyst   root   188 May 19  2020 myFile.txt
[analyst@secOps second_drive]$
```

The command `chown` changes ownership of the file

```
[analyst@secOps second_drive]$ echo Test >> myFile.txt
[analyst@secOps second_drive]$ cat myFile.txt
This is a file stored in the /dev/sdb1 disk.
Notice that even though this file has been sitting in this disk for a while, it couldn't be accessed until the disk was properly mounted.
test
Test
[analyst@secOps second_drive]$
```

Appendin to the file and the changes have been applied to to permission changes

Step 2

```
[analyst@secOps second_drive]$ cd ~/lab.support.files/
[analyst@secOps lab.support.files]$ ls -l
total 592
-rw-r--r-- 1 analyst analyst      649 Mar 21  2018 apache_in_epoch.log
-rw-r--r-- 1 analyst analyst      126 Mar 21  2018 applicationX_in_epoch.log
drwxr-xr-x 4 analyst analyst    4096 Mar 21  2018 attack_scripts
-rw-r--r-- 1 analyst analyst      102 Mar 21  2018 confidential.txt
-rw-r--r-- 1 analyst analyst    2871 Mar 21  2018 cyops.mn
-rw-r--r-- 1 analyst analyst       75 Mar 21  2018 elk_services
-rw-r--r-- 1 analyst analyst     373 Mar 21  2018 h2_dropbear.banner
drwxr-xr-x 2 analyst analyst    4096 Apr  3  2018 instructor
-rw-r--r-- 1 analyst analyst      255 Mar 21  2018 letter_to_grandma.txt
-rw-r--r-- 1 analyst analyst   24464 Mar 21  2018 logstash-tutorial.log
-rw xr-x--- 1 analyst analyst      486 Jul 15  2020 long_commands
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 malware
-rw xr-xr-x 1 analyst analyst      172 Mar 21  2018 mininet_services
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 openssl_lab
drwxr-xr-x 2 analyst analyst    4096 Aug 11  2020 pcaps
drwxr-xr-x 2 analyst analyst    4096 Aug 11  2020 pems
drwxr-xr-x 7 analyst analyst    4096 Mar 21  2018 pox
-rw-r--r-- 1 analyst analyst  473363 Mar 21  2018 sample.img
-rw-r--r-- 1 analyst analyst       65 Mar 21  2018 sample.img_SHA256.sig
drwxr-xr-x 3 analyst analyst    4096 Mar 21  2018 scripts
-rw-r--r-- 1 analyst analyst   25553 Mar 21  2018 SQL_Lab.pcap
drwxr-xr-x 2 analyst analyst    4096 Aug 11  2020 traceroute_files
[analyst@secOps lab.support.files]$ █
```

Changing directory and listing all files in the directory

Part 3

Step 1

```
[analyst@secOps lab.support.files]$ cd ~
[analyst@secOps ~]$ ls -l
total 16
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  3 root    root    4096 May  4  2020 second_drive
[analyst@secOps ~]$
```

Changing directory to `/home/analyst` and checking files & directories

```
[analyst@secOps ~]$ ls -l /dev/
total 0
crw----- 1 root root 10, 175 Apr 2 18:20 agpgart
crw-r--r-- 1 root root 10, 235 Apr 2 18:20 autofs
drwxr-xr-x 2 root root 140 Apr 2 18:20 block
drwxr-xr-x 2 root root 100 Apr 2 18:20 bsg
crw----- 1 root root 10, 234 Apr 2 18:20 btrfs-control
lrwxrwxrwx 1 root root 3 Apr 2 18:20 cdrom -> sr0
drwxr-xr-x 2 root root 2700 Apr 2 18:20 char
crw----- 1 root root 5, 1 Apr 2 18:20 console
lrwxrwxrwx 1 root root 11 Apr 2 18:20 core -> /proc/kcor
crw----- 1 root root 10, 60 Apr 2 18:20 cpu_dma_latency
crw----- 1 root root 10, 203 Apr 2 18:20 cuse
drwxr-xr-x 6 root root 120 Apr 2 18:20 disk
```

Checking files and directories inside `/dev` directory

```

crw-rw---- 1 root disk      10, 237 Apr 2 18:20 loop-control
drwxr-xr-x 2 root root      60 Apr 2 18:20 mapper
crw-r---- 1 root kmem      1,   1 Apr 2 18:20 mem
drwxrwxrwt 2 root root      40 Apr 2 18:20 mqueue
drwxr-xr-x 2 root root      60 Apr 2 18:20 net
crw-rw-rw- 1 root root      1,   3 Apr 2 18:20 null
crw----- 1 root root      10, 144 Apr 2 18:20 nvram
crw-r---- 1 root kmem      1,   4 Apr 2 18:20 port
crw----- 1 root root     108,   0 Apr 2 18:20 ppp
crw----- 1 root root      10,   1 Apr 2 18:20 psaux
crw-rw-rw- 1 root tty       5,   2 Apr 2 18:38 ptmx
drwxr-xr-x 2 root root      0 Apr 2 18:20 pts
crw-rw-rw- 1 root root      1,   8 Apr 2 18:20 random
crw----- 1 root root      10, 242 Apr 2 18:20 rfkill
lrwxrwxrwx 1 root root      4 Apr 2 18:20 rtc -> rtc0
crw----- 1 root root    249,   0 Apr 2 18:20 rtc0
brw-rw---- 1 root disk      8,   0 Apr 2 18:20 sda
brw-rw---- 1 root disk      8,   1 Apr 2 18:20 sda1
brw-rw---- 1 root disk      8,  16 Apr 2 18:20 sdb
brw-rw---- 1 root disk      8,  17 Apr 2 18:20 sdb1
drwxrwxrwt 2 root root      40 Apr 2 18:20 shm
crw----- 1 root root      10, 231 Apr 2 18:20 snapshot
drwxr-xr-x 2 root root      80 Apr 2 18:20 snd
brw-rw----+ 1 root optical  11,   0 Apr 2 18:20 sr0
lrwxrwxrwx 1 root root      15 Apr 2 18:20 stderr -> /proc/self/fd/2
lrwxrwxrwx 1 root root      15 Apr 2 18:20 stdin -> /proc/self/fd/0
lrwxrwxrwx 1 root root      15 Apr 2 18:20 stdout -> /proc/self/fd/1

```

```

[analyst@secOps ~]$ echo "symbolic" > file1.txt
[analyst@secOps ~]$ cat file1.txt
symbolic
[analyst@secOps ~]$ echo "hard" > file2.txt
[analyst@secOps ~]$ cat file2.txt
hard
[analyst@secOps ~]$ 

```

Creating 2 .txt files

```

[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
[analyst@secOps ~]$ 

```

Applying a symbolic link to 1 file and a hard link to the other

```
[analyst@secOps ~]$ ls -l
total 28
drwxr-xr-x  2 analyst analyst 4096 May 20  2020 Desktop
drwxr-xr-x  3 analyst analyst 4096 Jul 30  2020 Downloads
lrvwxrwxrwx  1 analyst analyst    9 Apr  2 18:41 file1symbolic -> file1.txt
-rw-r--r--  1 analyst analyst    9 Apr  2 18:40 file1.txt
-rw-r--r--  2 analyst analyst   5 Apr  2 18:40 file2hard
-rw-r--r--  2 analyst analyst   5 Apr  2 18:40 file2.txt
drwxr-xr-x 11 analyst analyst 4096 Aug 11  2020 lab.support.files
drwxr-xr-x  3 root    root    4096 May  4  2020 second_drive
[analyst@secOps ~]$
```

Checking directory to see changes made

```
[analyst@secOps ~]$ mv file1.txt file1new.txt
[analyst@secOps ~]$ mv file2.txt file2new.txt
[analyst@secOps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@secOps ~]$ cat file2hard
hard
[analyst@secOps ~]$
```

Replacing the names of the files and executing each file to see if the new file names work

Module 18: Cryptography

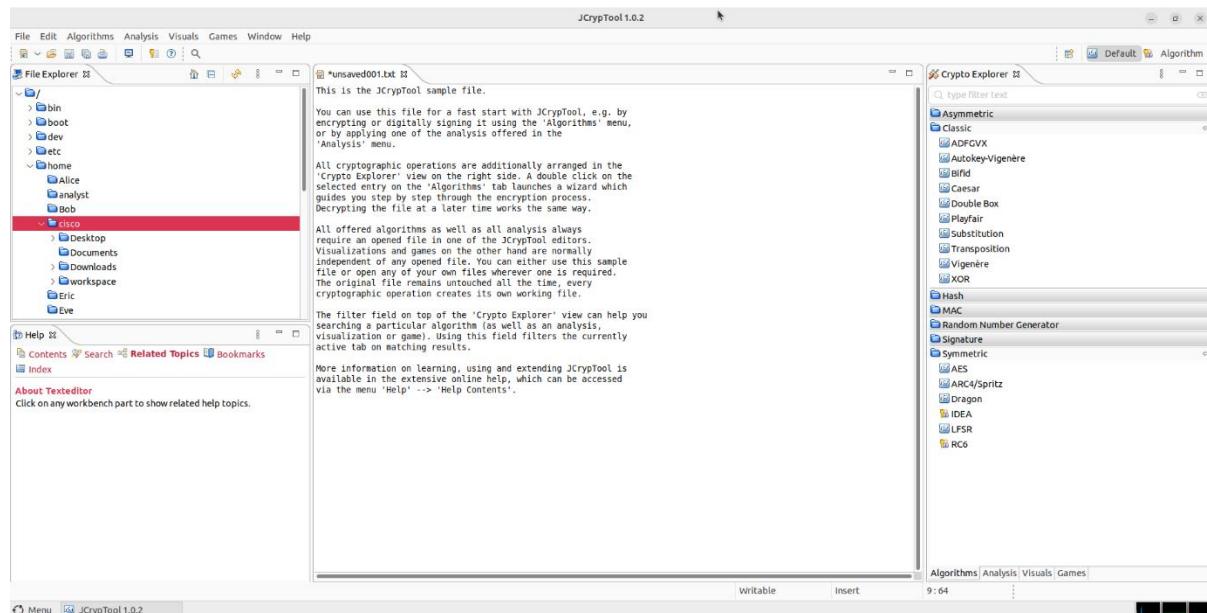
18.1.11 Lab - Use Classic and Modern Encryption Algorithms

Part 1

Step 1

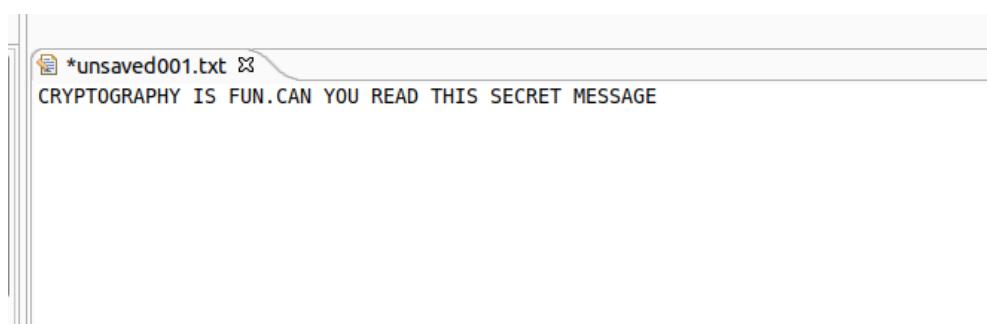
Opening the lab VM

Step 2



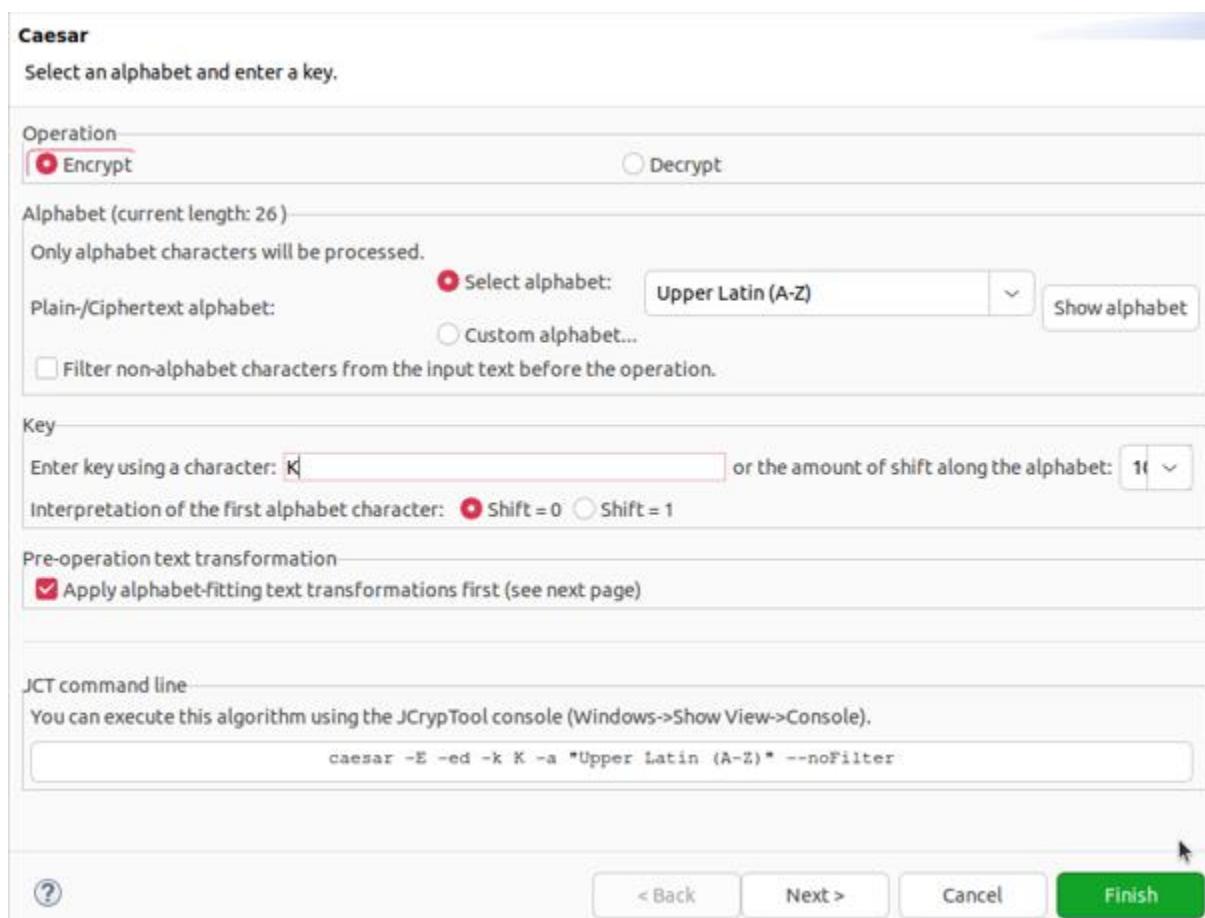
Opening the JCrypTool

Step 3



*unsaved001.txt
CRYPTOGRAPHY IS FUN. CAN YOU READ THIS SECRET MESSAGE

Replacing the message inside **unsaved001.txt**



Caesar
Select an alphabet and enter a key.

Operation
 Encrypt Decrypt

Alphabet (current length: 26)
Only alphabet characters will be processed.

Plain-/Ciphertext alphabet: Select alphabet: Custom alphabet...
Upper Latin (A-Z)

Filter non-alphabet characters from the input text before the operation.

Key
Enter key using a character: or the amount of shift along the alphabet:

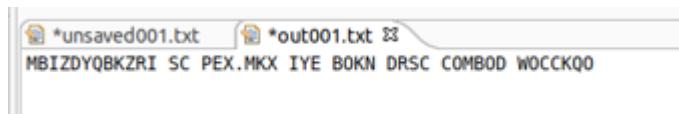
Interpretation of the first alphabet character: Shift = 0 Shift = 1

Pre-operation text transformation
 Apply alphabet-fitting text transformations first (see next page)

JCT command line
You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).
`caesar -E -ed -k K -a "Upper Latin (A-Z)" --noFilter`

< Back Next > Cancel **Finish**

Checking and setting parameters for **Caesar**



*unsaved001.txt *out001.txt
MBIZDYQBKZRI SC PEX.MKX IYE BOKN DRSC COMBOD WOCCKQO

Checking the output on the new **out001.txt** file

Step 4

Caesar
Select an alphabet and enter a key.

Operation
 Encrypt Decrypt

Alphabet (current length: 26)
Only alphabet characters will be processed.

Plain-/Ciphertext alphabet:
 Select alphabet: **Upper Latin (A-Z)**
 Custom alphabet...

Filter non-alphabet characters from the input text before the operation.

Key
Enter key using a character: K or the amount of shift along the alphabet: **16**

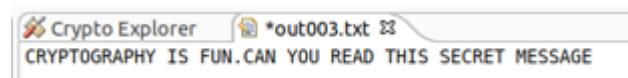
Interpretation of the first alphabet character: Shift = 0 Shift = 1

Pre-operation text transformation
 Apply alphabet-fitting text transformations first (see next page)

JCT command line
You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).
`caesar -D -ed -k K -a "Upper Latin (A-Z)" --noFilter`

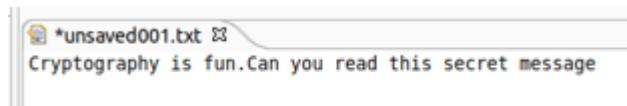
 < Back Next > Cancel **Finish**

Setting **Caesar** to decrypt the encrypted message



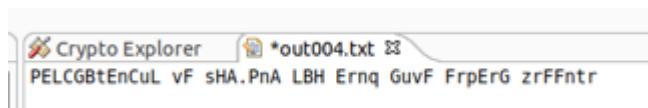
Decrypted message

Step 5



```
*unsaved001.txt
Cryptography is fun. Can you read this secret message
```

Creating a new file with a new message

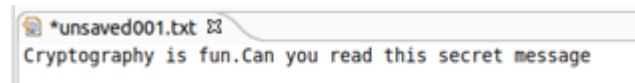


```
Crypto Explorer *out004.txt
PELCGBtEnCuL vF sHA. PnA LBH Ernq GuvF FrpErG zrFFntr
```

New encrypted message

Part 2

Step 1



```
*unsaved001.txt
Cryptography is fun. Can you read this secret message
```

Creating a new file with a new message

AES

To encrypt or decrypt a message with the AES algorithm, choose a key (just manually entered, or from the key store) and pick a padding and block cipher mode.

Operation

Encrypt

Decrypt

Key source

Custom key

Key from keystore

Custom key

Key length: 128

Key (hex): AA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF

Mode and padding scheme

Mode: (ECB) Electronic Codebook

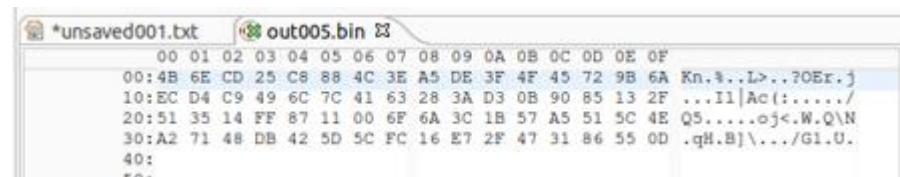
Padding: PKCS#5 Padding



Cancel

Finish

Setting **AES** to encrypt the message



```
*unsaved001.txt  out005.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:4B 6E CD 25 C8 88 4C 3E A5 DE 3F 4F 45 72 9B 6A Kn.%..L>.,?OER,j
10:EC D4 C9 49 6C 7C 41 63 28 3A D3 0B 90 85 13 2F ...I1|Ac(:..../
20:51 35 14 FF 87 11 00 6F 6A 3C 1B 57 A5 51 5C 4E Q5....oj<.W.Q\N
30:A2 71 48 DB 42 5D 5C FC 16 E7 2F 47 31 86 55 0D .qH.B]\.../G1.U.
40:
en.
```

Encrypted message

Step 2

AES

To encrypt or decrypt a message with the AES algorithm, choose a key (just manually entered, or from the key store) and pick a padding and block cipher mode.

Operation

Encrypt Decrypt

Key source

Custom key Key from keystore

Custom key

Key length: 128

Key (hex): AA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF

Mode and padding scheme

Mode: (ECB) Electronic Codebook

Padding: PKCS#5 Padding

?

Cancel

Finish

Setting **AES** to decrypt the message

```
Explorer out006.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:43 72 79 70 74 6F 67 72 61 70 68 79 20 69 73 20 Cryptography is
10:66 75 6E 2E 43 61 6E 20 79 6F 75 20 72 65 61 64 fun. Can you read
20:20 74 68 69 73 20 73 65 63 72 65 74 20 6D 65 73 this secret mes
30:73 61 67 65 sage
```

Decrypted message

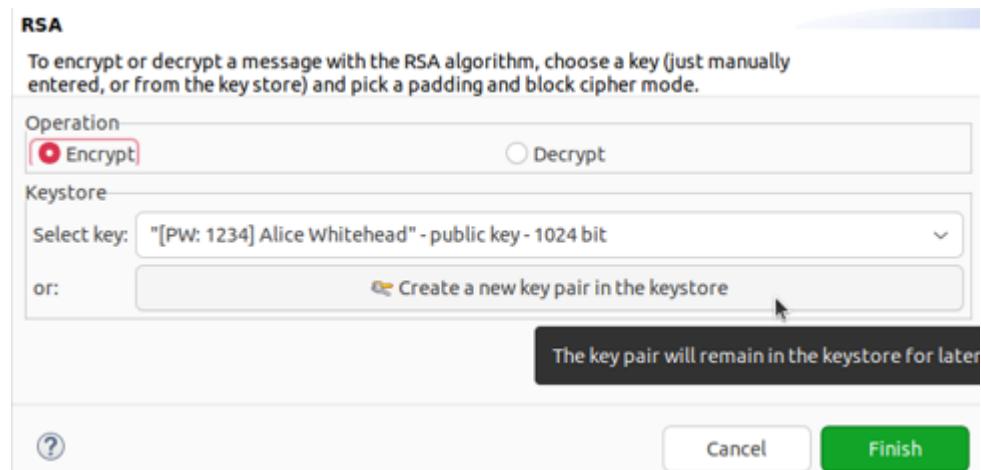
Part 3

Step 1



```
*unsaved001.txt
Cryptography is fun. Can you read this secret message
```

Creating a new file with a new message



RSA

To encrypt or decrypt a message with the RSA algorithm, choose a key (just manually entered, or from the keystore) and pick a padding and block cipher mode.

Operation

Encrypt Decrypt

Keystore

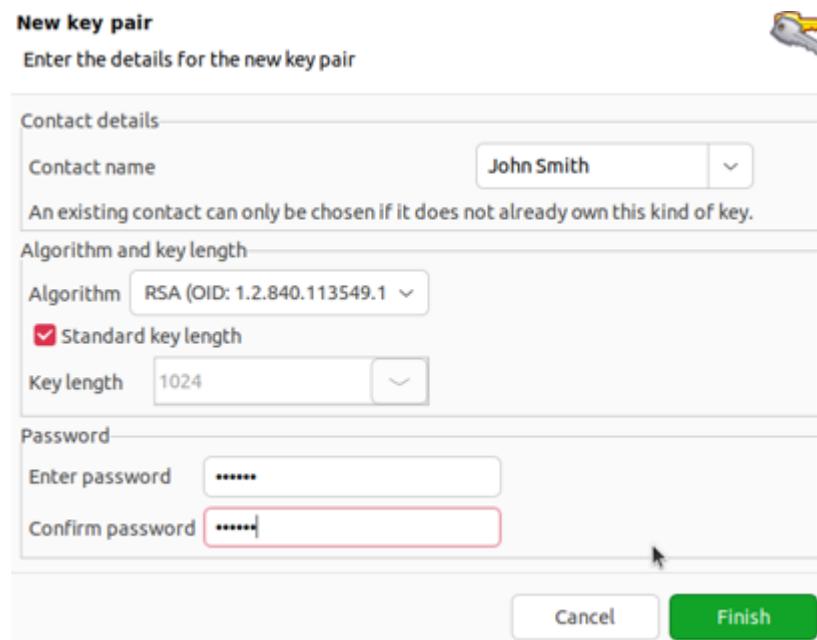
Select key: [PW: 1234] Alice Whitehead - public key - 1024 bit

or: [Create a new key pair in the keystore](#)

The key pair will remain in the keystore for later use.

Cancel Finish

Opening the **RSA** algorithm



New key pair

Enter the details for the new key pair

Contact details

Contact name: John Smith

An existing contact can only be chosen if it does not already own this kind of key.

Algorithm and key length

Algorithm: RSA (OID: 1.2.840.113549.1)

Standard key length

Key length: 1024

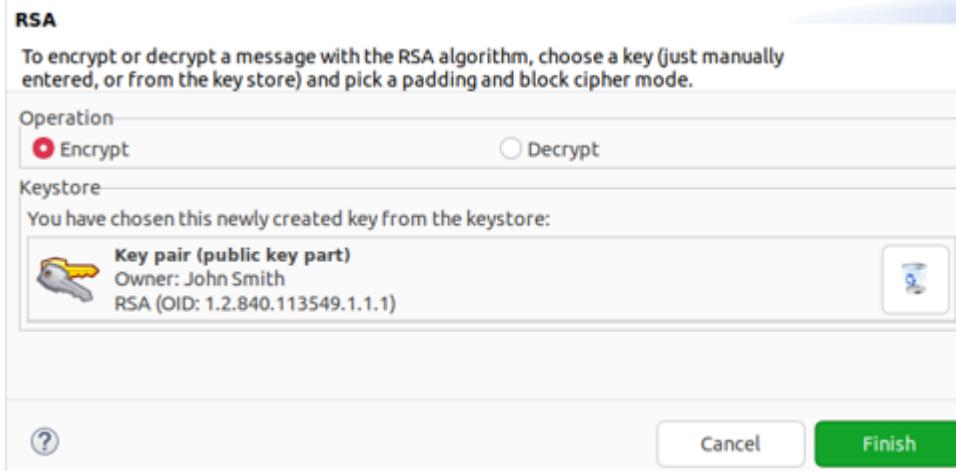
Password

Enter password: *****

Confirm password: *****

Cancel Finish

Creating a new **key pair**

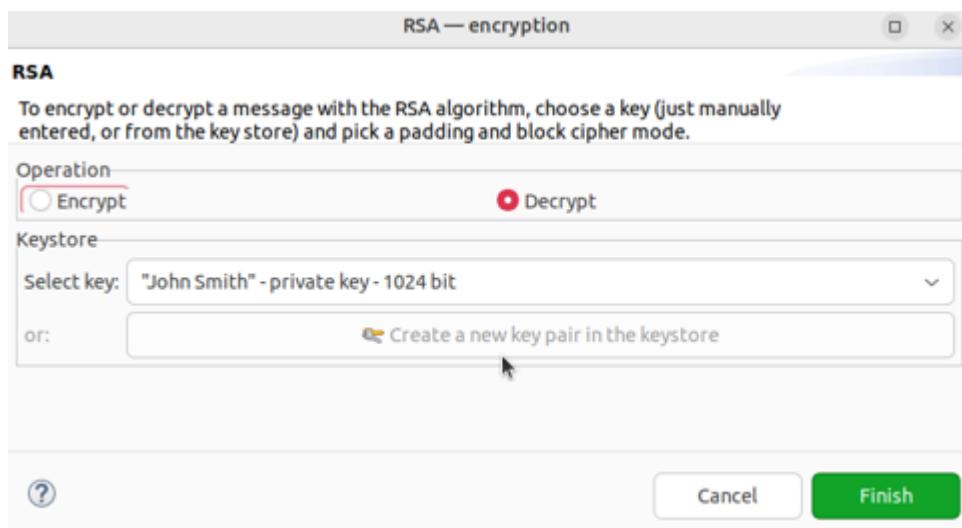


Using the new key pair

```
Explorer [out007.bin]
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:40 31 7A 2F 3C C1 98 3C 79 43 2A 84 5F A7 DE CB @1z/<..<yC*._...
10:57 6F 7F 19 78 78 B8 5A 93 AA A0 96 CD 4E 85 07 Wo..xx.Z....N.,
20:EF F2 3D C2 B0 09 AF 5E D9 7D D4 97 8F 8E 44 90 ..=....^}....D.
30:33 9A 32 26 11 D4 9B E0 76 9C 7F E7 4D 7D 9F 13 3.25....v...M}..
40:7A 08 11 FF 08 48 5B D9 4F FC 17 80 10 AC 03 8F z....H[.O.....
50:61 74 E5 4C 8B 16 4A 02 A3 3A 75 E0 16 04 9F 0E at.L..J..;u.....
60:17 5E 4F 0B 28 FA C2 A7 FF 20 47 52 4D 5C 8A 3D .^O. .... GRM\.=
70:DB 3A 82 B2 73 41 8F 62 47 54 CA 16 9B 3F D6 6F .:..sA.BGT...?o
80:.
```

Decrypted message

Step 2



Setting **RSA** to decrypt the message

```
Explorer out008.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:43 72 79 70 74 6F 67 72 61 70 68 79 20 69 73 20 Cryptography is
10:66 75 6E 2E 43 61 6E 20 79 6F 75 20 72 65 61 64 fun.Can you read
20:20 74 68 69 73 20 73 65 63 72 65 74 20 6D 65 73 this secret mes
30:73 61 67 65
40:
```

The screenshot shows the 'Explorer' window with a file named 'out008.bin'. The file content is displayed in both hex and ASCII formats. The ASCII text reads: 'Cryptography is fun. Can you read this secret message?'.

Decrypted message

18.4.10 Lab – Hashing Things Out

Part 1

```
[analyst@secOps ~]$ cd /home/analyst/lab.support.files/  
[analyst@secOps lab.support.files]$
```

Opening a **terminal** and changing directory to **/lab.support.files**

```
[analyst@secOps lab.support.files]$ cat letter_to_grandma.txt  
Hi Grandma,  
I am writing this letter to thank you for the chocolate chip cookies you sent me.  
. I got them this morning and I have already eaten half of the box! They are absolutely delicious!  
  
I wish you all the best. Love,  
Your cookie-eater grandchild.
```

Executing the **.txt** file using the **cat** command to check its contents

```
[analyst@secOps lab.support.files]$ openssl sha256 letter_to_grandma.txt  
SHA256(letter_to_grandma.txt)= deff9c9bbece44866796ff6cf21f2612fbb77aa1b2515a900  
bafb29be118080b
```

Hashing the **.txt** file using the **sha256** algorithm

```
GNU nano 4.9.2          letter_to_grandma.txt          Modified  
Hi Grandpa,  
I am writing this letter to thank you for the chocolate chip cookies you sent me.  
  
I wish you all the best. Love,  
Your cookie-eater grandchild.
```

Altering the contents of the **.txt** file using **nano**

```
[analyst@secOps lab.support.files]$ openssl sha256 letter_to_grandma.txt  
SHA256(letter_to_grandma.txt)= 43302c4500b7c4b8e574ba27a59d83267812493c029fd054c  
9242f3ac73100bc
```

Hashing the **.txt** file again using the same algorithm, but this time given a different output

```
[analyst@secOps lab.support.files]$ openssl sha512 letter_to_grandma.txt  
SHA512(letter_to_grandma.txt)= 7c35db79a06aa30ae0f6de33f2322fd419560ee9af9cedeb6e251f2f1c4e99e0bbe5d2fc32ce501468891150e3be7e288e3e568450812980c9f8288e3103a1d3
```

Hashing the .txt file again using a bit length of 512 (rather than the previous 256)

```
[analyst@secOps lab.support.files]$ sha256sum letter_to_grandma.txt  
43302c4500b7c4b8e574ba27a59d83267812493c029fd054c9242f3ac73100bc letter_to_gran  
dma.txt
```

```
[analyst@secOps lab.support.files]$ sha512sum letter_to_grandma.txt  
7c35db79a06aa30ae0f6de33f2322fd419560ee9af9cedeb6e251f2f1c4e99e0bbe5d2fc32ce5014  
68891150e3be7e288e3e568450812980c9f8288e3103a1d3 letter_to_grandma.txt
```

Generating the hash of both bit lengths using the **sum** appendix to the **shaXXX** command

The hashes are the same as shown in the previous screenshots as the same hash bit-length has been specified as before (per each bit length)

Part 2

```
[analyst@secOps lab.support.files]$ cat sample.img_SHA256.sig  
c56c4724c26eb0157963c0d62b76422116be31804a39c82fd44ddf0ca5013e6a
```

Using the **cat** command to display the contents of the **.sig** file

```
[analyst@secOps lab.support.files]$ sha256sum sample.img  
c56c4724c26eb0157963c0d62b76422116be31804a39c82fd44ddf0ca5013e6a sample.img
```

Calculating the hash of the **.img** file

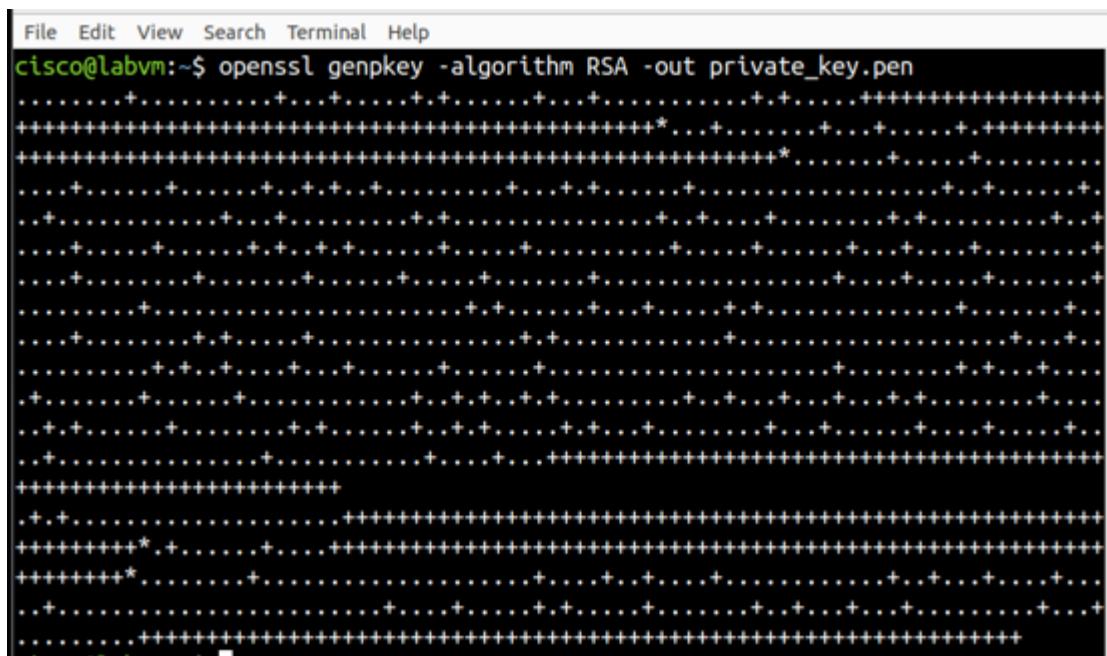
The image was downloaded without errors as the has value of the **.img** is the same as the **.sig** file, resulting in a match

18.5.5 Lab - Generate and Use a Digital Signature

Part 1

Opening the lab VM

Part 2



The screenshot shows a terminal window with a black background and white text. At the top, there is a menu bar with options: File, Edit, View, Search, Terminal, and Help. Below the menu, the command `openssl genkey -algorithm RSA -out private_key.pen` is entered. The output consists of a large amount of asterisks ('*') and plus signs ('+') arranged in a grid pattern, which is standard for OpenSSL's key generation progress indicator.

Generating a private key using the **openssl genkey** command alongside the **RSA** algorithm and outputting it into a **private_key.pen** file

```
cisco@labvm:~$ cat private_key.pen
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDMZAJM5YVR3cka
XFkRWM6UTOKMzp8tWdwBiU/AkHwpfJgjDBTwpn+IQtm2XpfSt/Zn2OC6yVKu6y8P
TuAqdLrDfAT5YGD9wXRKumWQDf1dpBoH2FW2zs5pmF4JIRpccYhmJZIuHlGDVuqS
DXP6uxNSkXjAZIuHpoAYWlKLukUNwVLKC/LNI6tERFkhaDCfaf6M7hL1YANZFkbV
7wb4NrKPUc8uYB16WwLNPWC2WfIg/bJ6HurrsaNdWUsuerIRU4ljqVCQw9M5wU+
Qb5CH5KhJNV8WbodTCvYoVE69YmpW/ScbGkKoBcoE5rVnx+pt8Yxzl1PSAkUS0tZ
9Qz/HgfdAgMBAECggEAYQHteZ7CDR4HscQ83dfZjFeFezEiKYMpwwZrdkjdnU+W
YaP9WE6d3w1jiYQR6Qg5Iga0etLMtIqZNlnIWT79SyTUu4uD3UxxJnqbc6jAJ56a
0DhkTjSPkVyo3QpiGZglFd4lKFBStaSOBq3t6wXZYOn8dsWB0Ws8BtLY7JqG5cS0
XtN5aLs8LtbizX0NeTwe0NgDK3HkApvVMcvyqHll/0lcXqMJi69wDZq6t9/VsYSl
Z3+3NiSnhiryfEUrgvm9t0CHSVqnE/JBbfYauXfB0Ej1d55oGJrlFQ49IxL9Aeq
8BRAAYixixyRqKVzDngaLZBwsGL0veyh1brylOU+vQKBgQDNRV5aGbtwHQgg6Q1l
5mLuERkYDWsFjJn4bmR51o+wWrZqUf0RBrP1E7aemDThTDQpxLiOoEhbAxA4a5WM
/D7g2kf5LXTBpFG9CA5ryL3uAlmctm9waP4+DyWcPLmGWZNsC+gia5mhbUrvRS+R
R14Dol1ypKurqdaJQ9sH0J2yYwKBgQD+5v6AtMB09j2H+c5xW2Vl/Mix0+E15EFy
EaQ+AMGZbjj+XLVqNEFyD+oNtloLy+akG1eGFga/M7HM/HfUnXCuYvqXRK1c2tFE
0WLmvWSwWGt1r0V5bJHY0/d+s1AdeyBqaUPwladNQ23C63HEWad2z/oLDYZ87nLi
NskXGZ1QvwKBgQC9YA8TNFY2srIDGr8fmZL/q4qJJcfuMK8EAWR0+zvxLLNKF2Xv
xU1U9uDjI+H1UMZ3GmRiQQE/5e2a/7YzIawo6Xipi/bxh1VZngsf6U1APC8Bo1Xg
URztyC+cmmFwv2FAtyNsTfSodxpA8IVRfmXR2IN59u3iK4gfjxiNdytlnQKBgQDx
nbF1/F853tbaUg6+YnzN3Hu7i9/gvnj0kCxX3U2li4wXR3dqsRer76vSzZuy/Nal
jYk7/xrsGCsb+9/20D08AnQ3+Ix1CLE+gyVF6WxMv7M0fSvkeeYQyl7ByWRSXYtP
dTJCFQjdculHS1mwjSzwyodchUh29xCQ/iuC3tb7pbwKBgGvzqquFdQPT61cpVXh4
/P2ArZa/BePfkwE0UsAZNmD0a2JfDEg2r9holm2rrRqta5igkALAtU7FpAod1tm0
X8Ta9maR+G0qocfQG6XhGRk1P2HNTRYtA2om93qILIunm1CwHcQXATivdBUBj2Y
qhWUy4G2nLsVLq3NRZ/KBge9
-----END PRIVATE KEY-----
```

Using the **cat** command to show the contents of the **.pen** file

Part 3

```
cisco@labvm:~$ openssl pkey -in private_key.pen -pubout -out public_key.pen
cisco@labvm:~$ cat public_key.pen
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzGQCTOWFd3JGlxZEVj0
lEzijM6fLVncAYlPwJB8KXyYIwwU8KZ/iELZtl6X0rf2Z9jguslSrusvD07gKnZa
w3wE+WBg/cF0SrplkA39XaQaB9hVts70aZheCSEaXHGIZiWSLh4hg1bqkg1z+r5T
UpF4wGSLh6aAGFoi7pFDcFSygvyzS0rRERZIWgwn2n+j04S9WADWRZG1e8G+Day
j1HPLmAdelsJCzT1gtln4hv2yeh7q67GjXVLLnqyEVOJY0FQkMPT0cFPkG+Qh+S
oSTVfFm6HUwr2KFR0vWJqVv0nGxpCqAXKB0a1Z8fqbfGMc5dT0gJFEtLWFUM/x4H
3QIDAQAB
-----END PUBLIC KEY-----
```

Generating a public key using the **openssl pkey** command, by using the **private_key.pen** file as the input and outputting a new file called **public_key.pen**

This new file is then executed with the **cat** command

Part 4

```
cisco@labvm:~$ echo Please trasfer 2,000,00 US dollars to Mr. Jester by 6pm today! > contract.txt
cisco@labvm:~$ cat contract.txt
Please trasfer 2,000,00 US dollars to Mr. Jester by 6pm today!
```

Creating a new **.txt** file and using the **cat** command to check its contents

Part 5

```
cisco@labvm:~$ openssl dgst -sha256 -sign private_key.pen -out signature contract.txt
```

Creating a signature for the previously created **.txt** file

```
cisco@labvm:~$ cat signature
&k++++Ai@{++I++}++el+A
          X++
++L+ZG=+<X!+)++++ ++
++o0++++X++++W+      d+5+_,++lo+
++{+YR++++Z)+8B+i++++>;+x++p+S++eq 2+eey+yJKV+9+S+âT++++P>q+0++ZrM+$/+23Dqf+D+o
7+G++%f+J+)+"y++&+0"++6&|+|++++d++cisco@labvm:~$
```

Checking the contents of the signature file using the **cat** command

Part 6

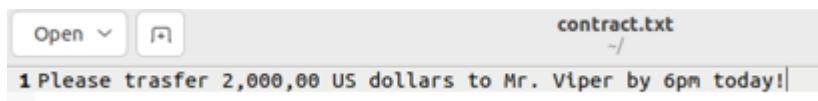
```
cisco@labvm:~$ openssl dgst -sha256 -verify public_key.pem -signature signature  
contract.txt  
Verified OK
```

Checking if the file has not been tampered using the **openssl dgst** command, returning a positive validation

Part 7



Opening the **.txt** file using the command **gedit**



Changing the contents of the file

Part 8

```
cisco@labvm:~$ gedit contract.txt  
cisco@labvm:~$ openssl dgst -sha256 -verify public_key.pem -signature signature  
contract.txt  
Verification failure
```

Rechecking the validity of the file using the **openssl dgst** command, and this time it returns with a verification failure

Module 19: Technologies and Protocols (ACL)

Please complete the **two** multiple choice quizzes available under **19.1 Monitoring Common Protocols** and **19.2 Security Technologies** and provide a screenshot of your completed experience/defender points shield, e.g.:



19.1.7 Check Your Understanding - Identify the Monitored Protocol

X



19.1. Monitoring Common Protocols

Carry Payloads	+12 defender points
Decoding Captures	+12 defender points
Exfiltrate Data	+12 defender points
Event Correlation	+12 defender points

19.2.6 Check Your Understanding - Identify the Impact of the Technology on Security and Monitoring

X



19.2. Security Technologies

Spreads Infected Files	+12 defender points
Spoofed IP Addresses	+12 defender points
Attachments Unreadable	+12 defender points
Hides Identity	+12 defender points

Reflective Report (cryptography and access control)

Through completing these allocated labs and content that has been made available on the Cisco website, it has helped strengthen my understanding on different security measures that are available to secure devices, and methods that are potentially used in businesses, such as setting up user accounts or limiting access to specific users.

More specifically the usage of Linux and hashing inside of the terminal was one of my key learning points as one of the tasks to complete was verifying a download. This was done by checking the hash value of the downloaded file and comparing it to the **.sig** file (signature) hash value – if the hash output was the same then the download was successful, if not then it failed. Another key task that was completed was changing privileges of files and which user / groups can access it, which is displayed by “**-r—r—r—**” which would give the owner reading privileges, owner groups reading privileges and other users reading privileges – for a file, if it was a directory then it would start with “**d**” instead of “**-**“