Exercise 5: Performing Password Exploitation and Lateral Movement

In this exercise, you will exploit insecure passwords to move laterally across the target network.

Perform Password Exploitation

You will review a couple of dictionary files, and then use one of them to attempt a dictionary-based brute force attack against the Windows-Client VM.

To review the password lists

1. Return to the Kali Linux VM.
2. If the RDP session has ended, on the bastion host desktop, double-click the **Kali Linux** RDP shortcut, and then log in with the following credentials:

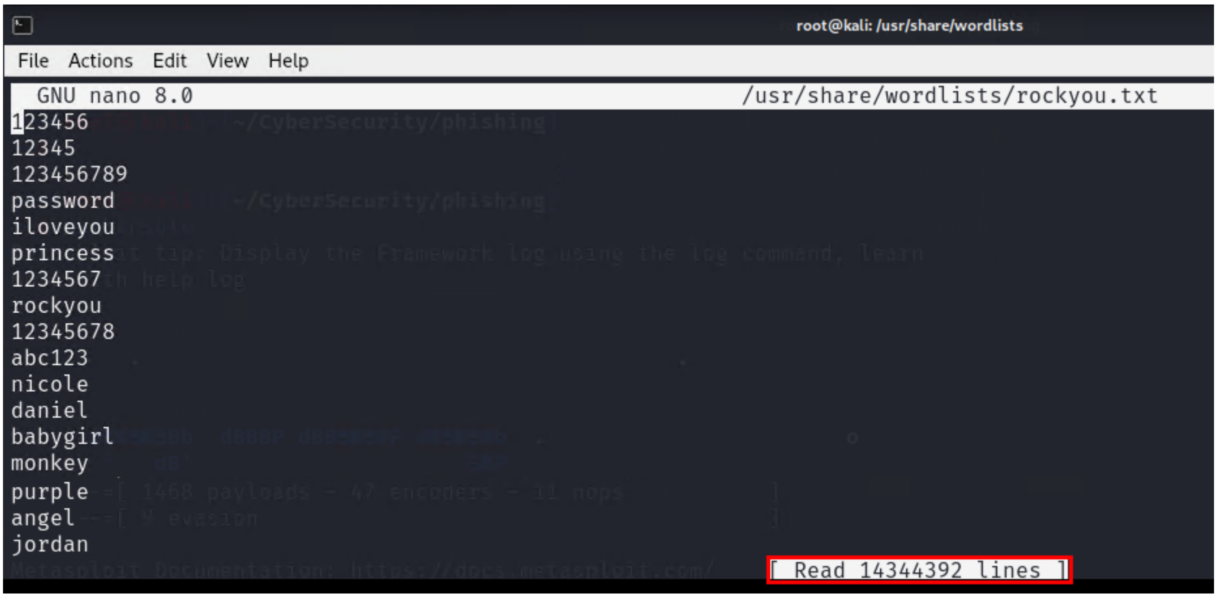
- Username: root
- Password: Passw0rd

3. Open a new terminal session.

Do not use or close the active Meterpreter session from the previous exercise. You will use it later in this exercise.

4. Enter the following command to view a dictionary file:

```
nano /usr/share/wordlists/rockyou.txt
```



```
  GNU nano 8.0                                     /usr/share/wordlists/rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
purple
angel
jordan
                                                   [ Read 14344392 lines ]
```

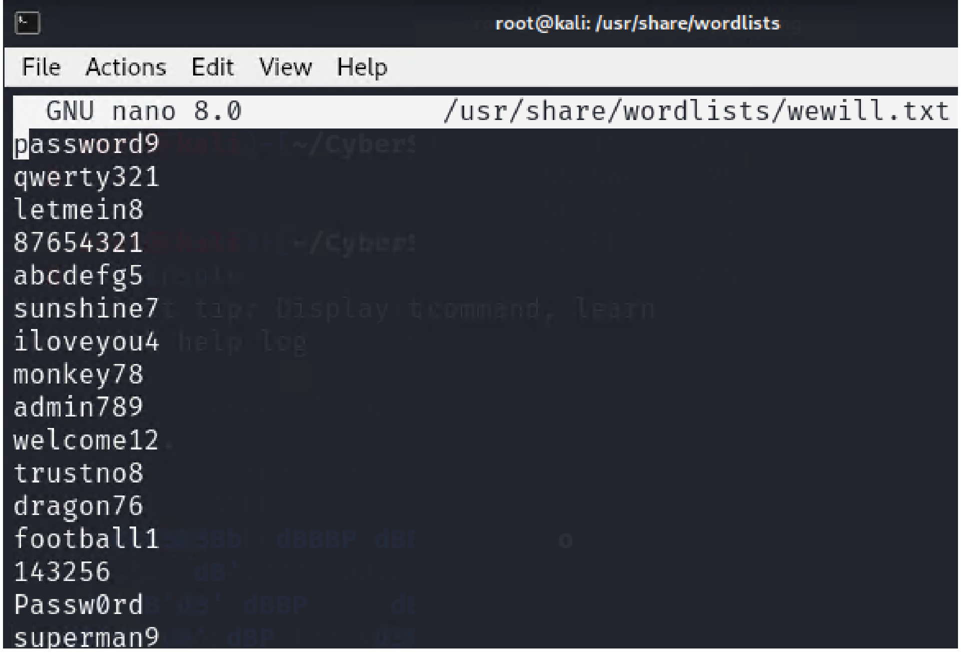
It may take a minute for it to load. The file contains over a million entries of some of the most commonly used or leaked passwords.

5. Press Ctrl+X, and then press Enter to exit the text file.

If you are prompted to save the file, type N, and then press Enter.

6. Enter the following command to view a smaller dictionary file:

```
nano /usr/share/wordlists/wewill.txt
```



```
  GNU nano 8.0              /usr/share/wordlists/wewill.txt
password9
qwerty321
letmein8
87654321
abcdefg5
sunshine7
iloveyou4
monkey78
admin789
welcome12
trustno8
dragon76
football1
143256
Passw0rd
superman9
```

7. Press Ctrl+X, and then press Enter to exit the text file.

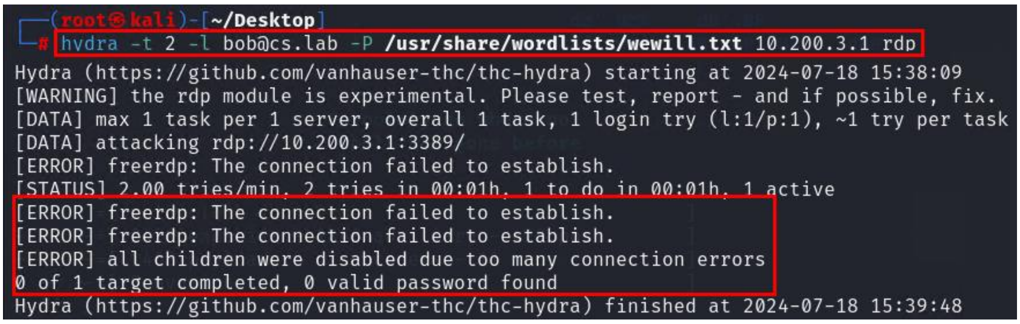
If you are prompted to save the file, type N, and then press Enter.

You will use a smaller dictionary file for password exploitation due to time constraints.

In this exercise, the user's password is extremely insecure. In a real-world environment, the password will probably be much more secure. As such, to give the exploitation a higher chance of success, the attacker may tailor the password file with strings that match the user's personal information (such as combining Bob with other characters), or see if the user's email address has been part of any data breaches.

8. Enter the following command to attempt to brute force the password against the Windows Server VM:

```
hydra -t 2 -l bob@cs.lab -P /usr/share/wordlists/wewill.txt 10.200.3.1 rdp
```



```
┌──(root㉿kali)-[~/Desktop]
└─# hydra -t 2 -l bob@cs.lab -P /usr/share/wordlists/wewill.txt 10.200.3.1 rdp
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-18 15:38:09
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://10.200.3.1:3389/
[ERROR] freerdp: The connection failed to establish.
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-18 15:39:48
```

This command should fail after a few minutes. The Kali Linux VM RDP attempts are blocked by the edge FortiGate.

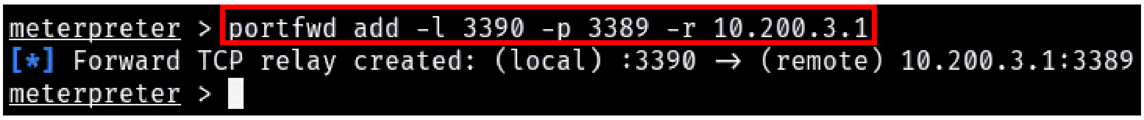
9. Leave this terminal session open.

Instead of using the Kali Linux VM to connect to the Windows server domain controller over RDP, you will establish port forwarding in Meterpreter to forward the local RDP requests through the compromised host.

To port forward RDP traffic

1. Return to your active Meterpreter session.
2. At the Meterpreter prompt, enter the following command to establish port forwarding:

```
portfwd add -l 3390 -p 3389 -r 10.200.3.1
```

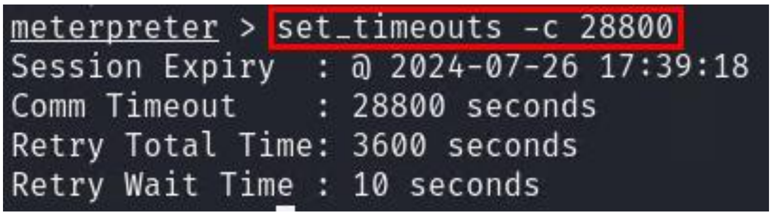


```
meterpreter > portfwd add -l 3390 -p 3389 -r 10.200.3.1
[*] Forward TCP relay created: (local) :3390 → (remote) 10.200.3.1:3389
meterpreter > 
```

This command configures the Kali Linux VM to listen for port 3390 traffic on its loopback IP address and forward the request to 10.200.3.1:3389.

3. To make the session more stable, enter the following command:

set_timeouts -c 28800



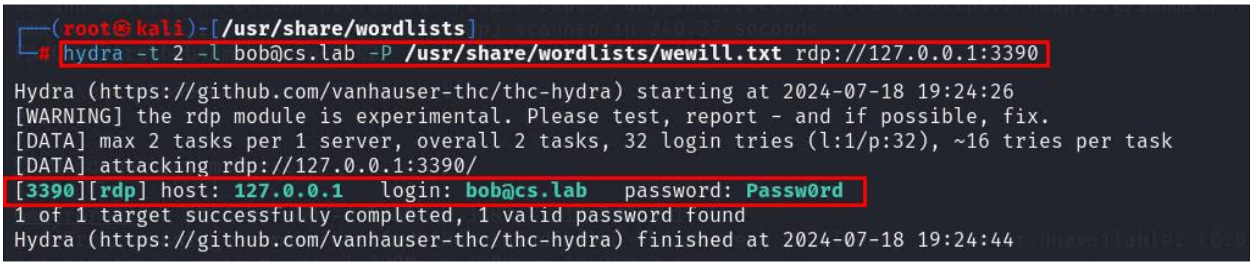
```
meterpreter > set_timeouts -c 28800
Session Expiry  : @ 2024-07-26 17:39:18
Comm Timeout    : 28800 seconds
Retry Total Time: 3600 seconds
Retry Wait Time : 10 seconds
```

If this session ends or if you change to a different session, you must set up the port forward again in the new session.

Also, if you close the active Meterpreter window, you must restart the handler. For more information, see To configure the listener on page 1.

4. Return to the other terminal session, and then enter the following command:

hydra -t 2 -l bob@cs.lab -P /usr/share/wordlists/wewill.txt rdp://127.0.0.1:3390



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -t 2 -l bob@cs.lab -P /usr/share/wordlists/wewill.txt rdp://127.0.0.1:3390

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-18 19:24:26
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 2 tasks per 1 server, overall 2 tasks, 32 login tries (l:1/p:32), ~16 tries per task
[DATA] attacking rdp://127.0.0.1:3390/
[3390][rdp] host: 127.0.0.1   login: bob@cs.lab   password: Passw0rd
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-18 19:24:44
```

You have found a credential match for bob@cs.lab with Passw0rd.

If your dictionary attack fails, make sure that you entered the command correctly. If the attack still fails, perform the following steps to restart the active session and reestablish port forwarding:

1. At the meterpreter prompt, enter exit.

This terminates the active session and returns to the msfconsole.

1. Do *not* disconnect from the msfconsole.

A new session initiates automatically because of persistence.

1. Enter sessions -i <ID #> to log in to the new session.
2. Enter the following command:

portfwd add -l 3390 -p 3389 -r 10.200.3.1

1. Enter the following command:

set_timeouts -c 28800

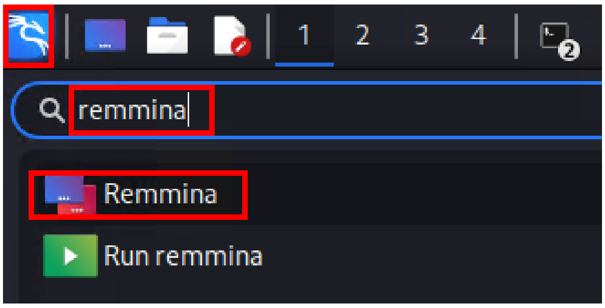
1. Try the dictionary attack again.

Move Laterally Across the Network

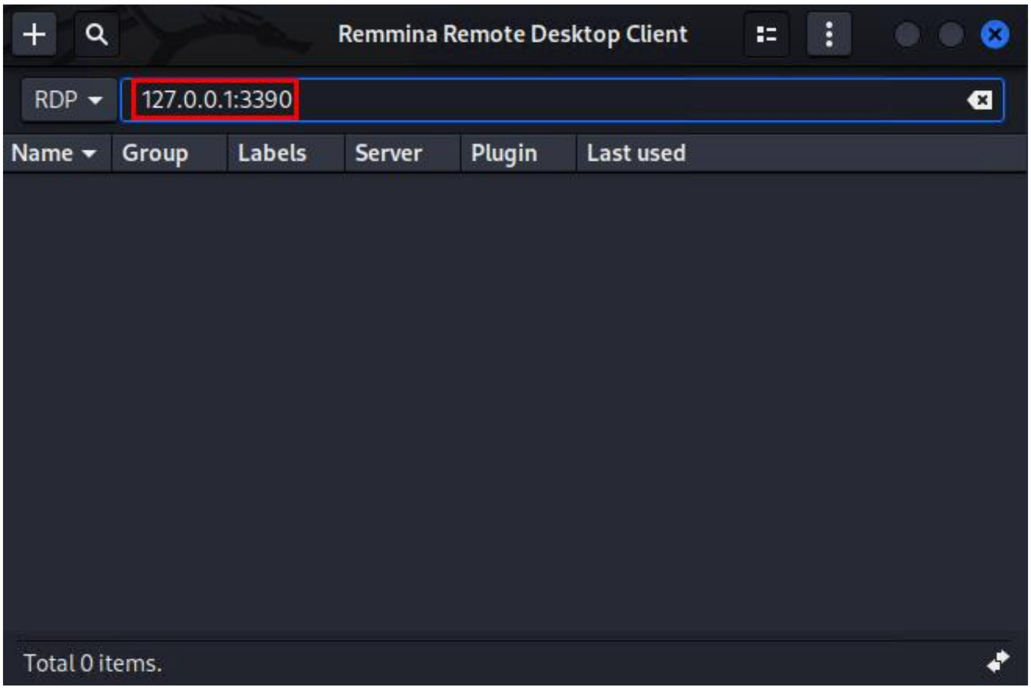
Now that you have discovered Bob's insecure password, you will use his Active Directory credentials to move laterally on the network.

To connect over RDP to the domain controller and test access

1. On the Kali Linux VM, click the start menu icon.
2. Search for Remmina.

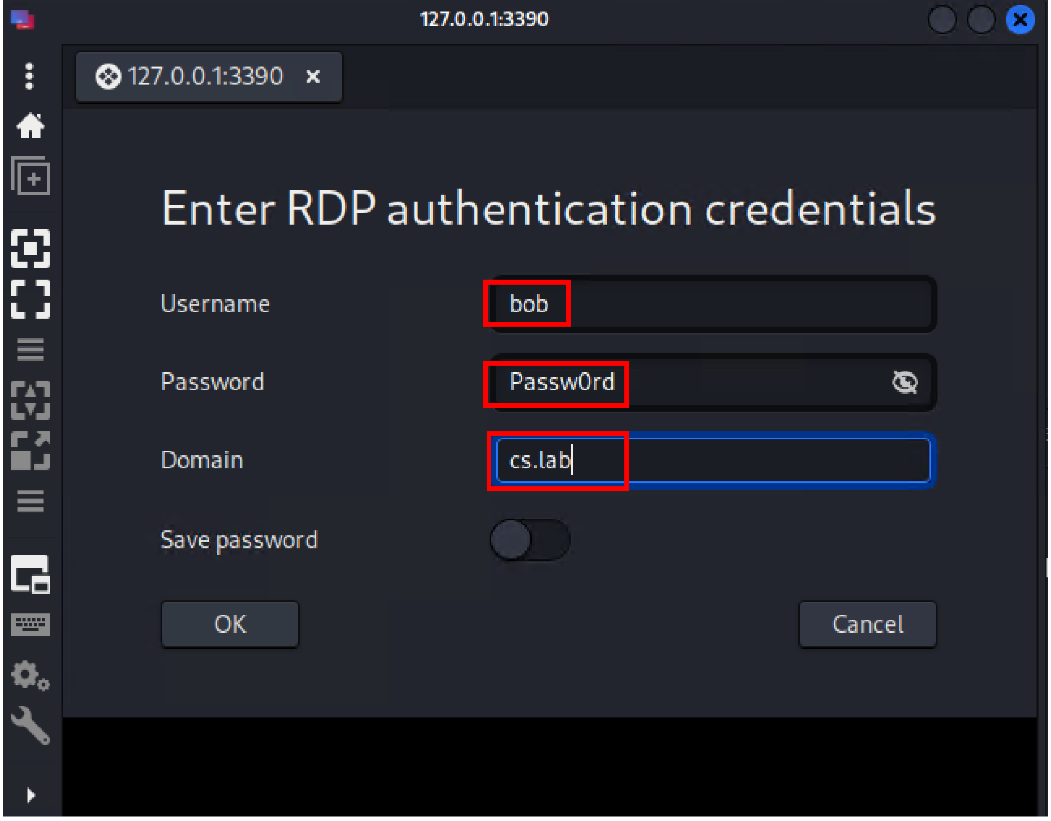


3. Click the **Remmina** icon to start the program.
4. In the search field beside **RDP**, type 127.0.0.1:3390.



5. Press Enter.
6. Enter the following information:

Field	Value
Username	bob
Password	Passw0rd
Domain	cs.lab



127.0.0.1:3390

Enter RDP authentication credentials

Username: bob

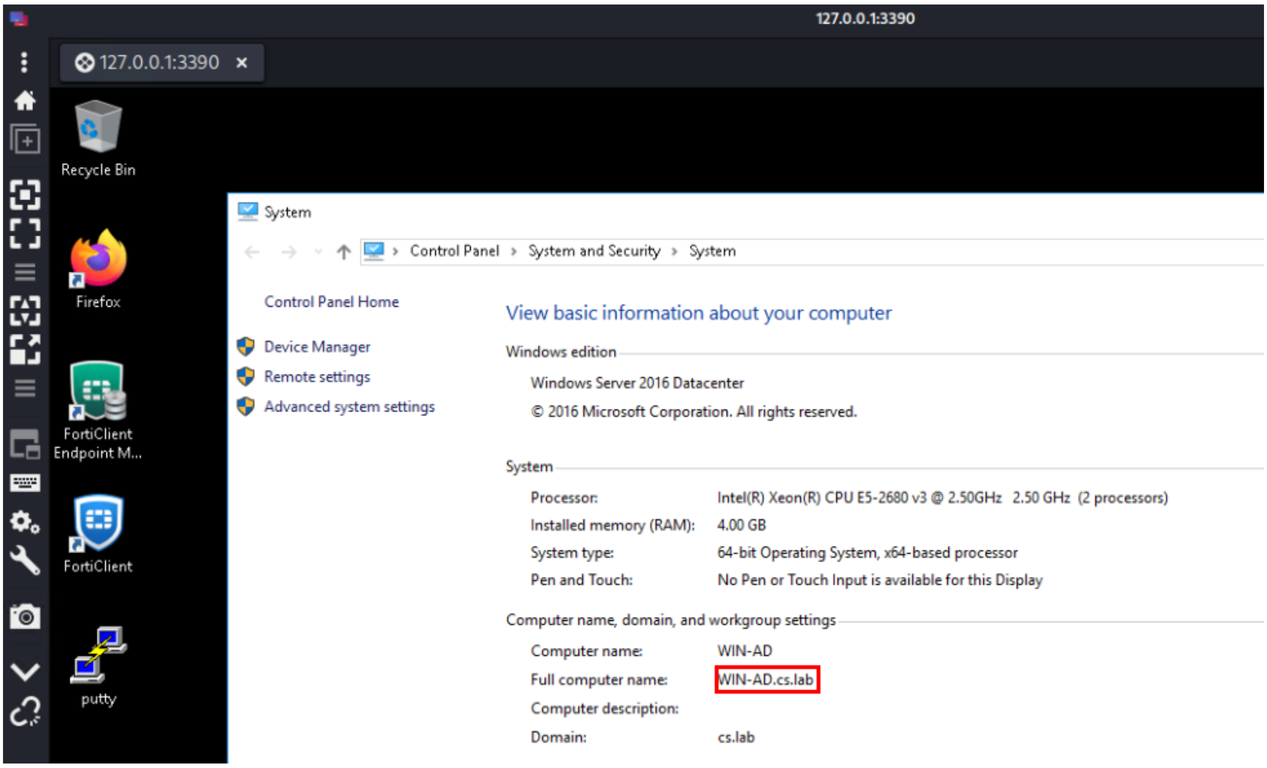
Password: Passw0rd

Domain: cs.lab

Save password

7. Click **OK**.
8. Accept the certificate warning.

The RDP session to the domain controller establishes.



View basic information about your computer

Windows edition

Windows Server 2016 Datacenter

© 2016 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Xeon(R) CPU E5-2680 v3 @ 2.50GHz 2.50 GHz (2 processors)

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: WIN-AD

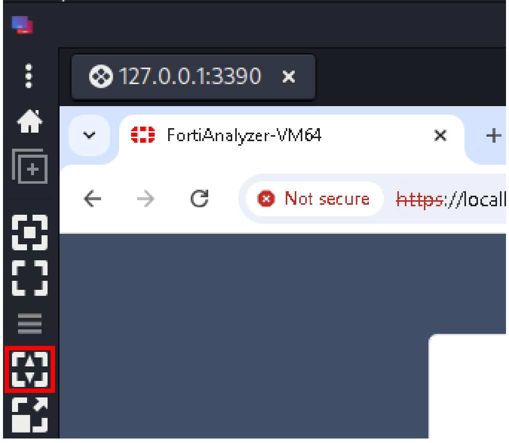
Full computer name: WIN-AD.cs.lab

Computer description:

Domain: cs.lab

If the RDP window is too small, you can drag the window to enlarge it, and then update the resolution by toggling the dynamic resolution update, as shown in the following image.

If you enter fullscreen mode and cannot exit this mode, hover near the top of the page to see the menu bar.



In the To perform reconnaissance on a remote subnet on page 1 procedure, you discovered the following five IP addresses on the DMZ network:

- 10.200.200.12
- 10.200.200.100
- 10.200.200.213
- 10.200.200.238
- 10.200.200.254

9. Open a command prompt, and then ping each of the IP addresses above.

The pings should work for all the hosts.

10. Open Chrome, and then connect using HTTPS to each of the IP addresses above.

Only 10.200.200.12 should respond with a web page.

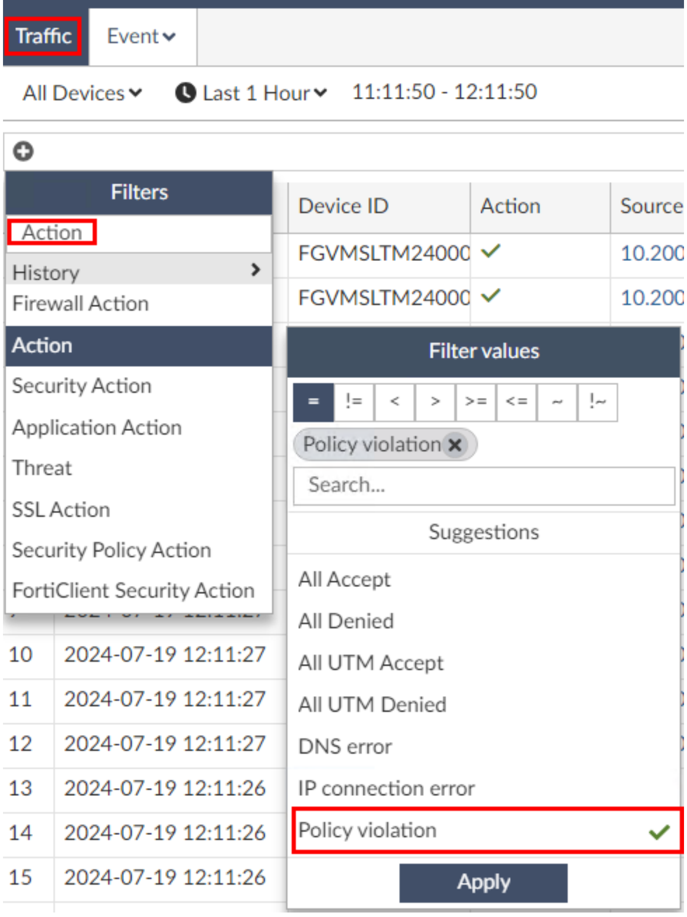
11. Open PuTTY, and then connect using SSH to each of the IP addresses above.

Only 10.200.200.12 should respond with a shell.

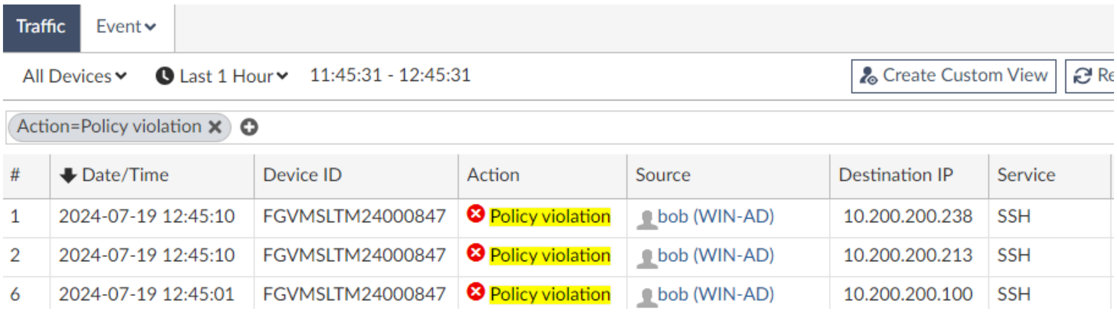
12. On the bastion host, return to the FAZ-SiteB GUI (10.200.4.238), and then log in with the following credentials:

- Username: admin
- Password: Fortinet1!

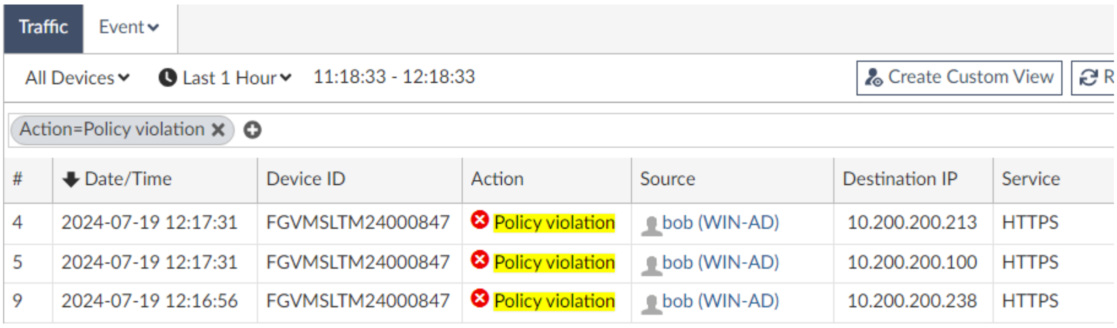
13. Click **Log View** > **FortiGate**.
14. In the filter field, click **+**.
15. If there are any existing filters, remove them.
16. Click **Action**, and then click **Policy violation**.
17. Ensure the **Traffic** log type is selected.



18. Click **Apply**.
19. Review the search results.



#	Date/Time	Device ID	Action	Source	Destination IP	Service
1	2024-07-19 12:45:10	FGVMSLTM24000847	Policy violation	bob (WIN-AD)	10.200.200.238	SSH
2	2024-07-19 12:45:10	FGVMSLTM24000847	Policy violation	bob (WIN-AD)	10.200.200.213	SSH
6	2024-07-19 12:45:01	FGVMSLTM24000847	Policy violation	bob (WIN-AD)	10.200.200.100	SSH



#	Date/Time	Device ID	Action	Source	Destination IP	Service
4	2024-07-19 12:17:31	FGVMSLTM24000847	Policy violation	bob (WIN-AD)	10.200.200.213	HTTPS
5	2024-07-19 12:17:31	FGVMSLTM24000847	Policy violation	bob (WIN-AD)	10.200.200.100	HTTPS
9	2024-07-19 12:16:56	FGVMSLTM24000847	Policy violation	bob (WIN-AD)	10.200.200.238	HTTPS

You have confirmed that a firewall policy has blocked your connection attempts.

Note that the images above are edited and taken from two separate searches. You may see slightly different results. You will not see results for 10.200.200.254, which is a FortiGate. From the perspective of the firewall, the denied attempts are considered local traffic, and are not listed in the **Traffic** logs.

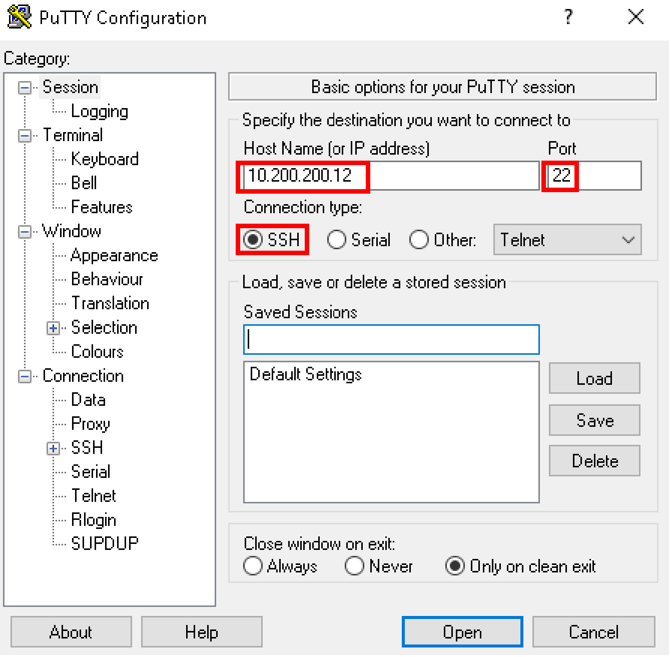
To bypass the firewall rule

1. Return to the **Windows Server** Remmina RDP session on the Kali Linux VM.

Ensure 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 procedure.

2. On the desktop, double-click the PuTTY shortcut.
3. Click **Session**, and then configure the following settings:

Field	Value
Host Name (or IP address)	10.200.200.12
Port	22
Connection type	SSH



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.200.200.12

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

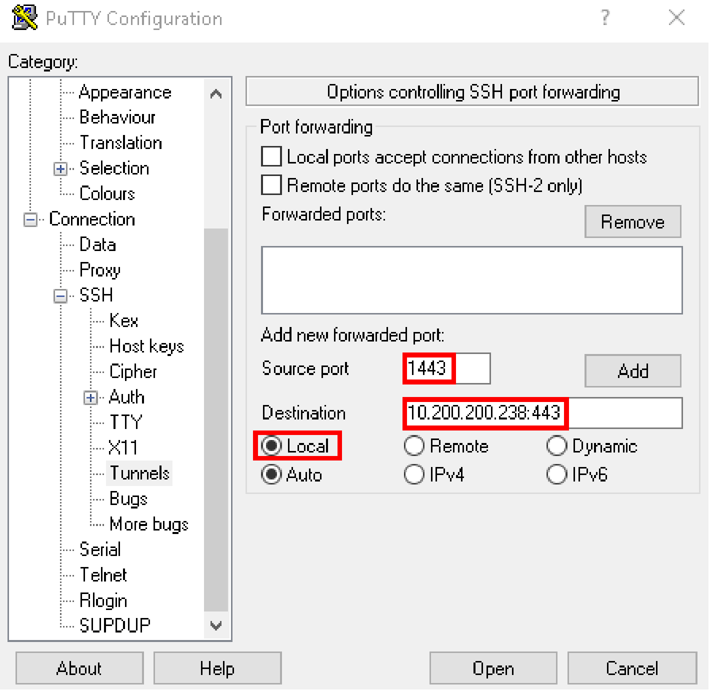
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

4. Navigate to **Connection** > **SSH** > **Tunnels**.
5. Configure the following settings:

Field	Value
Source port	1443
Destination	10.200.200.238:443
Local/Remote/Dynamic	Local



PuTTY Configuration

Options controlling SSH port forwarding

Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

Add new forwarded port:

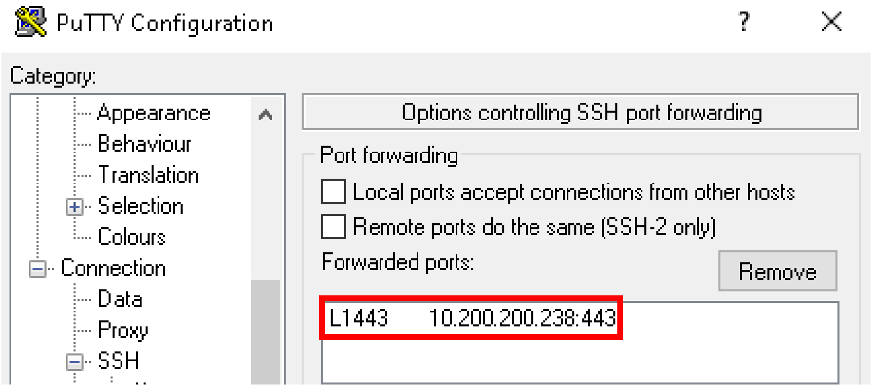
Source port: 1443

Destination: 10.200.200.238:443

● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

6. Click **Add**.
7. Confirm that you can see the SSH tunnel configuration.



Port forwarding

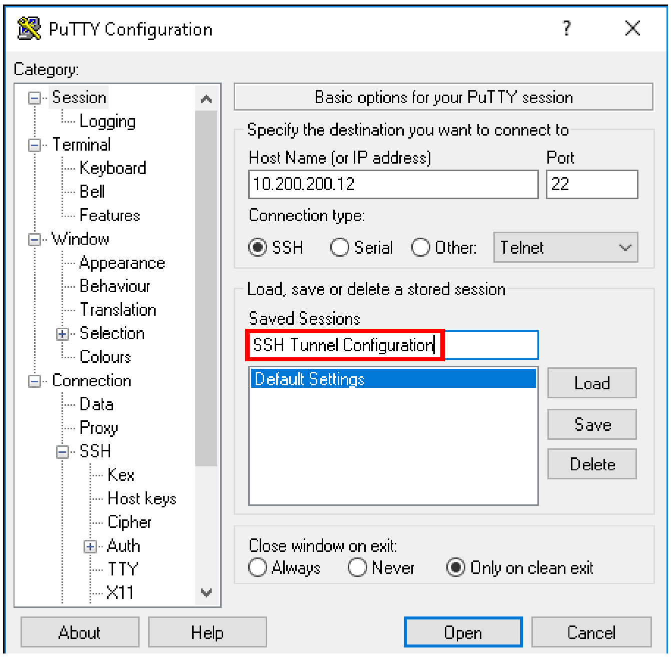
☐ Local ports accept connections from other hosts

☐ Remote ports do the same (SSH-2 only)

Forwarded ports:

L1443 10.200.200.238:443

8. In the **Category** field, click **Session** again.
9. In the **Saved Sessions** field, type SSH Tunnel Configuration.



Specify the destination you want to connect to

Host Name (or IP address): 10.200.200.12

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: SSH Tunnel Configuration

Default Settings

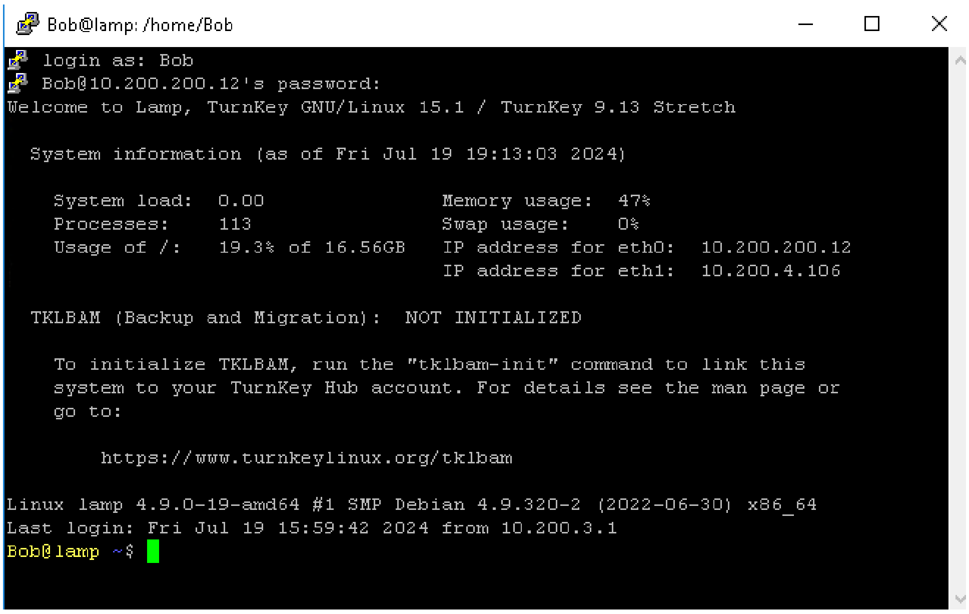
Close window on exit: ○ Always ○ Never ● Only on clean exit

10. Click **Save**.
11. Select the **SSH Tunnel Configuration** saved session, and then click **Open**.
12. Log in using the following case-sensitive credentials:

- Username: bob
- Password: Passw0rd

You may have noticed that you did not use password exploitation to confirm the user credentials for the SSH connection to the web server. Due to time constraints, assume that the attacker would try the same working user and password combination on every responding device.

13. You successfully logged in to the web server.

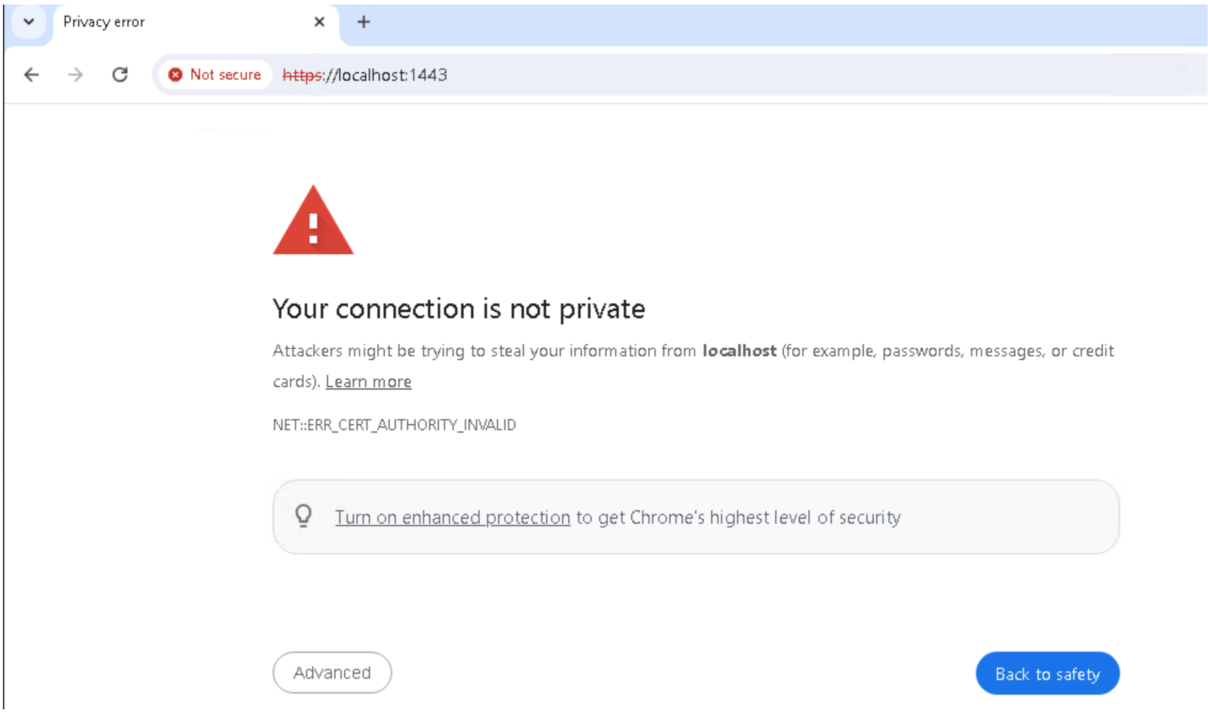


```
login as: Bob
Bob@10.200.200.12's password:
Welcome to Lamp, TurnKey GNU/Linux 15.1 / TurnKey 9.13 Stretch

  System information (as of Fri Jul 19 19:13:03 2024)

    System load:  0.00              Memory usage:  47%
    Processes:    113               Swap usage:    0%
    Usage of /:   19.3% of 16.56GB  IP address for eth0:  10.200.200.12
                                    IP address for eth1:  10.200.4.106

  TKLBAM (Backup and Migration):  NOT INITIALIZED

    To initialize TKLBAM, run the "tklbam-init" command to link this
    system to your TurnKey Hub account. For details see the man page or
    go to:

        https://www.turnkeylinux.org/tklbam

Linux lamp 4.9.0-19-amd64 #1 SMP Debian 4.9.320-2 (2022-06-30) x86_64
Last login: Fri Jul 19 15:59:42 2024 from 10.200.3.1
Bob@lamp ~$
```

14. On the Windows Server desktop, open a Chrome tab.
15. Enter the following URL:

https://localhost:1443

You should see a **Your connection is not private** warning.



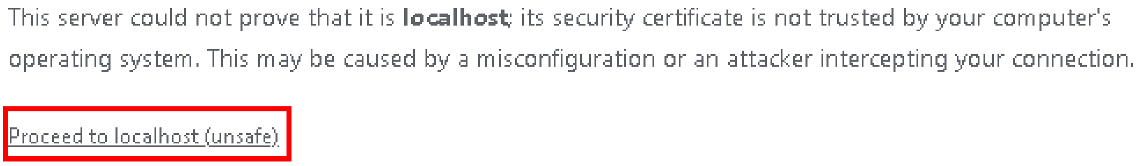
Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

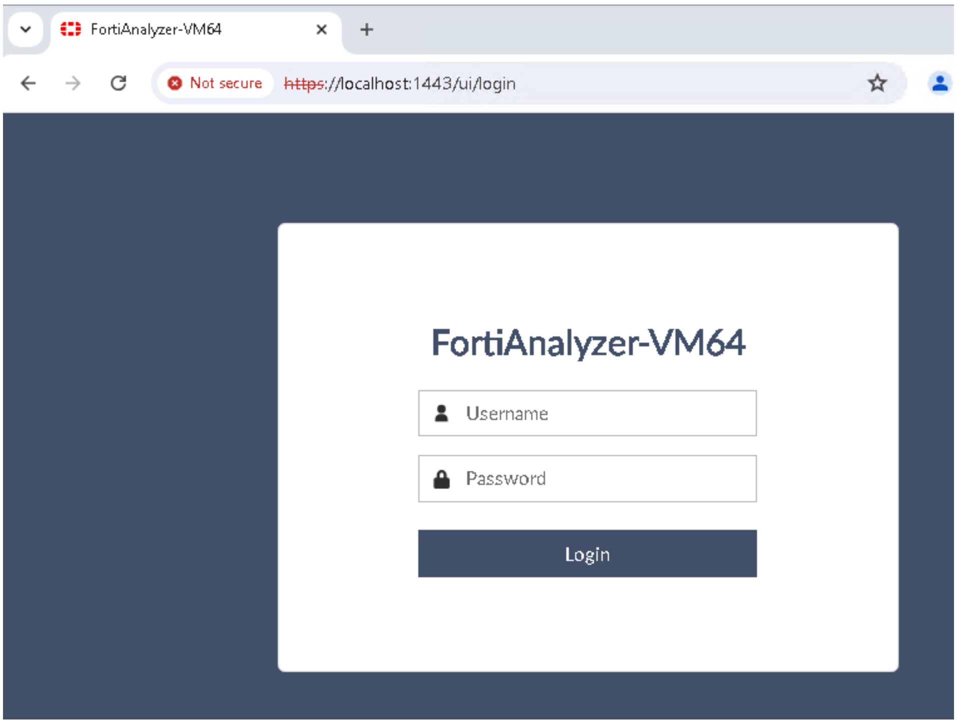
16. Click **Advanced**.
17. Click **Proceed to localhost (unsafe)**.



This server could not prove that it is **localhost**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to localhost (unsafe)

18. You should see the FortiAnalyzer GUI.



19. Close the PuTTY session, and then attempt to reload the FortiAnalyzer page.

It should fail to load.

You have successfully used SSH tunneling to bypass a firewall rule.

You should be aware that not all devices allow SSH tunneling, which is also known as SSH TCP forwarding. Some devices also allow you to disable the function even though they support it. As you can see from this exercise, it can be considered a security risk to have it enabled on your network.

In addition, note that not all devices in the DMZ are configured to respond on SSH or HTTPS. It is important to remember to only enable remote access on interfaces where you are expecting administrators to access the device.

For example, in this topology, administrators are not expected to access the FortiGate on 10.200.200.254. Therefore, disabling that service is a security best practice.

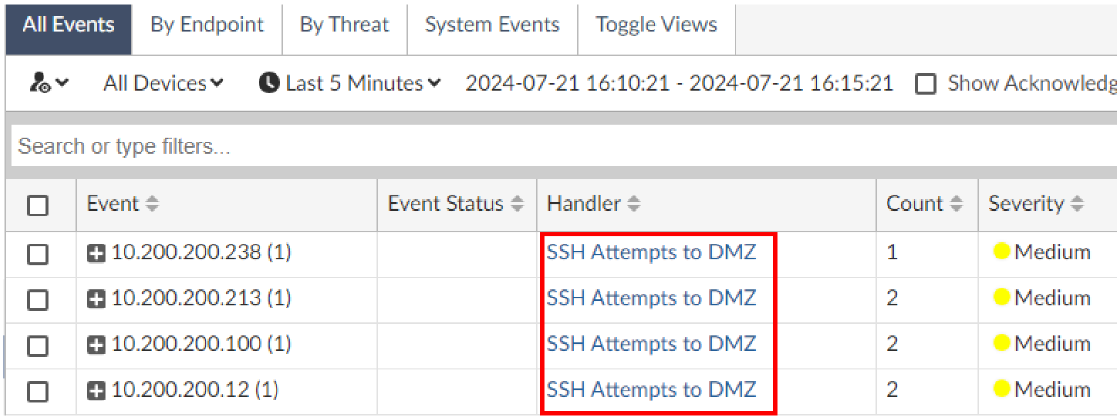
This exercise also involves only two networks (LAN and DMZ). In a real-world scenario, you can have a case where access from LAN to DMZ is blocked, but attackers can exploit a *hop* in between, such as an IT network, to move laterally.

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: Fortinet1!

2. Click **Incidents & Events** > **Event Monitor**.
3. Click **All Events**.
4. Adjust the time range to include when you tried to log in to the DMZ servers using SSH.



2024-07-21 16:10:21 - 2024-07-21 16:15:21

□	Event	Event Status	Handler	Count	Severity
□	⊞ 10.200.200.238 (1)		SSH Attempts to DMZ	1	● Medium
□	⊞ 10.200.200.213 (1)		SSH Attempts to DMZ	2	● Medium
□	⊞ 10.200.200.100 (1)		SSH Attempts to DMZ	2	● Medium
□	⊞ 10.200.200.12 (1)		SSH Attempts to DMZ	2	● Medium

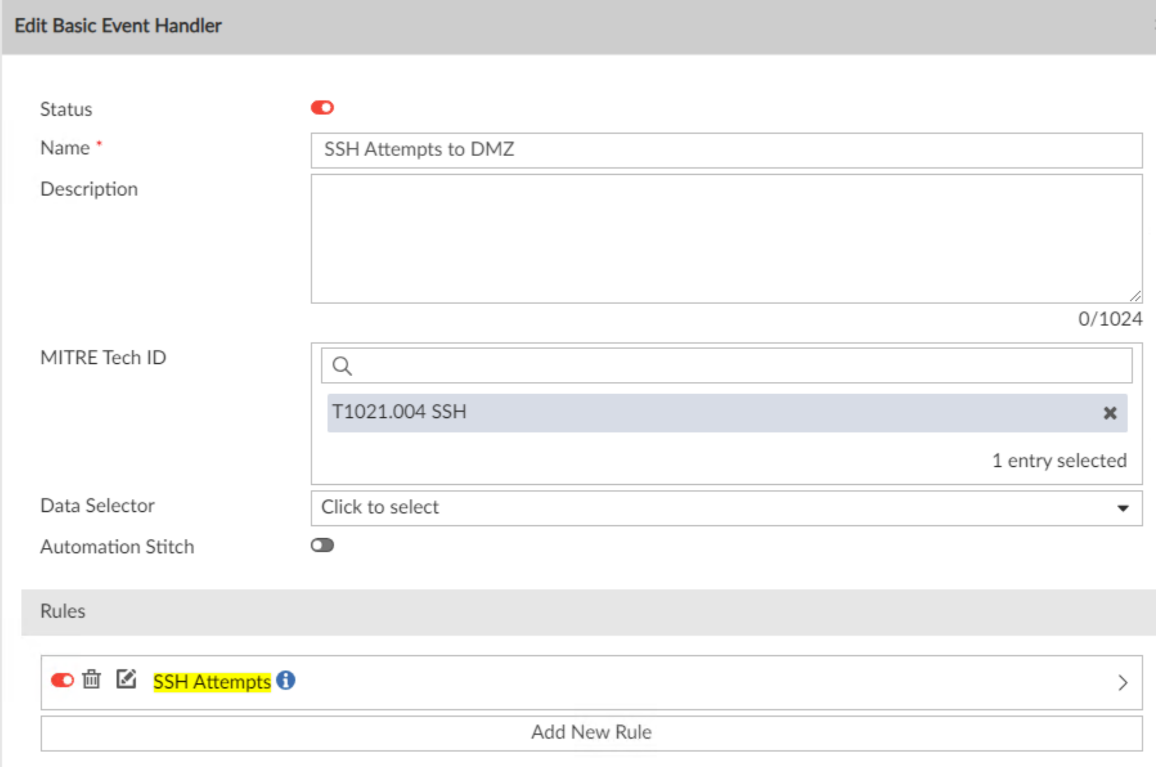
Stop and think!

Why are the attempts that FortiGate blocked shown as events on FortiAnalyzer?

On FortiAnalyzer, the configured event handler is matching results on a network level. It will try to find a match in the destination IP address and destination port.

From a security perspective, you may want to see all attempts to connect remotely to sensitive servers, and not filter by success and failures.

5. In any of the results, click the **SSH Attempts to DMZ** event handler.
6. Review the basic event handler configuration, including the MITRE information.



Edit Basic Event Handler

Status ●

Name * SSH Attempts to DMZ

Description

0/1024

MITRE Tech ID T1021.004 SSH ✖

1 entry selected

Data Selector Click to select

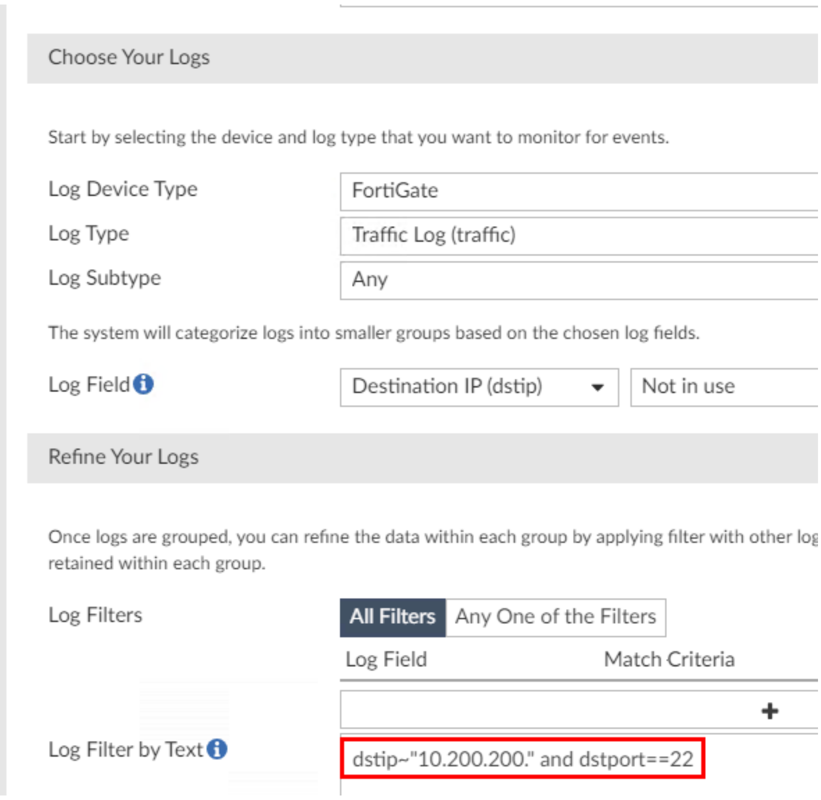
Automation Stitch ○

Rules

SSH Attempts

Add New Rule

7. Click the ✎ icon to view the matching rule.



Choose Your Logs

Start by selecting the device and log type that you want to monitor for events.

Log Device Type FortiGate

Log Type Traffic Log (traffic)

Log Subtype Any

The system will categorize logs into smaller groups based on the chosen log fields.

Log Field Destination IP (dstip) Not in use

Refine Your Logs

Once logs are grouped, you can refine the data within each group by applying filter with other log
retained within each group.

Log Filters All Filters Any One of the Filters

Log Field Match Criteria

Log Filter by Text dstip~"10.200.200." and dstport==22