Exercise 4: Performing Active Reconnaissance

In this exercise, you will use various tools to perform active reconnaissance on the target's infrastructure. Even though you have been given a topology diagram of the lab environment, you will learn useful commands and processes by performing active reconnaissance.

Perform Active Reconnaissance

You will upload Nmap, a network scanning tool, to the Windows-Client VM in preparation for performing active reconnaissance on the target network. Then, you will gather information about the network to find potential weaknesses that you can exploit.

To upload Nmap to the compromised host

1. At the Meterpreter prompt, enter the following command:

upload /root/Desktop/nmap.zip C:\\Users\\Bob\\nmap.zip

```
meterpreter > upload /root/Desktop/nmap.zip C:\\Users\\Bob\\nmap.zip
[*] Uploading  : /root/Desktop/nmap.zip → C:\Users\Bob\nmap.zip
[*] Uploaded 8.00 MiB of 21.83 MiB (36.64%): /root/Desktop/nmap.zip → C:\Users\Bob\nmap.zip
[*] Uploaded 16.00 MiB of 21.83 MiB (73.29%): /root/Desktop/nmap.zip → C:\Users\Bob\nmap.zip
[*] Uploaded 21.83 MiB of 21.83 MiB (100.0%): /root/Desktop/nmap.zip → C:\Users\Bob\nmap.zip
[*] Completed  : /root/Desktop/nmap.zip → C:\Users\Bob\nmap.zip
meterpreter >
```

2. Wait for the upload to complete.

To perform active reconnaissance on the local subnet

1. Continuing at the Meterpreter prompt, enter shell to access the command prompt.
2. Enter powershell to access PowerShell.
3. Enter the following command to gather the network information that is configured on the client:

ipconfig /all

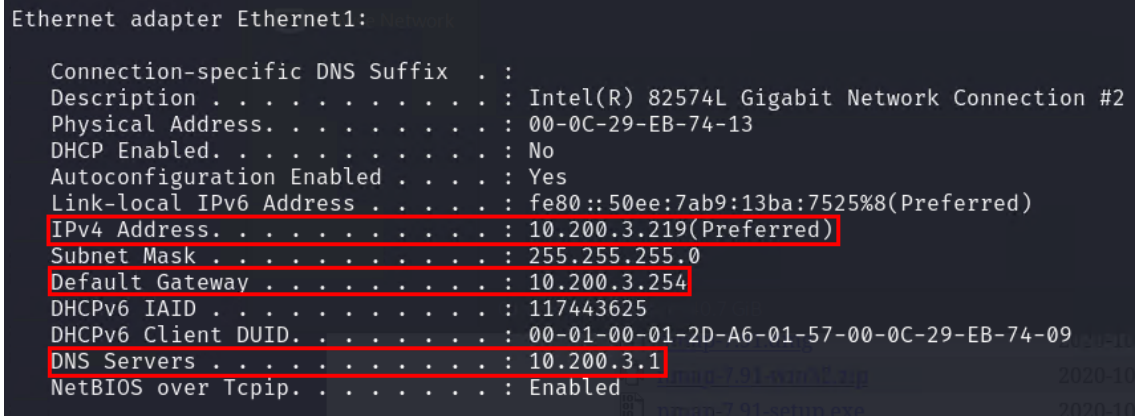
```
PS C:\users\bob\nmap\nmap-7.92> ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-CLIENT
   Primary Dns Suffix  . . . . . . . : cs.lab
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cs.lab
```

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-EB-74-09
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1570:b671:e130:977d%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.4.219(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-A6-01-57-00-0C-29-EB-74-09
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

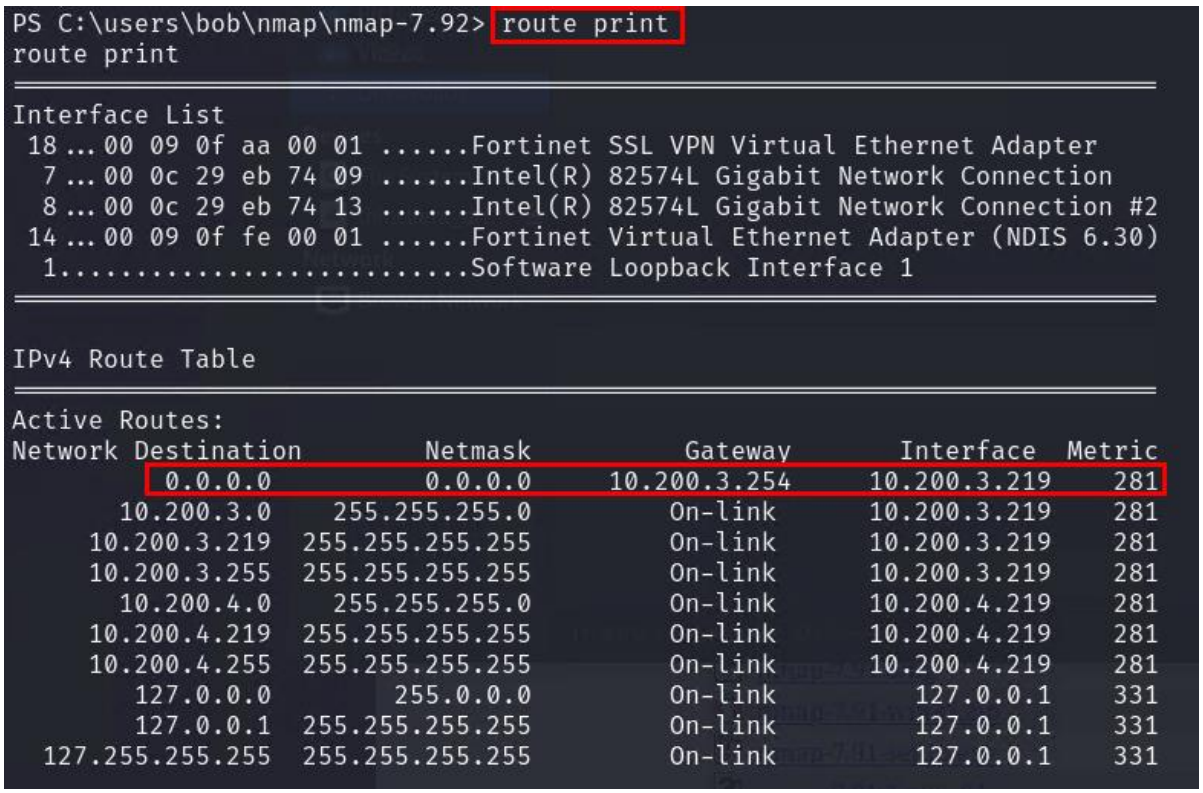


The following table contains a few important observations you can make by looking at the network configuration:

Finding	Significance
The domain name	You can use this to confirm the name and IP address of the domain controller.
The 10.200.4.219 interface	This has no default gateway configured, so it is probably not being used to route traffic.
	According to the lab topology diagram, this is the management interface that students can use to connect to the lab environment.
The 10.200.3.219 interface	The default gateway is configured with 10.200.3.254. This is likely a network device.
	The DNS server is configured with 10.200.3.1. This could be a DNS server only, but it is common for DNS services to be hosted on the domain controller also.

4. Enter the following command to print the client routing table:

route print



You can confirm that the default route uses the default gateway 10.200.3.254, and that there are no manual routes configured to reach remote subnets.

5. Enter the following command to extract the file:

Expand-Archive -Path "C:\Users\Bob\nmap.zip" -DestinationPath "C:\Users\Bob\nmap"

```
PS C:\Windows\system32> Expand-Archive -Path "C:\Users\Bob\nmap.zip" -DestinationPath "C:\Users\Bob\nmap"
Expand-Archive -Path "C:\Users\Bob\nmap.zip" -DestinationPath "C:\Users\Bob\nmap"
PS C:\Windows\system32>
```

6. Wait a few minutes while the file is being extracted.

You should see the PowerShell prompt once again.

7. Enter the following command to navigate to the Nmap folder:

```
cd C:\Users\Bob\nmap\nmap-7.92
```

You must stay in the C:\Users\Bob\nmap\nmap-7.92 folder to run nmap.exe in the subsequent steps.

Note that Windows, unlike Linux, is not case sensitive.

8. Enter the following command to confirm that Nmap can be executed:

```
.\nmap.exe --version
```

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap --version
.\nmap --version
Nmap version 7.92 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.5 openssl-1.1.1k nmap-libssh2-1.9.0 nmap-libz-1.2.11
Compiled without:
Available nsock engines: iocp poll select
PS C:\users\bob\nmap\nmap-7.92>
```

9. Enter the following command to find responding hosts on the 10.200.3.0/24 network:

```
.\nmap.exe -sn 10.200.3.0/24
```

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap.exe -sn 10.200.3.0/24
.\nmap.exe -sn 10.200.3.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-16 15:47 Pacific Daylight Time
Nmap scan report for 10.200.3.1
Host is up (0.0059s latency).
MAC Address: 00:0C:29:BA:2F:D1 (VMware)
Nmap scan report for 10.200.3.254
Host is up (0.0025s latency).
MAC Address: 00:0C:29:87:18:3F (VMware)
Nmap scan report for 10.200.3.219
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.44 seconds
```

This command scans using ICMP only. There is no port scanning.

You should detect the following three hosts:

- 10.200.3.1
- 10.200.3.219 (the Windows-Client VM)
- 10.200.3.254

Because of time constraints, you are scanning a /24 network only. However, you can use this method to scan for more IP addresses, such as 10.200.0.0/16, if you want to do your own testing outside of this lab environment.

Stop and think!

How does Nmap know, from the IP scan, that the interfaces are VMware?

The first six bytes of a MAC address contains the organizationally unique identifier (OUI), which specifies the manufacturer.

You can find OUI lookup tools on the internet, such as the Wireshark tools:

https://www.wireshark.org/tools/oui-lookup.html

In this lab environment, you will see a lot of virtual interfaces. However, on a physical network, you may see other vendor names, which could provide valuable information about high priority targets.

10. Enter the following command to find responding ports:

.\nmap.exe -p 1-65535 10.200.3.0/24

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap.exe -p 1-65535 10.200.3.0/24
.\nmap.exe -p 1-65535 10.200.3.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-17 10:38 Pacific Daylight Time
Nmap scan report for 10.200.3.1
Host is up (0.0063s latency).
Not shown: 65498 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1433/tcp  open  ms-sql-s
1551/tcp  open  hecmtl-db
1552/tcp  open  pciarray
1553/tcp  open  sna-cs
1556/tcp  open  veritas_pbx
1561/tcp  open  facilityview
1569/tcp  open  ets
1570/tcp  open  orbixd
1573/tcp  open  itscomm-ns
1580/tcp  open  tn-tl-r1
1602/tcp  open  inspect
3075/tcp  open  orbix-locator
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8013/tcp  open  unknown
8015/tcp  open  cfg-cloud
8443/tcp  open  https-alt
```

11. Wait a few minutes for the scan to complete.

Note that the output in the image is truncated, and not all hosts and ports are shown.

Looking at the services running for 10.200.3.1, it looks like a candidate for the domain controller.

12. Enter the following command to find service versions running on the potential domain controller:

.\nmap.exe -sV 10.200.3.1

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap.exe -sV 10.200.3.1
.\nmap.exe -sV 10.200.3.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-17 11:04 Pacific Daylight Time
Nmap scan report for 10.200.3.1
Host is up (0.0017s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-17 18:04:13Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: cs.lab, Site: Default-First-Site-Name)
443/tcp   open  ssl/https
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CSLAB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2017 14.00.1000
1556/tcp  open  msrpc         Microsoft Windows RPC
1580/tcp  open  msrpc         Microsoft Windows RPC
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cs.lab, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
8443/tcp  open  ssl/https-alt
50001/tcp open  http          Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
```

13. Wait a few minutes for the scan to complete.

You can see the cs.lab domain name, which you saw earlier in this exercise.

14. Enter the following command to confirm the IP address of the domain controller:

nltest /dclist:cslab

```
PS C:\users\bob\nmap\nmap-7.92> nltest /dclist:cslab
nltest /dclist:cslab
Get list of DCs in domain 'cslab' from '\\WIN-AD'.
    WIN-AD.cs.lab [PDC]  [DS] Site: Default-First-Site-Name
The command completed successfully
```

15. Enter the following command to ping the domain controller:

ping WIN-AD.cs.lab

```
PS C:\users\bob\nmap\nmap-7.92> ping WIN-AD.cs.lab
ping WIN-AD.cs.lab

Pinging WIN-AD.cs.lab [10.200.3.1] with 32 bytes of data:
Reply from 10.200.3.1: bytes=32 time<1ms TTL=128
Reply from 10.200.3.1: bytes=32 time<1ms TTL=128
Reply from 10.200.3.1: bytes=32 time=1ms TTL=128
Reply from 10.200.3.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.200.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

16. Enter the following command to find potential vulnerabilities:

.\nmap.exe --script vuln 10.200.3.1

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap.exe --script vuln 10.200.3.1
.\nmap.exe --script vuln 10.200.3.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-17 11:27 Pacific Daylight Time
Nmap scan report for 10.200.3.1
Host is up (0.0015s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
```

17. Wait a few minutes for the command to complete.

Note that the output in the image is truncated. There are other vulnerabilities that are not shown.

Stop and think!

It is a serious misconfiguration to have a client computer in the same subnet as a domain controller.

As seen in this exercise, if a client becomes compromised, it may have connectivity to a high priority target.

You want to isolate networks using microsegmentation, which is a network design that improves security by limiting potential lateral movement across the network with security policies.

Another problem with having all devices on the same subnet is that it may be harder to control traffic between clients. Traditional layer 2 traffic between hosts does not need to traverse firewalls. However, you can apply a policy to block intra-VLAN traffic on devices, such as FortiGate and FortiSwitch, which increases security.

To perform reconnaissance on a remote subnet

1. Enter the following command to scan a remote subnet:

.\nmap.exe -sn 10.200.200.0/24

Because of time constraints, again, you are scanning a /24 network only.

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap.exe -sn 10.200.200.0/24
.\nmap.exe -sn 10.200.200.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-17 12:43 Pacific Daylight Time
Nmap scan report for 10.200.200.12
Host is up (0.0030s latency).
Nmap scan report for 10.200.200.100
Host is up (0.0010s latency).
Nmap scan report for 10.200.200.213
Host is up (0.0011s latency).
Nmap scan report for 10.200.200.238
Host is up (0.0010s latency).
Nmap scan report for 10.200.200.254
Host is up (0.0040s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 37.42 seconds
```

2. Wait a few minutes for the scan to complete.

You should see the following five responding hosts:

- 10.200.200.12
- 10.200.200.100
- 10.200.200.213
- 10.200.200.238
- 10.200.200.254

3. Enter the following command to see more details about the hosts on the remote subnet:

.\nmap.exe -A 10.200.200.0/24

```
PS C:\users\bob\nmap\nmap-7.92> .\nmap -A 10.200.200.0/24
.\nmap -A 10.200.200.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-12 18:35 Eastern Daylight Time
Nmap scan report for 10.200.200.12
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 b5:99:08:f7:89:7b:b8:f8:79:25:1b:bf:0c:cf:75:d2 (ECDSA)
|_  256 2e:94:93:79:f1:b0:04:23:92:5e:55:74:6d:5a:68:68 (ED25519)
53/tcp   open  domain     ISC BIND 9.18.28-1~deb12u2 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.18.28-1~deb12u2-Debian
80/tcp   open  http       Apache httpd
|_http-server-header: Apache
|_http-title: TurnKey LAMP
443/tcp  open  ssl/http   Apache httpd
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
|_http-title: TurnKey LAMP
| ssl-cert: Subject: commonName=lamp
| Subject Alternative Name: DNS:lamp
```

4. Wait a few minutes for the scan to complete.

This scan may take longer than the previous ones. Note that the output in the image is truncated. There are other hosts and services running that are not included in the image.

5. Take a few minutes to review the output.

The following table contains a few important observations that you can make:

Finding	Significance
The devices seem to be servers	You can see that there is an Apache server (10.200.200.12), a mail server (10.200.200.100), and a server that uses TCP 514 (10.200.200.238). These are potentially high priority targets.
Remote services are open	SSH seems to be open on the web server 10.200.200.12.
Hop count	The devices are only two hops away from 10.200.3.219. The first hop is 10.200.3.254, which is the gateway for the Windows-Client VM. The second hop is the destination IP address. Using this evidence, you can reason that the devices are using the same layer 3 device for routing.

6. Enter exit to exit the PowerShell prompt.
7. Enter exit to exit the Windows command prompt.

You should see the Meterpreter prompt again.

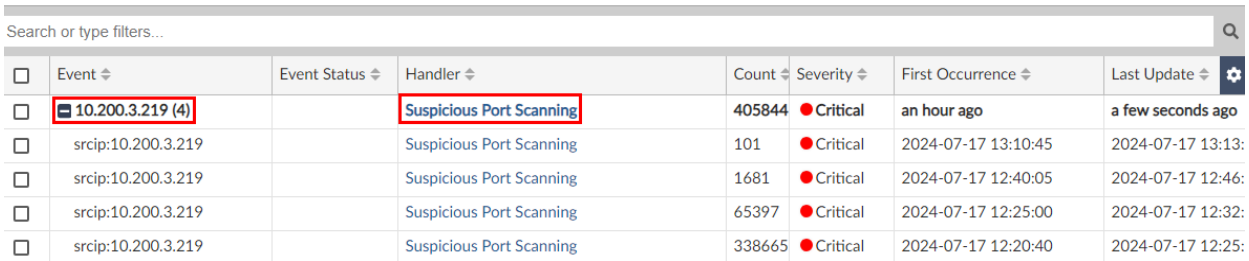
Keep the active Meterpreter session open for the next exercise. If the session is disconnected, follow the steps in To configure the listener on page 1 to reestablish an active session.

To review the port scanning event on FortiAnalyzer

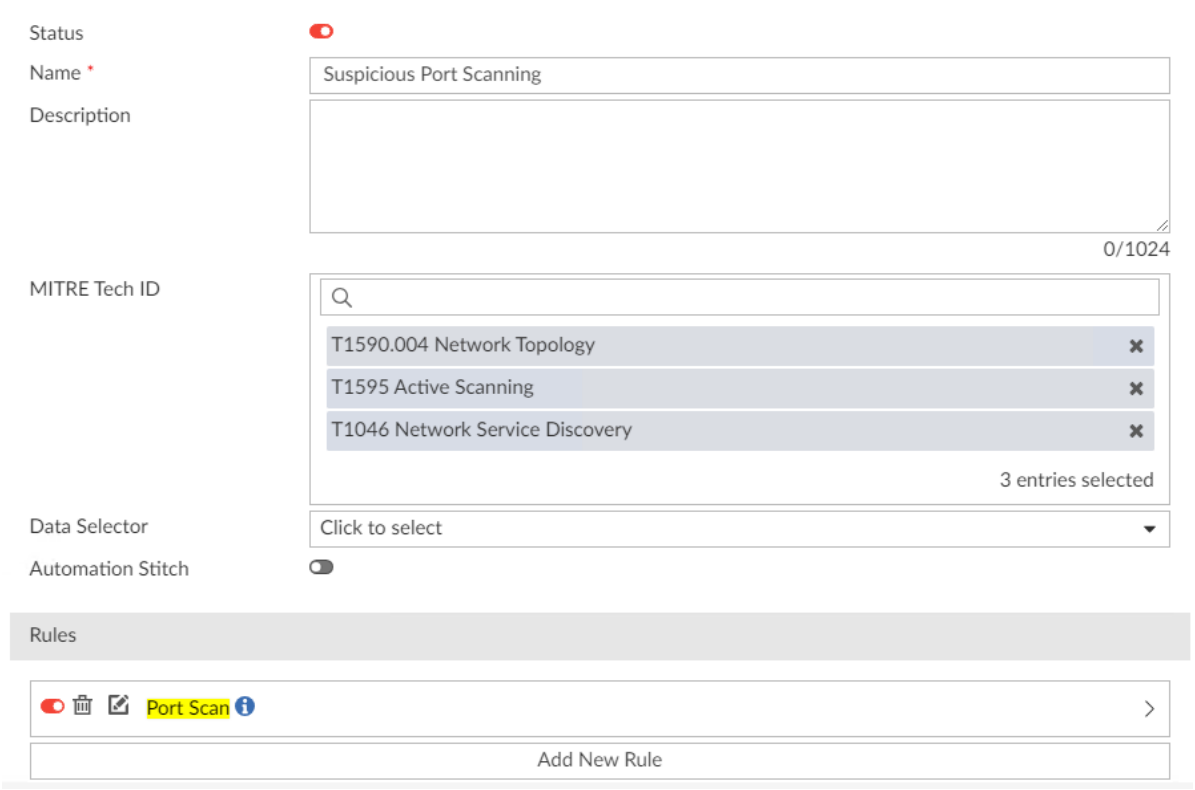
1. Log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:

- Username: admin
- Password: Fortinet1!

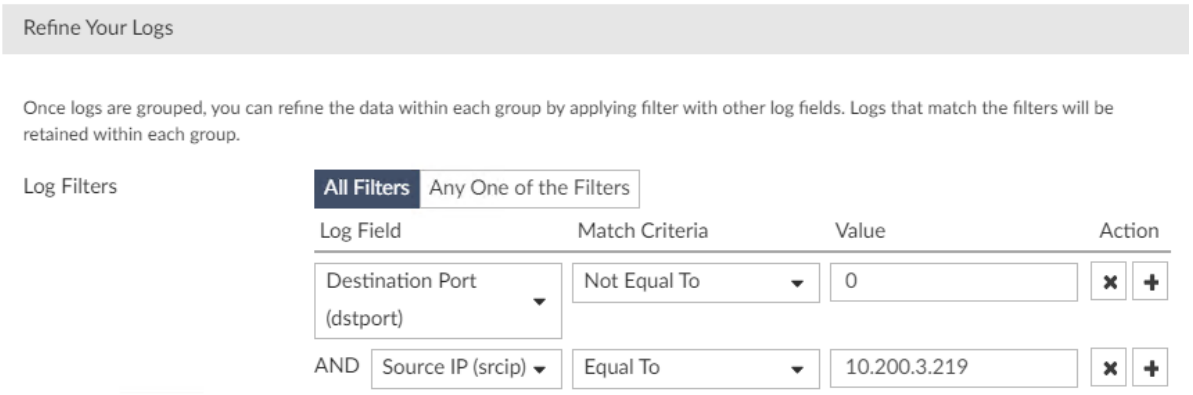
2. Click **Incidents & Events** > **Event Monitor**.
3. Search for the event named **10.200.3.219** , which the **Suspicious Port Scanning** event handler created.



4. Click the **Suspicious Port Scanning** event handler.
5. Review the event handler configuration.



6. Click the ⬚ icon to review the rule.



The example rule is simplified for this exercise. An event is generated when FortiAnalyzer receives logs that contain a destination port not equal to 0 (essentially meaning all ports), and coming from the source IP address 10.200.3.219. For this exercise, the port scan will come from that client, but in a real-world scenario, that is not realistic.

A rule that may make more sense is to select the destination IP address and define high priority targets.

LAB-CHALLENGE > Performing Active Reconnaissance