Updated: Mar 5, 2023

SEC 350: Practical Assessment

General Instructions - **Read First**

- Open internet, open notes, but no open neighbor nor remote support. You are ON YOUR OWN for this submission, so no communications with others during the formal assessment session (In class part).
- Make sure you follow the submission guidelines policy.

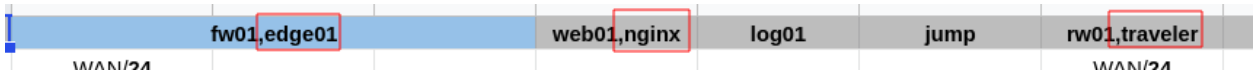
> 💣There a very few "on your own" activities in SEC350. This is one of them. Academic Integrity rules apply

Assessment Grading Policy

- Get in before the end of class - No points off
- Within 24 hours -10%
    - After assessment class, the assessment becomes a heavily weighted and late lab. If you are stuck, reach out to your instructor or a peer.
- Before our next class - 25%
    - At this point the Assessment gets a zero after that
- Look at the rubric to get a sense of weighting of individual assessment components before investing a lot of time on a trouble area.

Hints - Read Second

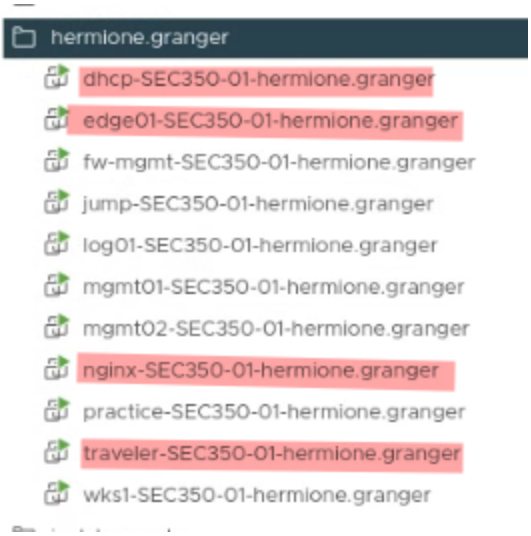
- You do not need to work serially through this assessment (*though recommended*); it is the end result that matters.
- Make sure to link your firewalls to the appropriate From and To zones.
- Review network assignments. Your new systems will reuse the IP addresses they are replacing.



- Restart any service if you modify a configuration file (network, nginx, dhcp etc…).
- Make sure you include the appropriate vmname label on all deliverables where your name is not obvious in the console.
- Check every VM's network settings to make sure they are moved from SEC350-WAN to the appropriate network segment such as DMZ or LAN.
- Don't forget to look at /var/log/messages on edge01 FW to debug firewall issues.
- The FW Rule Descriptions are mandatory for rules other than simple established/enabled rules!

Updated: Mar 5, 2023

Your Systems

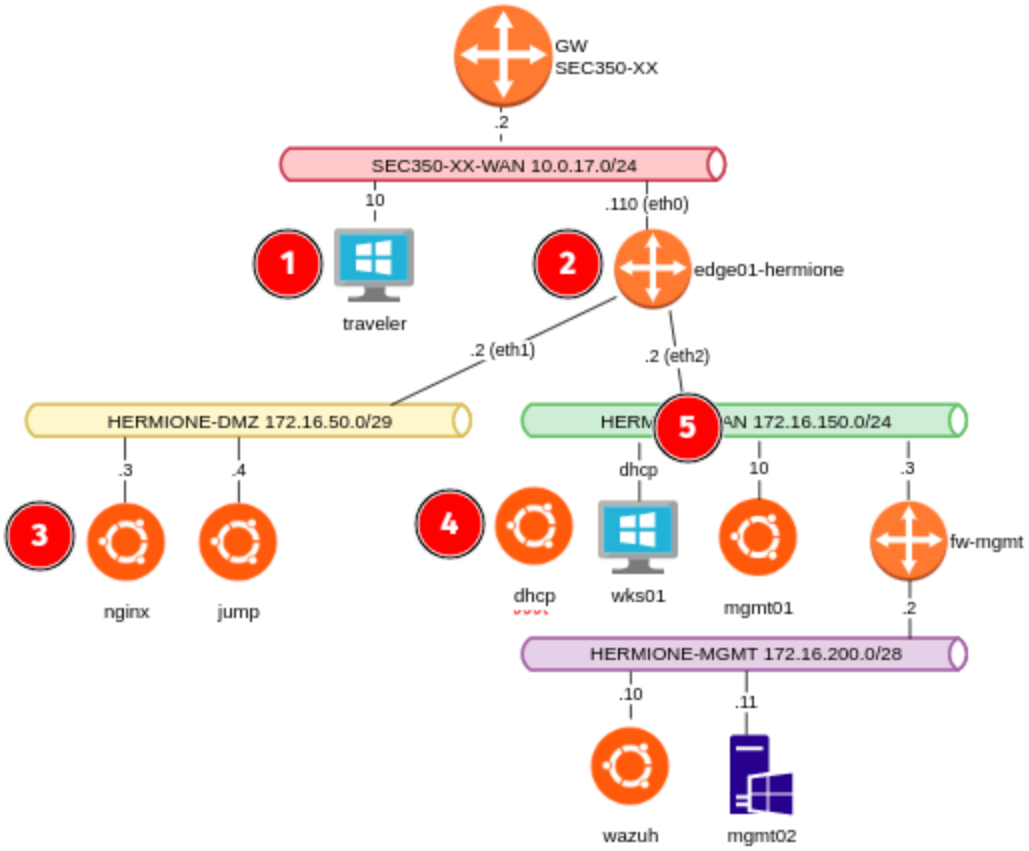


New Passwords

System	Type	Username	Password
edge01	Firewall	vyos	Ch@mpl@1n!22
nginx,dhcp	Linux Ubuntu	champuser	Ch@mpl@1n!22
traveler	Windows	champuser	Ch@mpl@1n!22

Updated: Mar 5, 2023

Overview



1. RW is gone, reuse that WAN IP address for traveler
2. fw1 is gone, reuse WAN IP for edge01 and configure your DMZ and LAN interfaces just as you did for fw1
3. web01 is history, replace with a new nginx web server using the same IP as web01
4. You have a new ubuntu server that will assign DHCP addresses within the LAN (pick your own IP in the LAN segement)
5. WKS01 should pick up a DHCP address

Network Assignments

SEC350-Network-Assignments You will see your new systems in the spreadsheet (likely next to the old ones). Be very careful with your WAN ip addresses (edge01's eth0 interface and travelers interface. Use **your** assigned IP and nooneone else's.

Updated: Mar 5, 2023

edge01 - Network Configuration

Assign the existing two interfaces to WAN and DMZ respectively, add a third interface and assign it to the LAN. On the WAN interface, the upstream gateway and DNS should be assigned to the class gateway: 10.0.17.2

edge01 routing requirements

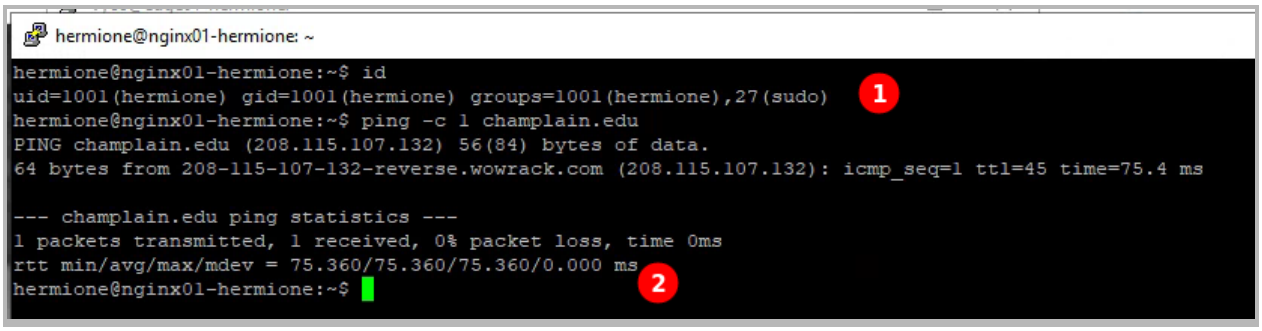
- Set your Hostname to edge01-your name
- Configure gateway, dns and all three ip addresses
- Set NAT source rules so that DMZ and LAN hosts are masqueraded by the WAN interface, don't forget to include the MGMT source network
- Forward DNS requests from DMZ and LAN interfaces and their networks. Don't forget to also accept MGMT traffic
- on edge01 Add RIP, advertising the DMZ Network (you may need to restart fw-mgmt for this relationship to work)

nginx

- Network Segment: SEC350-DMZ
- Set your hostname to nginx-yourname
- Configure networking
- Create a sudo user with your name, and use it instead of champuser, change the default champuser password
- Install and enable nginx, delete the default welcome page, create an index page with your hostname as its content

```
Deliverable 1.  Nginx:  Screenshot showing the current user's
group (id command) and a successful ping from nginx to
champlain.edu similar to the one below.  The user should be a
member of the sudo group. (Note, this is before your firewall
zones are active)
```

Updated: Mar 5, 2023



traveler

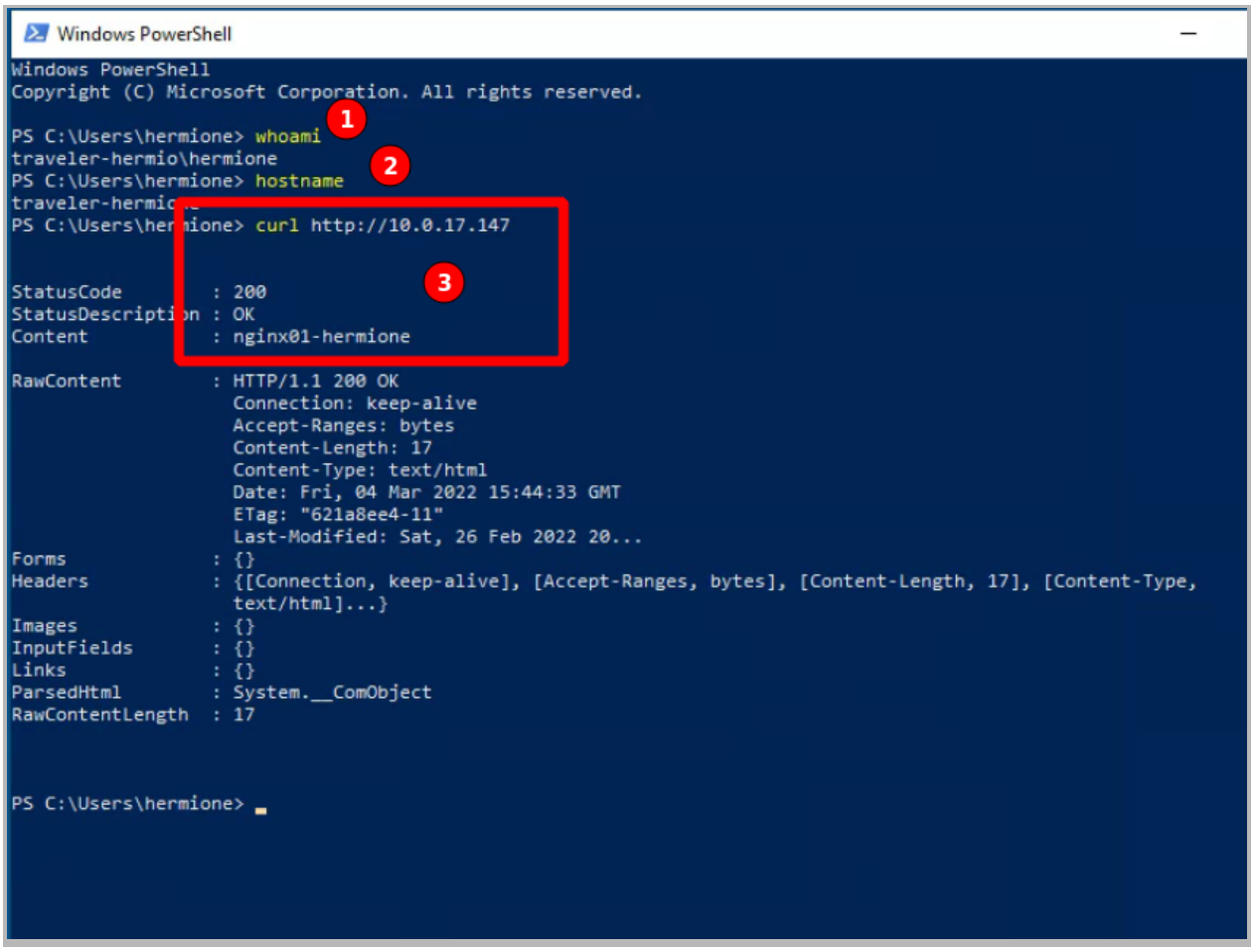
- Network Segment: SEC350-WAN
- Configure networking with YOUR ip address
- Set the Hostname to traveler-yourname
- Create a Named Administrative User
- This is a WAN system, so make sure the default gateway and DNS point to 10.0.17.2.

edge01 port forwarding

On edge01, configure port forwarding such that port 80 to edge01's WAN interface will be translated/forwarded to nginx. Make sure you have renamed the computer and are accessing it as a named user.

```
Deliverable 2.  Screenshot demonstrating port forwarding from your
eth0 address on edge01 (10.0.17.XX) to nginx from traveler similar to
the one below.  Also show that your system is named appropriately and
that you have a named user.
```

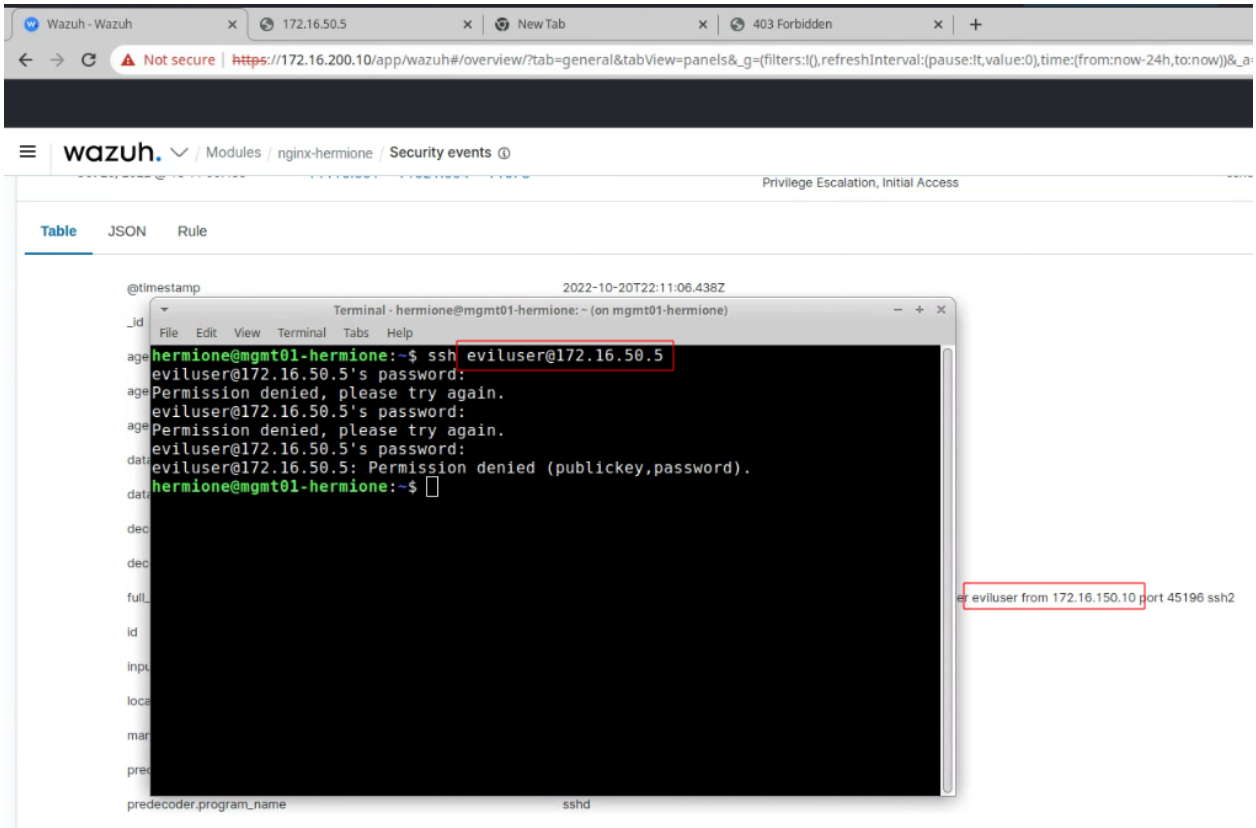
Updated: Mar 5, 2023



Updated: Mar 5, 2023

nginx wazuh agent

- Figure out how to delete the web01 agent from wazuh manager (it is gone and will be replaced by nginx)
- Install a Wazuh Agent on nginx
- Run the test shown below. SSH to nginx (from another host) Create a failed login attempt followed by a valid one and elevate to root. This is shown in the following screenshot.



Deliverable 3. Screenshot on wazuh that shows an invalid ssh user attempting to login to nginx similar to the one above.

Updated: Mar 5, 2023

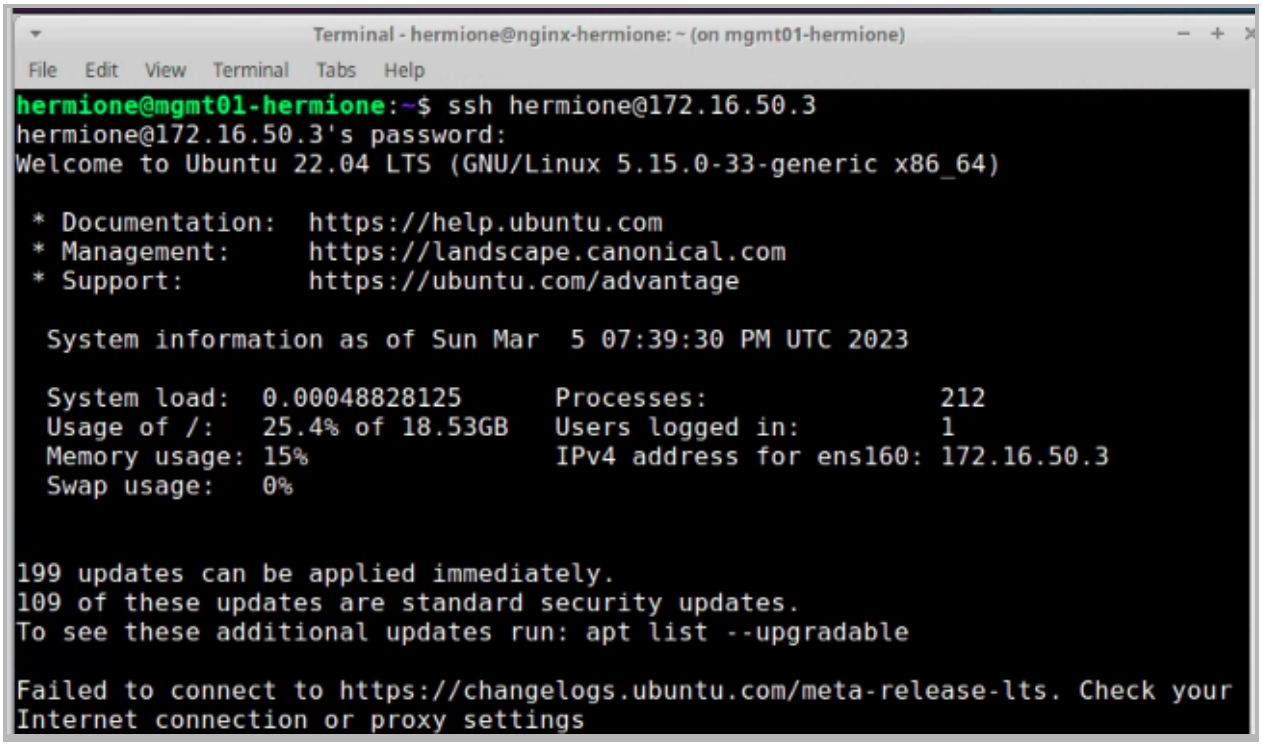
edge01 Zones and Firewalls

- Create WAN, DMZ and LAN Zones that default drops and logs, and are assigned to the appropriate interfaces
- Create the following firewalls and link them to the appropriate zones. Make sure the default action is drop, and default logging is enabled (this will help you debug).
- Make sure the tests described below work:

Firewall	Requirements	Test
WAN-TO-DMZ	established allowed back WAN can get to nginx on tcp/80 WAN can get to jump on tcp/22	ssh from traveler to jump http from traveler to nginx
DMZ-TO-WAN	established allowed back nginx can ping any host on the WAN (note, this won't work after firewall is up)	ping from nginx to champlain.edu
WAN-TO-LAN	established allowed back	on wks1 browse to a website
LAN-TO-WAN	accept all	on wks1 browse to a website
DMZ-TO-LAN	established allowed back tcp/1514-1515 allowed to wazuh	show a wazuh log event from nginx and jump on wazuh
LAN-TO-DMZ	established allowed back tcp/80 allowed to nginx tcp/22 allowed to all hosts on DMZ from mgmt01	from mgmt101 browse to nginx from mgmt01 ssh into nginx from mgmt01 ssh into jump

Updated: Mar 5, 2023

Deliverable 4. Screenshot from mgmt01 that shows a ssh session to nginx.



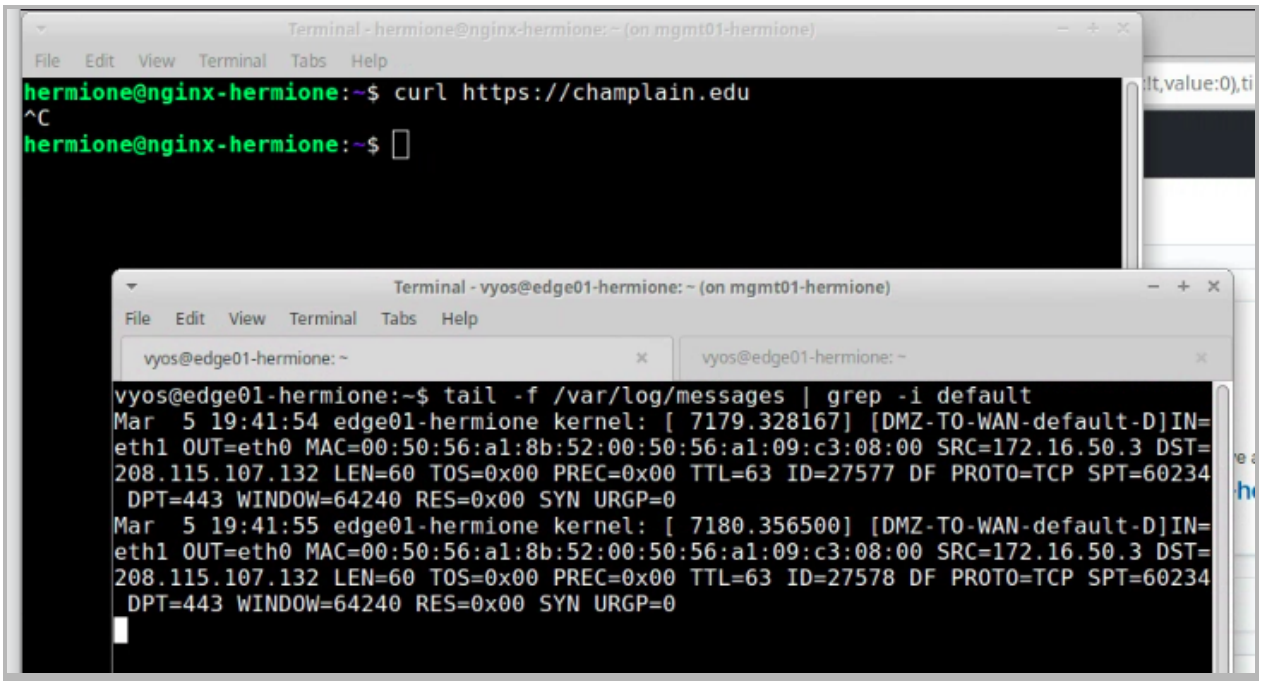
DMZ to WAN Drop

Nginx is not allowed to surf the internet. From attemptnginx, to curl https://champlain.edu

The following test should fail due to firewall restrictions:
nginx->http->champlain.edu

Deliverable 5. Provide a screenshot showing a DMZ-to-WAN drop message where the protocol is TCP, DPT=443 and the Destination is the IP presumably associated with champlain.edu

Updated: Mar 5, 2023



Updated: Mar 5, 2023

dhcp

Install a DHCP server on the LAN segment, you can choose your own unused IP in the 172.16.150.0/24 range. DHCP options should include

- an IP range of 172.16.150.100-172.16.150.150
- a router of 172.16.150.2
- a dns server of 172.16.150.2

Updated: Mar 5, 2023

Deliverable 6.
Run the following test on wks01:

- ipconfig /release
- ipconfig /renew
- ipconfig /all

Provide a screenshot similar to the one below that shows your DHCP server information similar to the screenshot below.

```
C:\Users\hermione>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : hermione.local
   IPv4 Address. . . . . . . . . . . : 172.16.150.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.150.2

C:\Users\hermione>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : wks1-hermione
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : hermione.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : hermione.local
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connecti
   Physical Address. . . . . . . . . : 00-50-56-A1-60-6B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.16.150.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, March 5, 2023 2:44:03 PM
   Lease Expires . . . . . . . . . . : Sunday, March 5, 2023 2:54:03 PM
   Default Gateway . . . . . . . . . : 172.16.150.2
   DHCP Server . . . . . . . . . . . : 172.16.150.5
   DNS Servers . . . . . . . . . . . : 172.16.150.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Deliverable 7. On wazuh, display an agent based security event for dhcp. You should repeat the invalid user test you did earlier.

Updated: Mar 5, 2023

wazuh. / Modules / dhcp-hermione / Security events

Oct 20, 2022 @ 18:37:57.444	T1110				Credential Access	syslog: U
Oct 20, 2022 @ 18:37:55.402	T1110.001	T1021.004	T1078		Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Att
Oct 20, 2022 @ 18:37:53.400	T1110.001	T1021.004	T1078		Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Att
Oct 20, 2022 @ 18:37:49.397	T1110.001	T1021.004	T1078		Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Att

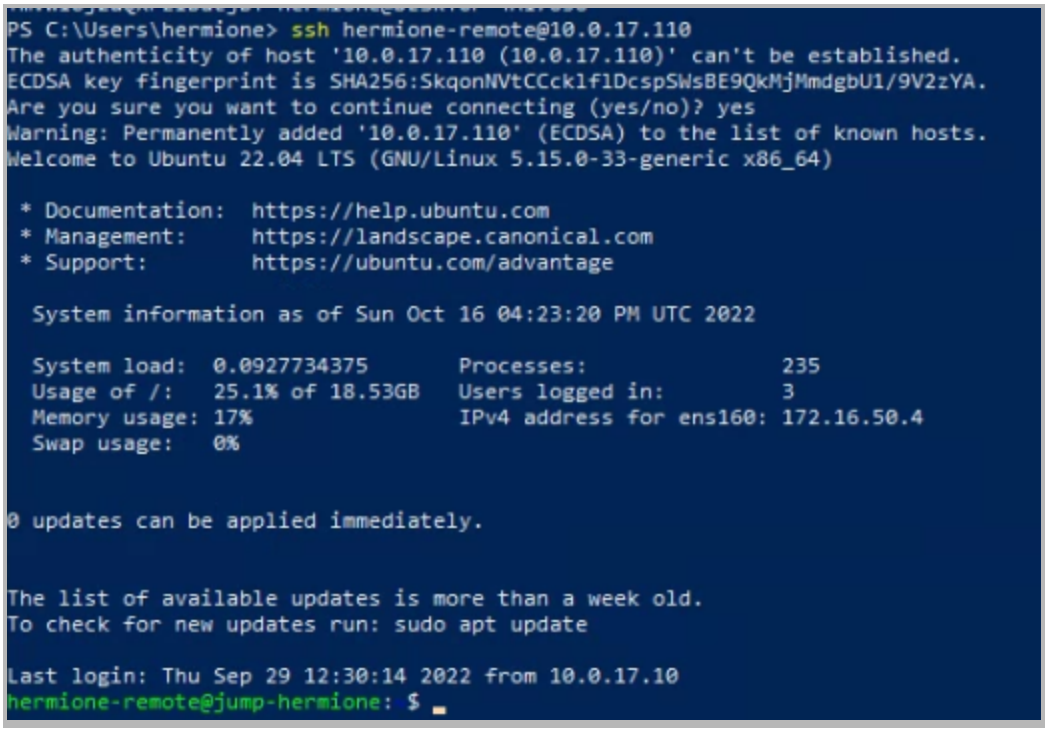
Table JSON Rule

@timestamp	2022-10-20T22:37:49.397Z
_id	HWqL94MBmMcpbyv8w7H6
agent.id	004
agent.ip	172.16.150.5
agent.name	dhcp-hermione
data.srcip	172.16.150.10
data.srcuser	eviluser
decoder.name	sshd
decoder.parent	sshd
full_log	Oct 20 22:37:49 ubuntu sshd[27743]: Failed password for invalid user eviluser from 172.16.150.10 port 55352 ssh2

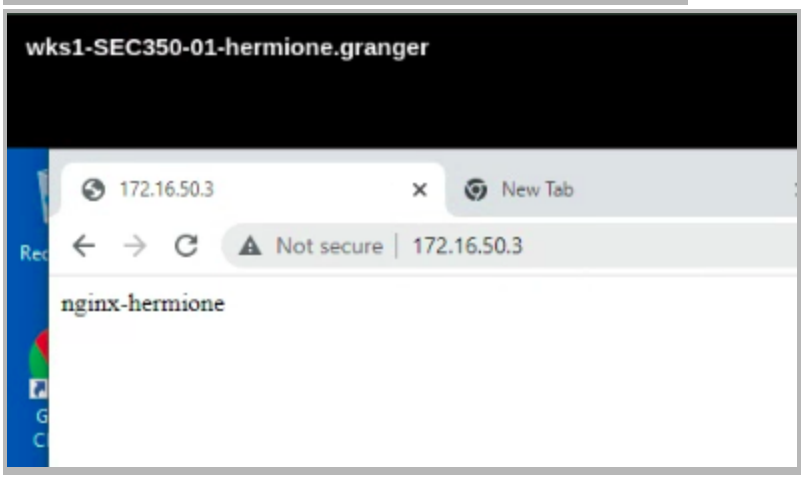
Updated: Mar 5, 2023

traveler->jump passwordless ssh

Deliverable 8. Demonstrate that you can functionally ssh into jump using an RSA keypair. Note, the passwordless functionality is not heavily weighted.



Deliverable 9. Demonstrate that wks01 can browse to nginx. Provide a screenshot similar to the one below.



Deliverable 10. Provide a link to your edge01 configuration on github. Your firewall will be evaluated for correctness and

Updated: Mar 5, 2023

thoroughness. Your firewall should be formatted as plaintext using the vyos configuration routine shown below. This is the only github requirement.

```
show configuration commands | grep -v "syslog
global\|ntp\|login\|console\|config\|hw-id\|loopback\|conntrack"
```