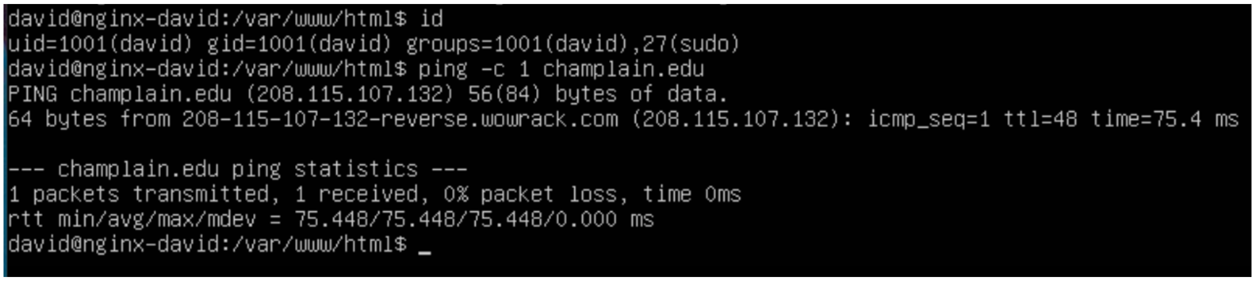
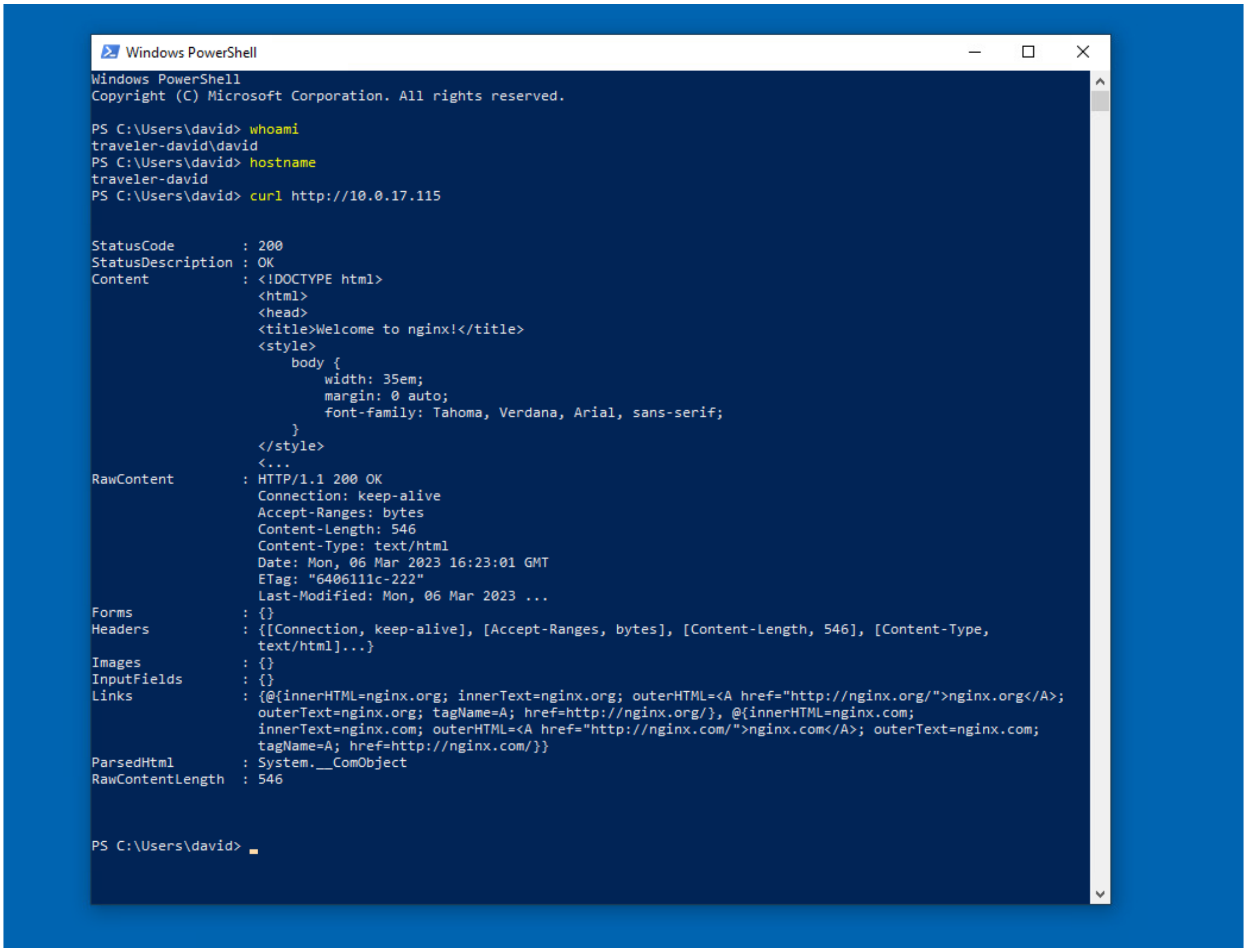
David Thomsen

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)

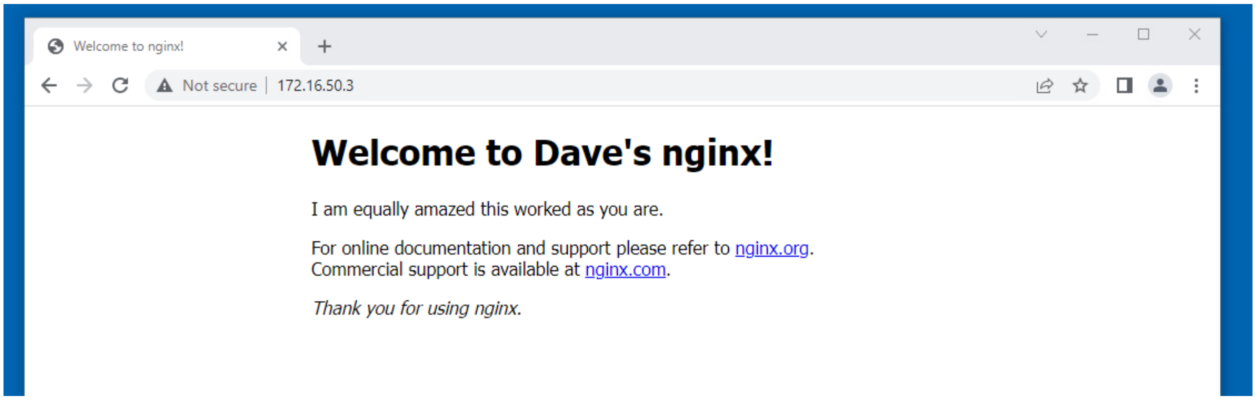


```
david@nginx-david:/var/www/html$ id
uid=1001(david) gid=1001(david) groups=1001(david),27(sudo)
david@nginx-david:/var/www/html$ ping -c 1 champlain.edu
PING champlain.edu (208.115.107.132) 56(84) bytes of data.
64 bytes from 208-115-107-132-reverse.wowrack.com (208.115.107.132): icmp_seq=1 ttl=48 time=75.4 ms

--- champlain.edu ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 75.448/75.448/75.448/0.000 ms
david@nginx-david:/var/www/html$ _
```

Deliverable 2. Screenshot demonstrating port forwarding from your eth0 address on edge01 (10.0.17.115) to nginx from traveler similar to the one below. Also show that your system is named appropriately and that you have a named user.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\david> whoami
traveler-david\david
PS C:\Users\david> hostname
traveler-david
PS C:\Users\david> curl http://10.0.17.115


StatusCode        : 200
StatusDescription : OK
Content           : <!DOCTYPE html>
                    <html>
                    <head>
                    <title>Welcome to nginx!</title>
                    <style>
                        body {
                            width: 35em;
                            margin: 0 auto;
                            font-family: Tahoma, Verdana, Arial, sans-serif;
                        }
                    </style>
                    <...
RawContent        : HTTP/1.1 200 OK
                    Connection: keep-alive
                    Accept-Ranges: bytes
                    Content-Length: 546
                    Content-Type: text/html
                    Date: Mon, 06 Mar 2023 16:23:01 GMT
                    ETag: "6406111c-222"
                    Last-Modified: Mon, 06 Mar 2023 ...
Forms             : {}
Headers           : {[Connection, keep-alive], [Accept-Ranges, bytes], [Content-Length, 546], [Content-Type,
                    text/html]...}
Images            : {}
InputFields       : {}
Links             : {@{innerHTML=nginx.org; innerText=nginx.org; outerHTML=<A href="http://nginx.org/">nginx.org</A>;
                    outerText=nginx.org; tagName=A; href=http://nginx.org/}, @{innerHTML=nginx.com;
                    innerText=nginx.com; outerHTML=<A href="http://nginx.com/">nginx.com</A>; outerText=nginx.com;
                    tagName=A; href=http://nginx.com/}}
ParsedHtml        : System.__ComObject
RawContentLength  : 546


PS C:\Users\david> _
```



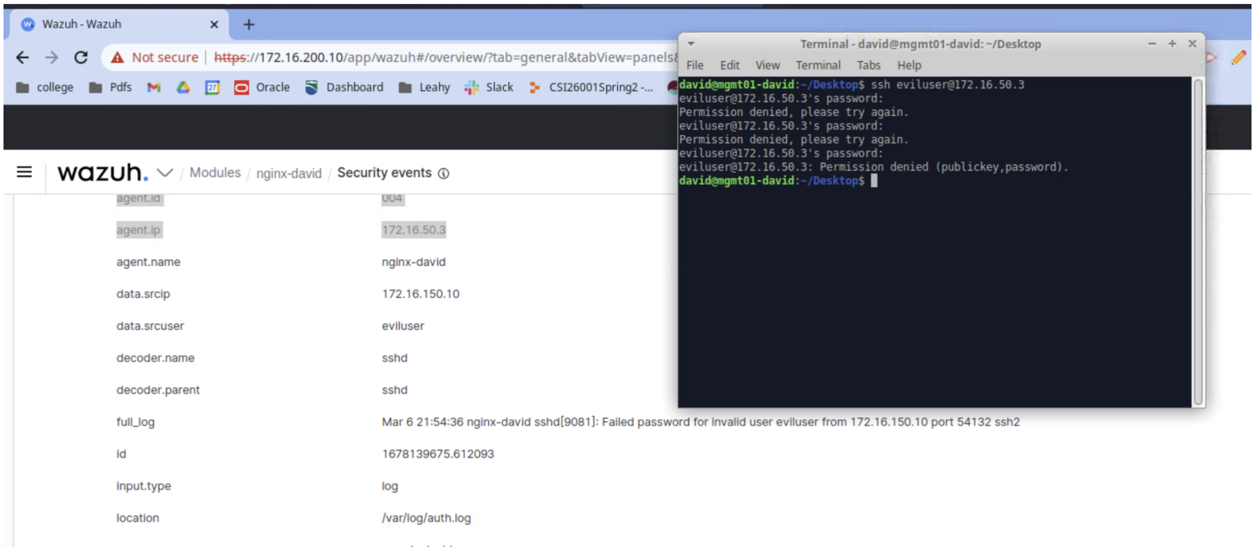
# Welcome to Dave's nginx!

I am equally amazed this worked as you are.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

*Thank you for using nginx.*

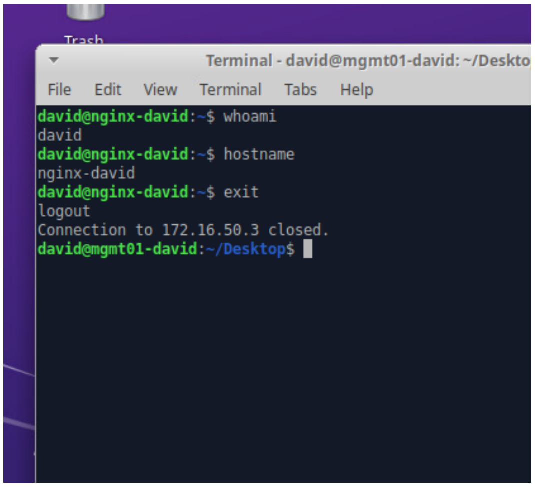
Deliverable 3. Screenshot on wazuh that shows an invalid ssh user attempting to login to nginx similar to the one above.


Wazuh - Wazuh
Not secure | https://172.16.200.10/app/wazuh#/overview/?tab=general&tabView=panels&
college
Pdfs
Oracle
Dashboard
Leahy
Slack
CSI26001Spring2 -...
wazuh.
Modules / nginx-david / Security events
Terminal - david@mgmt01-david: ~/Desktop
File Edit View Terminal Tabs Help

| | |
|---|---|
| agent.id | 004 |
| agent.ip | 172.16.50.3 |
| agent.name | nginx-david |
| data.srcip | 172.16.150.10 |
| data.srcuser | eviluser |
| decoder.name | sshd |
| decoder.parent | sshd |
| full_log | Mar 6 21:54:36 nginx-david sshd[9081]: Failed password for invalid user eviluser from 172.16.150.10 port 54132 ssh2 |
| id | 1678139675.612093 |
| input.type | log |
| location | /var/log/auth.log |

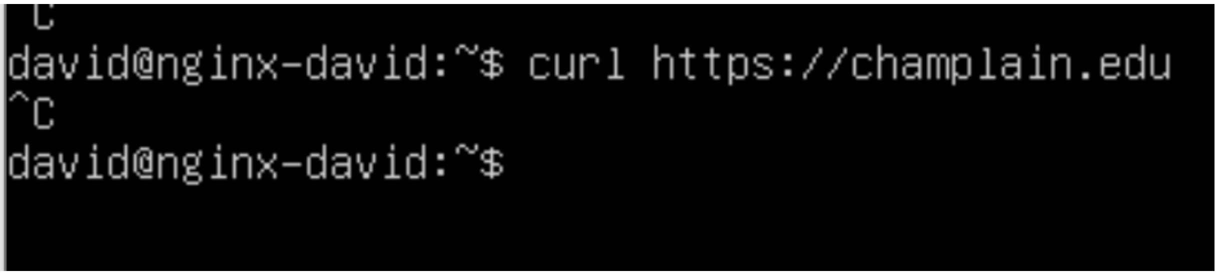
```
david@mgmt01-david:~/Desktop$ ssh eviluser@172.16.50.3
eviluser@172.16.50.3's password:
Permission denied, please try again.
eviluser@172.16.50.3's password:
Permission denied, please try again.
eviluser@172.16.50.3's password:
eviluser@172.16.50.3: Permission denied (publickey,password).
david@mgmt01-david:~/Desktop$
```

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

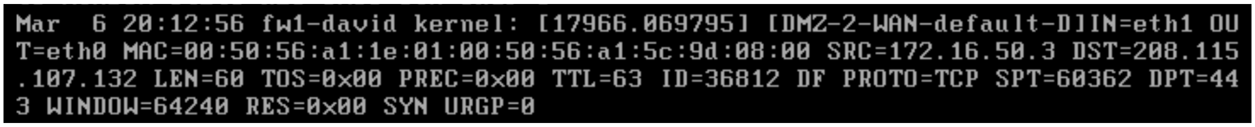

Trash
Terminal - david@mgmt01-david: ~/Deskto
File Edit View Terminal Tabs Help

```
david@nginx-david:~$ whoami
david
david@nginx-david:~$ hostname
nginx-david
david@nginx-david:~$ exit
logout
Connection to 172.16.50.3 closed.
david@mgmt01-david:~/Desktop$
```

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



```
^C
david@nginx-david:~$ curl https://champlain.edu
^C
david@nginx-david:~$
```

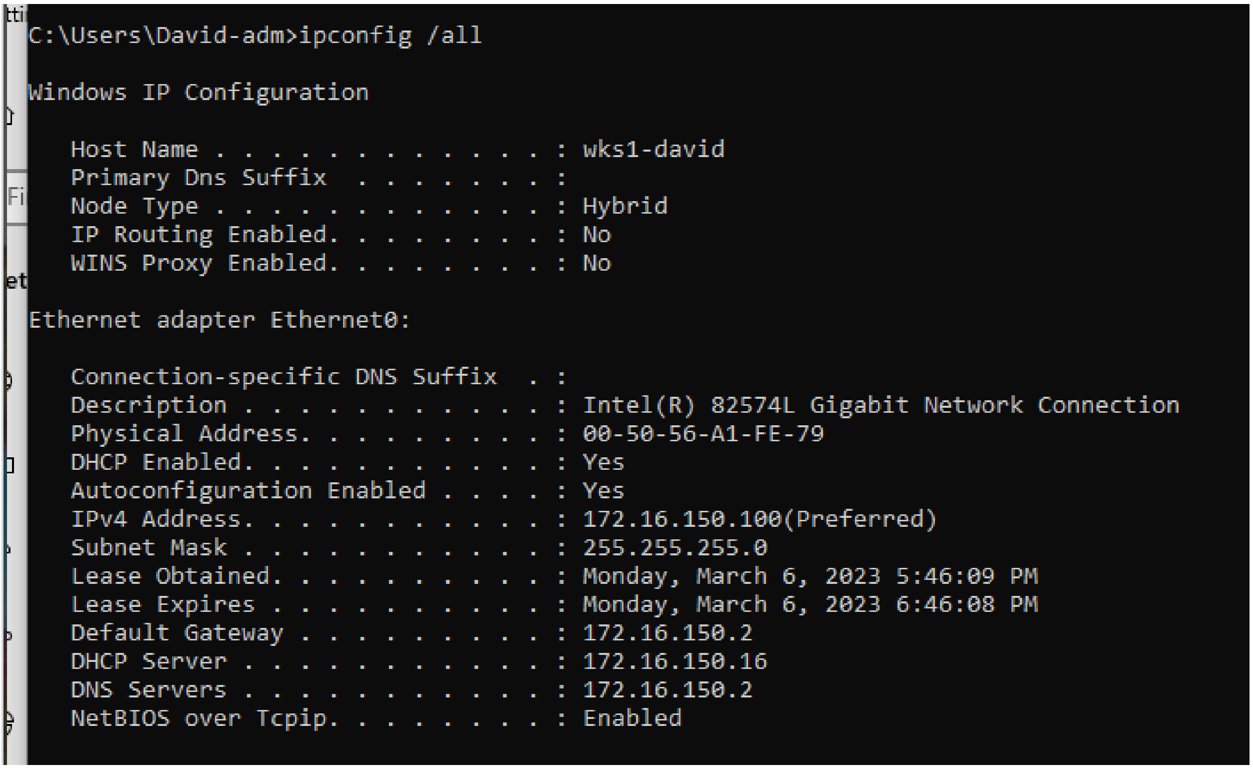


```
Mar  6 20:12:56 fw1-david kernel: [17966.069795] [DMZ-2-WAN-default-D]IN=eth1 OU
T=eth0 MAC=00:50:56:a1:1e:01:00:50:56:a1:5c:9d:08:00 SRC=172.16.50.3 DST=208.115
.107.132 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=36812 DF PROTO=TCP SPT=60362 DPT=44
3 WINDOW=64240 RES=0x00 SYN URGP=0
```

Deliverable 6.
Run the following test on wks01:

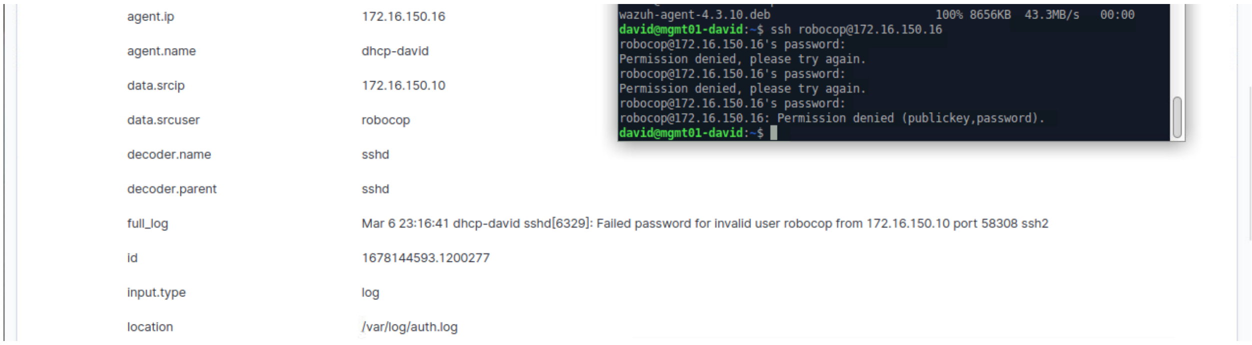
- ipconfig /release
- ipconfig /renew
- ipconfig /all

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



```
C:\Users\David-adm>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : wks1-david
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-A1-FE-79
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.16.150.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, March 6, 2023 5:46:09 PM
   Lease Expires . . . . . . . . . . : Monday, March 6, 2023 6:46:08 PM
   Default Gateway . . . . . . . . . : 172.16.150.2
   DHCP Server . . . . . . . . . . . : 172.16.150.16
   DNS Servers . . . . . . . . . . . : 172.16.150.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

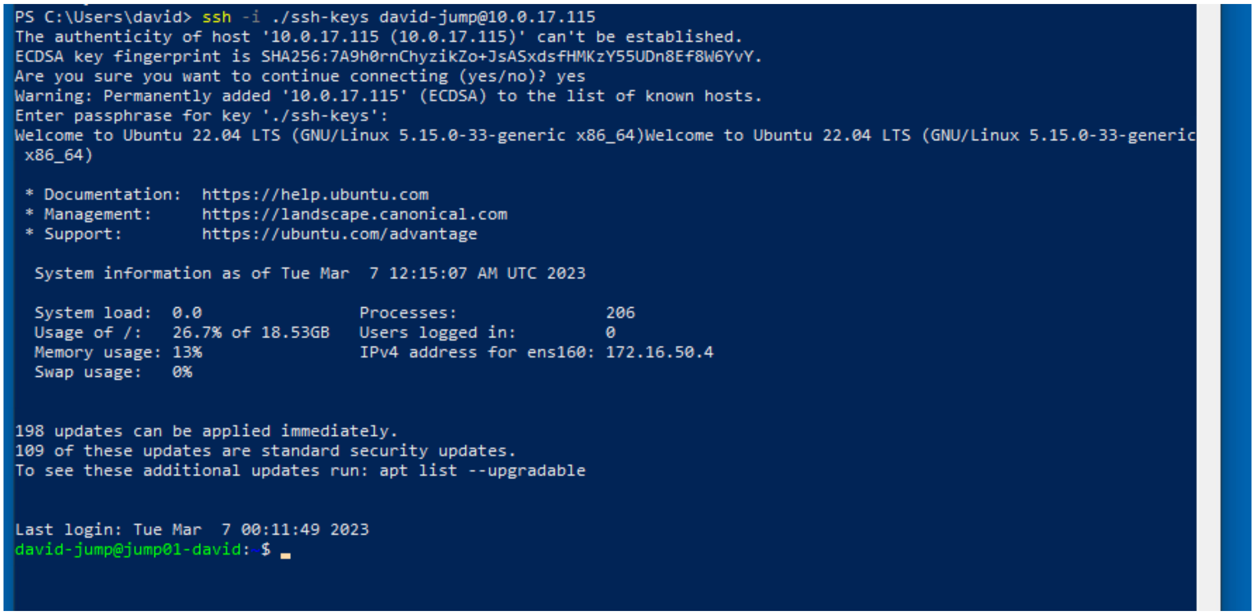
Deliverable 7.  On wazuh, display an agent based security event for dhcp.  You should repeat the invalid user test you did earlier.



| | |
|---|---|
| agent.ip | 172.16.150.16 |
| agent.name | dhcp-david |
| data.srcip | 172.16.150.10 |
| data.srcuser | robocop |
| decoder.name | sshd |
| decoder.parent | sshd |
| full_log | Mar 6 23:16:41 dhcp-david sshd[6329]: Failed password for invalid user robocop from 172.16.150.10 port 58308 ssh2 |
| id | 1678144593.1200277 |
| input.type | log |
| location | /var/log/auth.log |

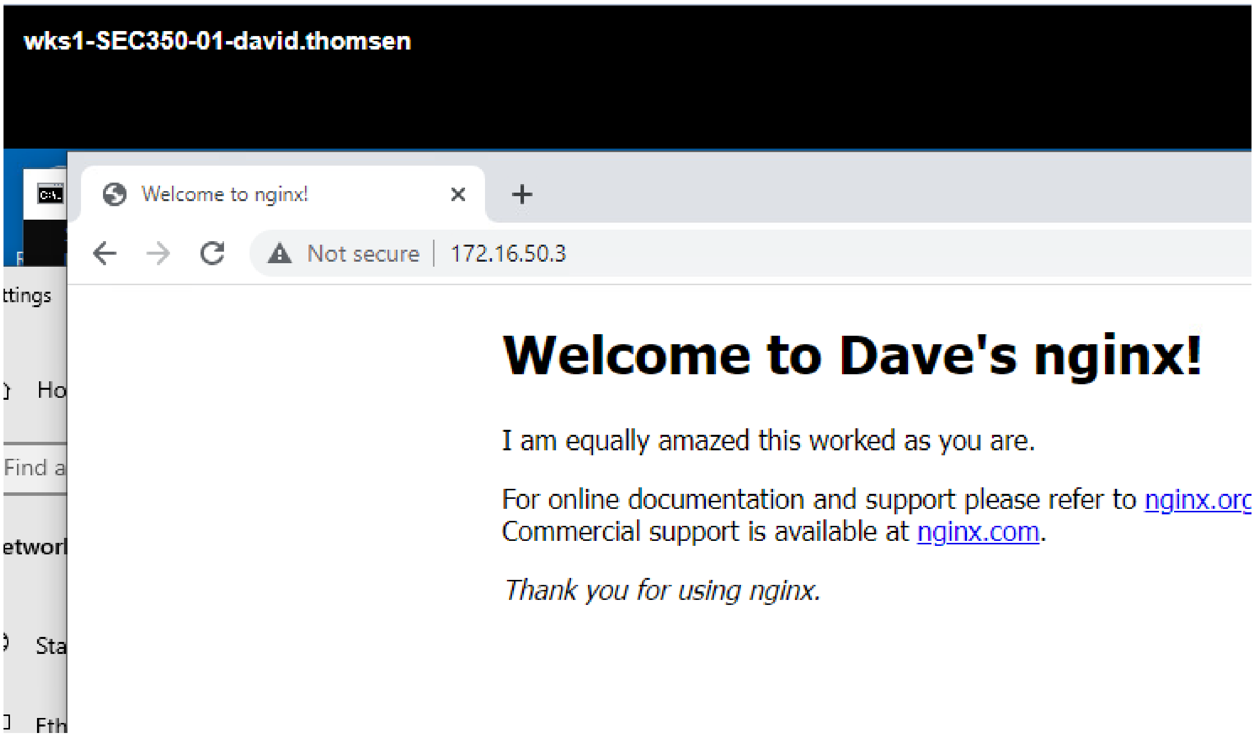
```
wazuh-agent-4.3.10.deb                            100% 8656KB  43.3MB/s   00:00
david@mgmt01-david:~$ ssh robocop@172.16.150.16
robocop@172.16.150.16's password:
Permission denied, please try again.
robocop@172.16.150.16's password:
Permission denied, please try again.
robocop@172.16.150.16's password:
robocop@172.16.150.16: Permission denied (publickey,password).
david@mgmt01-david:~$
```

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



```
PS C:\Users\david> ssh -i ./ssh-keys david-jump@10.0.17.115
The authenticity of host '10.0.17.115 (10.0.17.115)' can't be established.
ECDSA key fingerprint is SHA256:7A9h0rnChyzikZo+JsASxdsfHMKzY55UDn8Ef8W6YvY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.17.115' (ECDSA) to the list of known hosts.
Enter passphrase for key './ssh-keys':
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-33-generic x86_64)Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-33-generic
 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Mar  7 12:15:07 AM UTC 2023

  System load:  0.0               Processes:               206
  Usage of /:   26.7% of 18.53GB   Users logged in:         0
  Memory usage: 13%               IPv4 address for ens160: 172.16.50.4
  Swap usage:   0%


198 updates can be applied immediately.
109 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Tue Mar  7 00:11:49 2023
david-jump@jump01-david:~$
```

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



wks1-SEC350-01-david.thomsen

# Welcome to Dave's nginx!

I am equally amazed this worked as you are.

For online documentation and support please refer to nginx.org
Commercial support is available at nginx.com.

*Thank you for using nginx.*

Deliverable 10. Provide a link to your edge01 configuration on github. Your firewall will be evaluated for correctness and thoroughness. Your firewall should be formatted as plaintext using the vyos configuration routine shown below. This is the only github requirement.

**https://github.com/dthomsen116/SEC-350/blob/main/edgeConf**