

Colby Heilner
Professor Torres
11/19
IT 120
Lab 12

Part A: Wazuh

Review the videos below on Wazuh, and give your opinion on them

Review the Wazuh Proof-of-Concept guide. Choose any five (5) guides, and give your opinion.

[Video 1 Links to an external site.](#)

I have watched network chuck before, and I like his videos. This one was no different, it covered a lot of stuff you already had for us in class, but it was still useful information. Just mainly highlights the super friendly UI and how EASY it is to deploy agents. He connected three computers in a matter of 15-30 mins

[Video 2 Links to an external site.](#)

This video was very cool and I think it takes an approach I would normally take. He does the usally explantion of the tool and then he also does some self testing. He uses hydra for a brute force against ssh on the machine with the agent installed. He also gets the alert for the attack in many diffrent ways. It is important to note that the way to view recent attacks like this is in the threat hunting section. Becuse we will not be allowed to do manuall scans during our challenge I will most likely be living in this threat section. This takes advantage of auditd, which is just auditing for Linux. It can collect its logs and send it back to Wazuh then we get a good centralized SIEM.

[Wazuh Proof-of-Concept Guide](#)

[Links to an external site.](#)

- I looked at these five,
- Vulnerability detection
- Network IDS integration
- Monitoring execution of malicious commands
- Detecting and removing malware using VirusTotal integration
- Detecting hidden processes

I really like the Idea of stopping someone before they can even get in. But if they do manage to slip by then that is where most of these come in. I would really like to incorporate a general IDS in combination with monitoring execution of malicious commands. Both guides explained how to set up these features for Wazuh.

Part B: Linux Connections: [Netlab 2](#)

[Links to an external site.](#), NISGTC Linux+ Series 1, lab 1

- Log on to all 4 systems
- Add the below users to all systems
 - superman, batman, Wondersome, the flash, Ironman, Hulk, Spiderman, Blackwidow

I made a script for adding users and used scp to share the love,

```
[sysadmin@localhost ~]$ cat user.sh
#!/bin/bash

read -p "users wanted" user_count

for ((i=1; i<=user_count; i++)); do
    read -p "Enter name for usr $i: " username
    sudo useradd "$username"
    echo "User $username created."
    read -sp "enter pass for $username: " password
    echo
    echo "$username:$password" | sudo chpasswd
    echo "user $username created"
done

sysadmin@ubuntusrv:~$ scp user.sh sysadmin@192.168.1.2:/home/sysadmin/
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA key fingerprint is c2:0d:ff:27:4c:f8:69:a9:c6:3e:13:da:2f:47:e4:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.2' (RSA) to the list of known hosts.
sysadmin@192.168.1.2's password:
user.sh                                100% 320    0.3KB/s   00:00
sysadmin@ubuntusrv:~$
```

- On the Ubuntu Workstation, log on as Superman
- From Ubuntu Workstation SSH to Ubuntu server Batman
 - from here, SSH to the CentOS server Wonderwoman
 - from here, SSH to the Fedora workstation theflash
- From Ubuntu Workstation, as Blackwidow ssh to Ubuntu server as Ironman
 - from here, SSH to the CentOS server as Hulk
 - from here, SSH to fedora workstation as Spiderman
- on the Fedora Workstation
 - kill the Spiderman connection
 - show connections

```
[root@localhost sysadmin]# who
sysadmin :0          2024-11-19 02:52
sysadmin pts/0       2024-11-19 02:52 (:0)
sysadmin pts/1       2024-11-19 02:54 (:0)
theflash pts/2       2024-11-19 03:20 (example.com)
[root@localhost sysadmin]# echo I used pkill -u spiderman to kick him off
I used pkill -u spiderman to kick him off
[root@localhost sysadmin]# █
```

- on the centos server
 - kill the Hulk connection
 - show connections

```
File Edit View Scrollback Bookmarks Settings Help
[root@localhost sysadmin]# who
sysadmin tty1          2024-11-19 00:54 (:0)
sysadmin pts/0         2024-11-19 00:55 (:0.0)
wonderwoman pts/1      2024-11-19 02:18 (udesktop.example.com)
hulk pts/2             2024-11-19 02:23 (udesktop.example.com)
[root@localhost sysadmin]# pkill -u hulk
[root@localhost sysadmin]# who
sysadmin tty1          2024-11-19 00:54 (:0)
sysadmin pts/0         2024-11-19 00:55 (:0.0)
wonderwoman pts/1      2024-11-19 02:18 (udesktop.example.com)
[root@localhost sysadmin]# █
```

- on the Ubuntu server
 - kill the Batman connection
 - show connections

```
sysadmin@ubuntusrv:~$ who
sysadmin tty1          2024-11-19 00:41
batman pts/0           2024-11-19 02:17 (192.168.1.5)
ironman pts/1          2024-11-19 02:21 (192.168.1.3)
sysadmin@ubuntusrv:~$ sudo pkill -u batman
[sudo] password for sysadmin:
sysadmin@ubuntusrv:~$ who
sysadmin tty1          2024-11-19 00:41
ironman pts/1          2024-11-19 02:21 (192.168.1.3)
sysadmin@ubuntusrv:~$
```

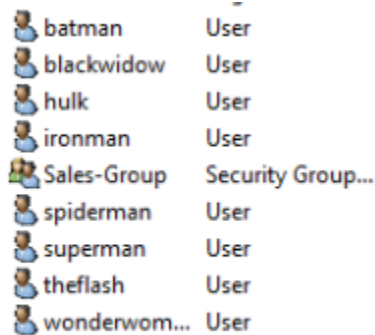
****5 points extra credit to authenticate on all systems. with public/private keys. Also known as key based authentication****

Part C: Windows Connections: [Netlab 3](#)

[Links to an external site.](#), MCSA 70-740: Configure Windows Server2016

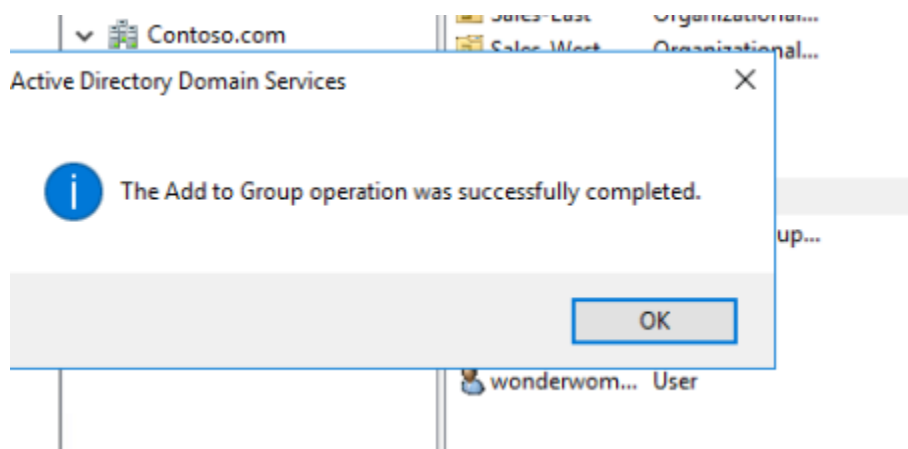
- Log on to all systems
- Add the below users to all systems
- superman, batman, Wonderwoman, theflash, Ironman, Hulk, Spiderman, Blackwidow

Hopefully, you don't mind, but instead of making users on all the commuters separate, I joined them all to the same domain! (got to love server class)

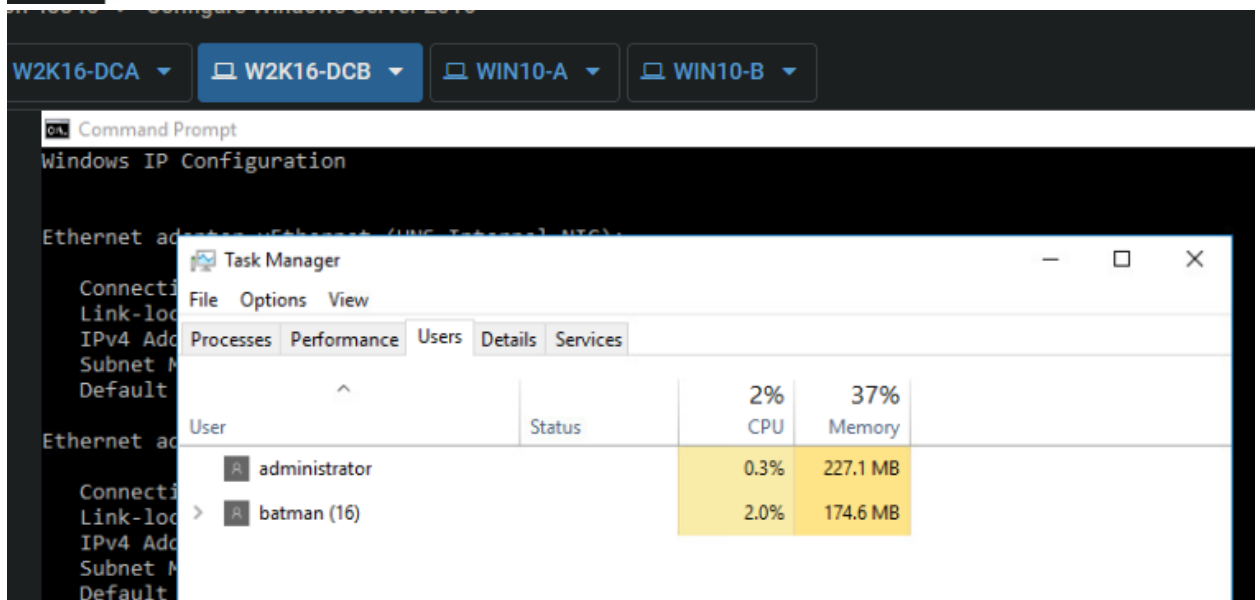
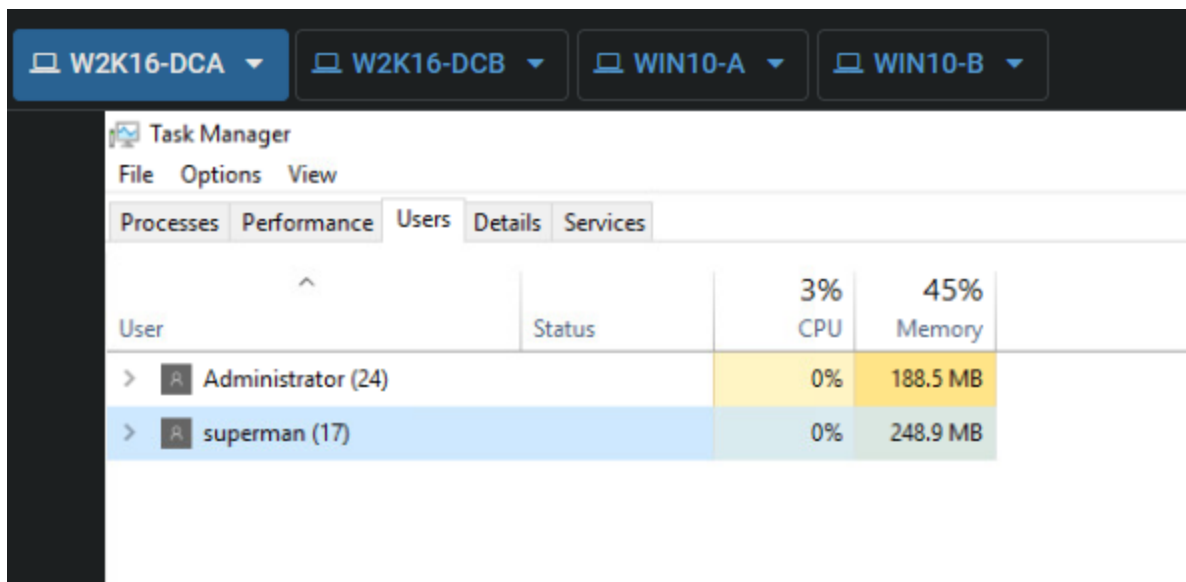


batman	User
blackwidow	User
hulk	User
ironman	User
Sales-Group	Security Group...
spiderman	User
superman	User
theflash	User
wonderwom...	User

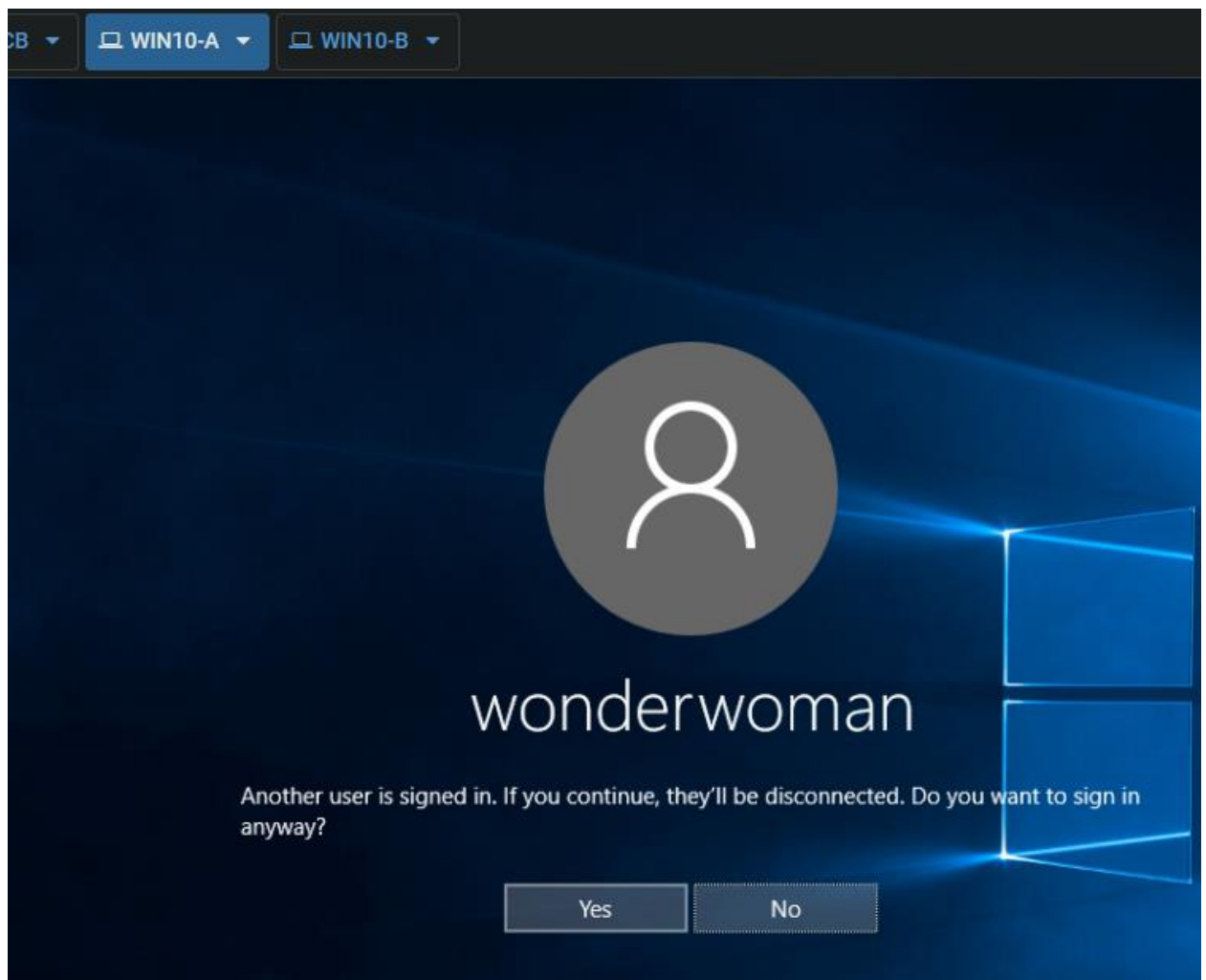
- Promote Superman and Ironman to admin on all systems
I then added ironman and superman to the admin group



- from Win10-PCA RDP to w2k16-DCA
- from here, RDP to w2k16-DCB
- from here, RDP to Win10-PCB
- from here, RDP to Win1-PCA (this last one disconnected me)
- log onto all systems, and show all connections within the Task Manager



I get my users logged out so I am unable to show more the on user for PCB and PCA



I used partially admin to RDP because of an issue with local login in domains.

- Log on to Win10-PCA and disconnect the Win10-PCB connection from within the Task Manager
- Log onto w2k16-DCB and disconnect the w2k16DCA connection from within the Task Manager
- Log onto all systems and show all of the connections via the command line or PowerShell

```
C:\Users\Administrator.CITCV2-SERVER>query user
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
administrator	console	1	Active	none	11/19/2024 8:47 AM
superman	rdp-tcp#6	2	Active	2	11/19/2024 9:20 AM

```
C:\Users\Administrator.CITCV2-SERVER>_
```

```
C:\Windows\system32>
```

```
C:\Windows\system32>query user
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
hulk		1	Disc	21	11/19/2024 12:04 PM
administrator	rdp-tcp#8	2	Active	.	11/19/2024 12:38 PM

```
C:\Windows\system32>_
```

```
C:\Windows\system32>query user
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
hulk		1	Disc	22	11/19/2024 12:04 PM
administrator	rdp-tcp#8	2	Active	.	11/19/2024 12:38 PM

```
C:\Windows\system32>logoff 1
```

```
C:\Windows\system32>query user
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
administrator	rdp-tcp#8	2	Active	.	11/19/2024 12:38 PM

```
C:\Windows\system32>
```

- Disconnect all connections from the Firewall on each system

I turned off all IN RDP allow rules in my firewall and it eventually disconnected


```
logins is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator.CITCV2-SERVER>query-user
'query-user' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator.CITCV2-SERVER>query user
USERNAME      SESSIONNAME    ID  STATE  IDLE TIME  LOGON TIME
>administrator console          1  Active   none      11/19/2024 8
:47 AM
>superman      rdp-tcp#6      2  Active   2         11/19/2024 9
:20 AM

C:\Users\Administrator.CITCV2-SERVER>query user
USERNAME      SESSIONNAME    ID  STATE  IDLE TIME  LOGON TIME
>administrator console          1  Active   none      11/19/2024 8
:47 AM
>superman      rdp-tcp#6      2  Active   5         11/19/2024 9
:20 AM

C:\Users\Administrator.CITCV2-SERVER>query user
USERNAME      SESSIONNAME    ID  STATE  IDLE TIME  LOGON TIME
>administrator console          1  Active   none      11/19/2024 8
:47 AM
>superman      rdp-tcp#6      2  Active   5         11/19/2024 9
:20 AM

C:\Users\Administrator.CITCV2-SERVER>query user
USERNAME      SESSIONNAME    ID  STATE  IDLE TIME  LOGON TIME
>administrator console          1  Active   none      11/19/2024 8
:47 AM
>superman      rdp-tcp#6      2  Active   5         11/19/2024 9
:20 AM

C:\Users\Administrator.CITCV2-SERVER>query user
USERNAME      SESSIONNAME    ID  STATE  IDLE TIME  LOGON TIME
>administrator console          1  Active   none      11/19/2024 8
:47 AM
>superman      rdp-tcp#6      2  Disc    .         11/19/2024 9
:20 AM

C:\Users\Administrator.CITCV2-SERVER>
```

Windows Firewall with Advanced Security

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Inbound Rules

Filtered by: Remote...

Name

Remote Desktop - Shadow (TCP-I

Remote Desktop - User Mode (TCI

Remote Desktop - User Mode (UD

Inbound

New

Filter

Filter

Filter

Clear

View

Refresh

Export

Help

****5 points extra credit to authenticate using PowerShell, and drop users with PowerShell****