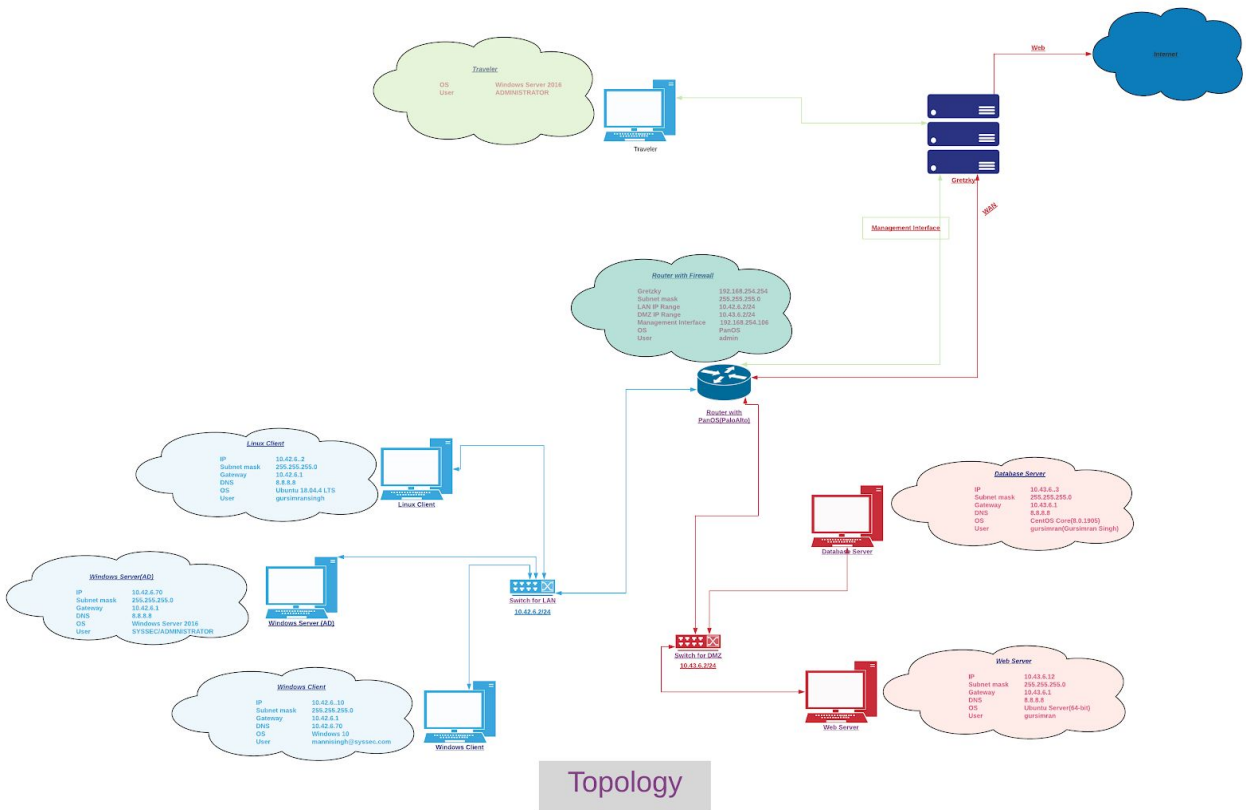
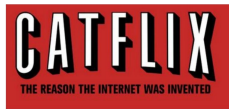


Final Project - CatFlix

Final Project - CatFlix	1
Task 1	2
Task 2	3
Task 3	16

Task 1





Task 2

Windows

IPs

Windows_10

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+De

```
Microsoft Windows [Version 10.0.18240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Gursimran>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a021:70b1:9770:41e3
    IPv4 Address. . . . . : 10.42.6.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.42.6.1

Tunnel adapter isatap.{304F1DF2-CF6A-49D4-8741-01C286A4B966}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Gursimran>
```

Windows_Server

Enforce US Keyboard Layout View Fullscreen Send Ctrl

```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

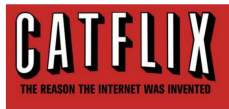
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9cb4:d9dc:54d:8727K3
    IPv4 Address. . . . . : 10.42.6.70
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.42.6.1

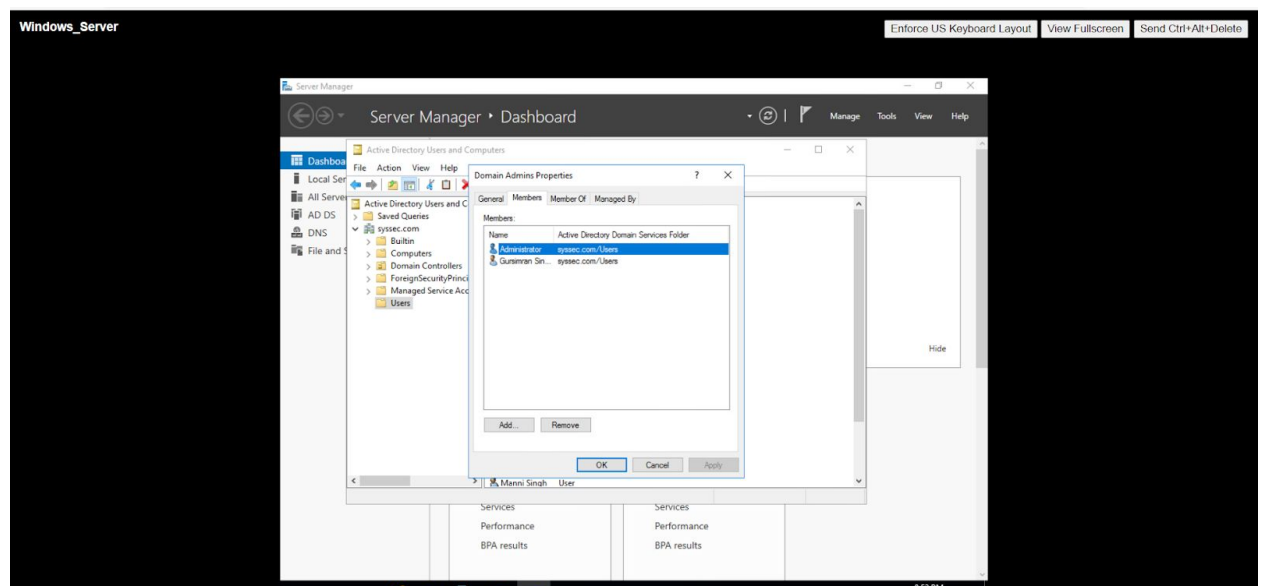
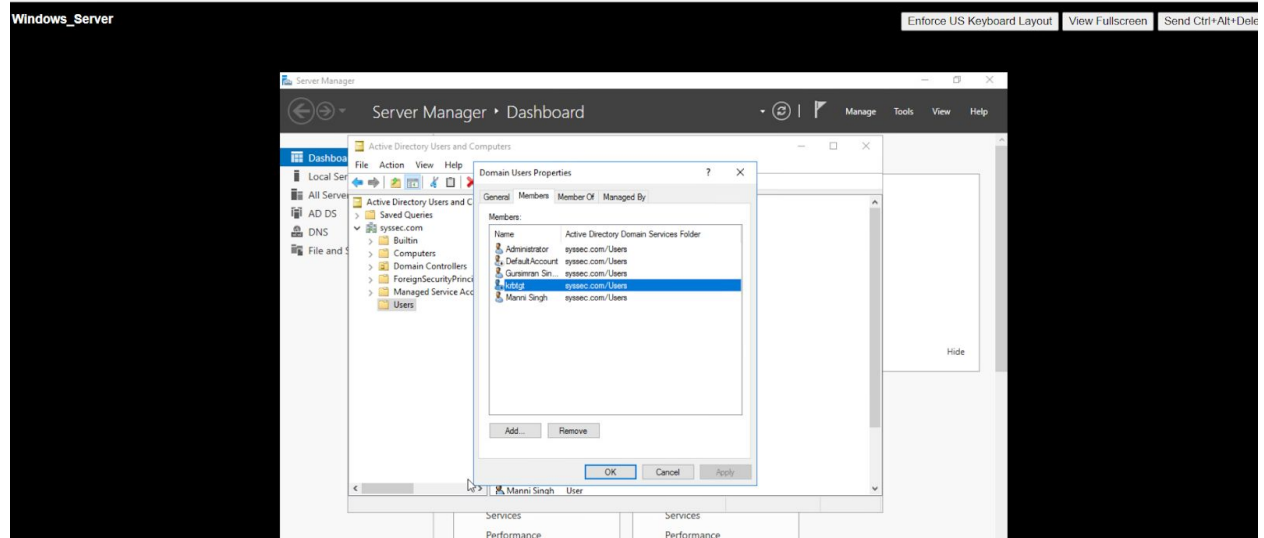
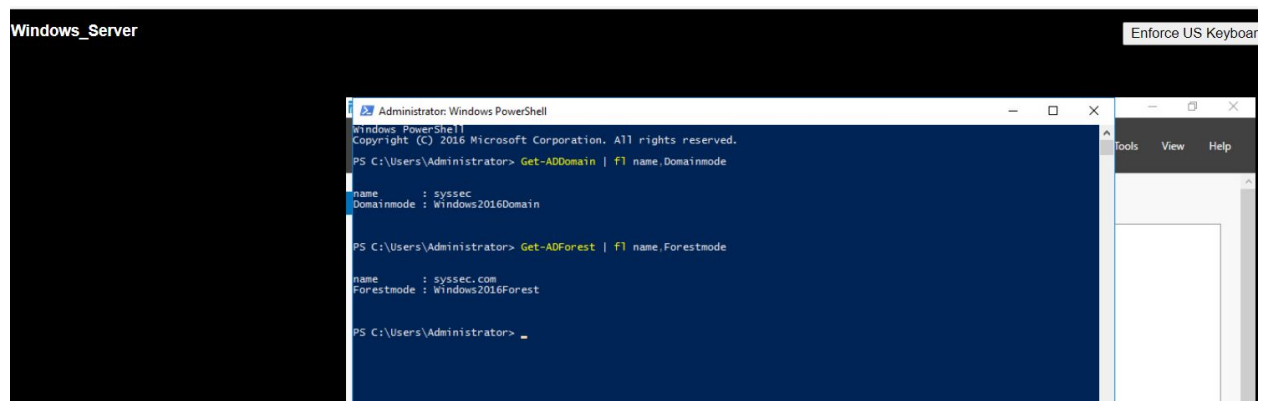
Tunnel adapter isatap.{AB7ED709-E648-4AE3-97E2-BCA40F47539B}:

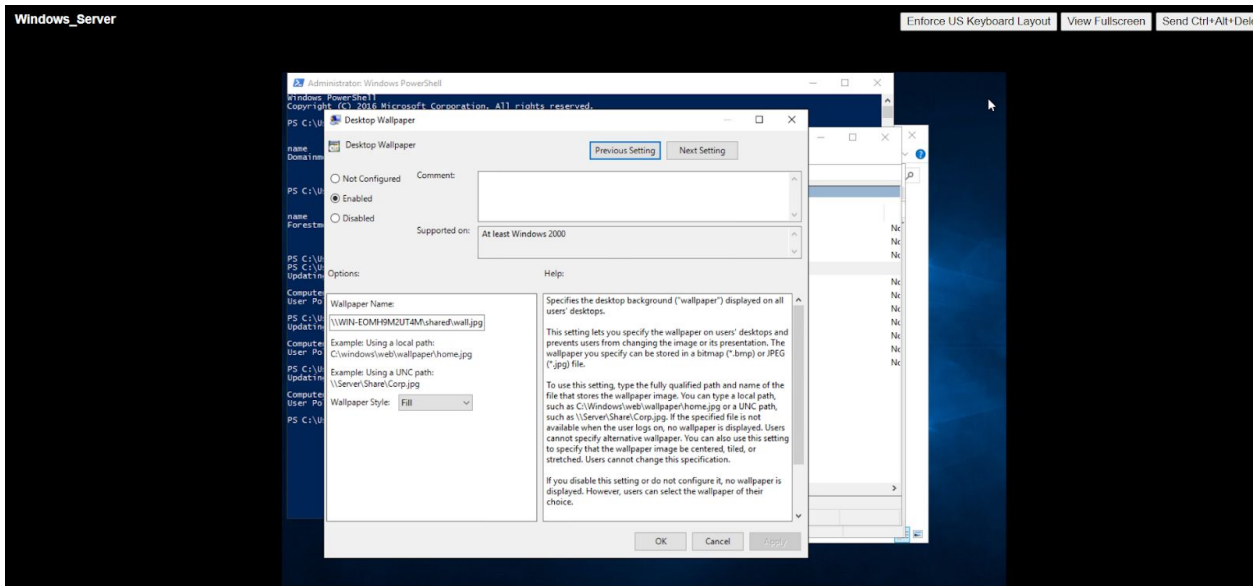
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

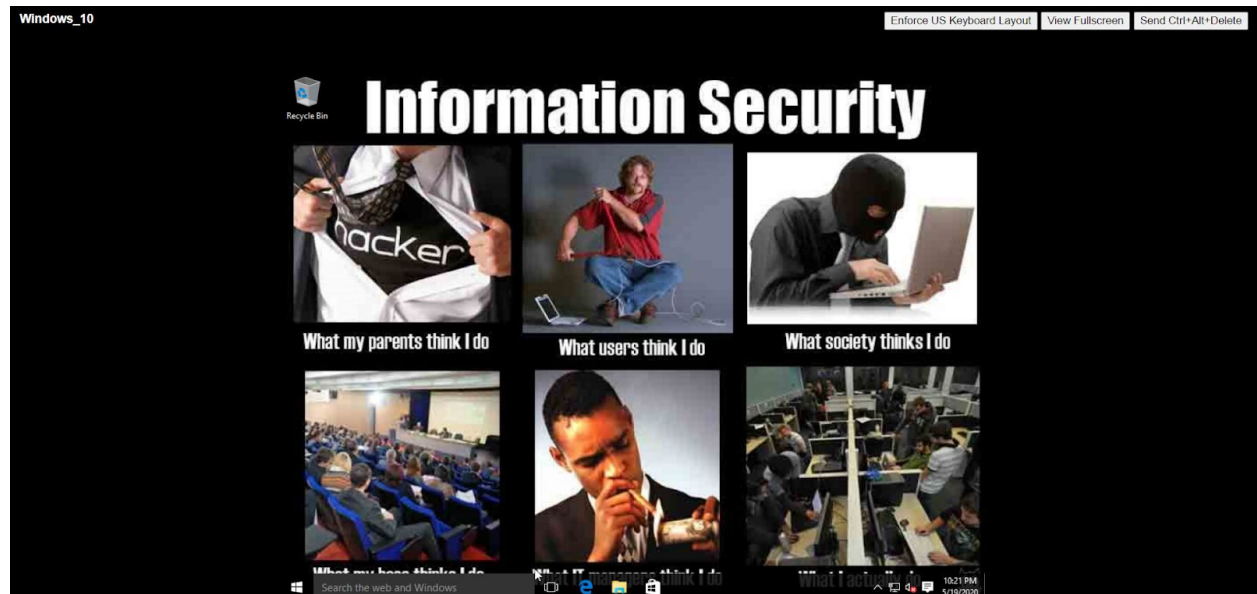
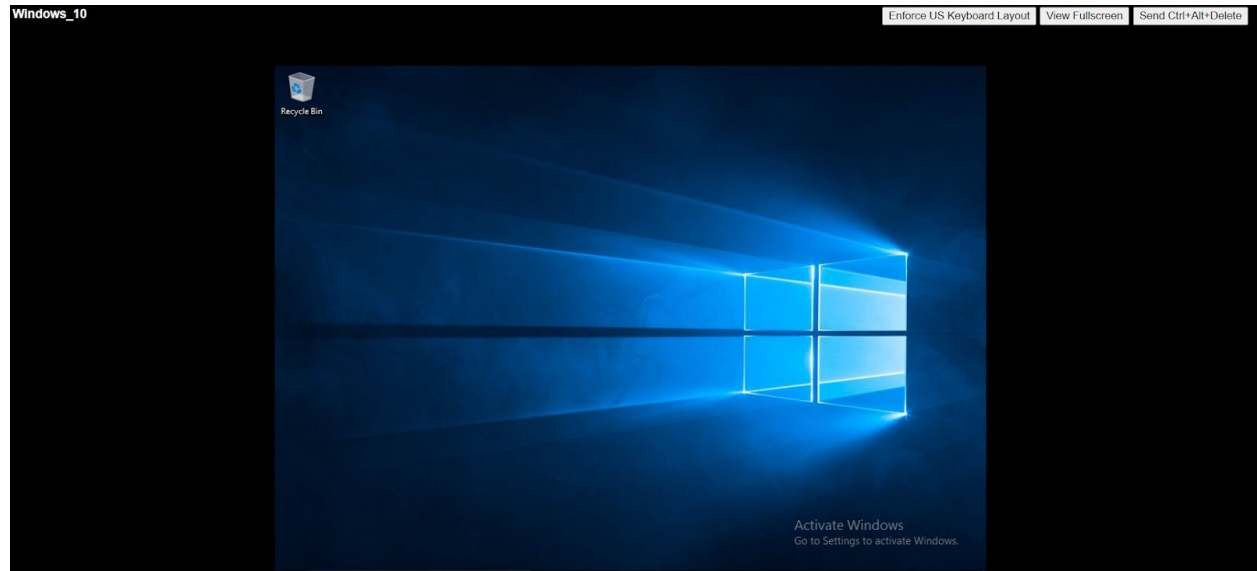
C:\Users\Administrator>
```

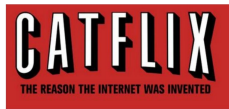


Windows Group Policy Implementation

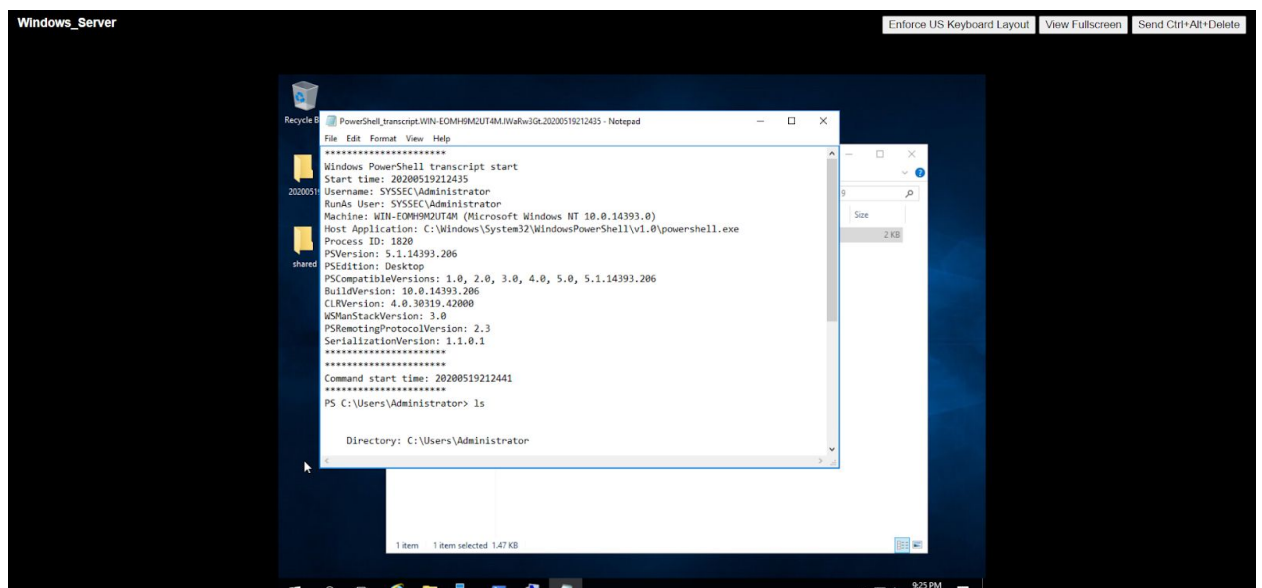
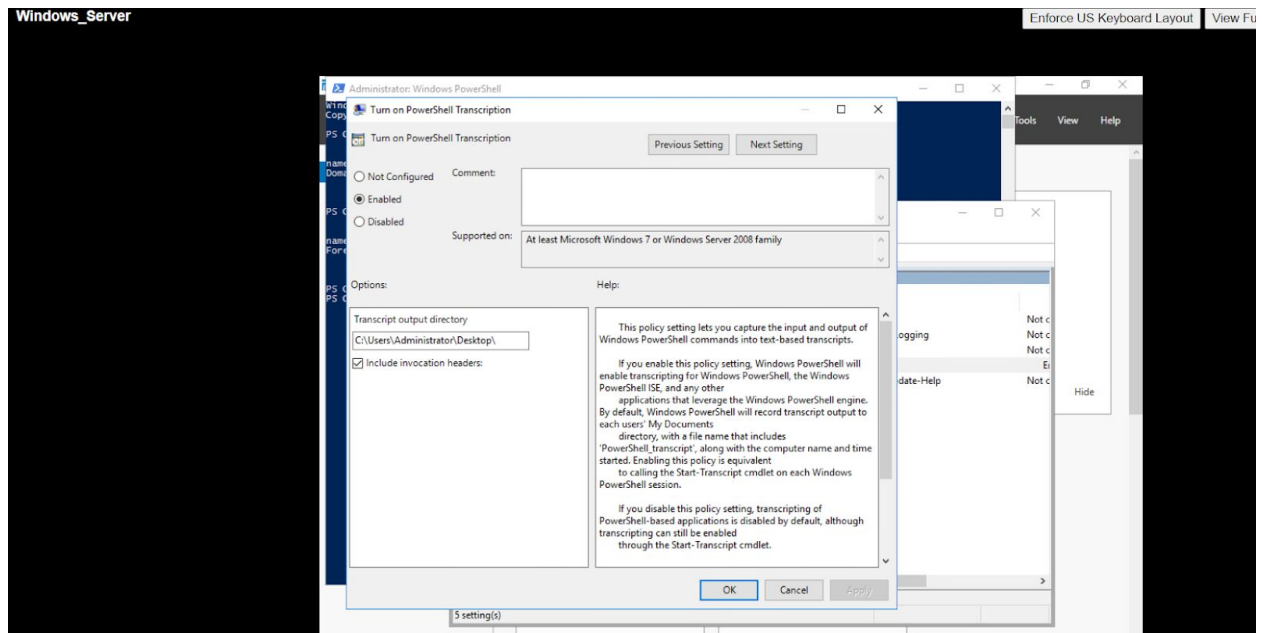








Powershell Transcripts





Linux(LAMP Stack)

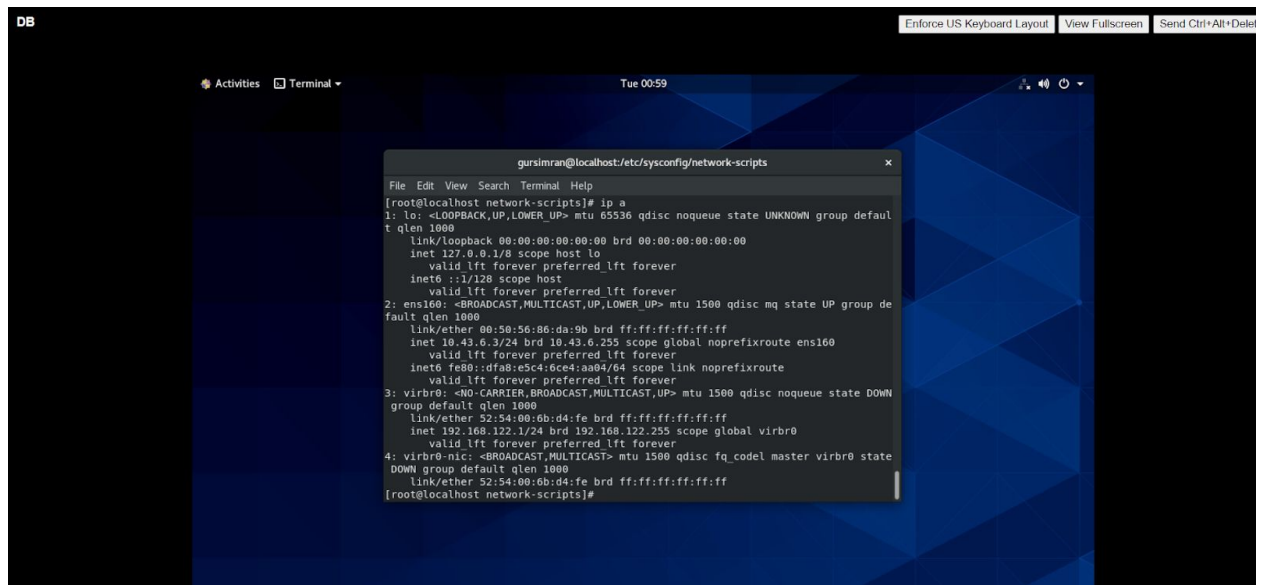
IPs

```
Linux_Client

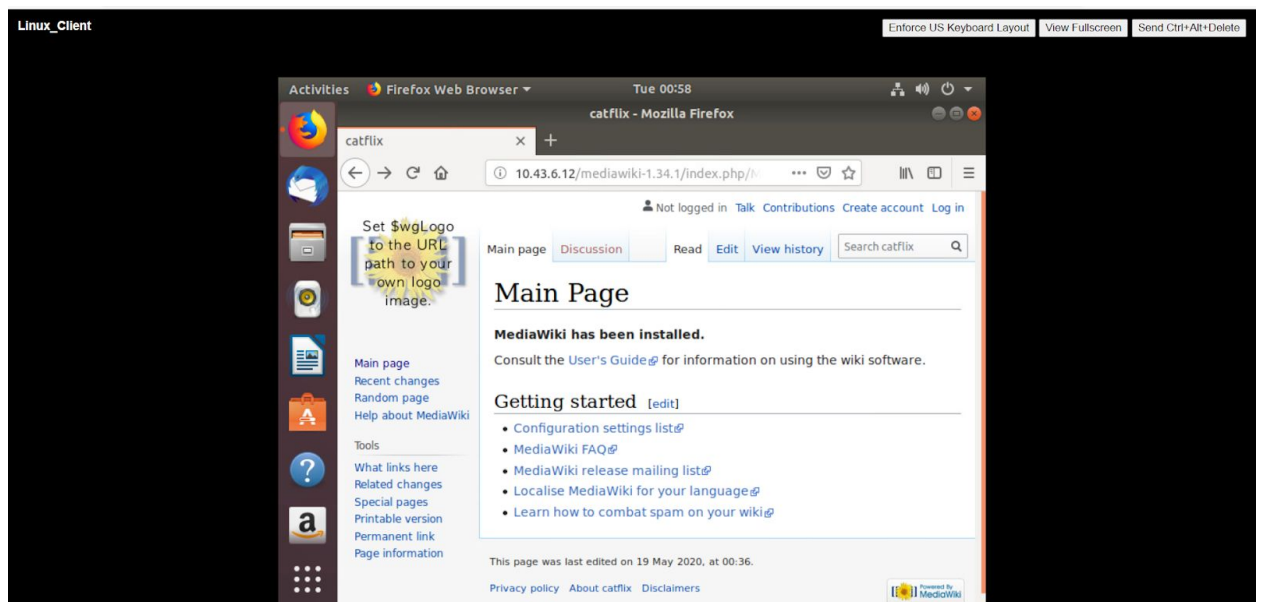
gursimran@gursimran-virtual-machine: ~
netns | l2tp | fou | macsec | tcp_metrics | token | netconf
| tlla |
vrf | sr }
OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
-h[uman-readable] | -iec |
-f[amily] { inet | inet6 | ipx | dnet | npls | bridge | lin
k } |
-4 | -6 | -I | -D | -B | -0 |
-l[oops] { maximum-addr-flush-attempts } | -br[ief] |
-o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename]
|
-rc[vbuf] [size] | -n[etns] name | -a[ll] | -c[olor]}
gursimran@gursimran-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
    link/ether 00:50:56:86:87:32 brd ff:ff:ff:ff:ff:ff
    inet 10.42.6.2/24 brd 10.42.6.255 scope global nopreflxroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::c0df:8013:4125:1fef/64 scope link nopreflxroute
        valid_lft forever preferred_lft forever
gursimran@gursimran-virtual-machine:~$
```

```
WEB

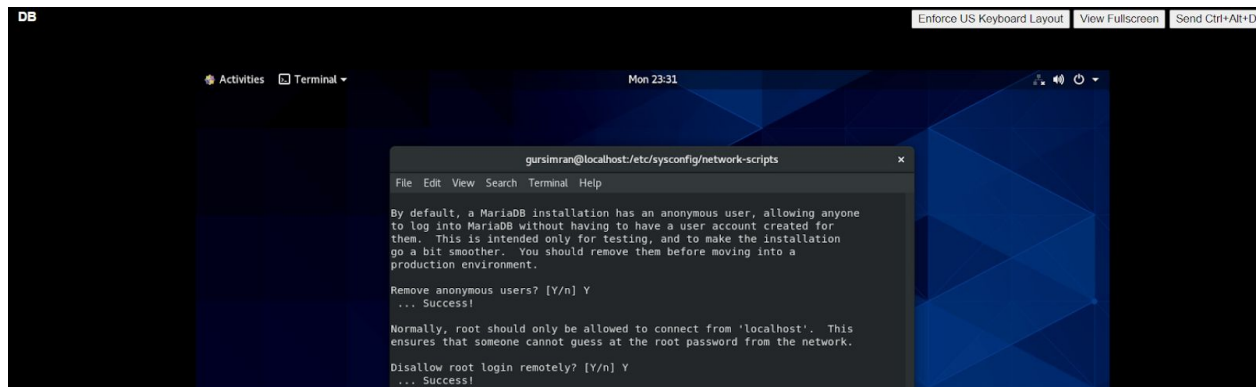
gursimran@gursimran:/home$ ls
gursimran
gursimran@gursimran:/home$ sudo mkdir gursimransingh
gursimran@gursimran:/home$ sudo chown gursimransingh: gursimransingh
gursimran@gursimran:/home$ sudo passwd gursimransingh
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
gursimran@gursimran:/home$ cd gursimransingh/
gursimran@gursimran:/home/gursimransingh$ ls
LocalSettings.php
gursimran@gursimran:/home/gursimransingh$ sudo mv LocalSettings.php /var/www/html/mediawiki-1.34.1/
gursimran@gursimran:/home/gursimransingh$ ls
gursimran@gursimran:/home/gursimransingh$ cd /var/www/html/mediawiki-1.34.1/
gursimran@gursimran:/var/www/html/mediawiki-1.34.1$ ls
api.php          desc            index.php       opensearch_desc.php  skins
cache            extensions      INSTALL         package-lock.json    tests
CODE_OF_CONDUCT.md  FAQ            jsduck.json     profileinfo.php       thumb_handler.php
composer.json      HISTORY        languages       README                thumb.php
composer.local.json-sample  images         load.php        RELEASE-NOTES-1.34   UPGRADE
COPYING           img_auth.php   LocalSettings.php  resources              vendor
CREDITS           include        maintenance     rest.php              SECURITY
gursimran@gursimran:/var/www/html/mediawiki-1.34.1$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:86:40:cf brd ff:ff:ff:ff:ff:ff
    inet 10.43.6.12/24 brd 10.43.6.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe86:d0cf/64 scope link
        valid_lft forever preferred_lft forever
gursimran@gursimran:/var/www/html/mediawiki-1.34.1$
```

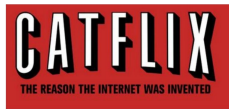



Mediawiki



Security Detail





Palo Alto

Interface Management

```
PaloAlto

-----
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 10000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:50:56:86:5f:a0

Ip address: 192.168.254.106
Netmask: 255.255.255.0
Default gateway: 192.168.254.254
Ipv6 address: unknown
Ipv6 link local address: fe80::250:56ff:fe86:5fa0/64
Ipv6 default gateway:
-----

Logical interface counters:
-----
bytes received          32816
bytes transmitted      452
lines 1-24
```

Config and Basic Implementation

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM Apache2 Ubuntu Default Page: It x +

192.168.254.106/7#network/vsys1:network/zones

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Interfaces

Zones

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

DNS Proxy

GlobalProtect

Portals

Gateways

MDM

Device Block List

Clientless Apps

Clientless App Groups

QoS

LLDP

Network Profiles

GlobalProtect IPSec Cr

IKE Gateways

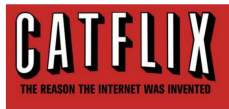
IPSec Crypto

TKP Crypto

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	Included Networks	Excluded Networks
dmc	layer3	ethernet1/3				<input type="checkbox"/>	any	none
lan	layer3	ethernet1/2				<input type="checkbox"/>	any	none
outside	layer3	ethernet1/1				<input type="checkbox"/>	any	none

admin | Logout | Last Login Time: 05/18/2020 22:04:26

Tasks | Logout



Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM Apache2 Ubuntu Default Page: // x +

Not secure 192.168.254.106/?#networkcvsys1:network/interfaces

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Help

Interfaces

Ethernet VLAN Loopback Tunnel

9 items

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3		Dynamic DHCP Client		default	Untagged	none	outside		
ethernet1/2	Layer3			10.42.6.1/24	default	Untagged	none	lan		
ethernet1/3	Layer3			10.43.6.1/24	default	Untagged	none	dmz		
ethernet1/4			none		none	Untagged	none	none		
ethernet1/5			none		none	Untagged	none	none		
ethernet1/6			none		none	Untagged	none	none		
ethernet1/7			none		none	Untagged	none	none		
ethernet1/8			none		none	Untagged	none	none		
ethernet1/9			none		none	Untagged	none	none		

Add Subinterface Delete PDF/CSV

admin | Logout | Last Login Time: 05/18/2020 22:04:26

5:59 AM 5/19/2020

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM Apache2 Ubuntu Default Page: // x +

Not secure 192.168.254.106/?#networkcvsys1:network/virtual-routers

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Help

Virtual Router - default

Router Settings Static Routes Redistribution Profile RIP OSPF OSPFv3 BGP Multicast

IPv4 IPv6

1 item

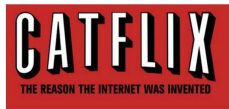
Name	Destination	Interface	Type	Next Hop Value	Admin Distance	Metric	BFD	Route Table
default	0.0.0.0/0	ethernet1/1	ip-address	192.168.254.254	default	10	None	unicast

Add Delete Name

OK Cancel

admin | Logout | Last Login Time: 05/18/2020 22:04:26

6:00 AM 5/19/2020



Traveler Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM Apache2 Ubuntu Default Page: 192.168.254.106/?#policies:vsys1:policies/nat-rulebase

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection

Policy Optimizer

- Rule Usage
- Unused in 30 days
- Unused in 90 days
- Unused

Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count
1 source web	none	dmz	outside	any	10.43.6.12	any	any	static-ip 192.168.254.166	none	136
2 source data	none	dmz	outside	any	10.43.6.3	any	any	static-ip 192.168.254.136	none	456
3 dest web	none	outside	outside	any	any	192.168.254.166	any	none	destination-translation address: 10.43.6.12	15
4 dest data	none	outside	outside	any	any	192.168.254.136	any	none	destination-translation address: 10.43.6.3	11
5 out dynamic	none	lan	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none	1494

Object: Addresses

Add Delete Clone Enable Disable Move PDF/CSV Highlight Unused Rules Reset Rule Hit Counter View Rulebase as Groups Test Policy Match

Traveler Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

PA-VM Apache2 Ubuntu Default Page: 192.168.254.106/?#policies:vsys1:policies/security-rulebase

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection

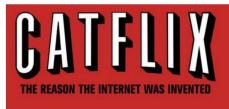
Policy Optimizer

- No App Specified
- Unused Apps
- Rule Usage
- Unused in 30 days
- Unused in 90 days
- Unused

Name	Tags	Type	Zone	Address	User	HPD Profile	Zone	Address	Application	Service	Action	Profile
1 block ssh web	none	universal	outside	any	any	any	any	192.168.254.166	ssh	application-d...	Deny	none
2 block ssh db	none	universal	outside	any	any	any	any	192.168.254.136	ssh	application-d...	Deny	none
3 block ping db	none	universal	outside	any	any	any	any	192.168.254.136	ping	application-d...	Deny	none
4 block ping web	none	universal	outside	any	any	any	any	192.168.254.166	ping	application-d...	Deny	none
5 default	none	universal	any	any	any	any	any	any	any	application-d...	Allow	none
6 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none
7 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none

Object: Addresses

Add Delete Clone Override Repeat Enable Disable Move PDF/CSV Highlight Unused Rules Reset Rule Hit Counter View Rulebase as Groups Test Policy Match




Traveler

Enforce US Keyboard LayoutView FullscreenSend Ctrl+Alt+Delete

PA-VM

Apache2 Ubuntu Default Page

Not secure | 192.168.254.166



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|-- ...  
|-- ...
```


Traveler

Enforce US Keyboard LayoutView FullscreenSend Ctrl+Alt+Delete

PA-VM

Administrator: Command Prompt

Not secure | 192.168.254.166



paloo

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection

Policy Optimizer

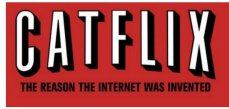
- Rule Usage
- Unused in 30
- Unused in 90
- Unused

```
C:\Users\Administrator>ping 192.168.254.136  
  
Pinging 192.168.254.136 with 32 bytes of data:  
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62  
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62  
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62  
Reply from 192.168.254.136: bytes=32 time=2ms TTL=62  
  
Ping statistics for 192.168.254.136:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 2ms, Maximum = 2ms, Average = 2ms  
  
C:\Users\Administrator>
```

CommitConfigSearch

5 items

Source Translation	Destination Translation	Hit Count
static-ip	none	130
192.168.254.166	none	435
static-ip	none	0
192.168.254.136	destination-translation address: 10.43.6.12	0
static-ip	destination-translation address: 10.43.6.3	0
dynamic-ip-and-port	none	1452
hermet1/1		



Security Blocks

Traveler

Enforce US Keyboard Layout View Fullscreen Send Ctrl

PA-VM Administrator: Command Prompt

```
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
C:\Users\Administrator>ssh gursimran@192.168.254.166
C:\Users\Administrator>ssh gursimran@192.168.254.136
The authenticity of host '192.168.254.136 (192.168.254.136)' can't be established.
ECDSA key fingerprint is SHA256:VBqEe6pFXsI2VqI76shPeWVb08NyxHzXDScLcYhZeJM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.254.136' (ECDSA) to the list of known hosts.
gursimran@192.168.254.136's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon May 18 22:25:53 2020
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon May 18 22:25:53 2020
[gursimran@localhost ~]$ exit
logout
Connection to 192.168.254.136 closed.

C:\Users\Administrator>ssh gursimran@192.168.254.136
C:\Users\Administrator>ping 192.168.254.136

Pinging 192.168.254.136 with 32 bytes of data:
Control-C
C:\Users\Administrator>ping 8.8.8.8
```

/etc/apache2/

Traveler IP

Traveler

Enforce US Keyboard Layout View

PA-VM Administrator: Command Prompt

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : cse.buffalo.edu
    Link-local IPv6 Address . . . . . : fe80::7c81:6448:a745:4998%4
    IPv4 Address. . . . . : 192.168.13.176
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 192.168.0.1

C:\Users\Administrator>
```

paloma

Security

NAT

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Policy Optimizer

No App Specified

Unused Apps

Rule Usage

Unused in 30

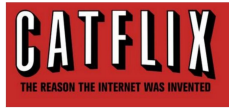
Unused in 90

Unused

Application	Service
254.166	ssh
254.136	ssh
254.136	ping
254.166	ping
any	any
any	any
any	any

Object: Addresses

Add Delete Clone Override Revert Enable Disable Move PDF/CSV Highlight Unused Rules Reset Rule Hit Counter Group View Rulebase as Groups Test Policy Match



Task 3

Hardware Inventory list

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Devices (BYOD) which might be out of synch with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. But attackers have shown the ability, patience, and willingness to "inventory and control" our assets at very large scale in order to support their opportunities.

Managed control of all devices also plays a critical role in planning and executing system backup, incident response, and recovery.

Name	Category	IP	MAC	OS
Windows Server	Domain Controller, AD	10.42.6.70	00-50-56-86-7d-2b	Windows Server 2016
Windows Client	Client	10.42.6.10	00-50-56-86-3c-a7	Windows 10
Linux Client	Client	10.42.6.2	00-50-56-86-87-32	Ubuntu 18.04.4 LTS
WEB	Web Server	10.43.6.12	00-50-56-86-d0-cf	Ubuntu Server



DB	Database Server	10.43.6.3	00-50-56-86-da-9b	CentOS Core(8.0.1905)
Palo Alto	Router , Firewall	MI - 192.168.254.106 ,10.42.6.1, 10.43.6.1	00-50-56-86-d3-78 00-50-56-86-49-db	PanOS
Traveler	Client, Outside	192.168.13.176	00-50-56-86-53-ce	Windows Server 2016

Finding MAC

```
PS C:\Users\Administrator> arp -a

Interface: 10.42.6.70 --- 0x3
Internet Address      Physical Address      Type
10.42.6.1             00-50-56-86-d3-78     dynamic
10.42.6.2             00-50-56-86-87-32     dynamic
10.42.6.10            00-50-56-86-3c-a7     dynamic
10.42.6.255           ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\Users\Administrator>
```

```
[root@localhost network-scripts]# arp
Address                HWtype  HWaddress           Flags Mask          Iface
10.43.6.12             ether   00:50:56:86:d0:cf   C                   ens16
0
_gateway              ether   00:50:56:86:49:d8   C                   ens16
0
[root@localhost network-scripts]#
```

```
gursimransingh@gursimran-virtual-machine:~/Downloads$ arp
Address                HWtype  HWaddress           Flags Mask          Ifac
10.42.6.70             ether   00:50:56:86:7d:2b   C                   ens1
50
10.42.6.10             ether   00:50:56:86:3c:a7   C                   ens1
50
_gateway              ether   00:50:56:86:d3:78   C                   ens1
50
```



```
gursimran@localhost:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help
[root@localhost network-scripts]# ifconfig -a
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.43.6.3  netmask 255.255.255.0  broadcast 10.43.6.255
    inet6 fe80::dfa8:e5c4:6ce4:aa04  prefixlen 64  scopeid 0x20<link>
    ether 00:50:56:86:da:9b  txqueuelen 1000  (Ethernet)
    RX packets 714251  bytes 937836091 (894.3 MiB)
    RX errors 0  dropped 364  overruns 0  frame 0
    TX packets 98297  bytes 12016949 (11.4 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 15  bytes 1254 (1.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 15  bytes 1254 (1.2 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
```

```
Administrator: Command Prompt
Host Name . . . . . : WIN-2HV9DA4P6S0
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cse.buffalo.edu

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . : cse.buffalo.edu
    Description . . . . . : vmxnet3 Ethernet Adapter
    Physical Address. . . . . : 00-50-56-86-53-CE
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::7c81:6448:a745:4998%4(Preferred)
    IPv4 Address. . . . . : 192.168.13.176(Preferred)
    Subnet Mask . . . . . : 255.255.240.0
    Lease Obtained. . . . . : Tuesday, May 19, 2020 5:24:14 AM
    Lease Expires . . . . . : Wednesday, May 20, 2020 3:24:14 AM
    Default Gateway . . . . . : 192.168.0.1
    DHCP Server . . . . . : 192.168.0.1
    DHCPv6 IAID . . . . . : 100683862
    DHCPv6 Client DUID. . . . . : 00-01-00-01-26-55-19-70-00-50-56-86-53-CE
    DNS Servers . . . . . : 192.168.0.2
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

Software Inventory list

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet



been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

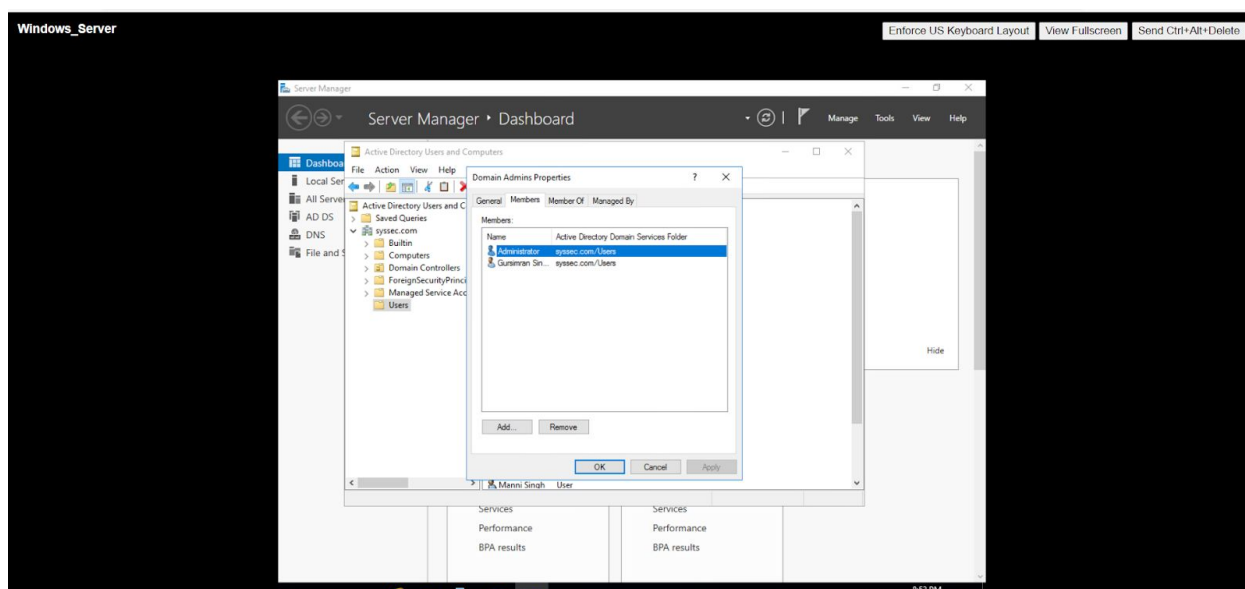
Managed control of all software also plays a critical role in planning and executing system backup, incident response, and recovery.

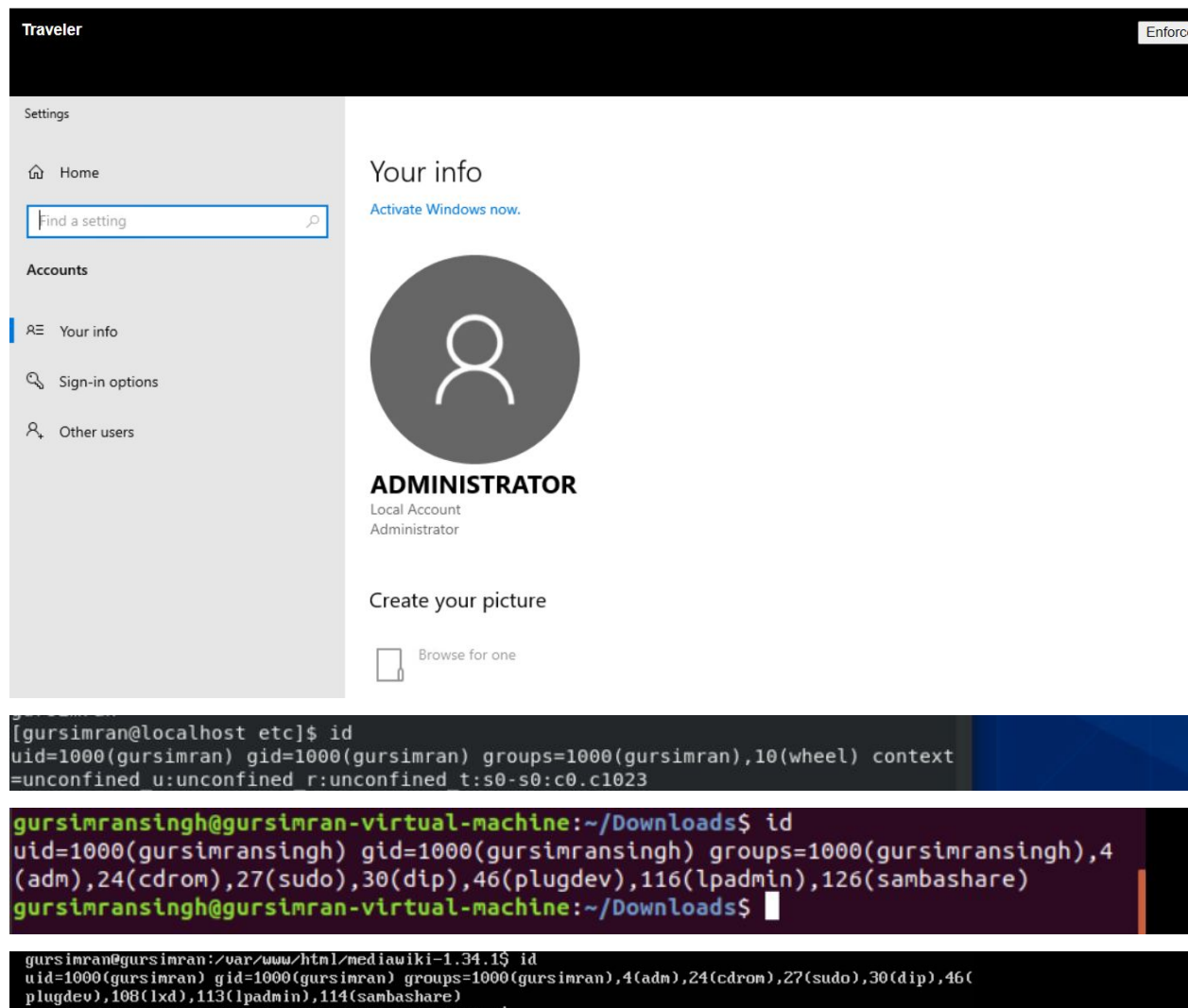
<u>Name</u>	<u>Category</u>	<u>Use</u>	<u>Usage</u>
Apache2	WebServer	Hosting HTTP Server	WebServer
Mediawiki	WebService	Software App	WebServer
MariaDB	Database	Maintaining DB for WebServer	Database
net-tools	Network tools	Used for Networking tasks like ifconfig, arp, etc	Linux Client

Controlled use of Admin Privileges

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user, is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrative passwords and other sensitive data. Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

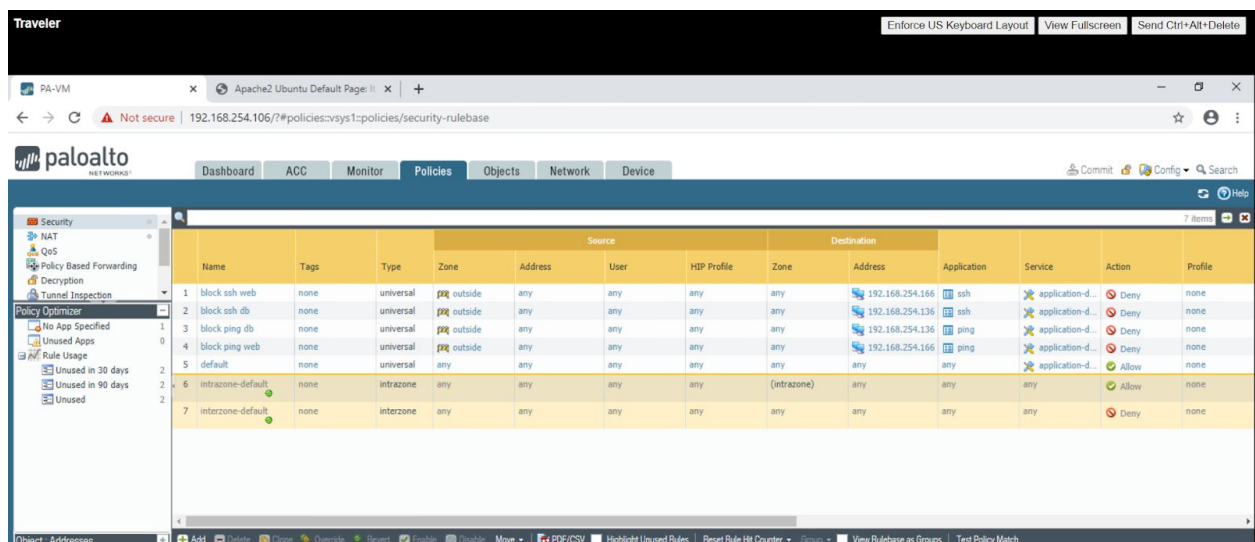
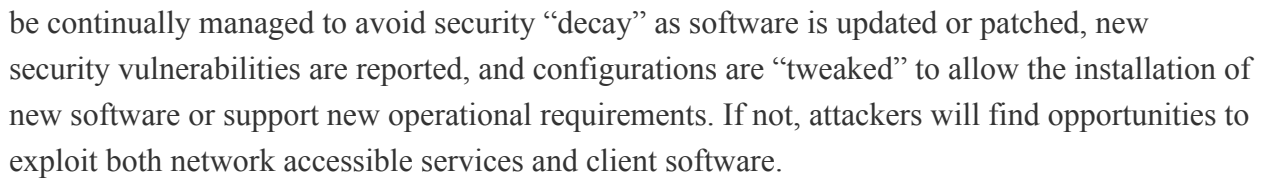




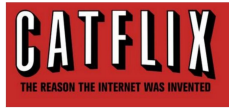
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, preinstallation of unneeded software; all can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tool section below provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it must



Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details



of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.



DB

Enforce US Keyboard Layout View Fullscreen Send

```
File Edit View Search Terminal Help
--destination-port 67 --jump ACCEPT' failed: iptables: Bad rule (does a matching rule exist in that chain?).

[gursimran@localhost log]$ sudo cat firewallld
2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table mangle --delete POSTROUTING --out-interface virbr0 --protoc
ol udp --destination-port 68 --jump CHECKSUM --checksum-fill' failed: iptables: Bad rule (does a matching rule exist in that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table nat --delete POSTROUTING --source 192.168.122.0/24 --destin
ation 224.0.0.0/24 --jump RETURN' failed: iptables: Bad rule (does a matching rule exist in that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table nat --delete POSTROUTING --source 192.168.122.0/24 --destin
ation 255.255.255.255/32 --jump RETURN' failed: iptables: Bad rule (does a matching rule exist in that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table nat --delete POSTROUTING --source 192.168.122.0/24 -p tcp !
--destination 192.168.122.0/24 --jump MASQUERADE --to-ports 1024-65535' failed: iptables: Bad rule (does a matching rule exist in that chai
n?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table nat --delete POSTROUTING --source 192.168.122.0/24 -p udp !
--destination 192.168.122.0/24 --jump MASQUERADE --to-ports 1024-65535' failed: iptables: Bad rule (does a matching rule exist in that chai
n?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table nat --delete POSTROUTING --source 192.168.122.0/24 --dest
ination 192.168.122.0/24 --jump MASQUERADE' failed: iptables: Bad rule (does a matching rule exist in that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table filter --delete FORWARD --destination 192.168.122.0/24 --ou
t-interface virbr0 --match conntrack --ctstate ESTABLISHED,RELATED --jump ACCEPT' failed: iptables: Bad rule (does a matching rule exist in
that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table filter --delete FORWARD --source 192.168.122.0/24 --in-inte
rface virbr0 --jump ACCEPT' failed: iptables: Bad rule (does a matching rule exist in that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table filter --delete FORWARD --in-interface virbr0 --out-interfa
ce virbr0 --jump ACCEPT' failed: iptables: Bad rule (does a matching rule exist in that chain?).

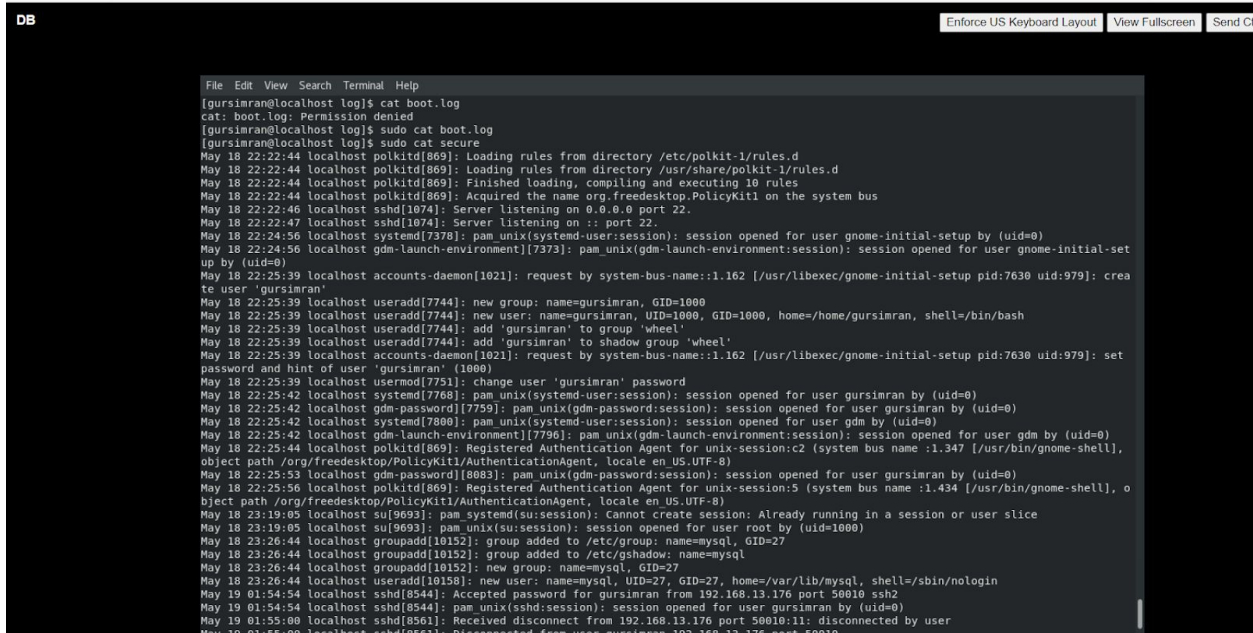
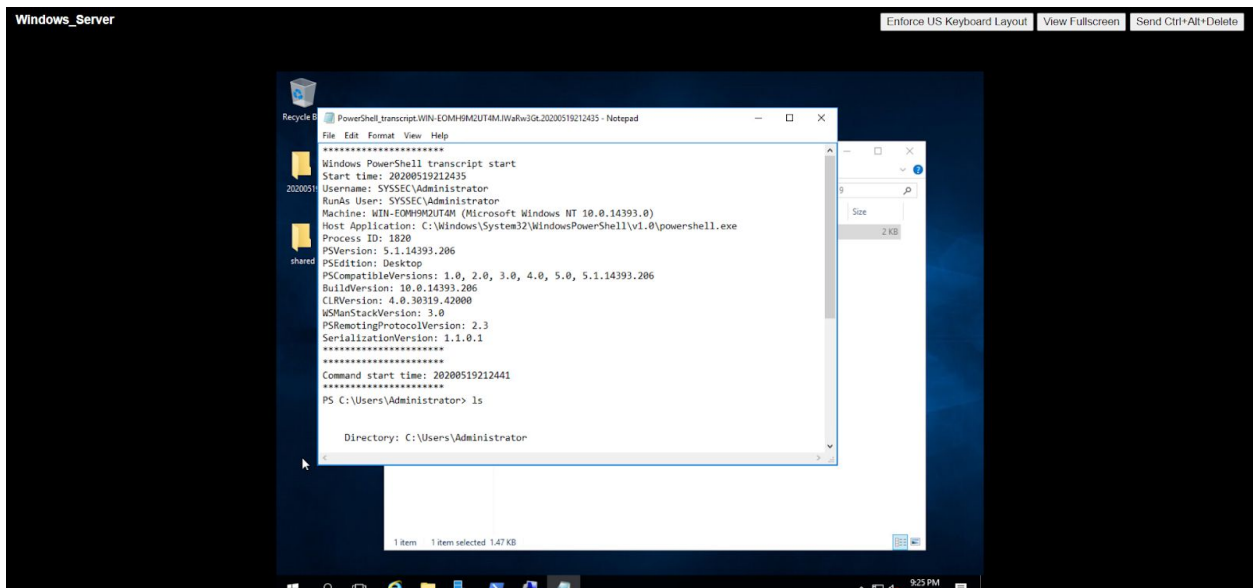
2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table filter --delete FORWARD --out-interface virbr0 --jump REJEC
T' failed: iptables: Bad rule (does a matching rule exist in that chain?).

2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table filter --delete FORWARD --in-interface virbr0 --jump REJECT
' failed: iptables: Bad rule (does a matching rule exist in that chain?).

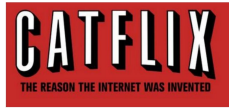
2020-05-18 23:36:16 WARNING: COMMAND FAILED: '/usr/sbin/iptables -w10 -w --table filter --delete INPUT --in-interface virbr0 --protocol udp
--destination-port 53 --jump ACCEPT' failed: iptables: Bad rule (does a matching rule exist in that chain?).
```

System Logs

Description	Time
User admin logged in via Web from 192.168.13.176 using https	05/19 19:51:04
authenticated for user 'admin'. From: 192.168.13.176.	05/19 19:51:04
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.254.106	05/19 19:45:10
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.254.106	05/19 19:29:21
Backup of PAN-DB finished successfully.	05/19 19:16:20
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.254.106	05/19 19:14:51
DHCP client assigned IP: 192.168.254.36 on interface: ethernet1/1 for lease time of: 0 days 2h:00m:00s from server: 192.168.254.254. Subnet mask:255.255.255.0 Gateway:192.168.254.254 DNS1:192.168.0.2 NTP1:128.205.32.2 NTP2:128.205.32.12 DNS Suffix:cse.buffalo.edu	05/19 19:08:09
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.254.106	05/19 18:59:08



Reference - <https://www.cisecurity.org/controls/cis-controls-list/>



Username and passwords

System	User	Password
Linux Client	gursimransingh(Gursimran)	Team6@123
Windows 10	mannisingh@syssec.com gursimran	Team6@123
Windows Server	SYSSEC/ADMINISTRATOR gursimransingh@syssec.com	Team6@123
WEB	Gursimran, gursimransingh	Team6@123
DB	Gursimran wikidb->wikiuser	Team6@123 wikipassbig
PaloAlto	admin	Change.me!
Traveler	Administrator	Pal0Alt0