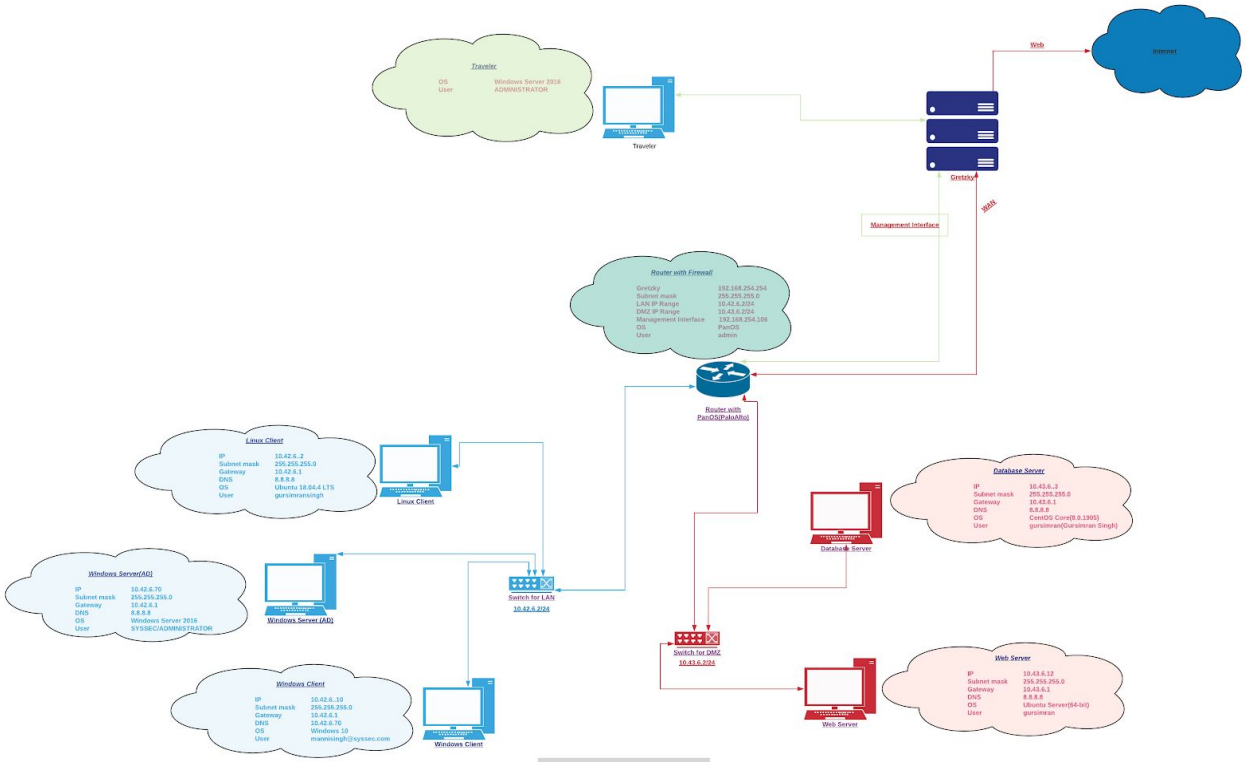
Final Project - CatFlix

Task 1

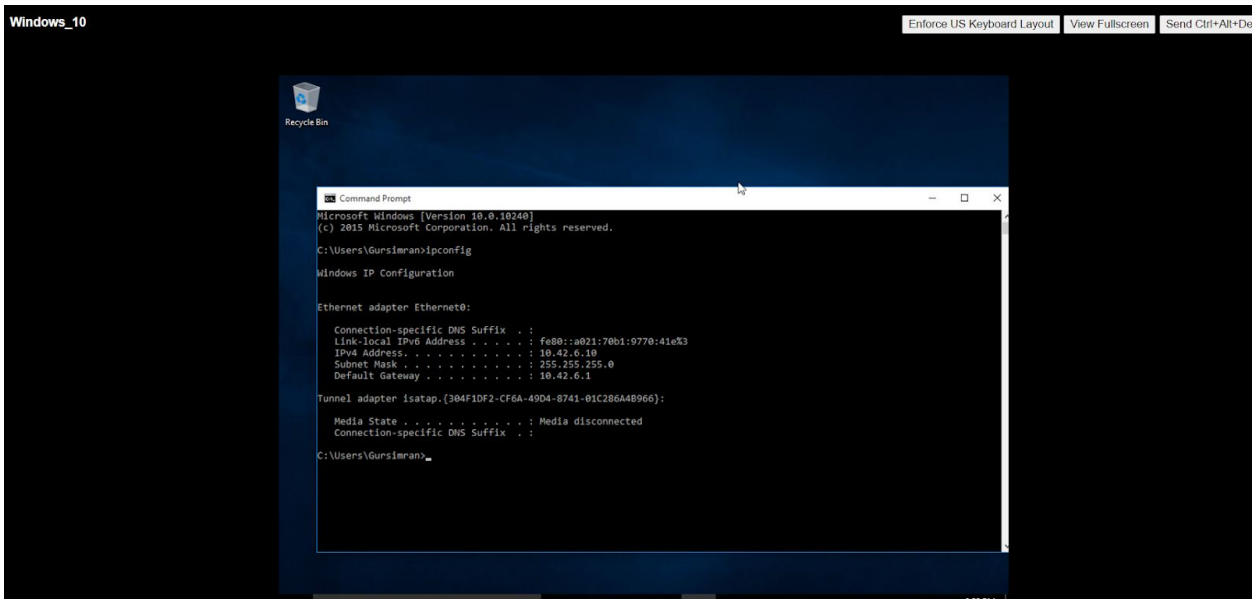


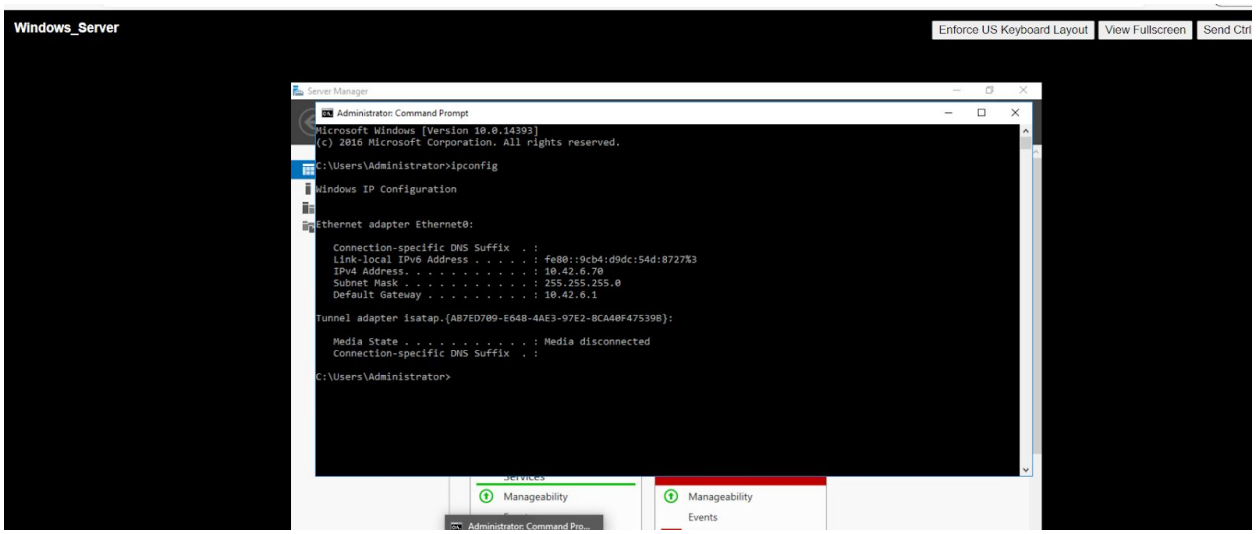
Topology

Task 2

Windows

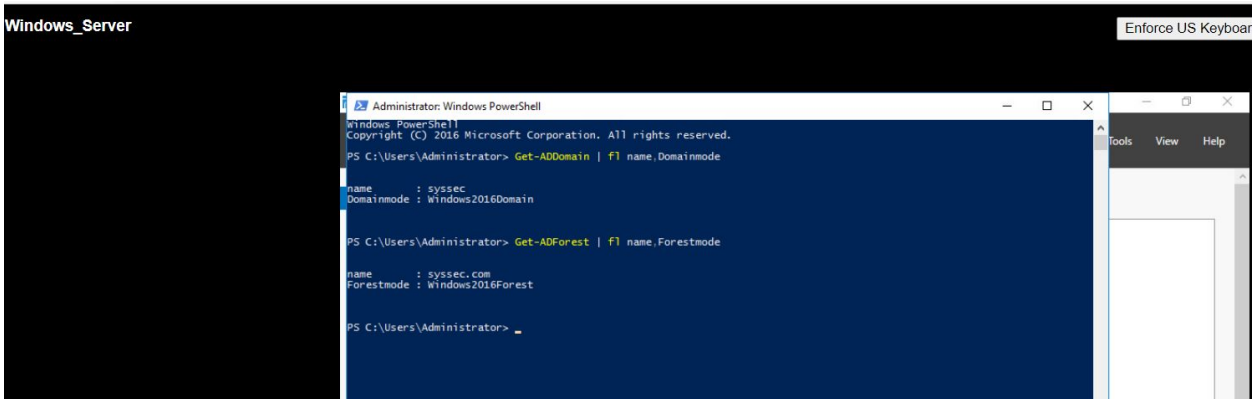
IPs

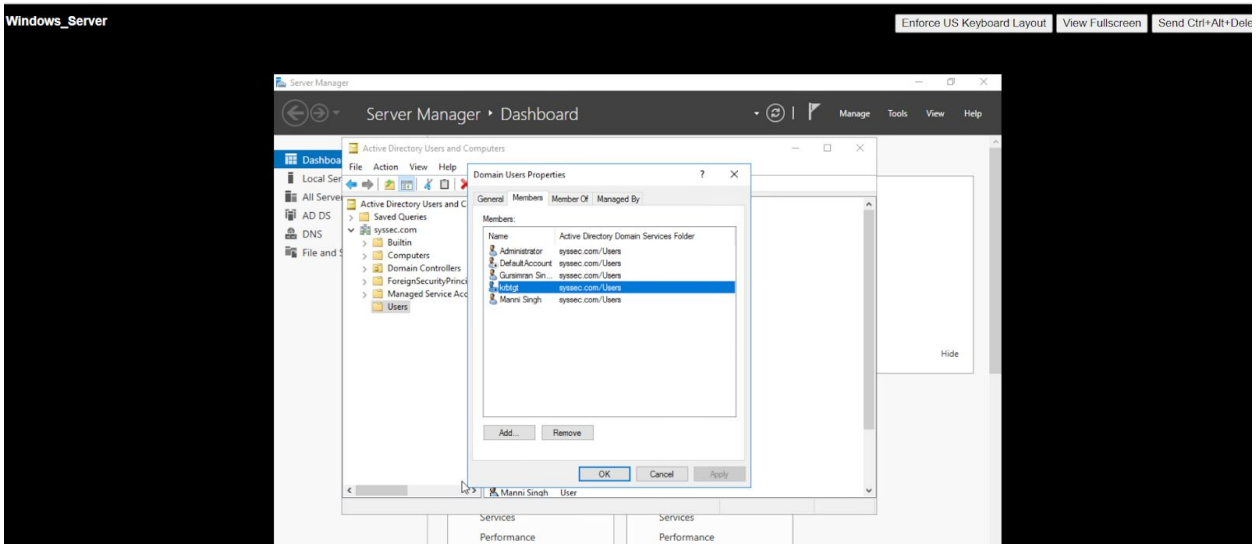


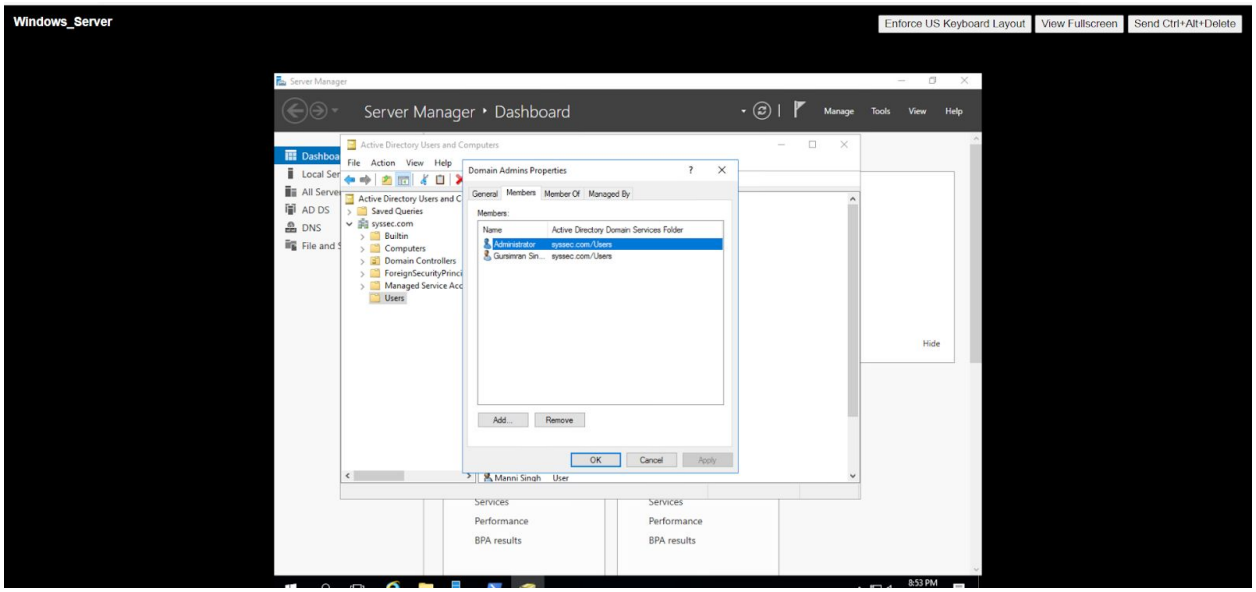


CATFLIX
THE REASON THE INTERNET WAS INVENTED

Windows Group Policy Implementation

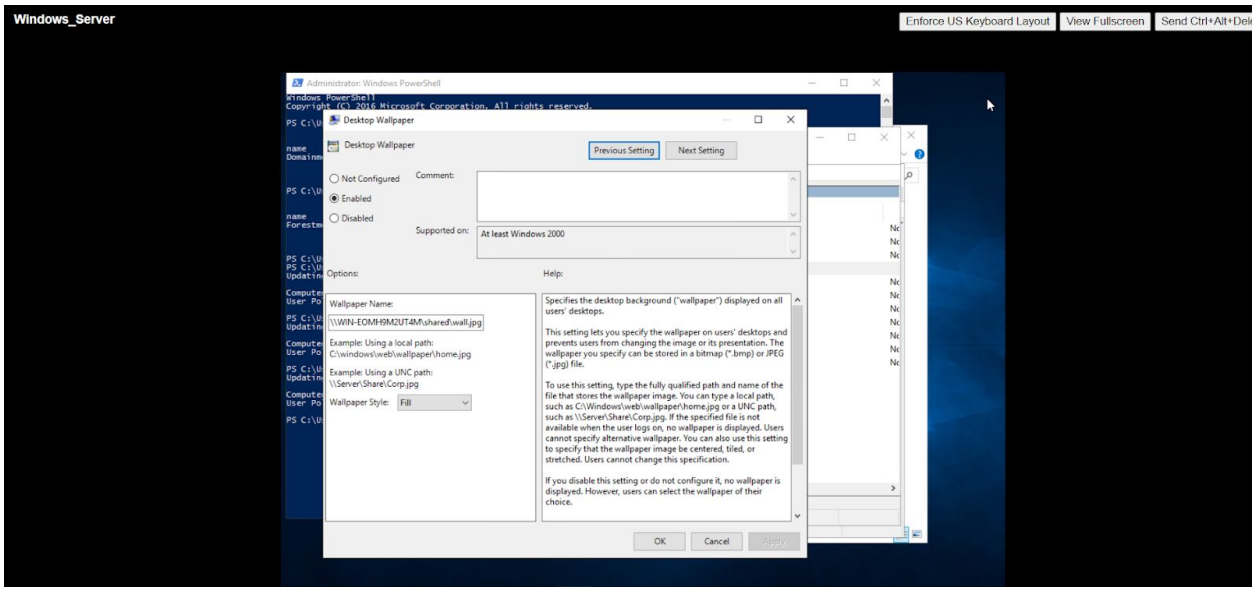






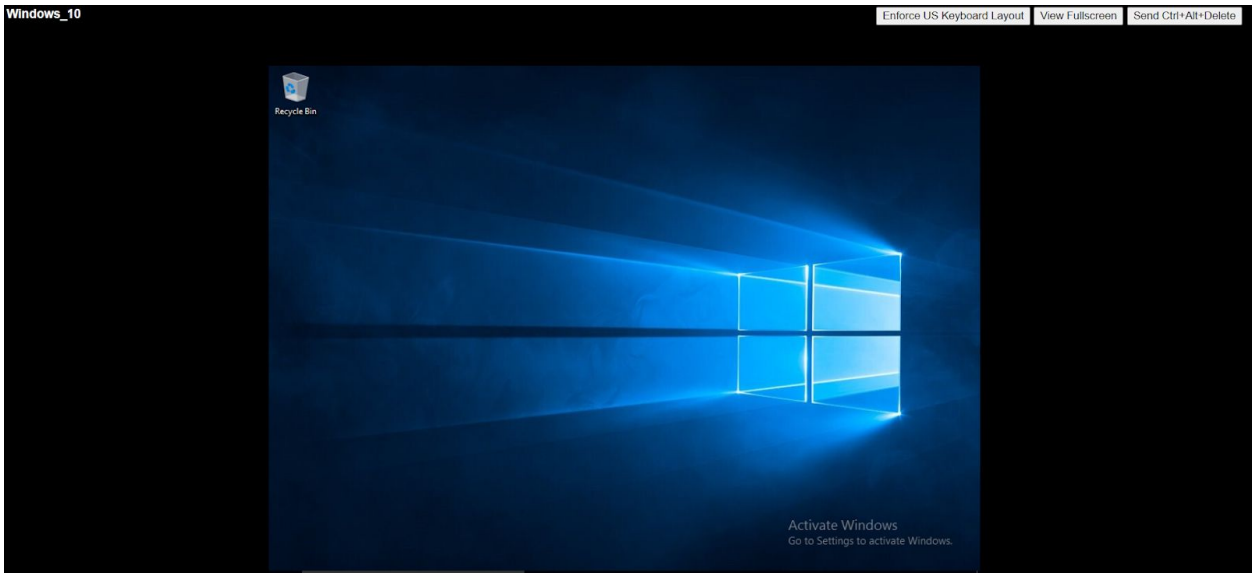
CATFLIX

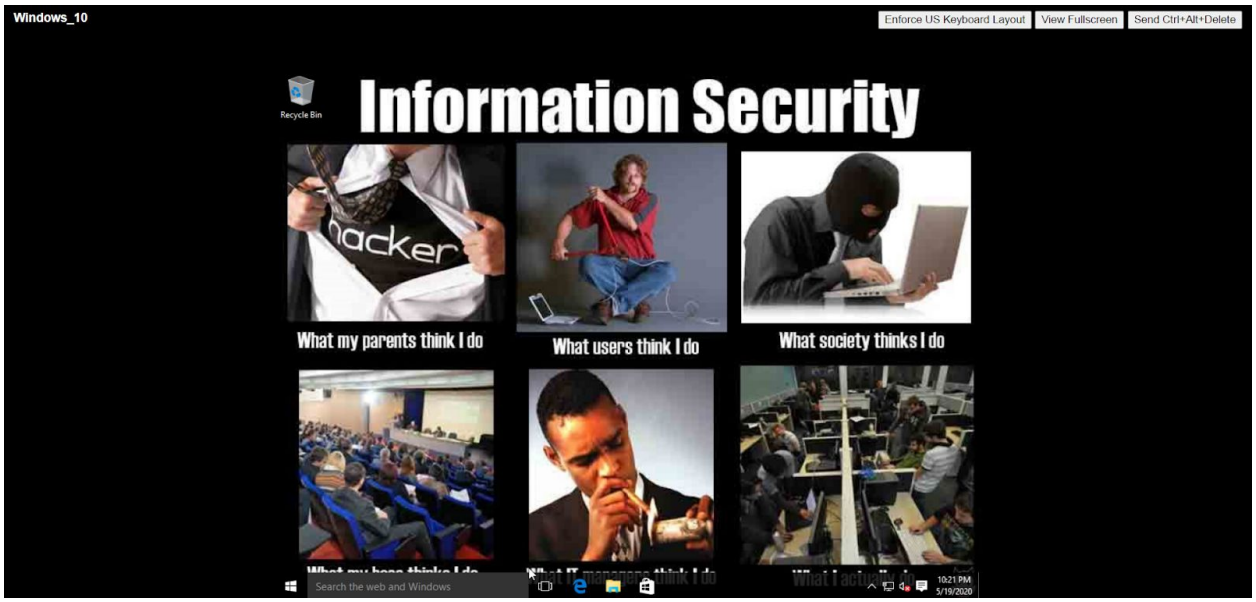
THE REASON THE INTERNET WAS INVENTED



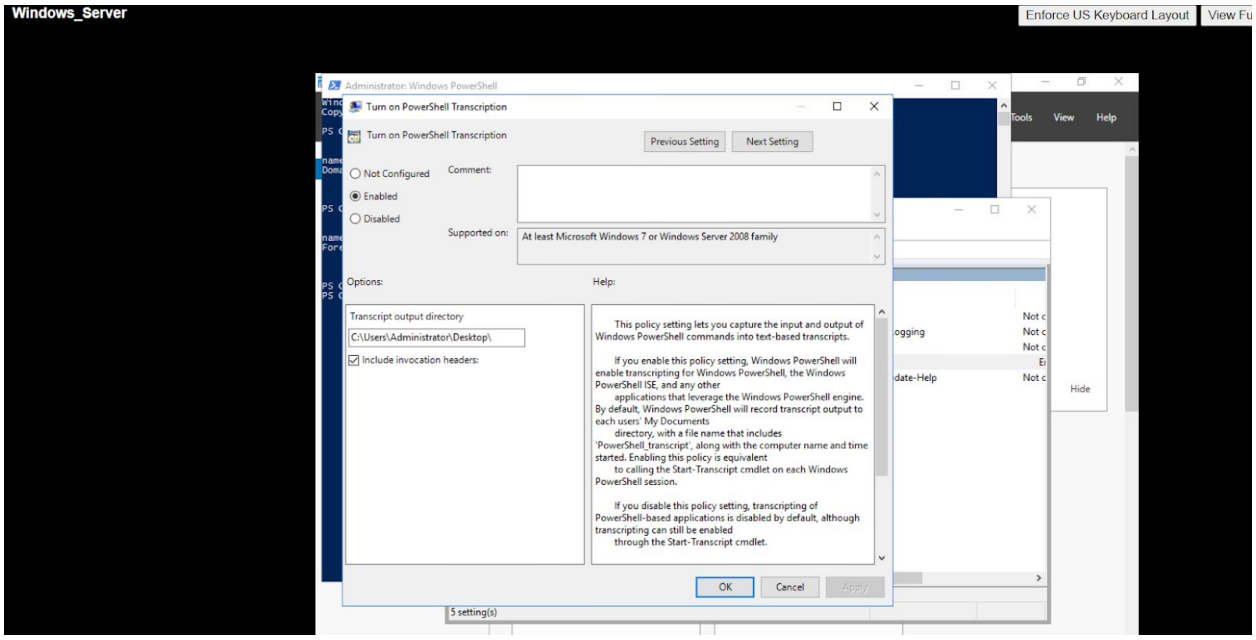
CATFLIX

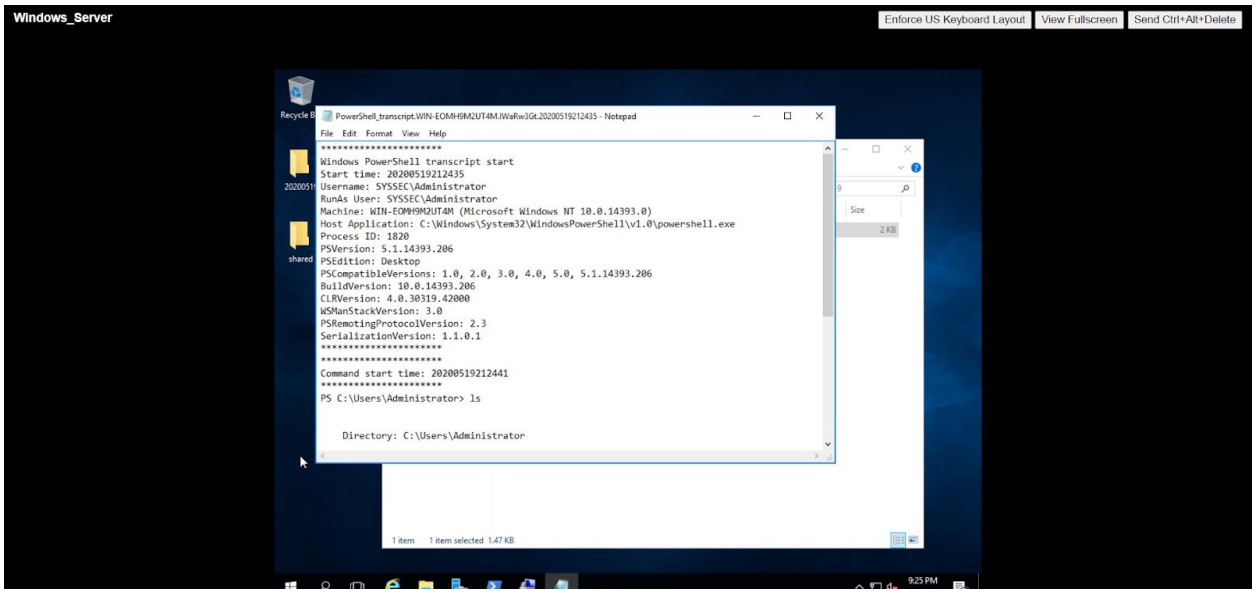
THE REASON THE INTERNET WAS INVENTED





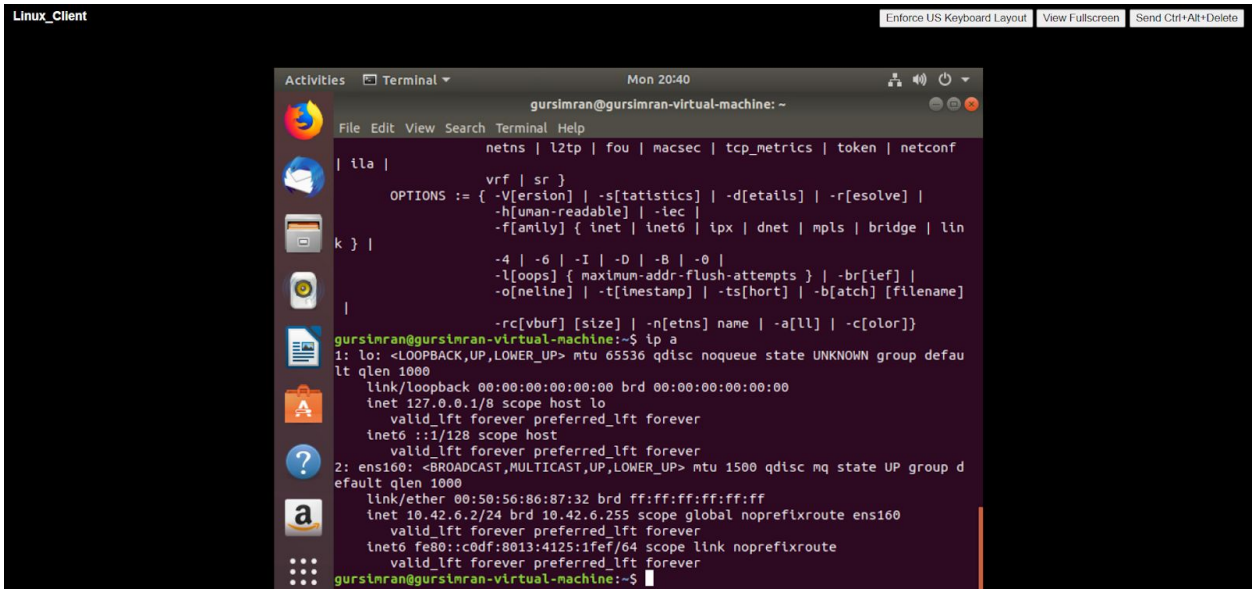
Powershell Transcripts

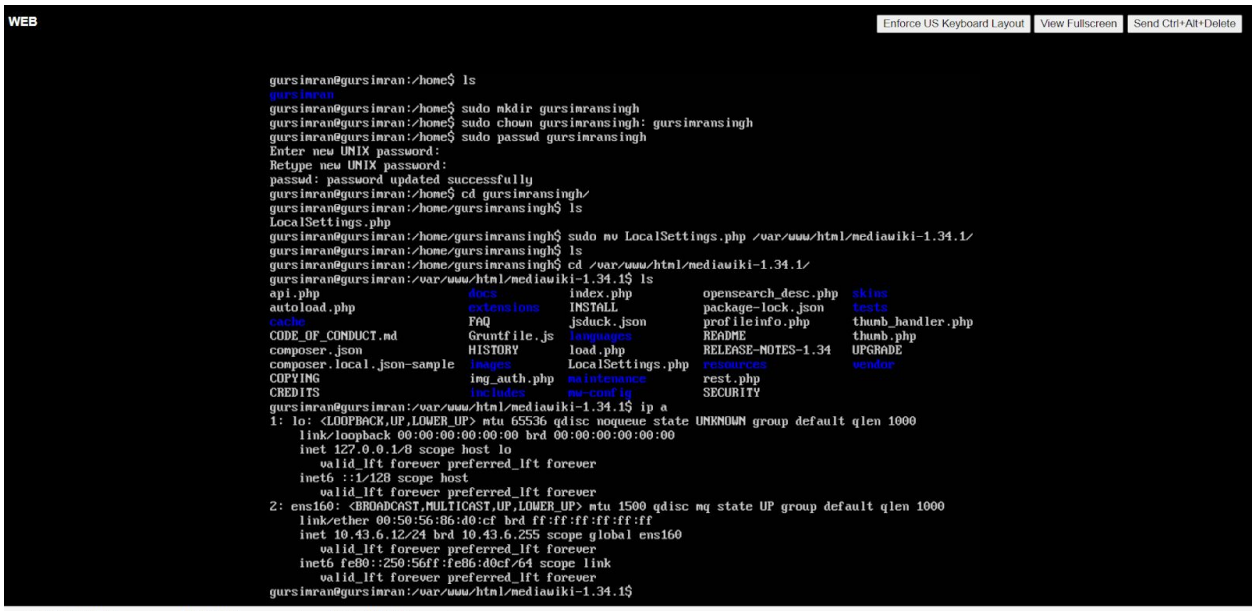


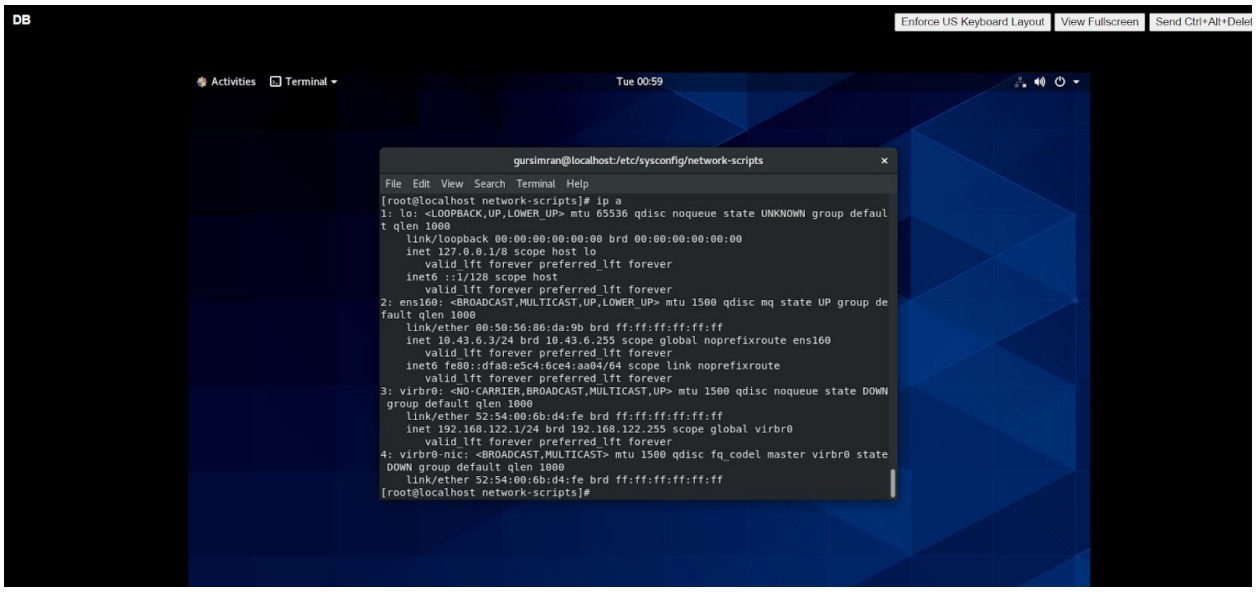


Linux(LAMP Stack)

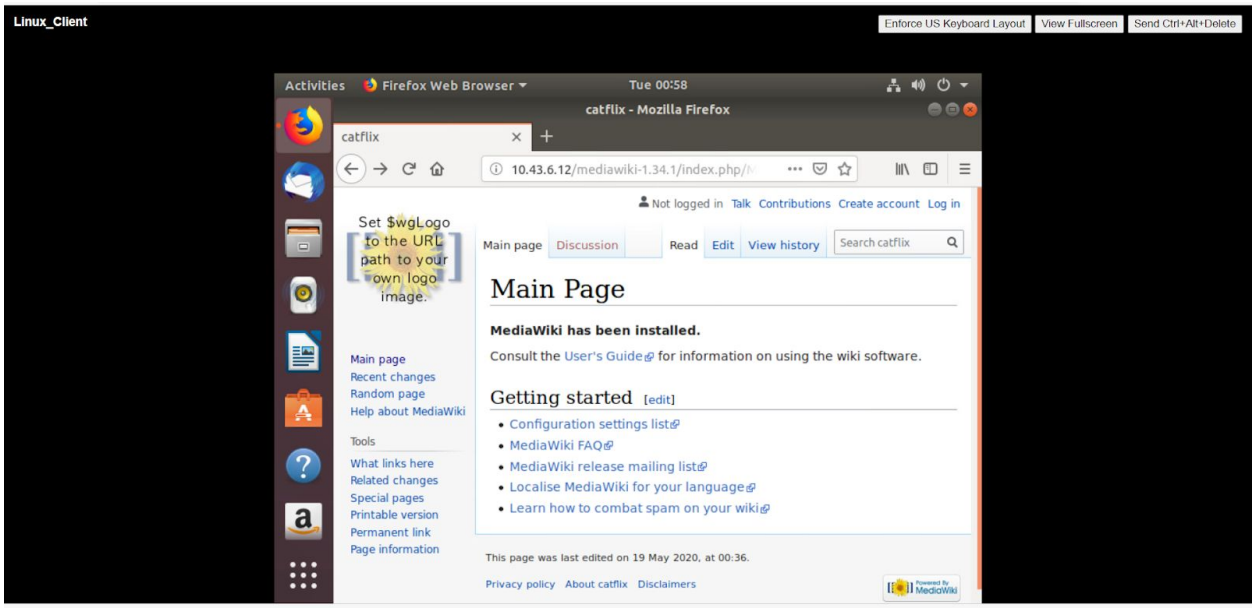
IPs







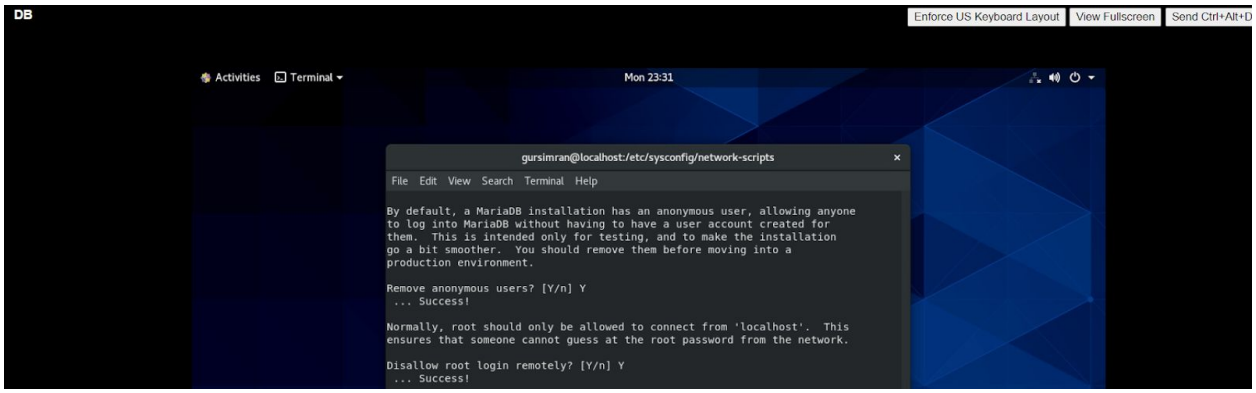
Mediawiki



Security Detail

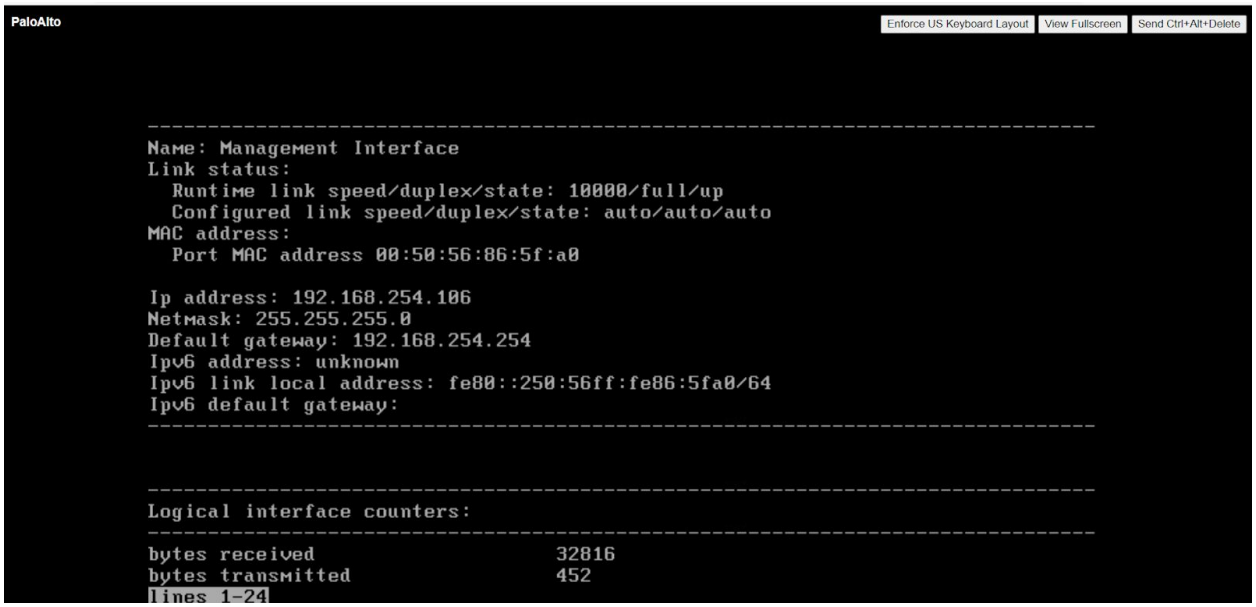
CATFLIX

THE REASON THE INTERNET WAS INVENTED

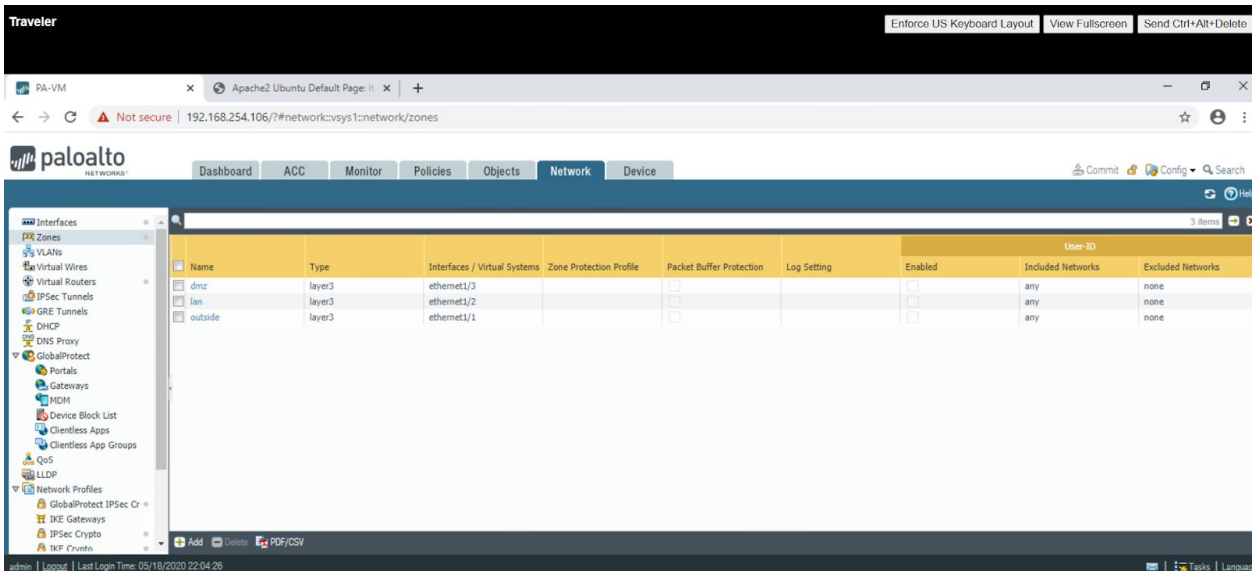


PaloAlto

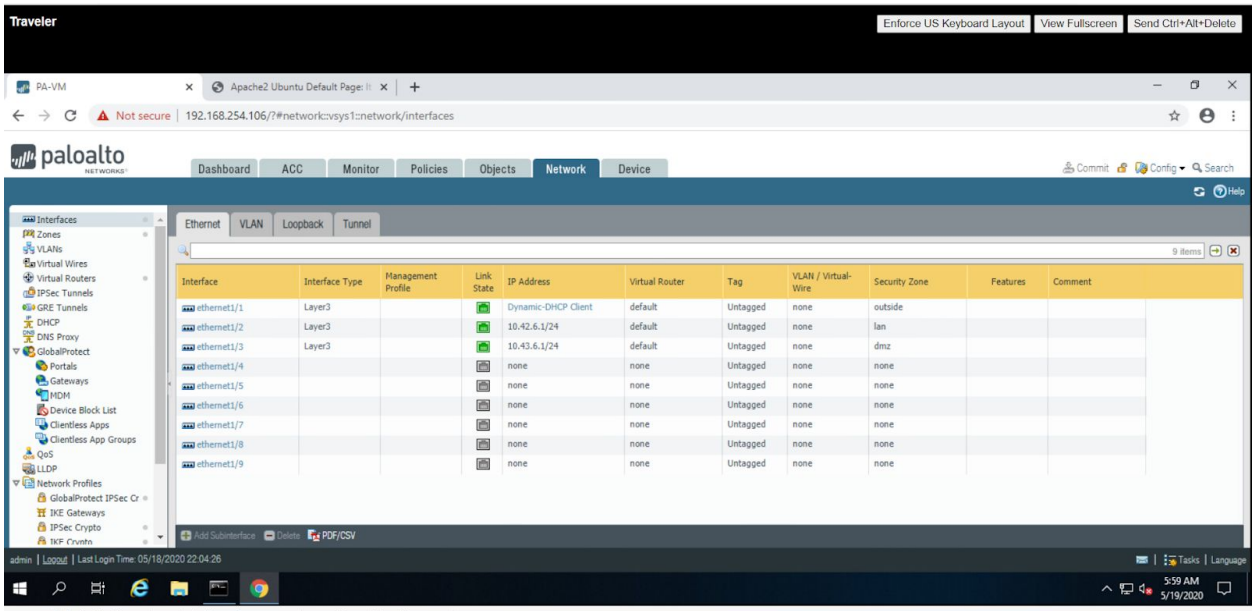
Interface Management

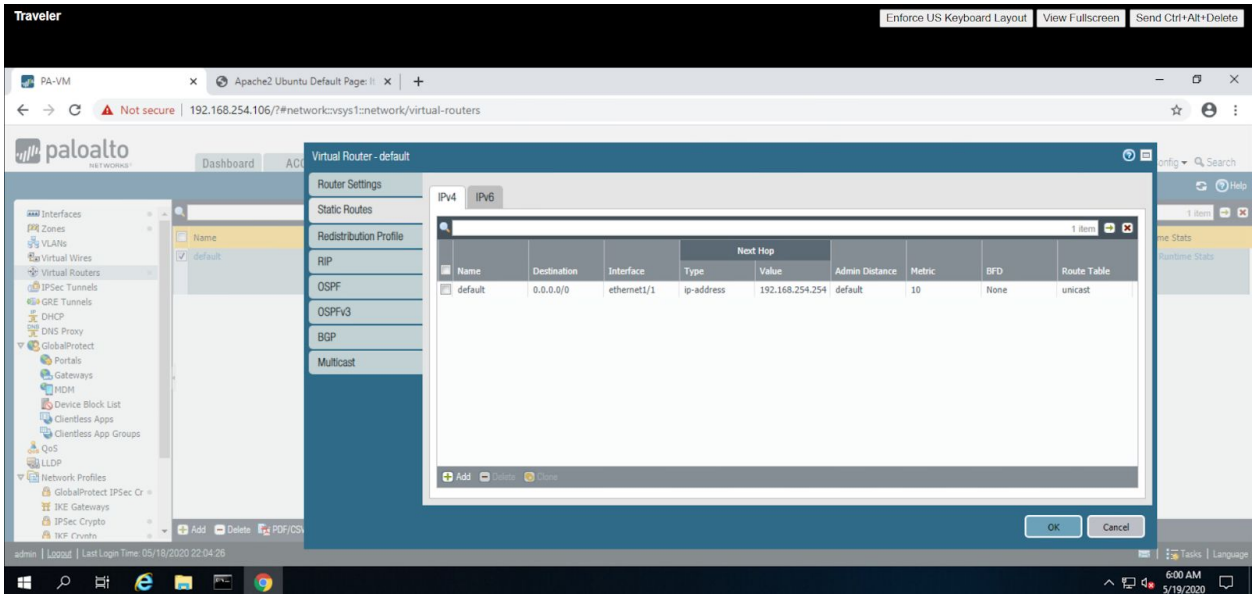


Config and Basic Implementation



CATFLIX
THE REASON THE INTERNET WAS INVENTED





CATFLIX
THE REASON THE INTERNET WAS INVENTED

Traveler

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

PA-VM | Apache2 Ubuntu Default Page: It

Not secure | 192.168.254.106/?#policies::vsys1::policies/nat-rulebase

paloalto NETWORKS

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit | Config | Search | Help

Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection

Policy Optimizer
Rule Usage
Unused in 30 days 0
Unused in 90 days 0
Unused 0

Object : Addresses

5 items

			Original Packet						Translated Packet		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit C
1	source web	none	dmz	outside	any	10.43.6.12	any	any	static-ip 192.168.254.166 bi-directional: no	none	136
2	source data	none	dmz	outside	any	10.43.6.3	any	any	static-ip 192.168.254.136 bi-directional: no	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

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

Traveler

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

PA-VM | Apache2 Ubuntu Default Page: It

Not secure | 192.168.254.106/?#policies::vsys1::policies/security-rulebase

paloalto NETWORKS

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit | Config | Search | Help

Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection

Policy Optimizer
No App Specified 1
Unused Apps 0
Rule Usage
Unused in 30 days 2
Unused in 90 days 2
Unused 2

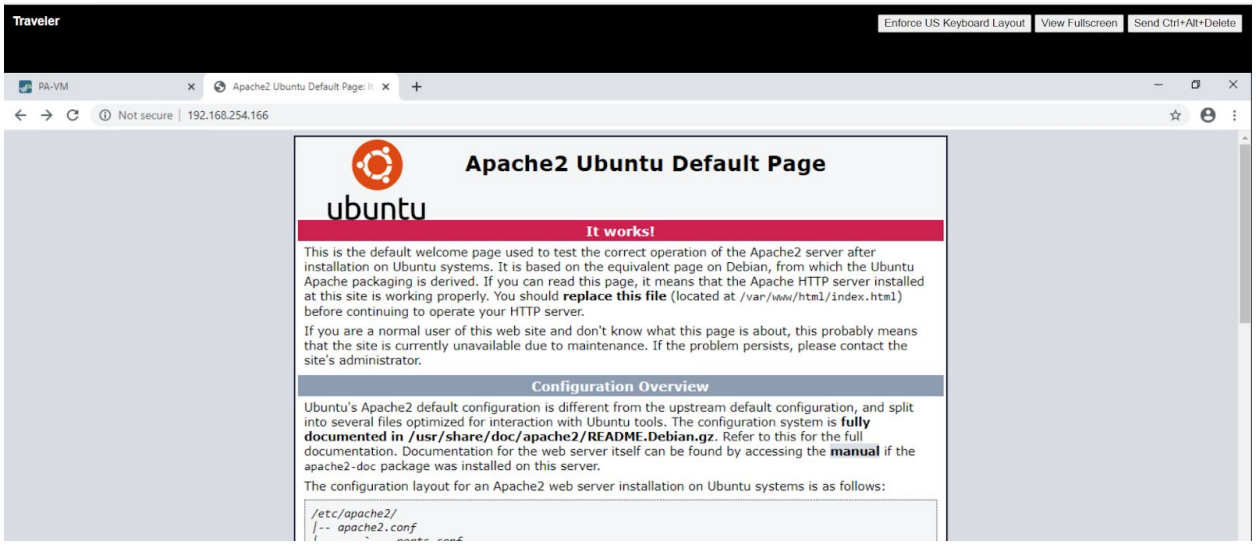
Object : Addresses

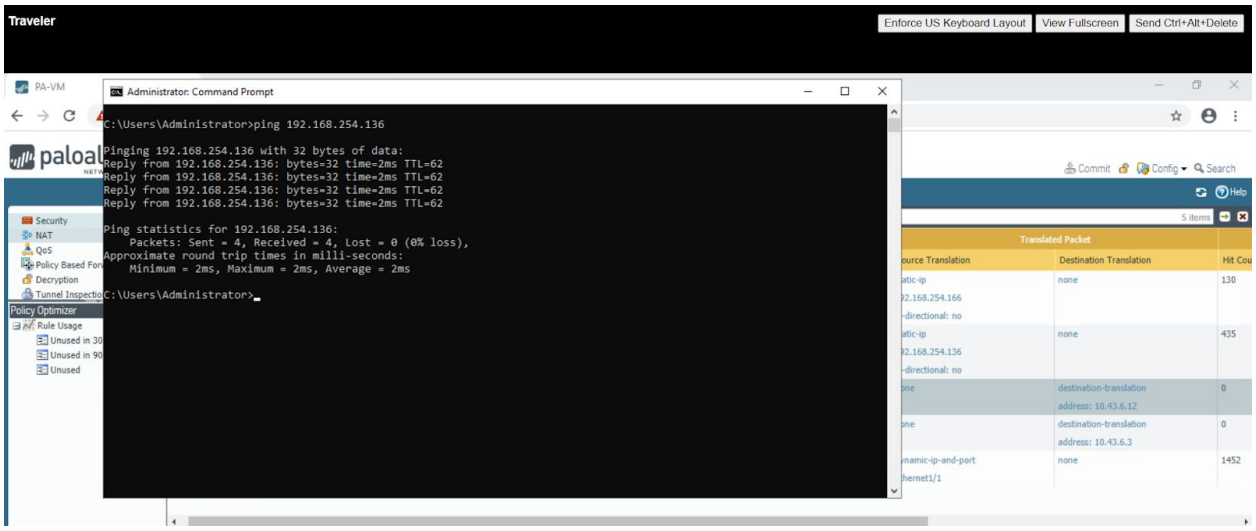
7 items

				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP 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

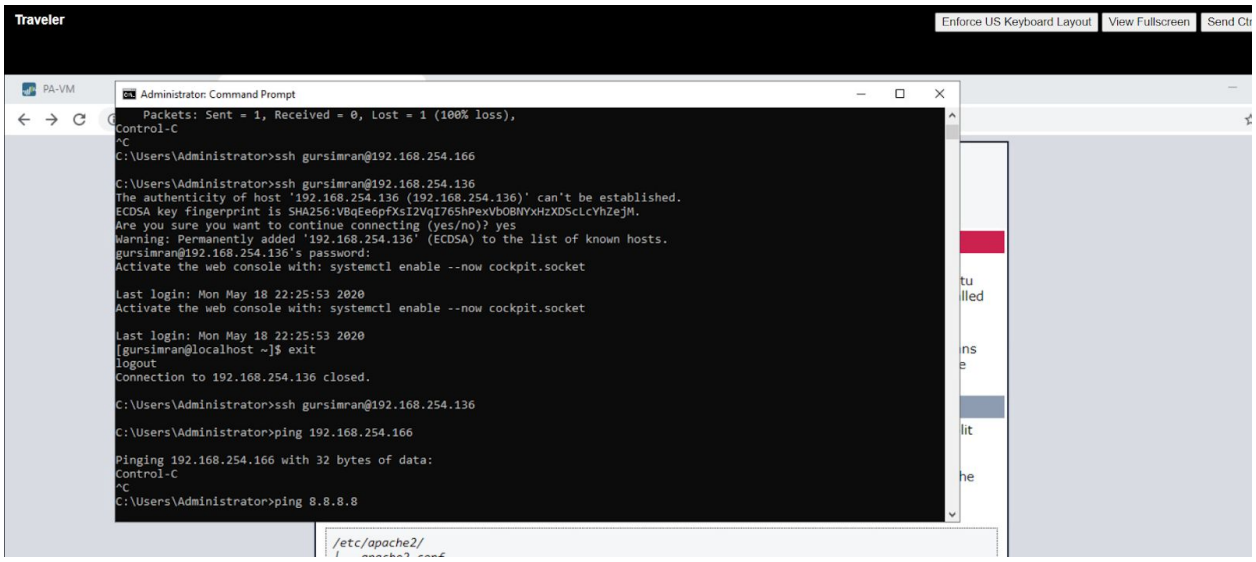
Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View Rulebase as Groups | Test Policy Match

CATFLIX
THE REASON THE INTERNET WAS INVENTED

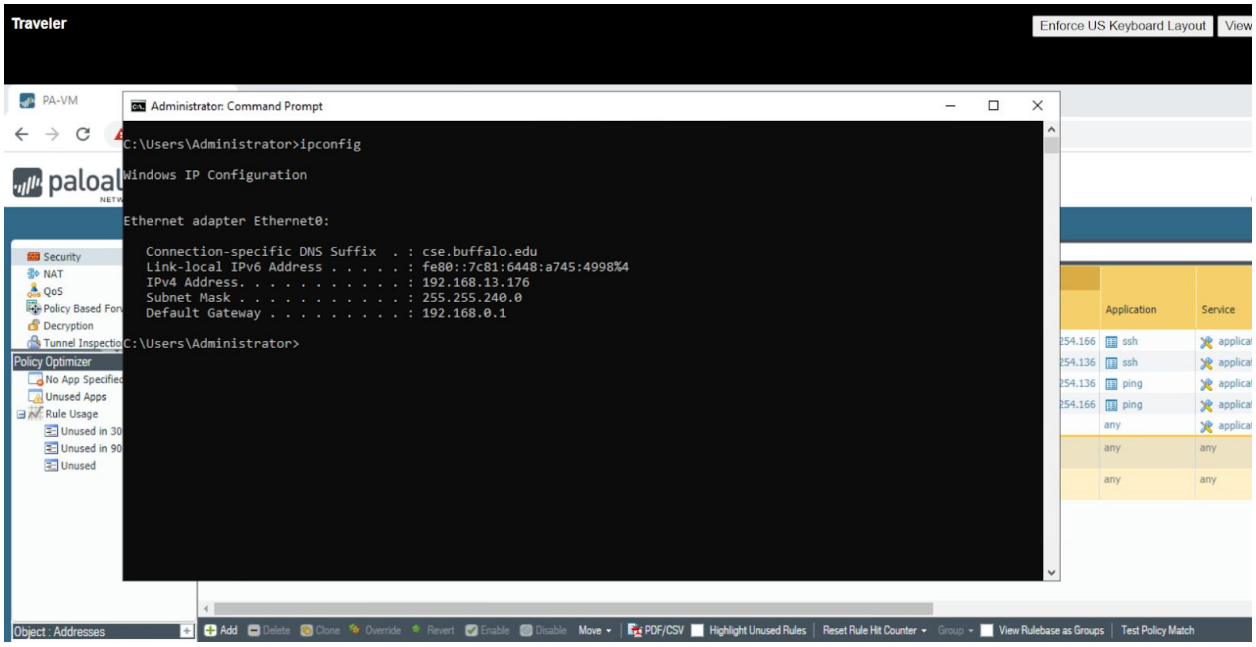




Security Blocks



Traveler IP



CATFLIX
THE REASON THE INTERNET WAS INVENTED

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

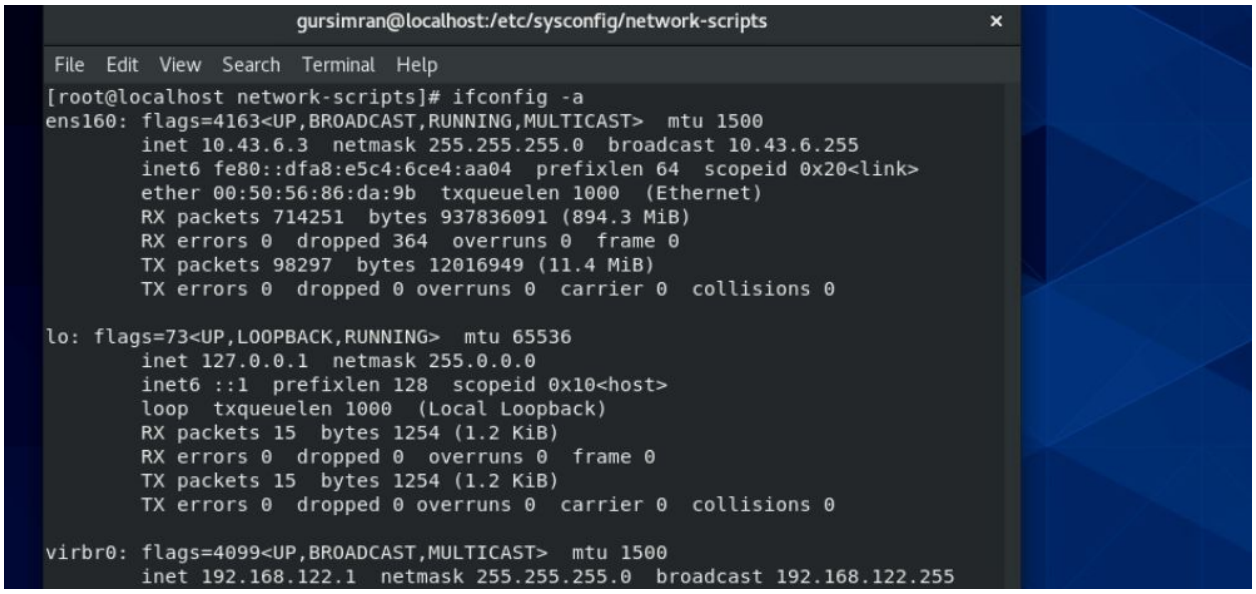
DB	Database Server	10.43.6.3	00-50-56-86-da-9b	CentOS Core(8.0.1905)
Palo Alto	Router , Firewall	MI - 192.168.254.106 ,10.42.6.1, 10.43.6.1	00-50-56-86-d3-78 00-50-56-86-49-db	PanOS
Traveler	Client, Outside	192.168.13.176	00-50-56-86-53-ce	Windows Server 2016

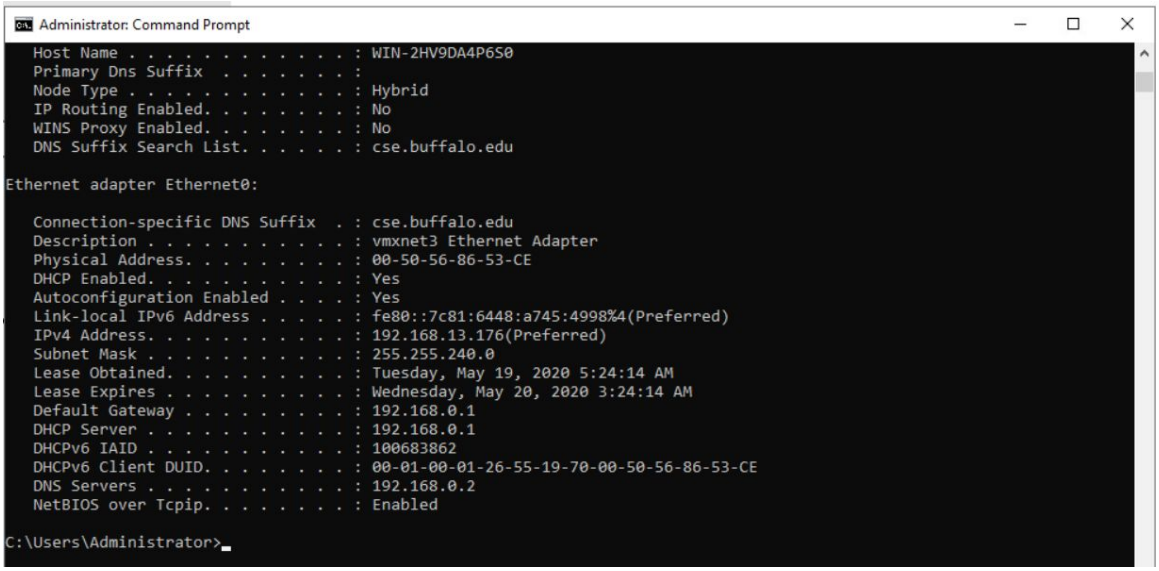
Finding MAC

```
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
e
10.42.6.70               ether   00:50:56:86:7d:2b   C                     ens1
60
10.42.6.10               ether   00:50:56:86:3c:a7   C                     ens1
60
_gateway                 ether   00:50:56:86:d3:78   C                     ens1
60
```





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.

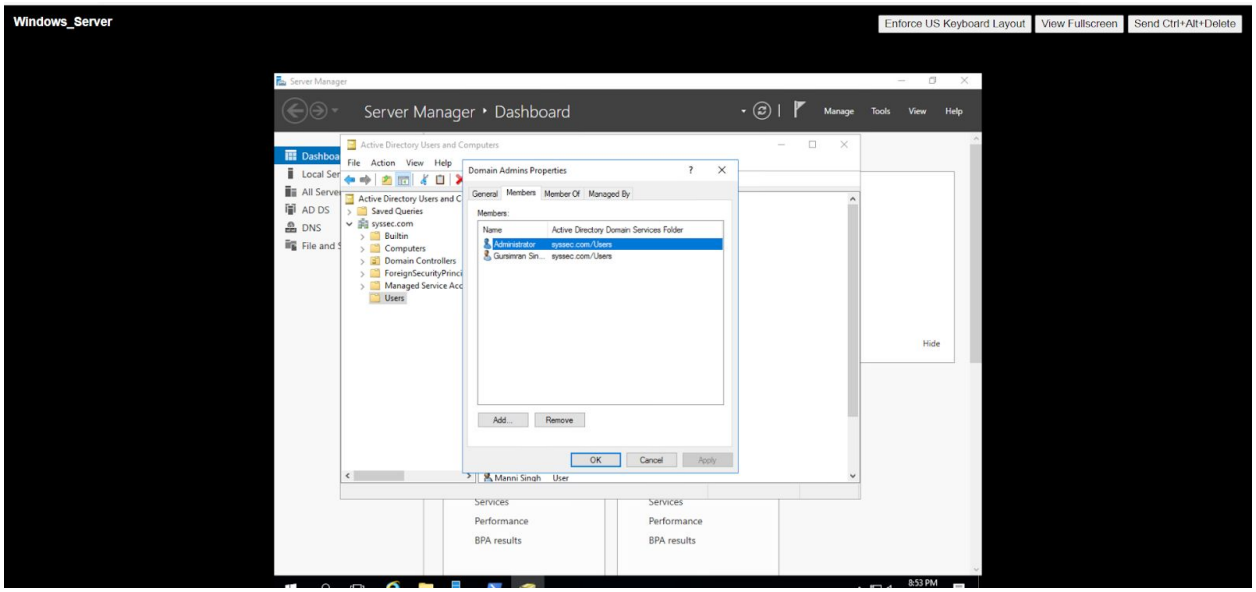
Name	**Category**	**Use**	**Usage**
Apache2	WebServer	Hosting HTTP Server	WebServer
Mediawiki	WebService	Software App	WebServer
MariaDB	Database	Maintaining DB for WebServer	Database
net-tools	Network tools	Used for Networking tasks like ifconfig, arp, etc	Linux Client

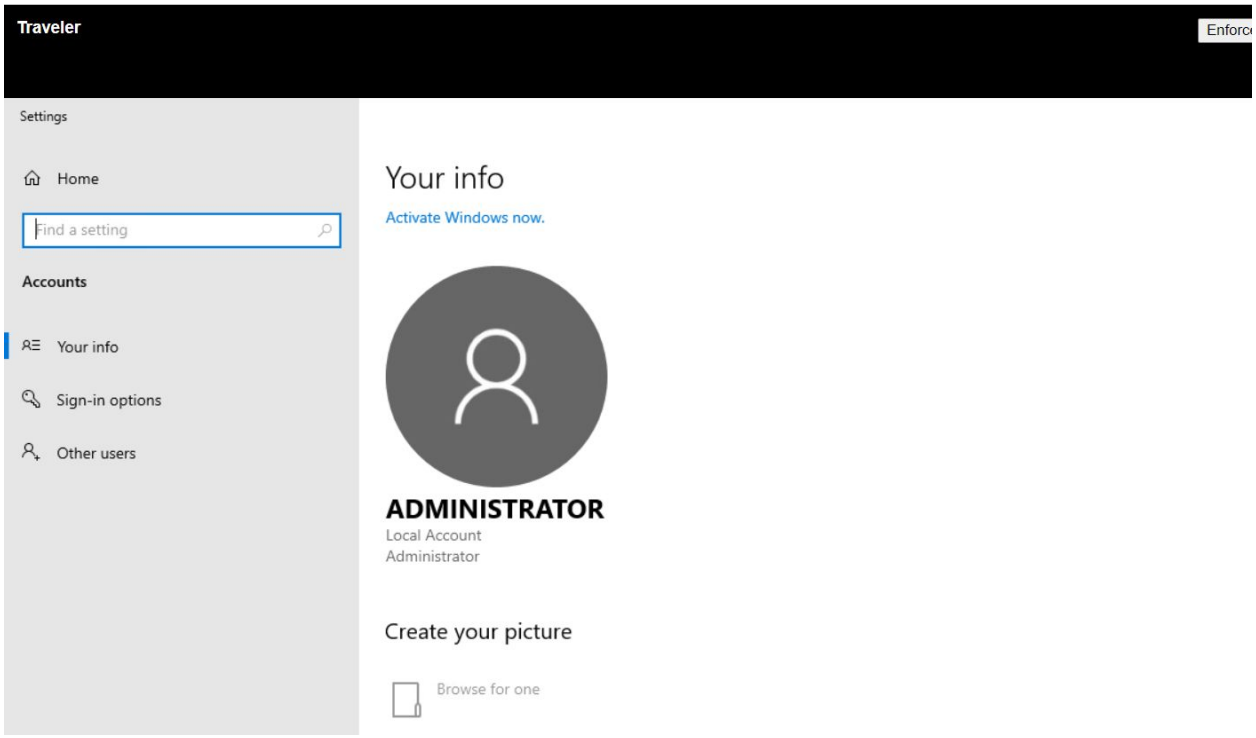
CATFLIX
THE REASON THE INTERNET WAS INVENTED

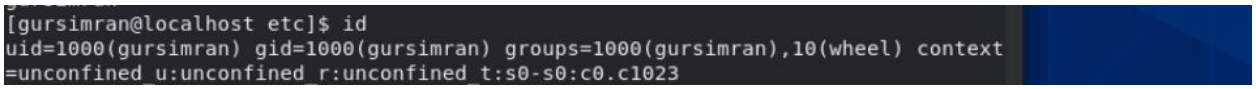
Controlled use of Admin Privileges

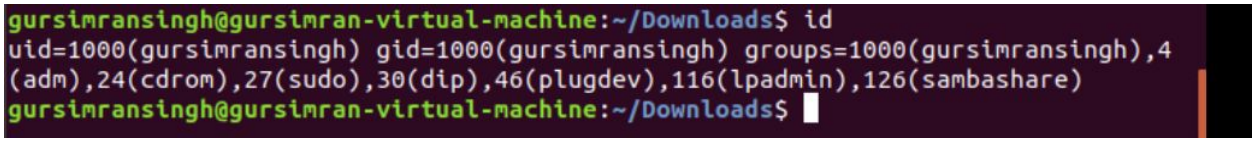
The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user, is fooled into opening a malicious 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.

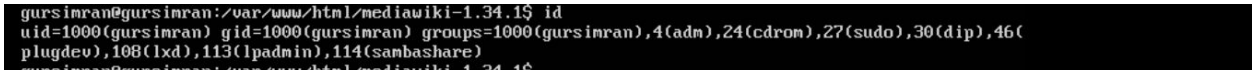
The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker 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.









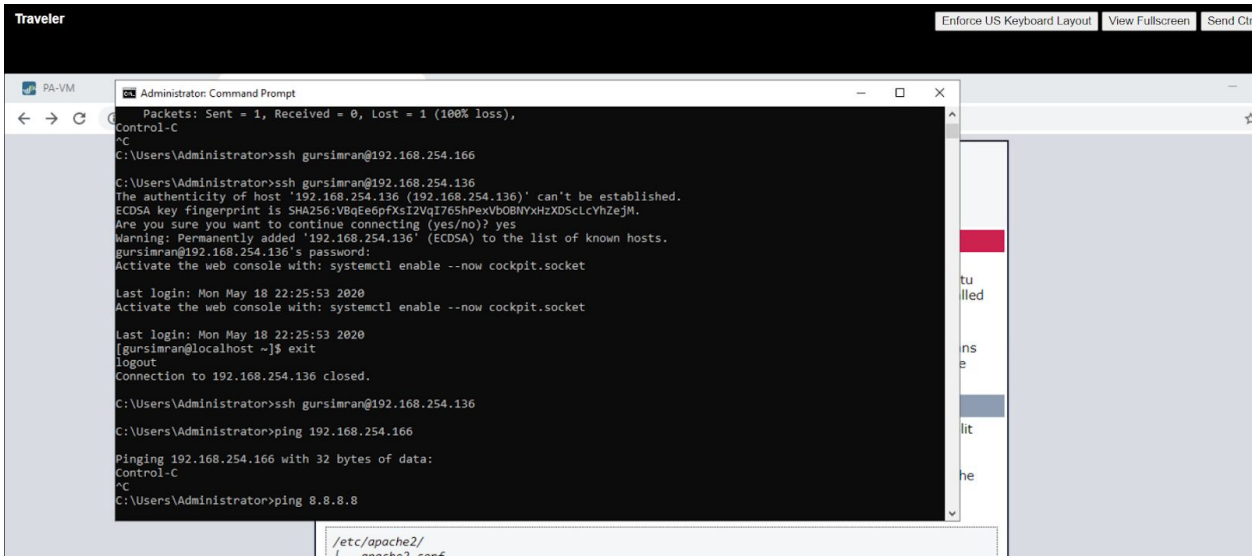


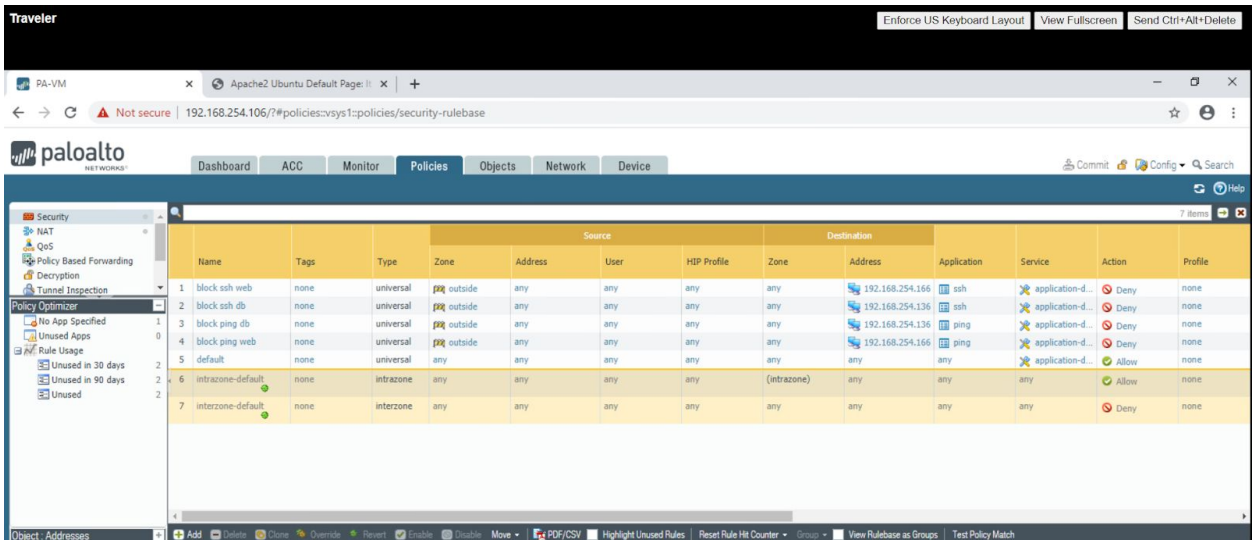
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

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

be continually managed to avoid security “decay” as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked” to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network accessible services and client software.





Maintenance, Monitoring, and Analysis of Audit Logs

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.

CATFLIX
THE REASON THE INTERNET WAS INVENTED

DB

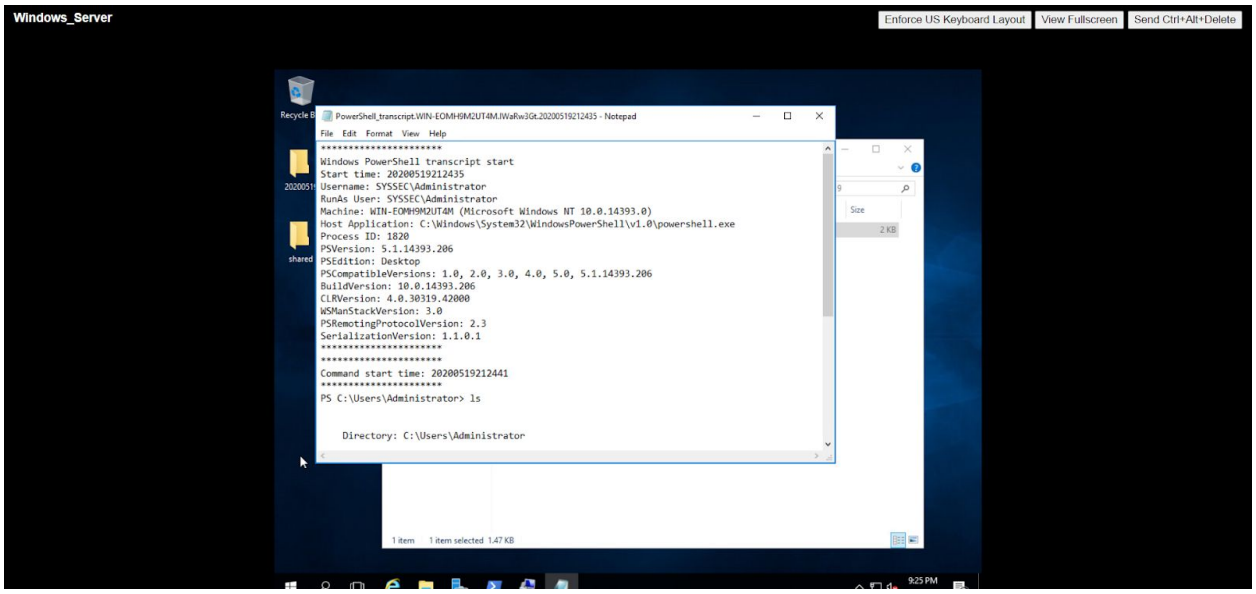
Enforce US Keyboard Layout | View Fullscreen | Send

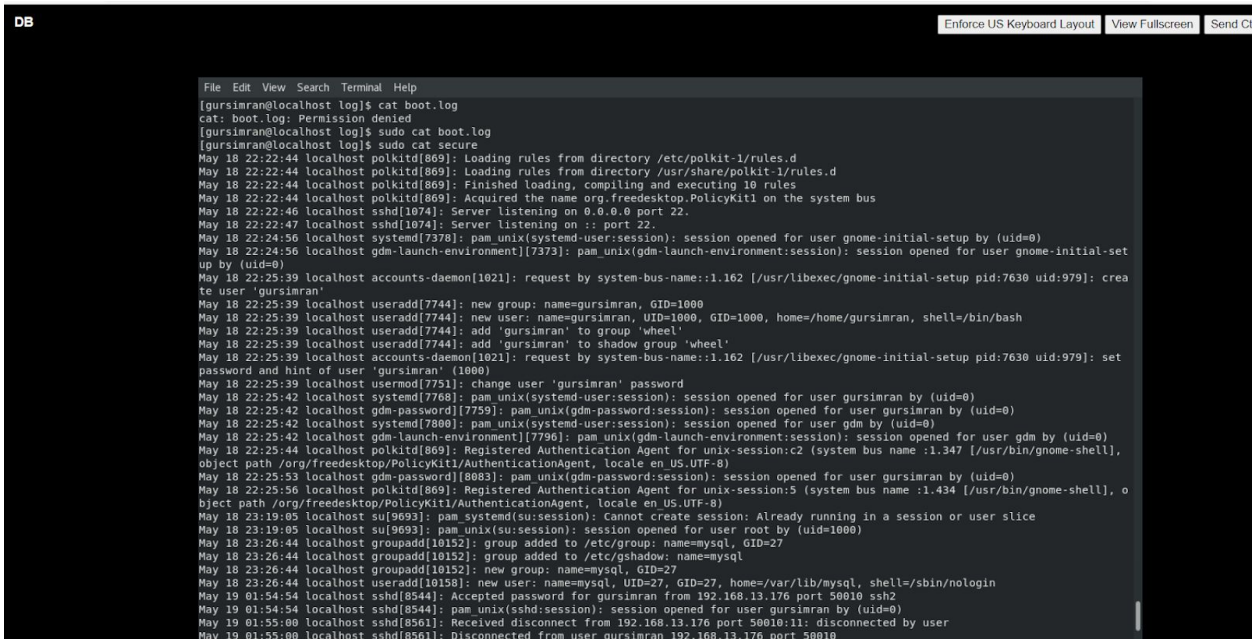
File Edit View Search Terminal Help

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

[gursimran@localhost log]$ sudo cat firewalld
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