Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Christopher DeArmond

Table of Contents

This document contains the following sections:

01 **Network Topology**

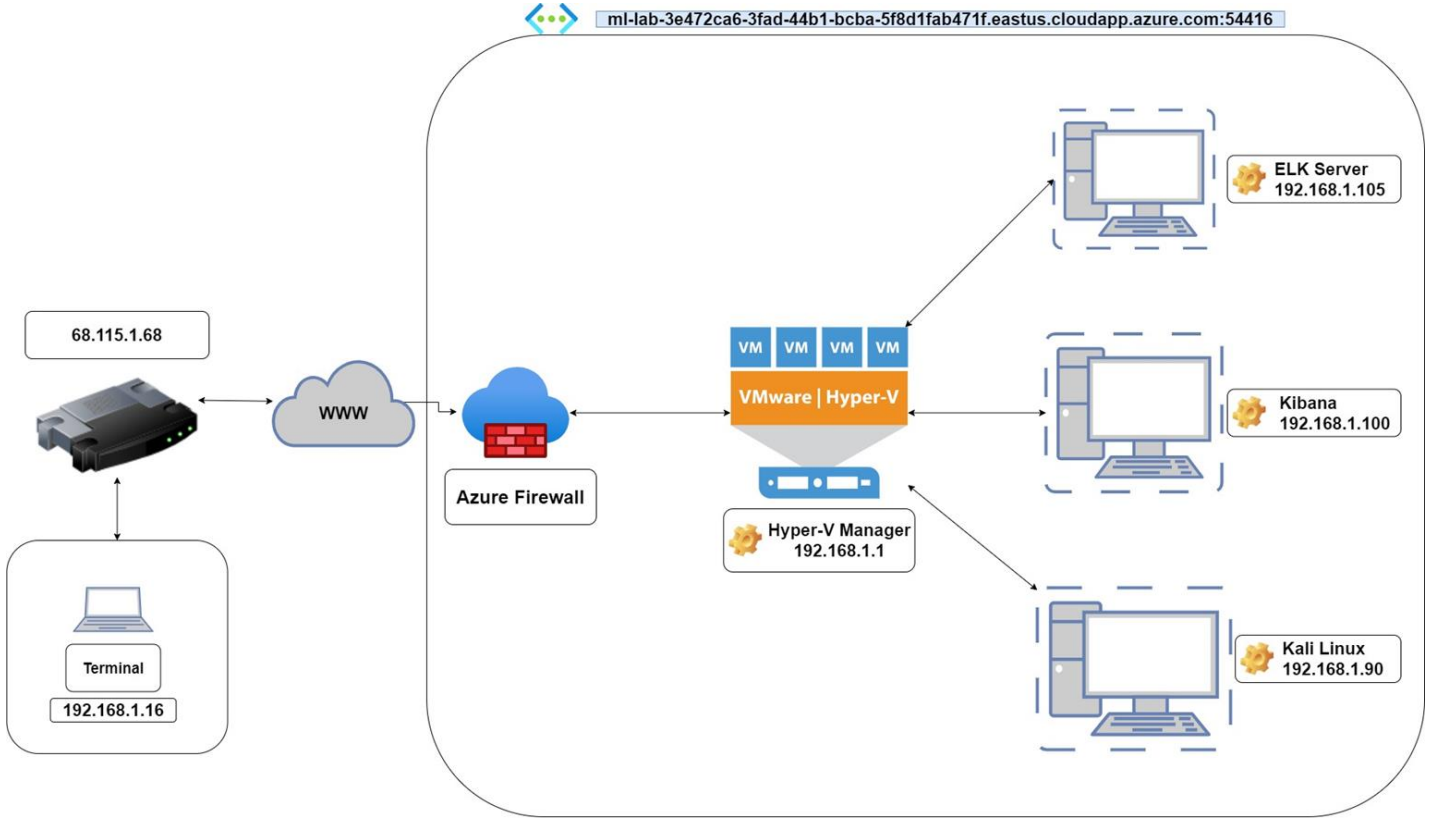
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: ML-REFVM-684427

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	NAT Switch
Elk Server	192.168.1.100	Log Manager and Visualization
Capstone	192.168.1.105	Web Server and Final Target
Kali Linux	192.168.1.90	Red Team Platform

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache 2.4.29 Directory Listing Enabled	A simple enumeration scan reveals the entire file structure of the site with indexed files.	Quickly map points of interest and shows what files are available to be investigated
WebDav Vulnerability	WebDav is essentially an FTP service.	WebDav can allow an actor with stolen credentials to upload and download resources directly.
Unsanitized txt file hosted on-site	Ashton.txt specifically refers to a hidden directory on the site.	Knowing that the hidden directory exists the attacker can put all of their energy into one target.
No password lockout policy	There is no lockout if an incorrect password is entered after a set amount of attempts.	Using Hydra against the secret folder revealed the users password.

Exploitation: Apache Directory Listing

01

Tools & Processes

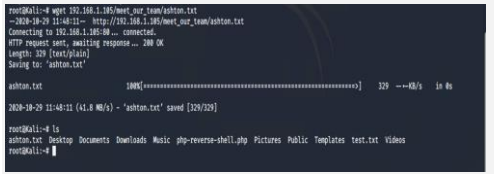
Using nmap with flags such as the -sS -O and -A I found a wealth of information and targets. Together with ‘nmap -v --script /root/hacking/http-enum.nse 192.168.1.105’ revealed the webdav application.

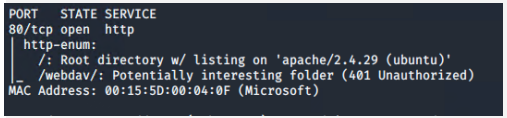
02

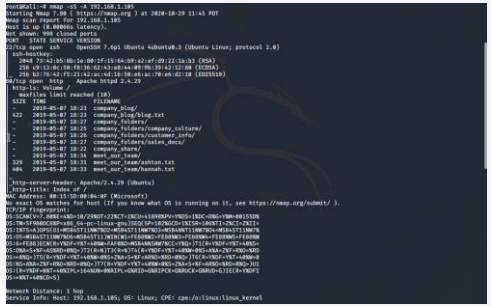
Achievements

I was able to locate the .txt file for ashton revealing the secret folder.

03







Exploitation: No Password Lockout Policy

01

Tools & Processes

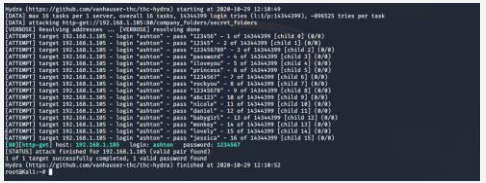
Knowing that the secret directory existed and knowing that Ashton was the page admin I used Hydra to attempt to bruteforce the password.

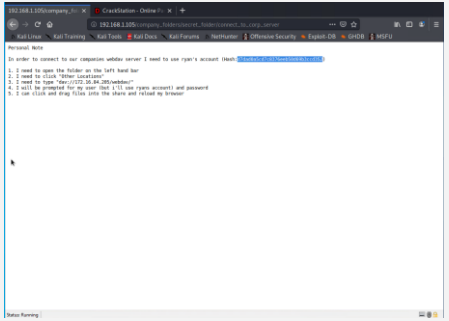
02

Achievements

Hydra was able to crack the password and I gained access to the secret Directory. Once in I found a .txt Document detailing how to access the Webdav server. The user name of Ryan and a hashed copy of his password were also in the file.

03





Exploitation: WebDav File Sharing

01

Tools & Processes

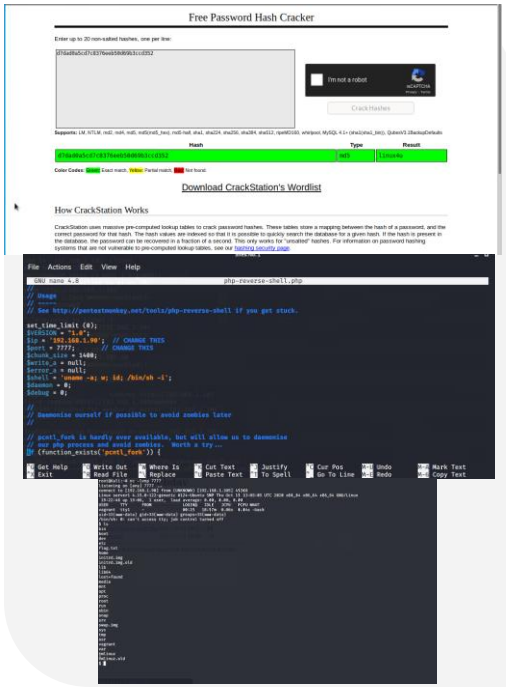
After obtaining Ryans hashed Password I used crackedstation.com and was able to obtain the plain text password. Using this I used Cadaver to connect to the Webdav server and was able to upload a reverse shell.

02

Achievements

I was able to generate a reverse shell with full access to the Webdav contents.

03



Blue Team
Log Analysis and Attack Characterization

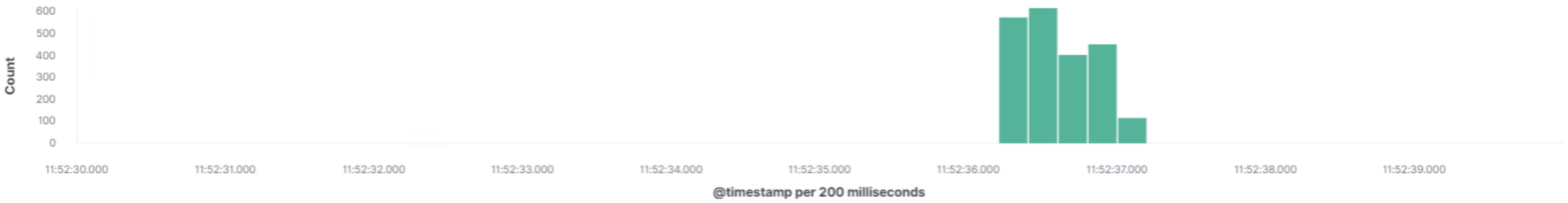
Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

2,158 hits

Oct 29, 2020 @ 11:52:30.000 - Oct 29, 2020 @ 11:52:40.000 — Auto

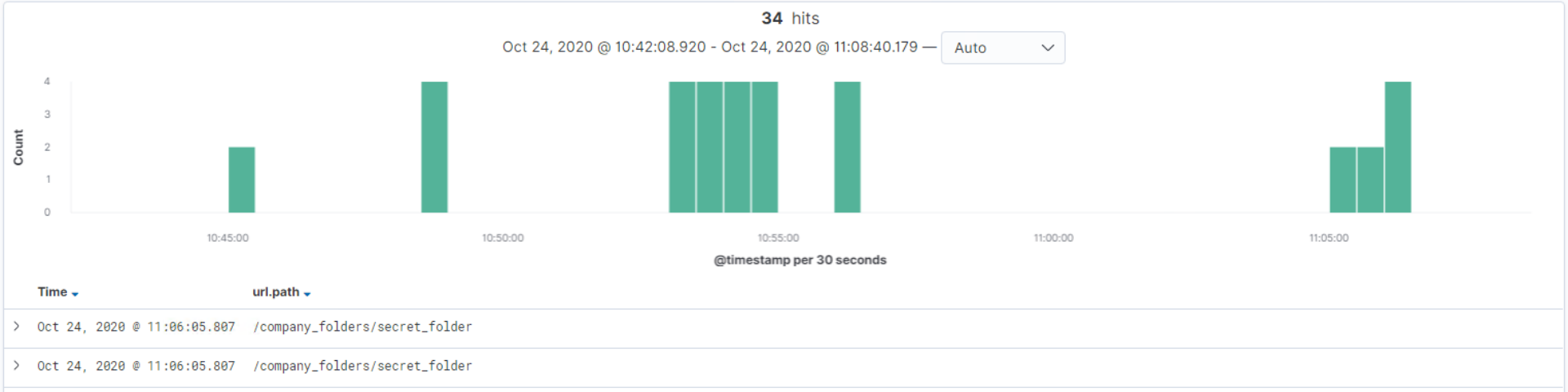


Time	user_agent.original	agent.name	source.ip	server.port	destination.packets
Oct 29, 2020 @ 11:52:37.179	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	-	192.168.1.90	80	-
Oct 29, 2020 @ 11:52:37.179	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	-	192.168.1.90	80	-
Oct 29, 2020 @ 11:52:37.179	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	-	192.168.1.90	80	-
Oct 29, 2020 @ 11:52:37.179	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	-	192.168.1.90	80	-

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

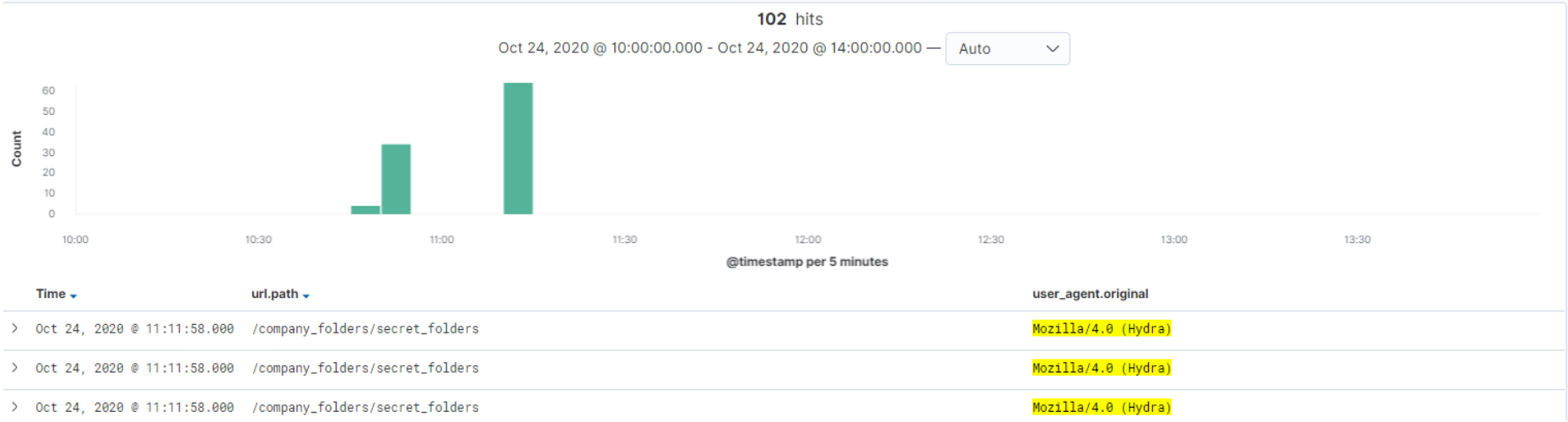


Time	url.path
Oct 24, 2020 @ 11:06:05.807	/company_folders/secret_folder
Oct 24, 2020 @ 11:06:05.807	/company_folders/secret_folder

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?

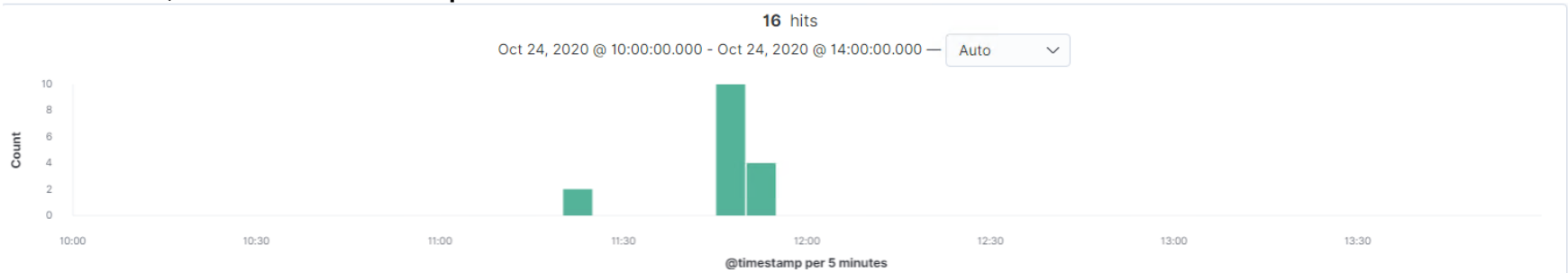


Time	url.path	user_agent.original
Oct 24, 2020 @ 11:11:58.000	/company_folders/secret_folders	Mozilla/4.0 (Hydra)
Oct 24, 2020 @ 11:11:58.000	/company_folders/secret_folders	Mozilla/4.0 (Hydra)
Oct 24, 2020 @ 11:11:58.000	/company_folders/secret_folders	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?
- Which files were requested?



Time	url.path	user_agent.original
Oct 24, 2020 @ 11:51:26.911	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Oct 24, 2020 @ 11:51:26.357	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Oct 24, 2020 @ 11:50:12.938	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Oct 24, 2020 @ 11:50:12.390	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Oct 24, 2020 @ 11:45:56.831	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Oct 24, 2020 @ 11:45:56.305	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Oct 24, 2020 @ 11:45:35.774	/webdav/	cadaver/0.23.3 neon/0.30.2
Oct 24, 2020 @ 11:45:35.773	/webdav/	cadaver/0.23.3 neon/0.30.2
Oct 24, 2020 @ 11:45:35.772	/webdav/	cadaver/0.23.3 neon/0.30.2
Oct 24, 2020 @ 11:45:35.250	/webdav/	cadaver/0.23.3 neon/0.30.2

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

A port ping and syn alarm can be set when the requests exceed more than 3 per second across multiple ports from the same originating IP.

System Hardening

What configurations can be set on the host to mitigate port scans?

1. Drop incoming Ping request Packets.
2. Implement a CMS Manager to deny ping sweeps and port scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

Alert SOC whenever an unknown IP attempts to access the directory.

System Hardening

What configuration can be set on the host to block unwanted access?

1. Whitelist authorized internal IP's and explicitly deny all others.
2. Set-up two-factor authentication
3. Scrub all public facing documents for any mention of secret directories or proprietary company information.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

Alert SOC when the number of failed logins exceeds 3, also alert SOC if the time between attempts is less than 5 seconds.

System Hardening

What configuration can be set on the host to block brute force attacks?

1. Enable user agent blocking from known Hydra sources.
2. Enable account lockout after 5 failed login attempts.
3. Enable account login delay timer between failed attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

Alert SOC when an IP outside of the Whitelist is attempting to access the WebDav Service.

Alert the SOC of any file upload(s) originating from outside the Corporate Network.

System Hardening

What configuration can be set on the host to control access?

1. Enable Two-factor Authentication
2. Deny access by IP's outside of the network.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Alert SOC if any attempt is made to upload files from outside the Corporate Network.

System Hardening

What configuration can be set on the host to block file uploads?

1. Deny uploading of .php files.
2. Deny uploads from IP's outside the Corporate Network.


The End