

X-CORP

Network Analysis

Security Engineering: CSIRT Division
Attack, Defense & Analysis of X-CORP'S Network

Table of Contents

This document contains the following resources:

01

Network Topology, Critical Vulnerabilities, and Incidents

02

Traffic Profiles

03

Normal Activity

04

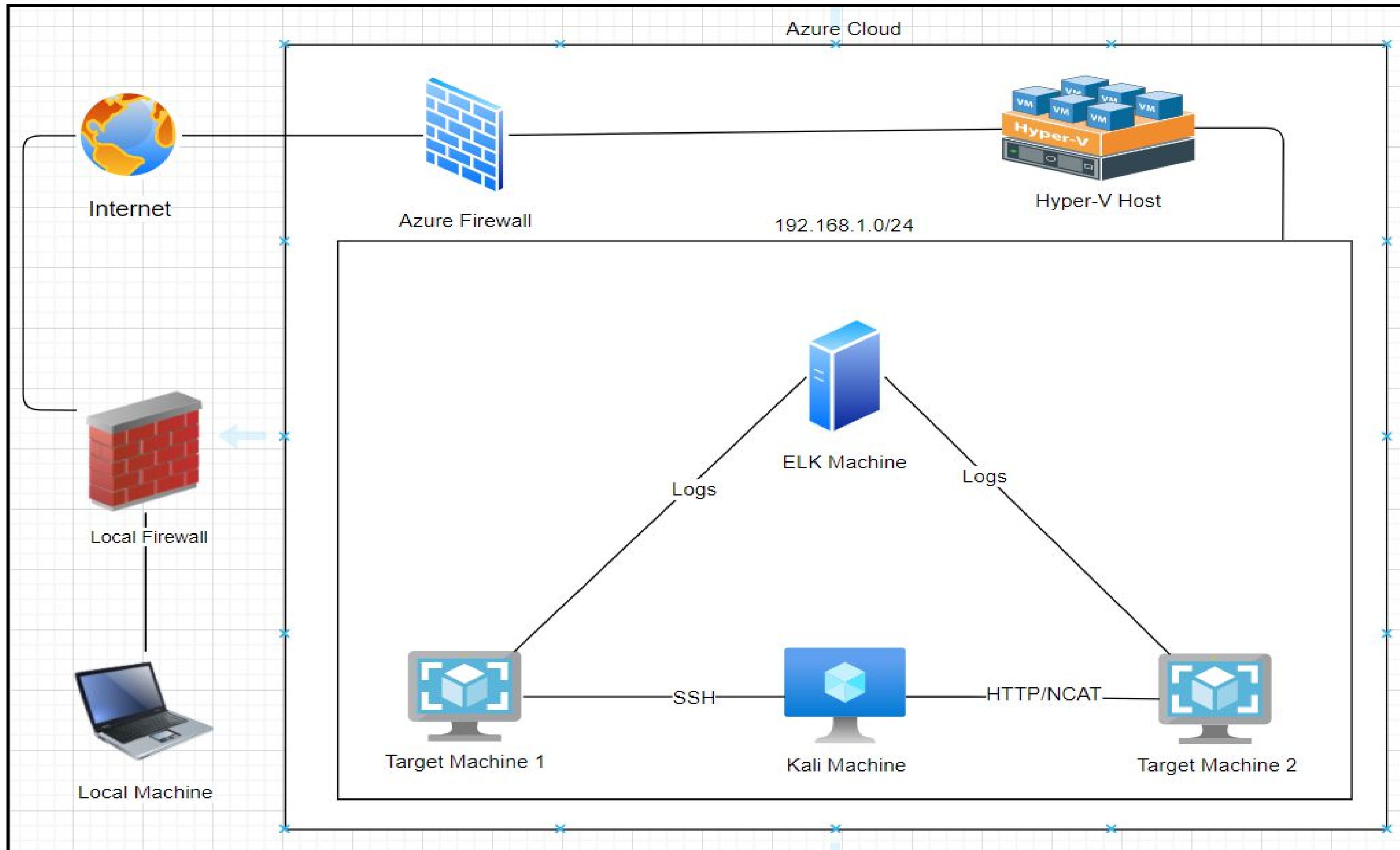
Malicious Activity

05

Recommendations

Network Topology & Critical Vulnerabilities

Network Topology – 192.168.1.0/24



Network

Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

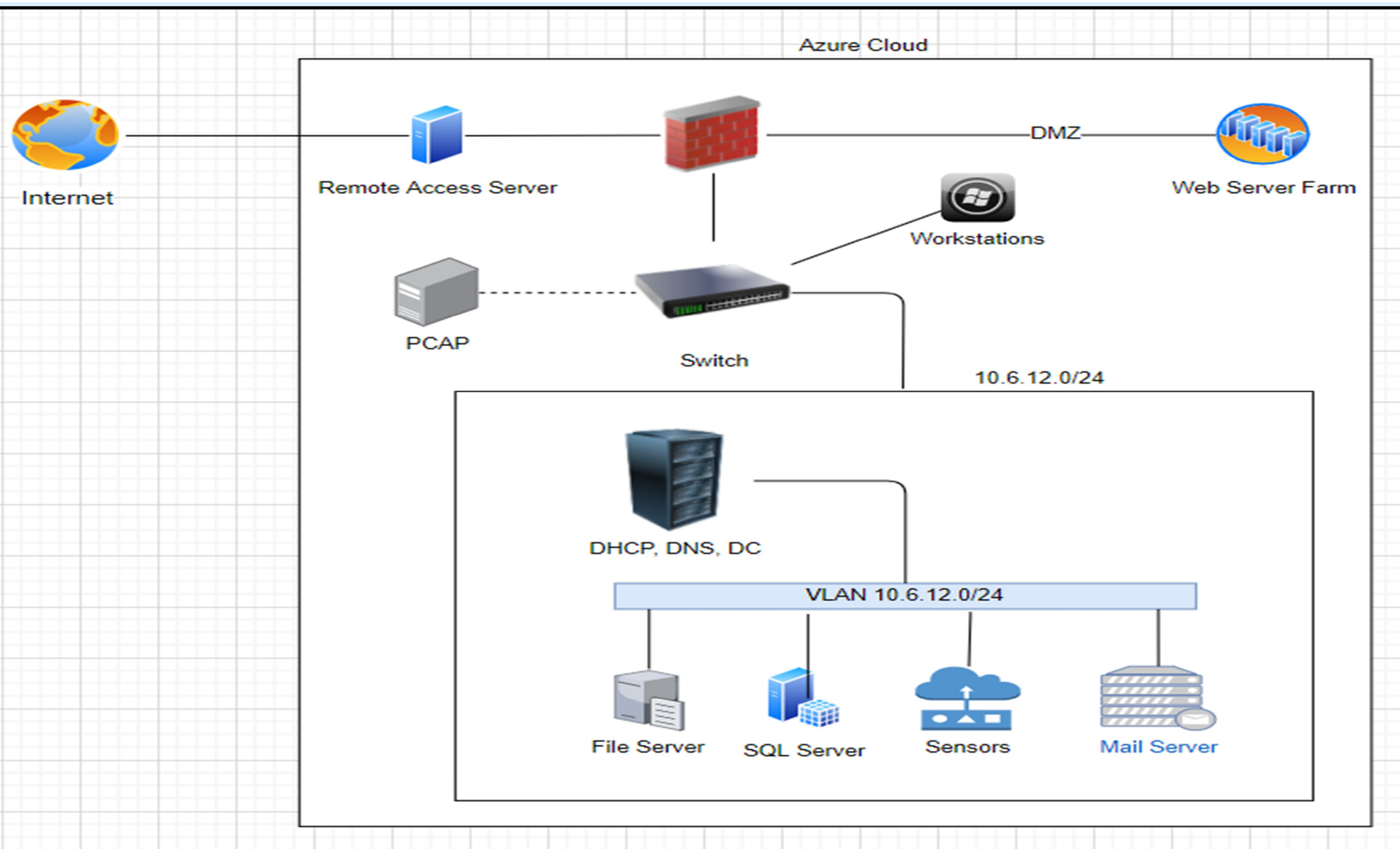
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Network Topology – 10.6.12.0/24



Network

Address Range:

10.6.12.0/24

Netmask: 255.255.255.0

Gateway: 10.6.12.1

Machines

IPv4: 172.16.4.205

OS: Windows

Hostname: ROTTERDAM-PC

IPv4: 10.0.0.201

OS: Windows

Hostname: BLANCO-DESKTOP

Recon: Describing the Target

Nmap identified the following hosts on the network: 192.168.1.0/24 & 10.6.12.0/24

<i>Hostname</i>	<i>IP Address</i>	<i>Role on Network</i>
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Windows host machine.
Kali	192.168.1.90	Linux OS, attack machine.
Target Machine 1	192.168.1.110	Target machine that is running on Linux.
Target Machine 2	192.168.1.115	Second target machine running on Linux.
ELK	192.168.1.100	ELK machine running on Linux. Hosts Kibana & Elasticsearch Watcher.
ROTTERDAM-PC	172.16.4.205	Windows machine, connected to X-CORP.
BLANCO-DESKTOP	10.0.0.201	Windows machine, connected to X-CORP.

Critical Vulnerabilities: Target 1

Assessment uncovered the following critical vulnerabilities in *Target 1*.

<i>Vulnerability</i>	<i>Description</i>	<i>Impact</i>
Unfiltered Web Port (Port 80)	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	With port 80 open, this allows web server access.
Unfiltered SSH Port (Port 22)	Port 22, also known as the secure shell port, allows a user to remotely connect to another machine via remote command execution.	SSH into target machine with discovered credentials.
User Enumeration	Web application vulnerability that allows attackers to use bruteforce techniques to validate users on a network.	Enumerate a list of users to target.

Critical Vulnerabilities: Target 1

Assessment uncovered the following critical vulnerabilities in *Target 1*.

<i>Vulnerability</i>	<i>Description</i>	<i>Impact</i>
Weak User Credentials	Short names, first name, or any simple combinations.	Password is easy to obtain through social engineering.
Misconfigured Security Controls CWE-284	Improper controls are implemented leaving systems vulnerable to exploits.	Allows unauthorized system level and network access.
Confidential Data Improperly Secured CWE-219	Confidential data, such as user login information, is easily accessible to the public with no security.	Database server authentication information easily accessible to public.

Critical Vulnerabilities: Target 2

Assessment uncovered the following critical vulnerabilities in *Target 2*.

<i>Vulnerability</i>	<i>Description</i>	<i>Impact</i>
WordPress XML-RPC DOS	WordPress XML-RPC parsing is susceptible to DOS attacks by executing pingback.ping.	Several affected WordPress installations can launch a botnet level attack.
WordPress XML-RPC Ping	Using HTTP POST request smuggling to bypass front-end security controls.	Application's internal layers can be targeted.
Cloudflare Protection Bypass	Execution of pingback.ping method can be used to bypass DNS level protection.	Target's public IP address can be revealed.

Critical Incidents: Network 10.6.12.0/24

Assessment uncovered the following critical incidents in **10.6.12.0/24**.

<i>Incident</i>	<i>Description</i>	<i>Impact</i>
Trojan Malware	Malicious computer virus.	Malware downloaded locally and infected multiple hosts on network.
Unauthorized Domain Setup	Private domain created without authorization.	Private domain created to conduct torrenting, avoid detection, and stream videos.
Illegal Torrenting	Downloading & uploading files through a torrent network.	Copyrighted materials downloaded.

Traffic Profiles

Traffic Profile on 192.168.1.0/24

Analysis identified the following characteristics of the traffic on the network:

<i>Feature</i>	<i>Value</i>	<i>Description</i>
Top Talker (192.168.1.90)	Ip.addr==192.168.1.0/24	Machine that sent the most traffic.
Most Common Protocols (HTTP, SSH, TCP, UDP)	Ip.addr==192.168.1.0/24	Most common protocols on the network.
3 Unique IP Addresses (192.168.1.90, 192.168.1.110, 192.168.1.115)	Ip.addr==192.168.1.0/24	Count of observed IP addresses.

Traffic Profile on 10.6.12.0/24

Analysis identified the following characteristics of the traffic on the network:

<i>Feature</i>	<i>Value</i>	<i>Description</i>
Top Talkers (172.16.4.205), (185.243.115.84), (166.62.11.64)	Ip.addr==10.6.12.0/24	Machines that sent the most traffic.
Most Common Protocols (HTTP, TCP, UDP)	Ip.addr==10.6.12.0/24	Most common protocols on the network.
2 Unique IP Addresses (172.16.4.205 & 185.243.115.84)	Ip.addr==10.6.12.0/24	Count of observed IP addresses.
1 Malware Species (Trojan malware)	Ip.addr==10.6.12.203 and http.request.method==GET	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity:

“Normal” Activity

- Employees accessing public KB
- Employees checking emails

Suspicious Activity

- Enumerating users – WPSCAN
- Executing pingback.ping command
- Accessing authentication logs & back-end DB server files – “wp.config.php” file
- Accessing DB servers and dumping hashes
- Setting up a private Active Directory Domain



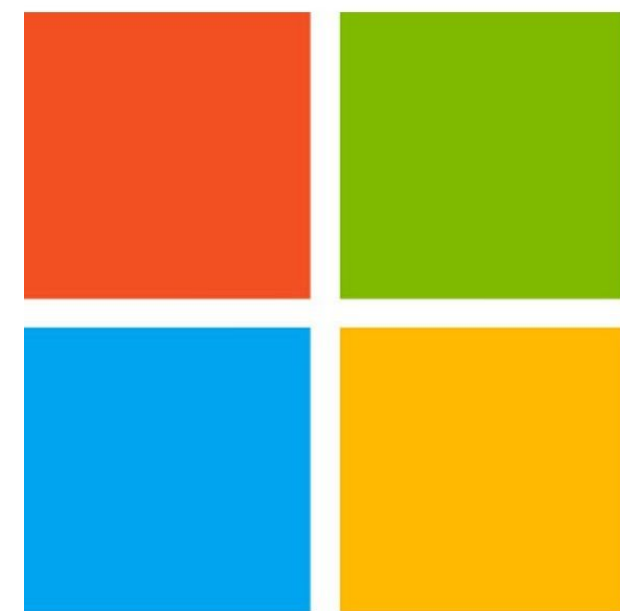


Normal Activity

Normal Behavior – Accessing Public Knowledgebase

Knowledgebase Articles:

- HTTPS to establish a secure connection to Microsoft's website.
- User accessed files on creating private domains.



Microsoft

Normal Behavior – Accessing Google Workspace

Accessing Email:

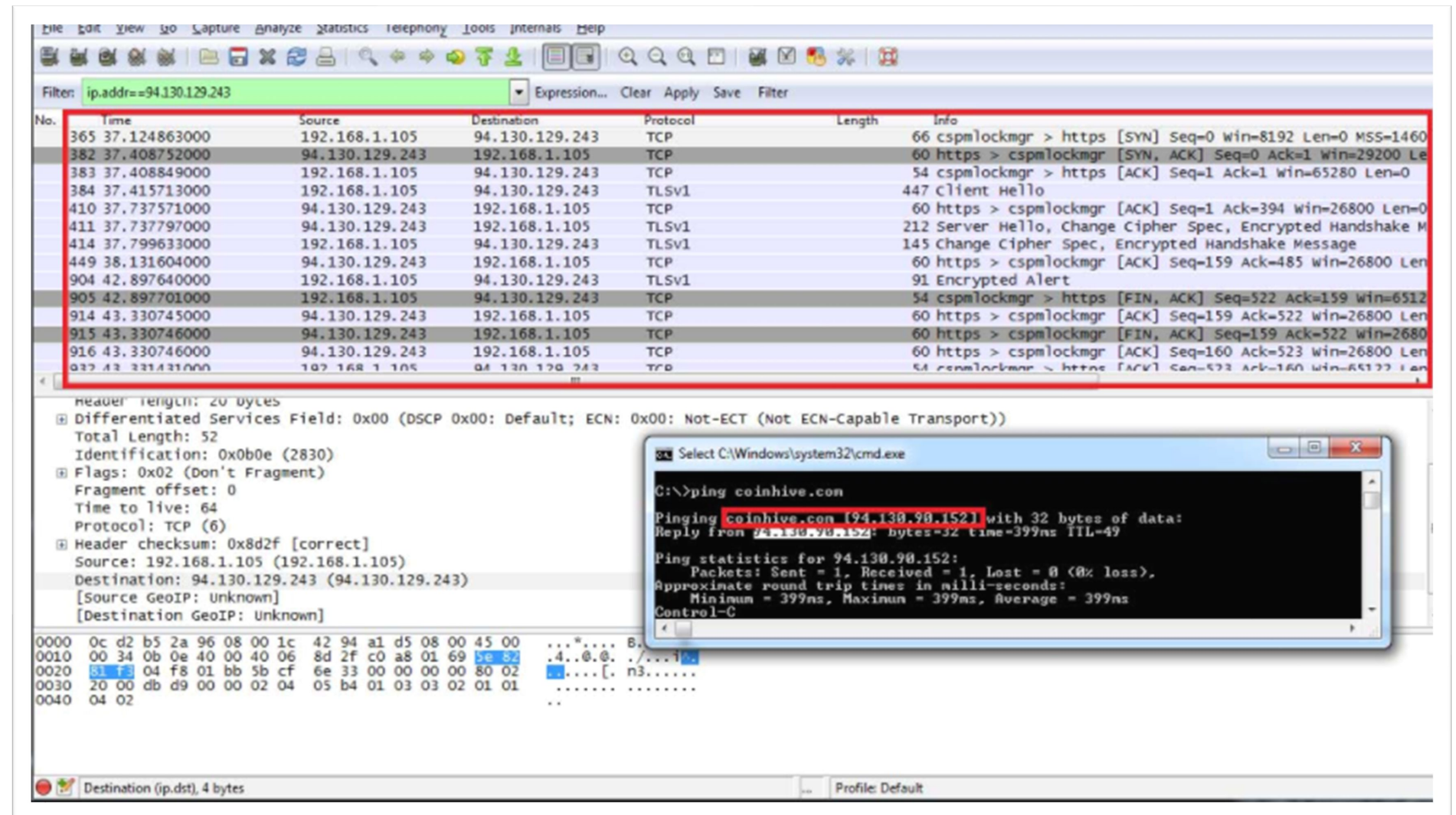
- HTTPS to establish a secure connection with the Google client
- Users authenticate to access email



Malicious Activity

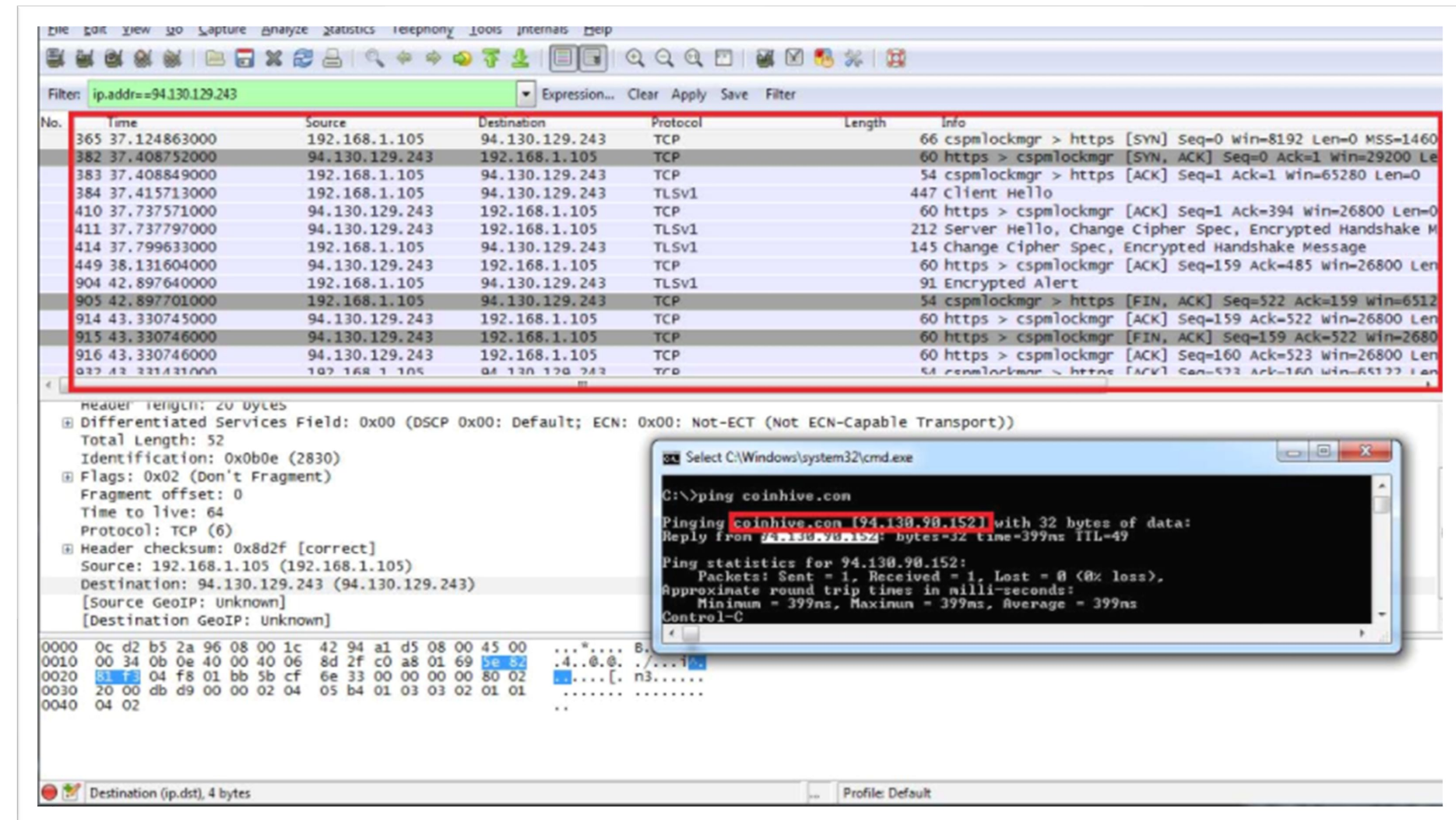
Malicious Behavior – Enumeration

- Excessive HTTP errors (400 errors)
- Attacker ran a WPSCAN to enumerate potential users to target.
 - Enumeration is noisy
 - Users targeted:
 - Michael
 - Steven



Malicious Behavior – XML-RPC Ping & DDOS

- XML-RPC
 - XML-RPC ping using HTTP POST smuggling to bypass front-end security controls
- Pingback.ping to bypass DNS level protection to launch a Cloudflare attack
 - Allowed for command & control – botnets



Malicious Behavior – Unauthorized Access & Dumping Hashes

- Improper implementation of security controls allows for exploitation
- Port 22 – unfiltered port allows for remote command execution
- Attacker SSH with Michael's discovered credentials to access SQL server to dump hashes

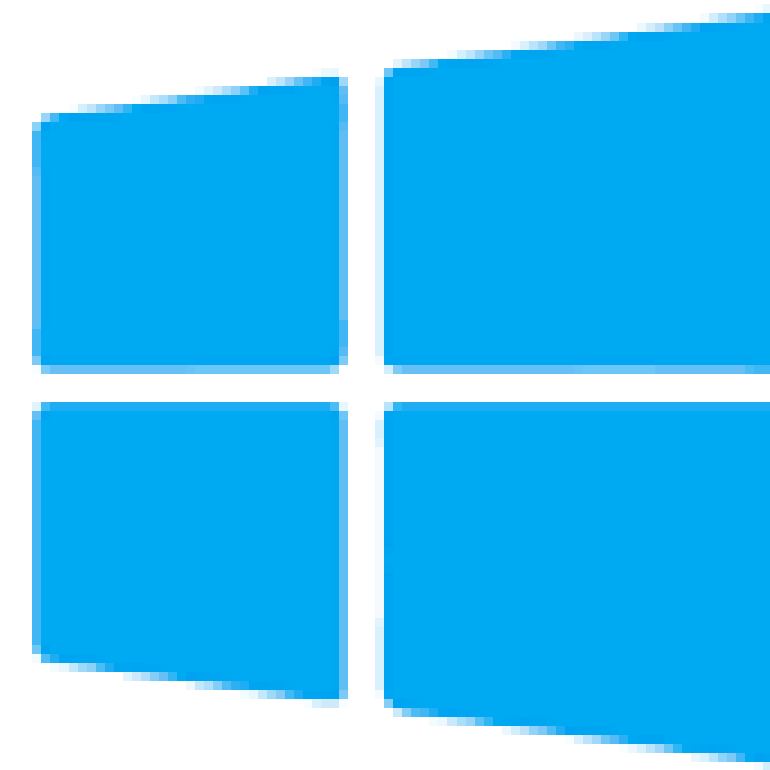
```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu Jun  3 11:46:44 2021 from 192.168.1.90
michael@target1:~$ █
```

Malicious Behavior – Creating a Private Domain

- Private domain created on corporate network.
- Users were constantly browsing videos on YouTube
- Trojan Malware downloaded
 - Additional hosts infected
 - Hosts infected:
 - 10.6.12.203
 - 172.16.4.205
 - 185.243.115.84 – suspicious activity detected
 - 166.62.11.64



Active Directory

Malicious Behavior – Illegal Torrenting on Private Domain

- Users torrenting on network
 - Downloading copyrighted material
 - User downloaded recipe files
- Copyright Infringement
 - This creates some legal complications





The End