Capstone Engagement

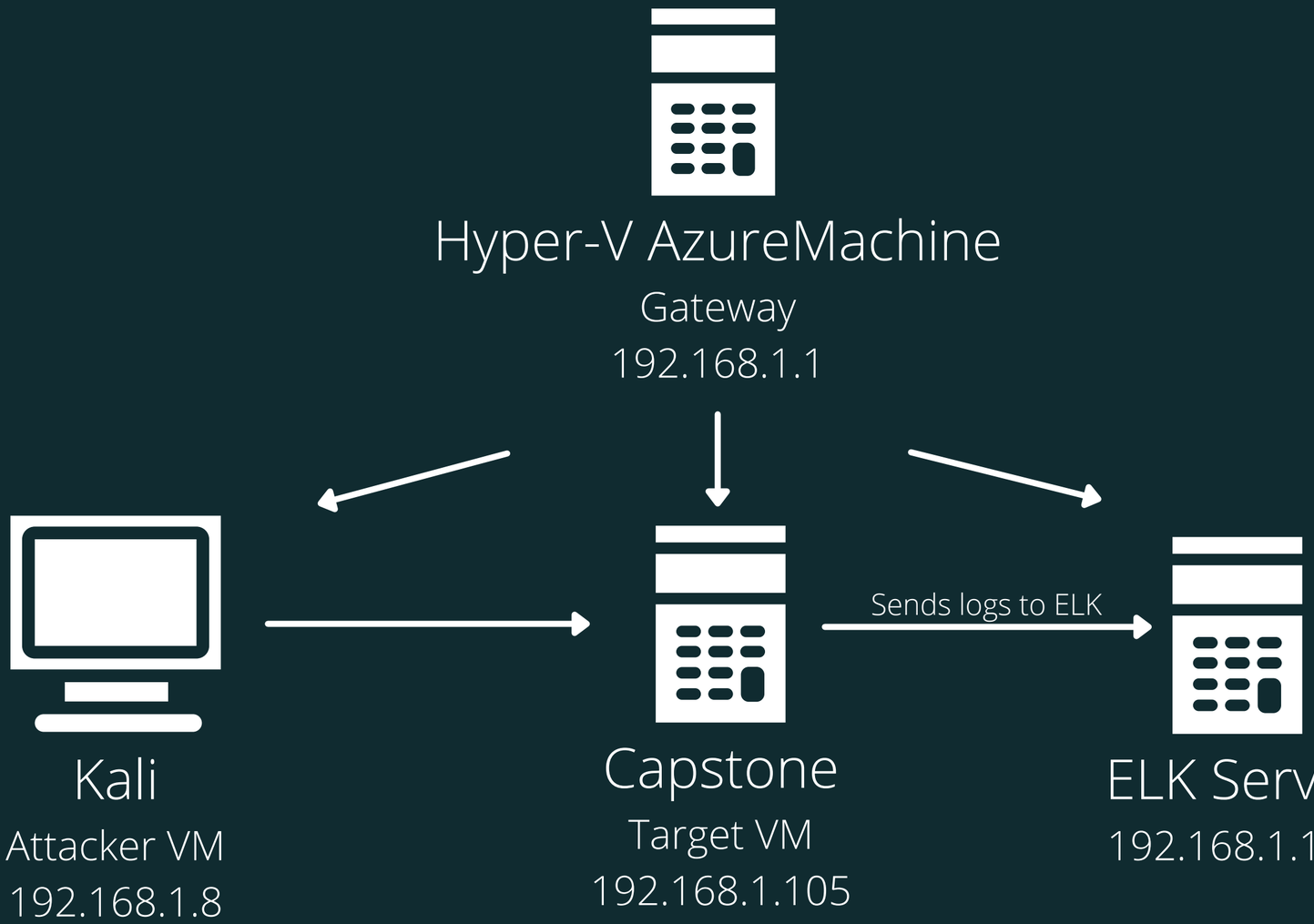
Assessment, Analysis, and Hardening of a Vulnerable System

KALEIGH GLATFELTER

Table of Contents

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

02

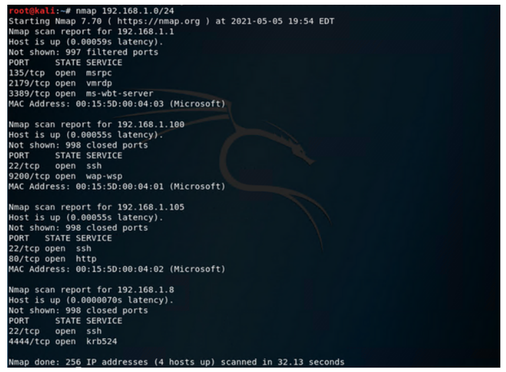
Achievements

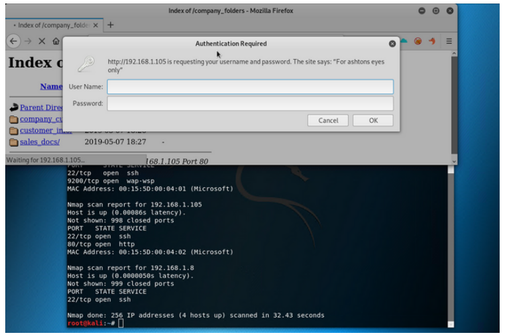
- secret_folder was revealed
- Directory has a login prompt, susceptible to a brute-force attack

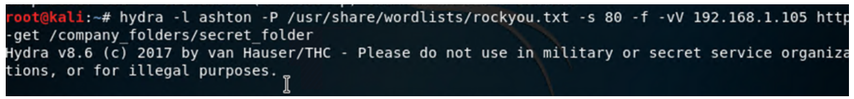
03

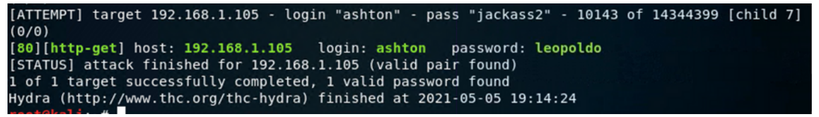
Exploitation

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









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

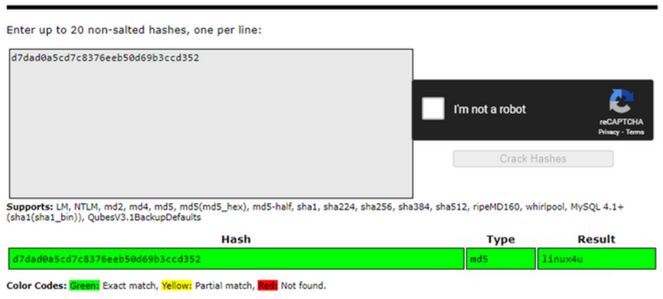
Achievements

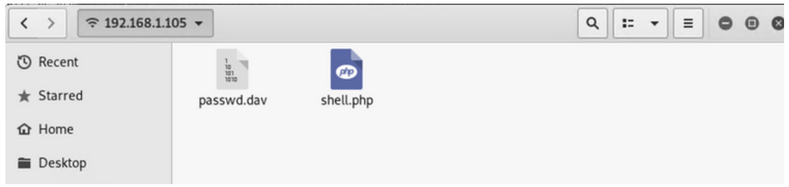
- By generating a web shell, bad actors are able to execute arbitrary shell commands on the target machine

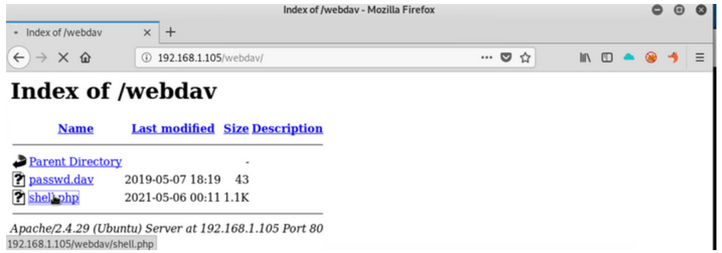
03

Aftermath

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







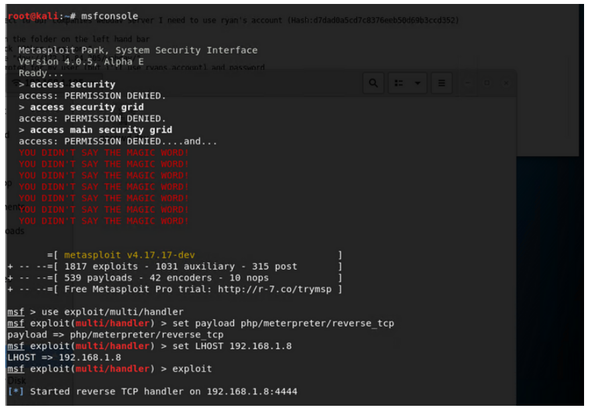
Exploitation:

Remote Code Execution

01

Tools & Processes

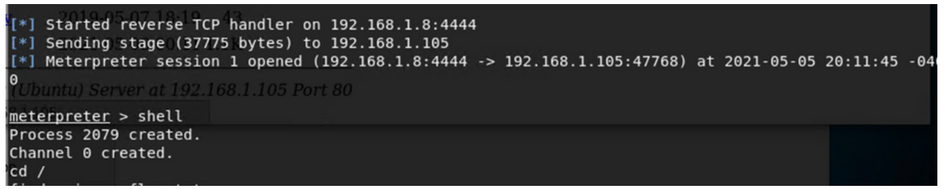
- Meterpreter is used to connect to the uploaded web shell
- Use Meterpreter shell to compromise target machine



02

Achievements

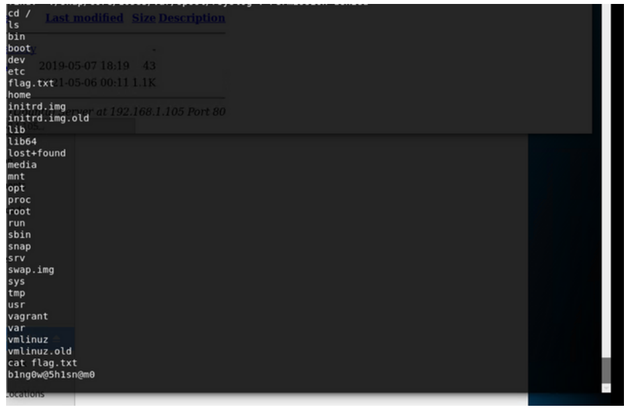
- Bad actors are able to exploit the Remote Code Execution to open a Meterpreter shell to the target machine
- Once in the Meterpreter shell, the file system is available for exploration



03

Aftermath

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

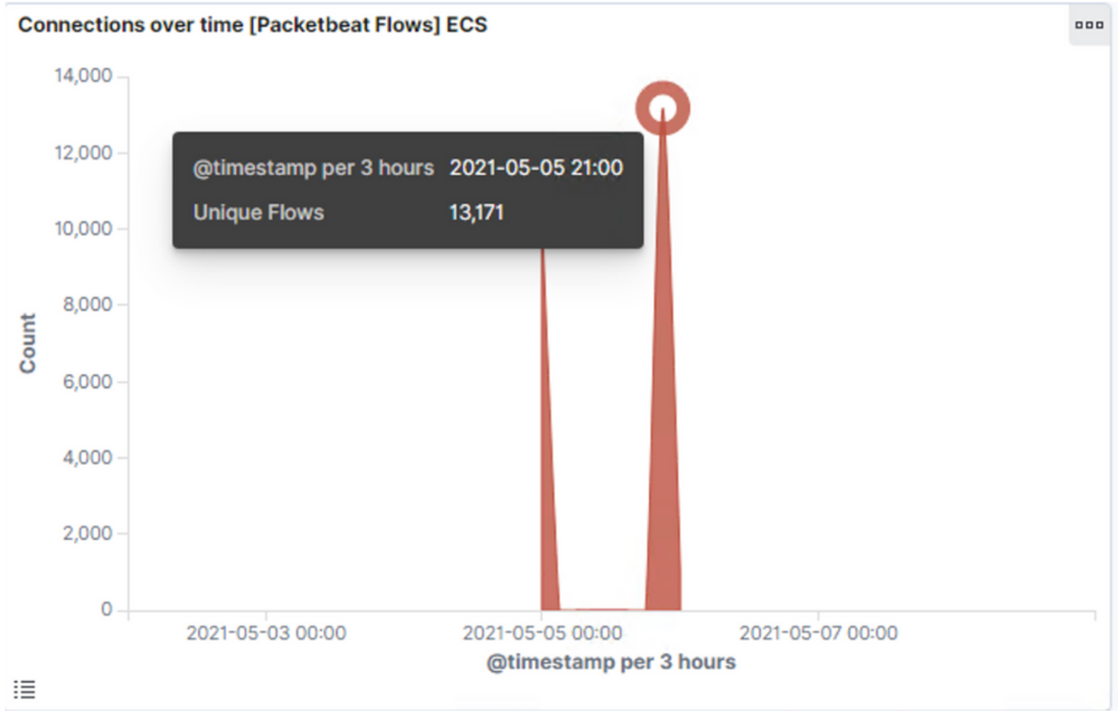


Blue Team

Log Analysis and Attack Characterization

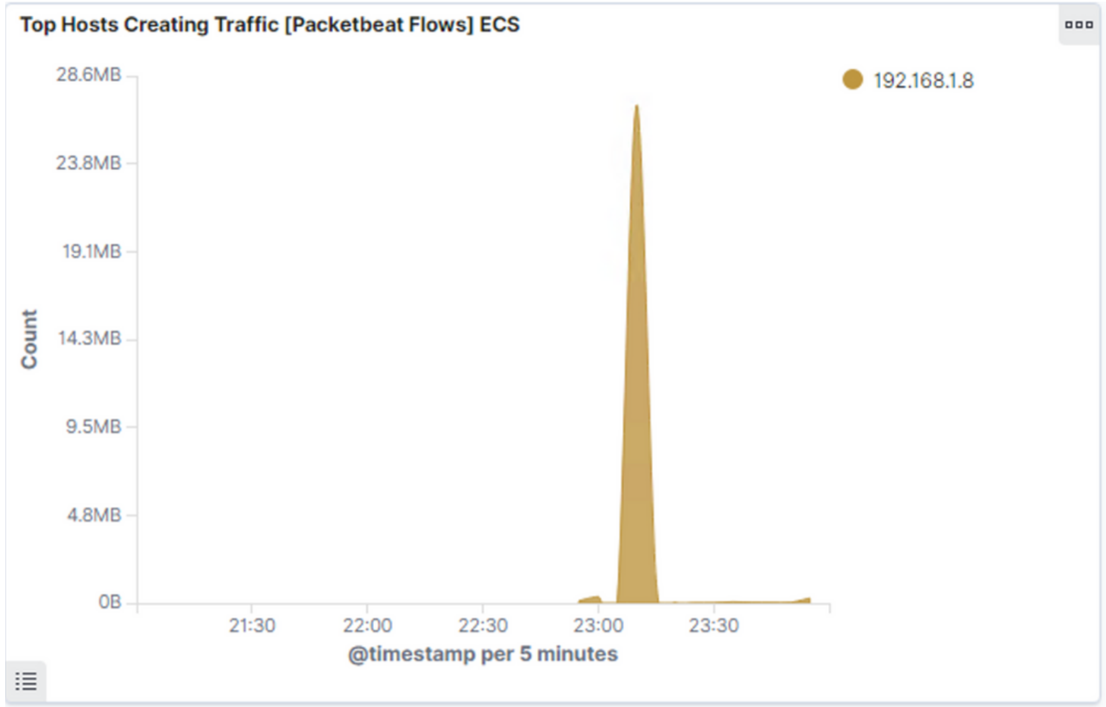
Analysis:

Identifying the Port Scan



What time did the port scan occur?

- 21:00 hours or 9:00 PM MST

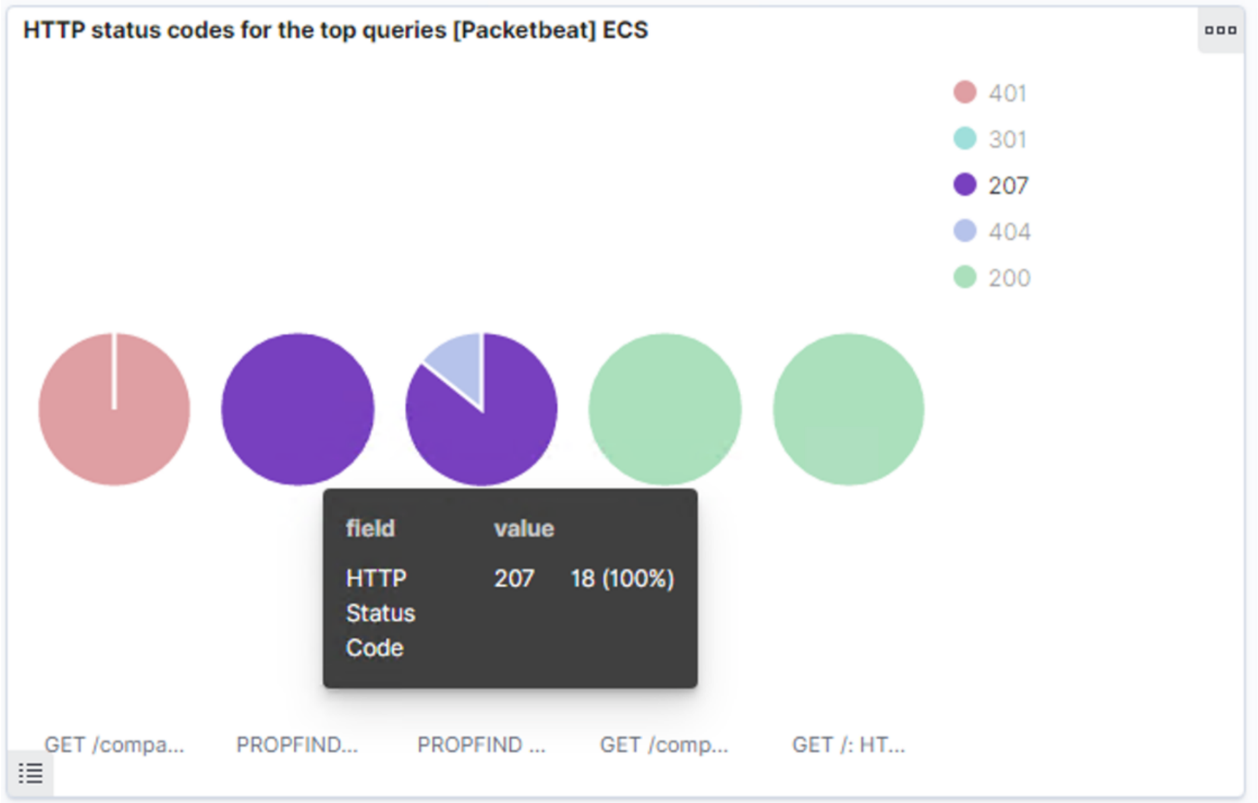


How many packets were sent, and from which IP?

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

Analysis:

Identifying the Port Scan (cont.)

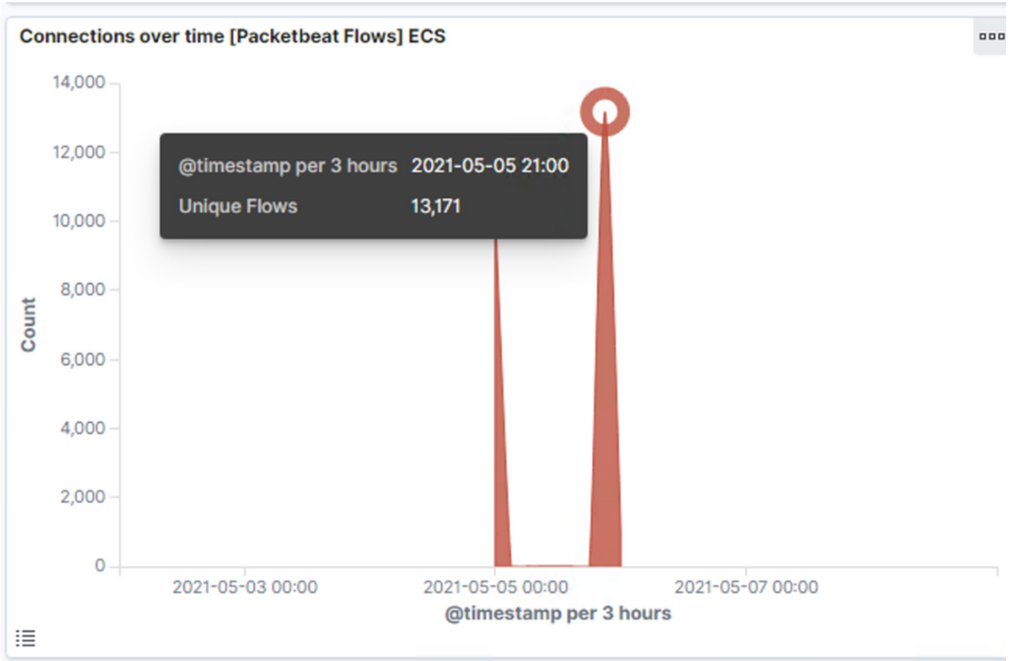


What indicates that this was a port scan?

- 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



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

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

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

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

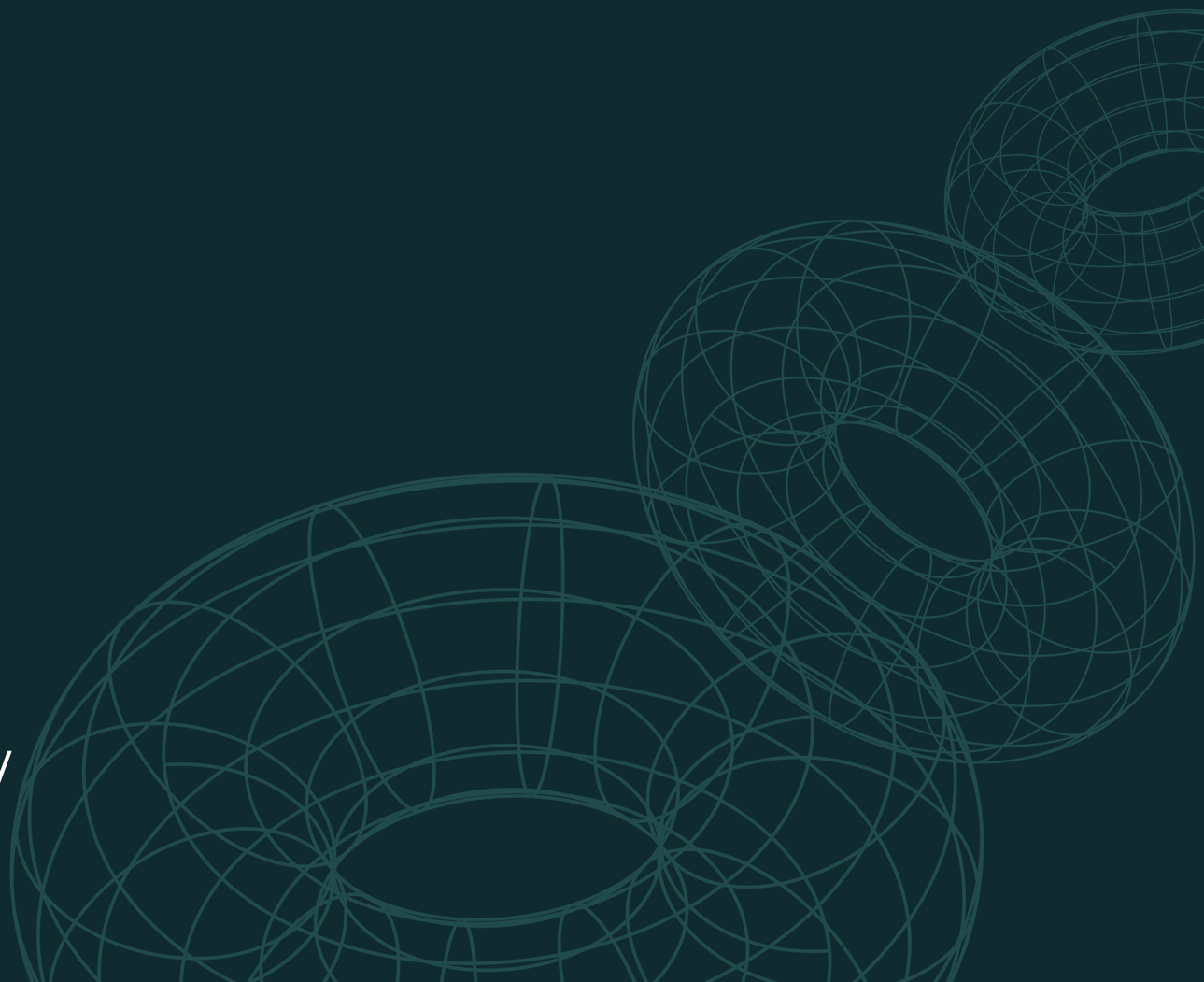
System Hardening

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.