Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

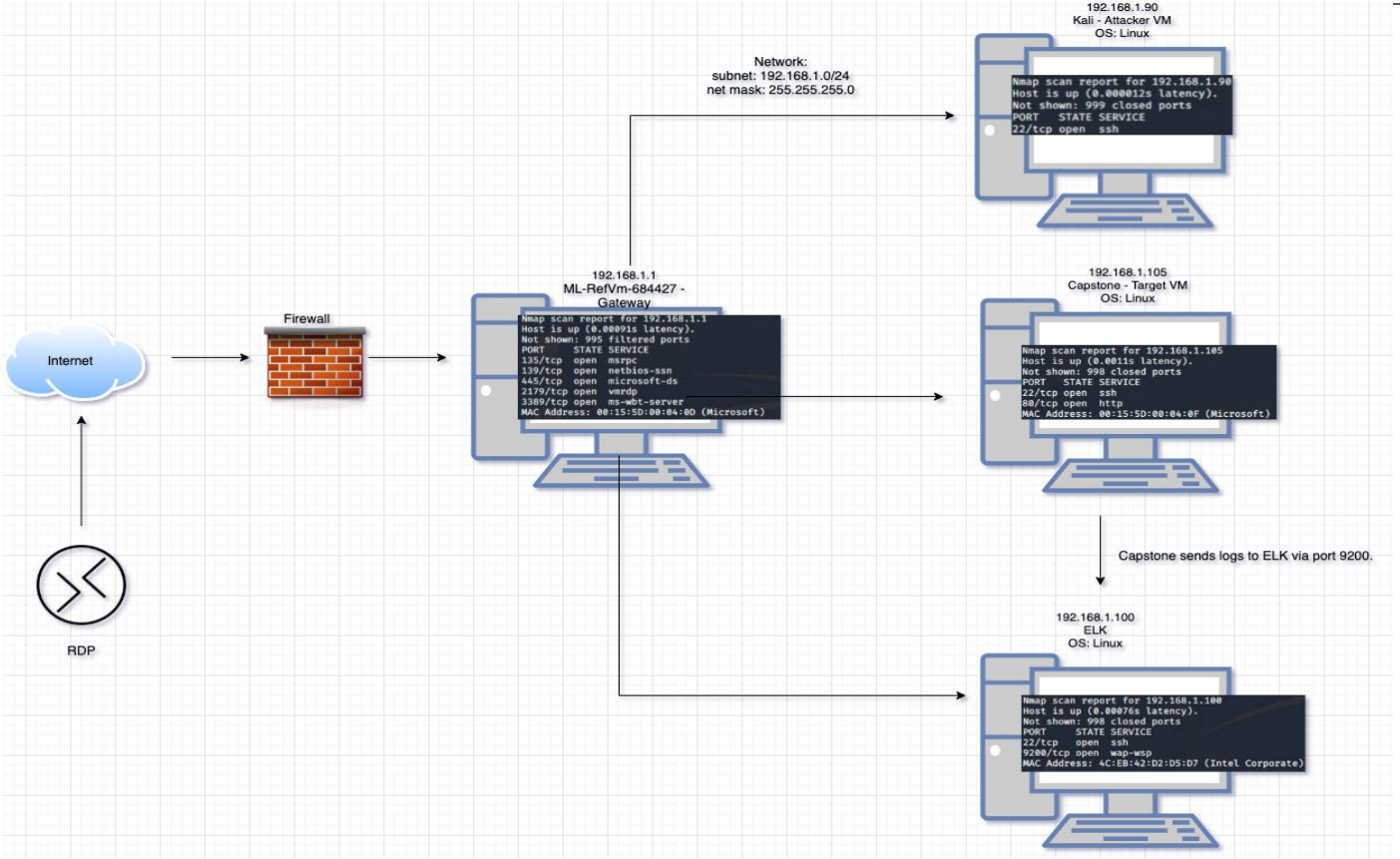
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali - Attacker VM

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone - Target VM

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali Linux	192.168.1.90	Attacker machine
Capstone	192.168.1.105	Web Server
ELK	192.168.1.100	SIEM System
ML-RefVm-684427	192.168.1.1	Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Sensitive Data Exposure OWASP Top 10 #3 || **Critical**	The secret_folder is publicly accessible, although it is intended for authorized personnel only.	Access to this folder exposed credentials to login to the server.
Unauthorized File Upload **Critical**	Lack of validations in uploading files, specifically php files puts the web server at risk for a wide range of attacks enabled by malicious files.	This vulnerability allowed attackers to upload malicious scripts directly to the server.
Remote Code Execution via Command Injection OWASP Top 10 #1 || **Critical**	Attackers can upload web shells and achieve arbitrary remote code execution on the web server.	Attackers can open a reverse shell to the servers.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

-Nmap service scan was used to detect open ports in addition to their version numbers to exploit vulnerabilities

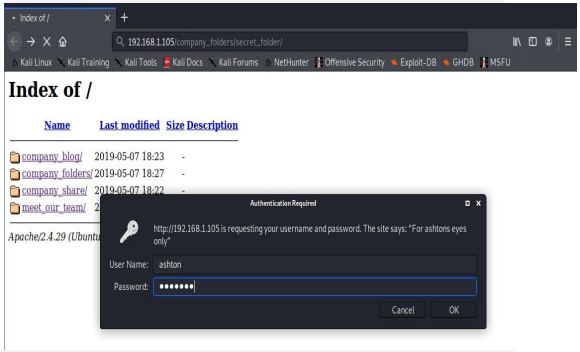
-dirb was utilized to find URLs on target site

02

Achievements

-A secret folder that was accessed via brute force attack

03




```
f 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 6] (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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-28 1
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

-Access to directory webdav with cracked credentials

-upload malicious php file generated from msfconsole

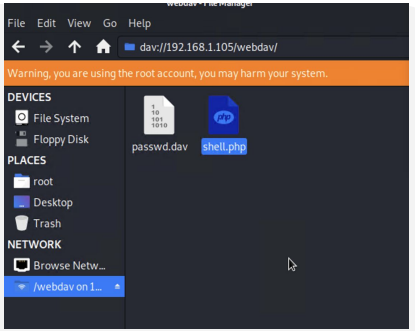
-upload php file to webdav

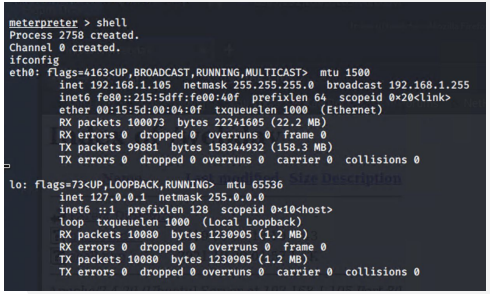
02

Achievements

-execute arbitrary shell commands on the target machine

03





Exploitation: Remote Code Injection via Command Injection

01

Tools & Processes
-use meterpreter to connect to uploaded shell

-shell was used to exploit target

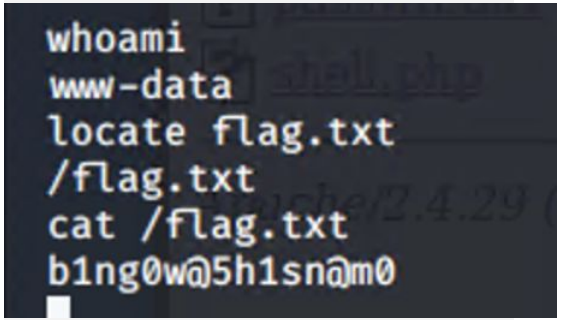
02

Achievements
-Remote code execution enabled a meterpreter shell connection to the target

-once the connection is established, the full file system is ready for exploitation

03

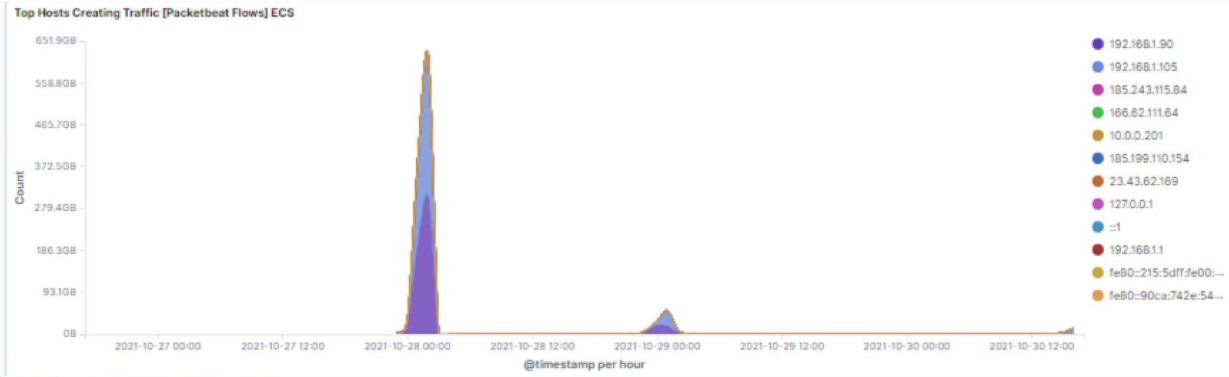
-capture the flag

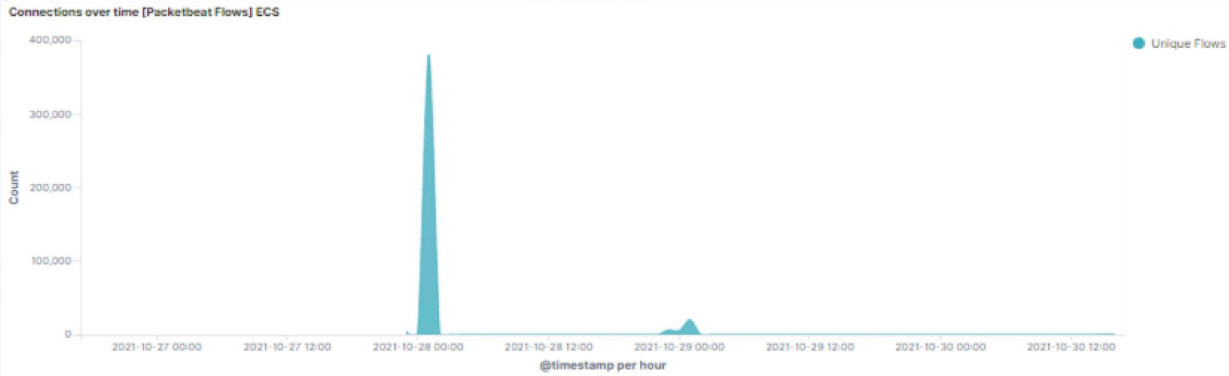


Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

A port scan was indicated by the spike in the Connections over time [Packetbeat Flows] ECS on 10-28-2021 at 00:00. The number of packets detected from 192.168.1.90 was 392,325 packets.





Connections over time [Packetbeat Flows] ECS

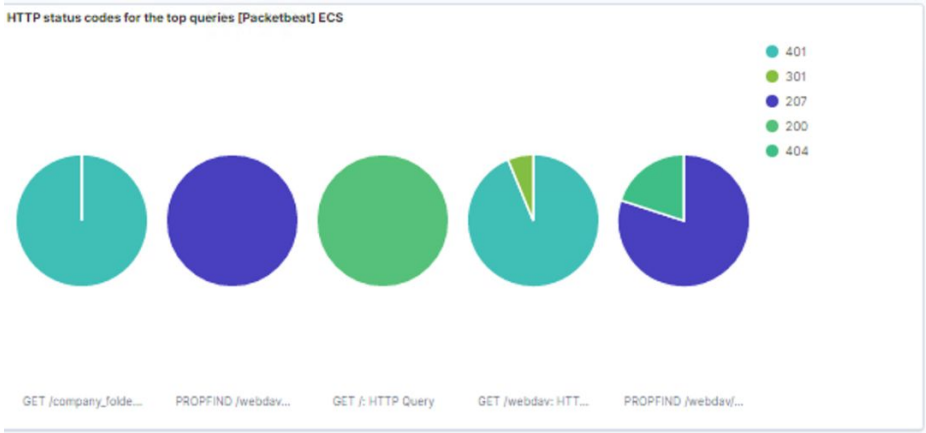
@timestamp per 3 hours	Unique Flows
2021-10-27 21:00	4,400
2021-10-28 00:00	392,325
2021-10-28 21:00	6,341
2021-10-29 00:00	26,381
2021-10-30 12:00	165
2021-10-30 15:00	1,634
2021-10-30 18:00	570
2021-11-01 21:00	3,906
2021-11-02 00:00	17,051

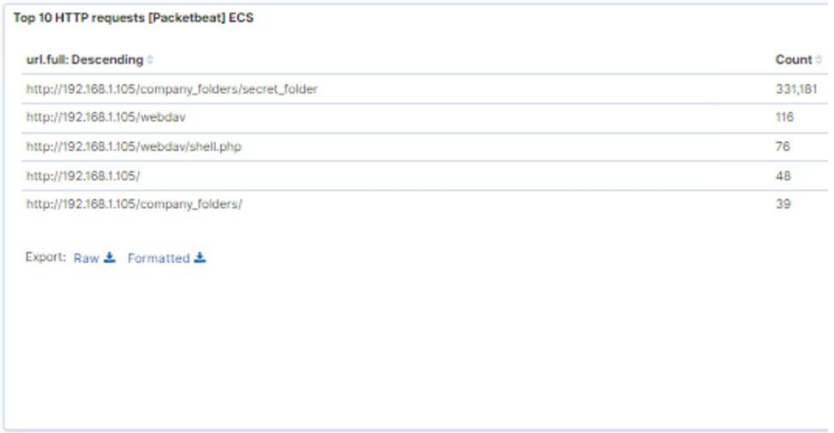
Analysis: Identifying the Port Scan Continued

What responses did the victim respond back with?

The top three hits for directories and files that were requested were

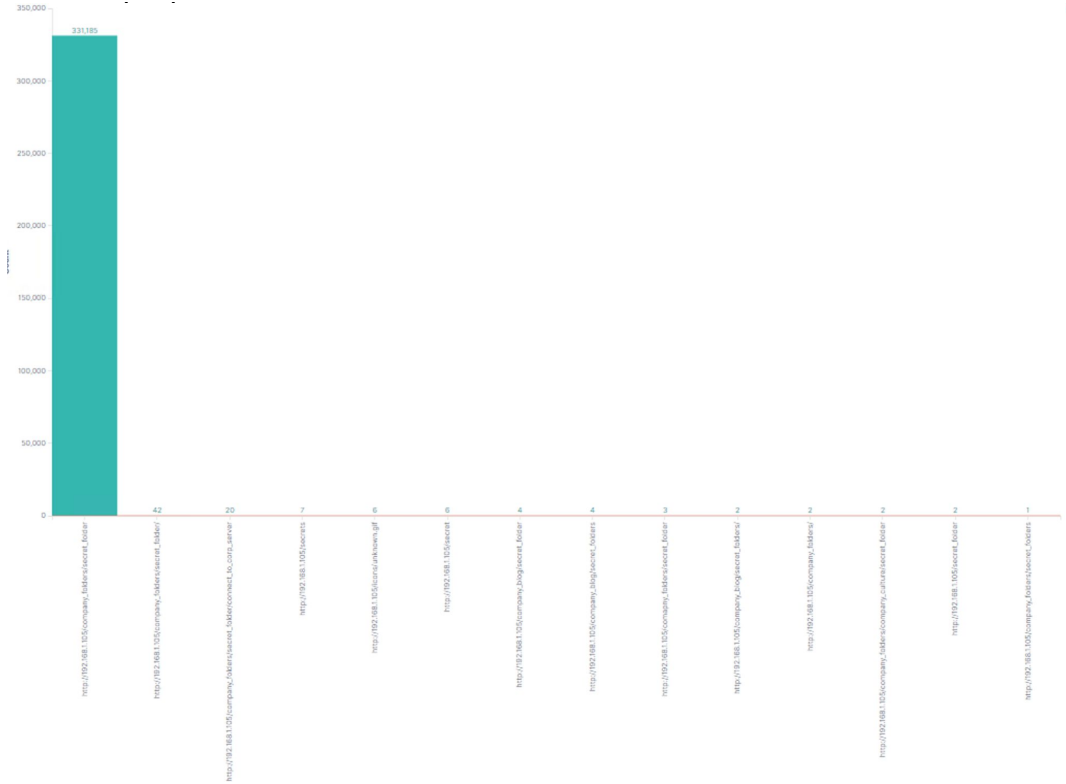
- http://192.168.1.105/company_folder/secret_folder
- http://192.168.1.105/company_folder/webdav
- http://192.168.1.105/webdav/shell.php





Analysis: Finding the Request for the Hidden Directory

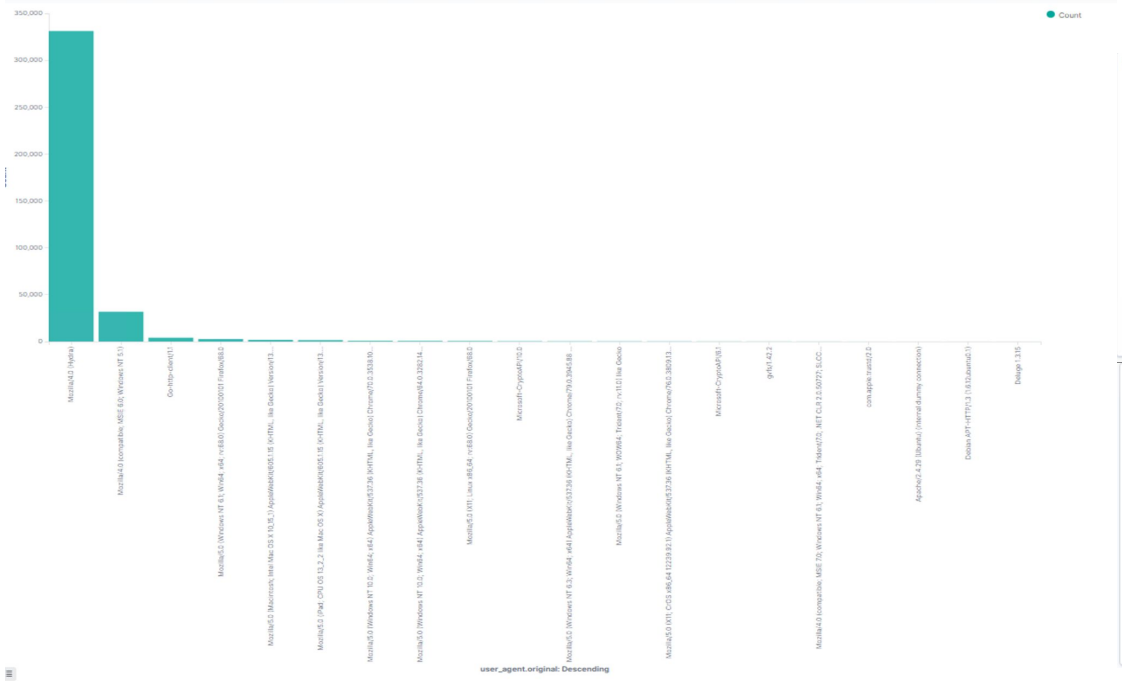
The hidden directory “company_folders/secret_folder” was accessed on 10-28-2021 and requested 331,185 times. The hidden directory contained a file “connect_to_corp_server” with sensitive information, such as



url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	331,185
http://192.168.1.105/company_folders/secret_folder/	42
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	20
http://192.168.1.105/secrets	7
http://192.168.1.105/icons/unknown.gif	6
http://192.168.1.105/secret	6
http://192.168.1.105/company_blog/secret_folder	4
http://192.168.1.105/company_blog/secret_folders	4
http://192.168.1.105/comapny_folders/secret_folder	3
http://192.168.1.105/company_blog/secret_folders/	2
http://192.168.1.105/company_folders/	2
http://192.168.1.105/company_folders/company_culture/secret_folder	2
http://192.168.1.105/secret_folder	2
http://192.168.1.105/company_folders/secret_folders	1

Analysis: Uncovering the Brute Force Attack

A total of 331,171 requests were made in the brute force attack, only 20 requests being successful.

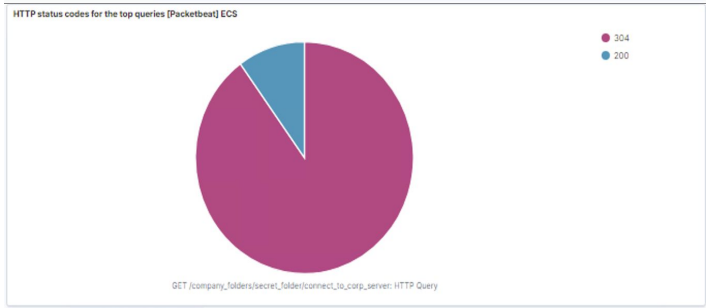


user_agent.original: Descending	Count
Mozilla/4.0 (Hydra)	331,171

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	20

Export: Raw Formatted



Analysis: Finding the WebDAV Connection

A total of 119 requests were made to the webDAV directory. The webDAV directory contained file shell.php and passwd.dav, which were requested 76 times and 8 times respectively.

url.full: Descending	Count
http://192.168.1.105/webdav	119
http://192.168.1.105/webdav/shell.php	76
http://192.168.1.105/webdav/	26
http://192.168.1.105/icons/back.gif	12
http://192.168.1.105/icons/blank.gif	12
http://192.168.1.105/icons/unknown.gif	12
http://192.168.1.105/webdav/passwd.dav	8
http://192.168.1.105/webdav_	6
http://192.168.1.105/	4
http://192.168.1.105/webdav/?C=N&O=D	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?

-Create an alert where a source ip has contacted destination ip over a reasonable threshold.

What threshold would you set to activate this alarm?

-Alarms should fire if a given IP address sends more than **10 requests per second** for **more than 5 seconds**

System Hardening

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

-The local firewall can be used to throttle incoming connections

-ICMP traffic can be filtered

-An IP allowed list can be enabled

"Set the Account Lockout Threshold to the Recommended Value." Microsoft, 5 Nov. 2020, docs.microsoft.com/en-us/services-hub/health/remediation-steps-ad/set-the-account-lockout-threshold-to-the-recommended-value.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

-Create an alert anytime this directory is accessed by an unauthorized machine

What threshold would you set to activate this alarm?

-This is a **binary** alarm: If the incoming IP is *not* allowed, it fires. Otherwise, it does not.

System Hardening

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

-Access to the sensitive file can be locally restricted to a specific user

This way, someone who gets a shell as, e.g., www-data will not be able to read it.

-The file should be encrypted at rest.

Mitigation: Preventing Brute Force Attacks

Alarm

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

-Set an alert that detects 401 Unauthorized codes returned from any server over 10 attempts per second for more than 5 seconds

-Create an alert if the user_agent.original value includes Hydra in the name

What threshold would you set to activate this alarm?

-More than 10 requests per second for 5 seconds should trigger the alarm

System Hardening

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

-Server can automatically drop traffic from the offending IP address for a period of 1 hour

-Display a lockout message and lock the page from login for a temporary period of time from that user

-Configuring fail2ban or a similar utility would mitigate brute force attacks

Mitigation: Detecting the WebDAV Connection

Alarm

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

-Monitor access to webdav with Filebeat

-Generate an alarm on any read performed on files within webdav

What threshold would you set to activate this alarm?

-Alarm will be triggered when an unauthorized IP address access the webdav directory or the files within the directory

System Hardening

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

-Connections to this shared folder should not be accessible from the web interface.

-Administrators must install and configure Filebeat on the host.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

-We can set an alert for any traffic moving over port 4444

-We can set an alert for any POST request containing for or file data of a .php file that is uploaded to a server

What threshold would you set to activate this alarm?

-Alarm will be triggered when malicious users upload malicious files

System Hardening

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

-Removing the ability to upload files to this directory over the web interface would take care of this issue

-Write permissions can be restricted on the host

-Uploads can be isolated into a dedicated storage partition

-Filebeat should be enabled and configured.


The End