Capstone Engagement

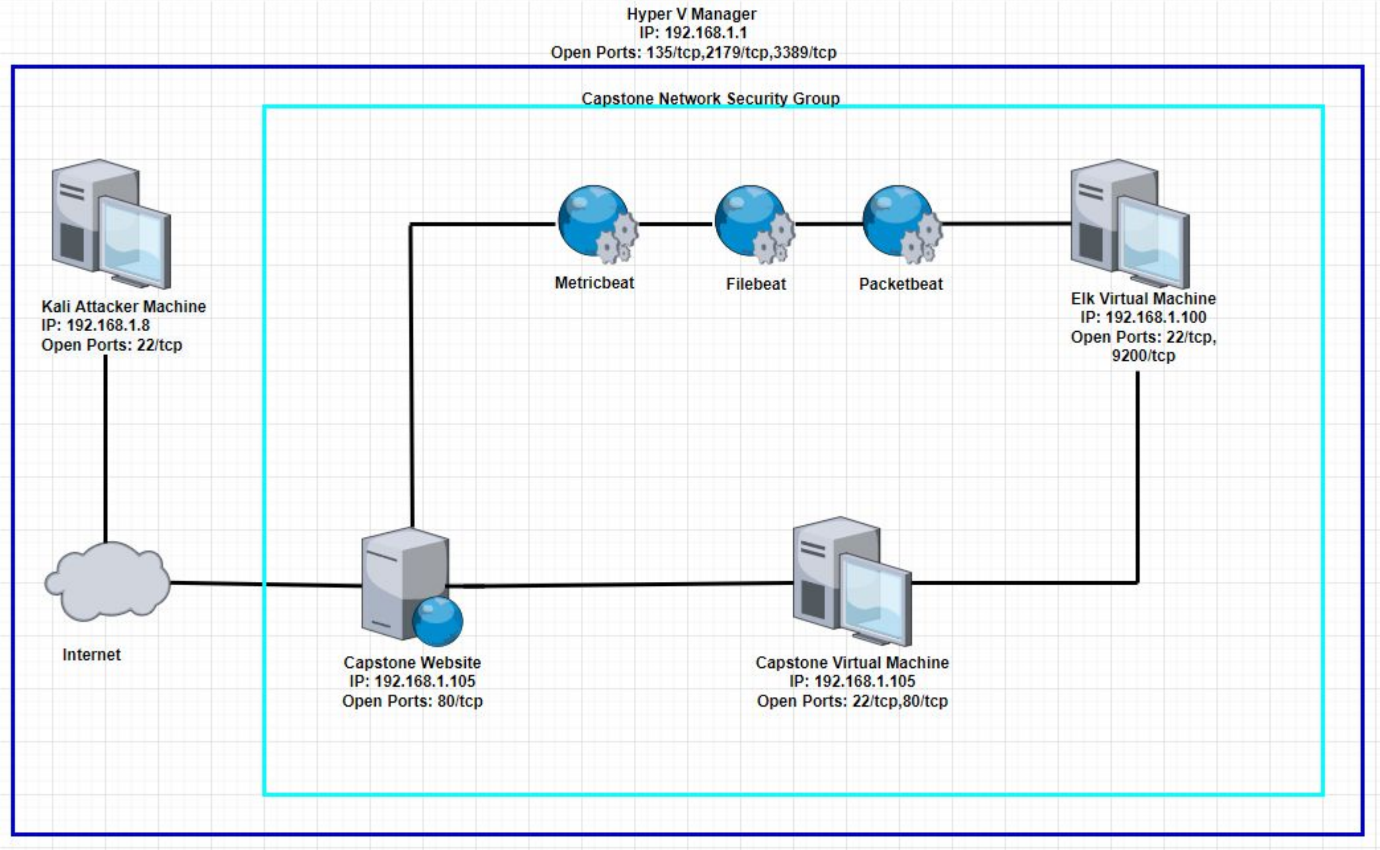
Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.8/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper V Manager

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk Virtual Machine

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone Virtual Machine

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali Attacker Virtual Machine

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper V Manager	192.168.1.1	Jumpbox provisioner hosting virtual machines/acts as router
Elk Virtual Machine	192.168.1.100	SEM used to record all vulnerability attempts conducted by Blue team
Capstone Virtual Machine	192.168.1.105	Target machine for vulnerability assessment
Kali Attacker Machine	192.168.1.8	Attacker Machine/Red team vulnerability assessment

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure Vulnerability	Sensitive Data Exposure not protected or hardened that can be accessed by unauthorized users.	Sensitive Data Exposure Vulnerability allow attackers to discover sensitive data that’s not properly hidden from the public’s view.
Dictionary Brute Force Attacks	Is a type of brute force attack that uses combinations of words, phrases, numbers and previous leaked passwords against a target’s username to gain login access to a specific website.	A Brute Force attack vulnerability allows attackers to gain login credentials of their targets causing greater harm with access to PII.
Reverse Shell Uploads	Is an attack that initiates a shell connection from target machine to the attacker machine bypassing the target machine’s firewall security.	A Reverse Shell Upload attack creates a shell connection to a target machine where information can be imported, exported and augmented.

Exploitation: Sensitive Data Exposure Vulnerability

01

Tools & Processes

Initial Reconnaissance:
Ifconfig
Nmap
Locating IP address of Capstone

Continued Reconnaissance of 192.168.1.105:
Investigated each web page uncovering further sensitive information and location of secret_folder

02

Achievements

Achieved initial reconnaissance of Capstone's website resulting in the discovery of their IP address and a sensitive hidden folder called "secret_folder" not intended for public viewing.

03

Evidence of vulnerability

LFI command path discovering login page of secret_folder on Capstone website.

- 192.168.1.105/company_folders/secret_folder

Images of secret_folder discovery:

- 192.168.1.105/meet_our_team/ashton.txt
- 192.168.1.105/company_folders/customer_info/customers.txt
- 192.168.1.105/company_folders/secret_folder

Exploitation: Directory Brute Force Attack Vulnerability

01

Tools & Processes

Hydra dictionary Brute Force Attack

https://crackstation.net

02

Achievements

The Directory Brute Force Attack resulted in discovering Ashton’s password gaining access to the secret_folder.

Discovered the CEO, Ryan’s hash password which was decrypted to gain access to Capstone’s Webdav server

03

Evidence of Vulnerability

Hydra command cracking user’s password

Result of Hydra command

Further Password cracking:

Further Exploit of hash password cracking

Free Password Hash Cracker

Success of CEO login

Exploitation: Reverse Shell Upload Vulnerability

01

Tools & Processes

Used msfvenom to create a reverse shell script for exploit

Used Msfconsole/Metasploit to setup Attacker machine listening for reverse shell upload exploit to initiate from Capstone's virtual machine

Executed reverse shell upload exploit through Webdav logged in as Ryan to have Capstone initiate shell connection to Attacker machine

02

Achievements

Created a shell that was initiated from Capstone's target machine to attacker machine, bypassing Capstone's firewall configurations

Attackers now have ability to import malicious scripts, export (PII) and continue to further exploit and maintain access

03

Evidence of Vulnerability

Reverse shell upload command

msfconsole setting attacker machine as listener

Upload of shell.php file to IP

Shell.php displayed in webdav server

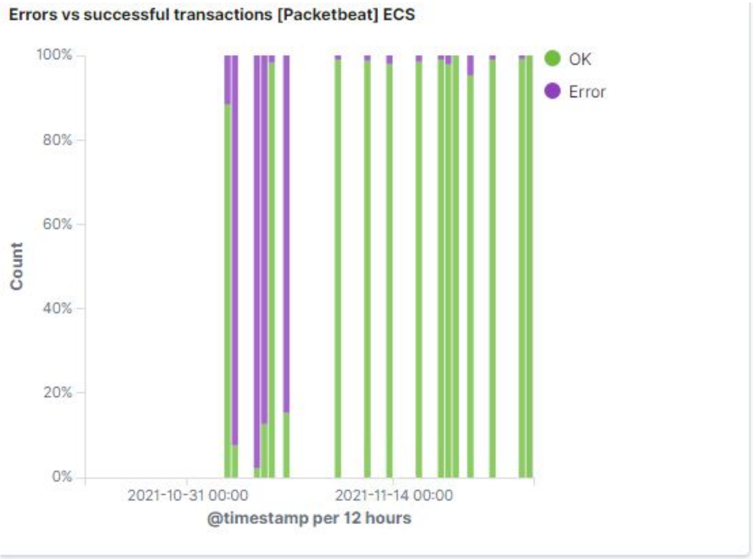
Blue Team

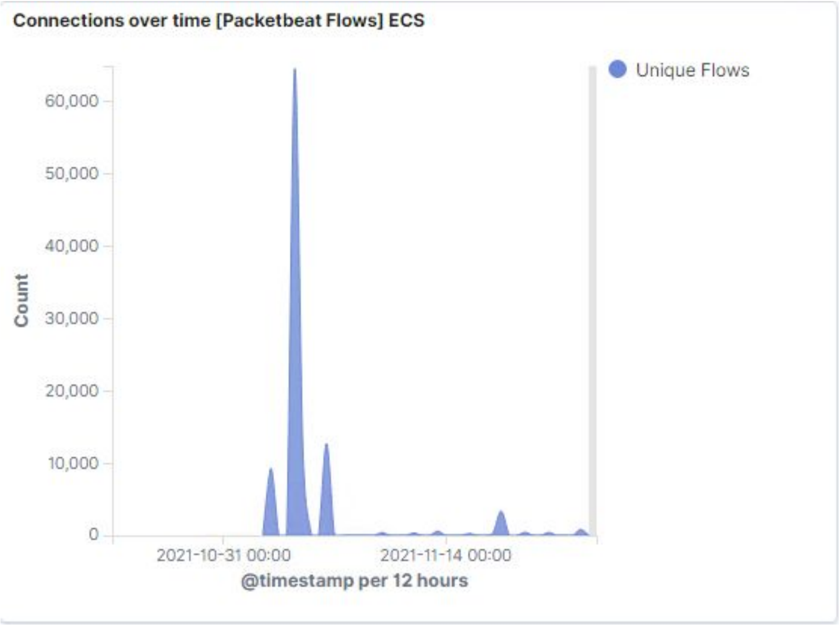
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



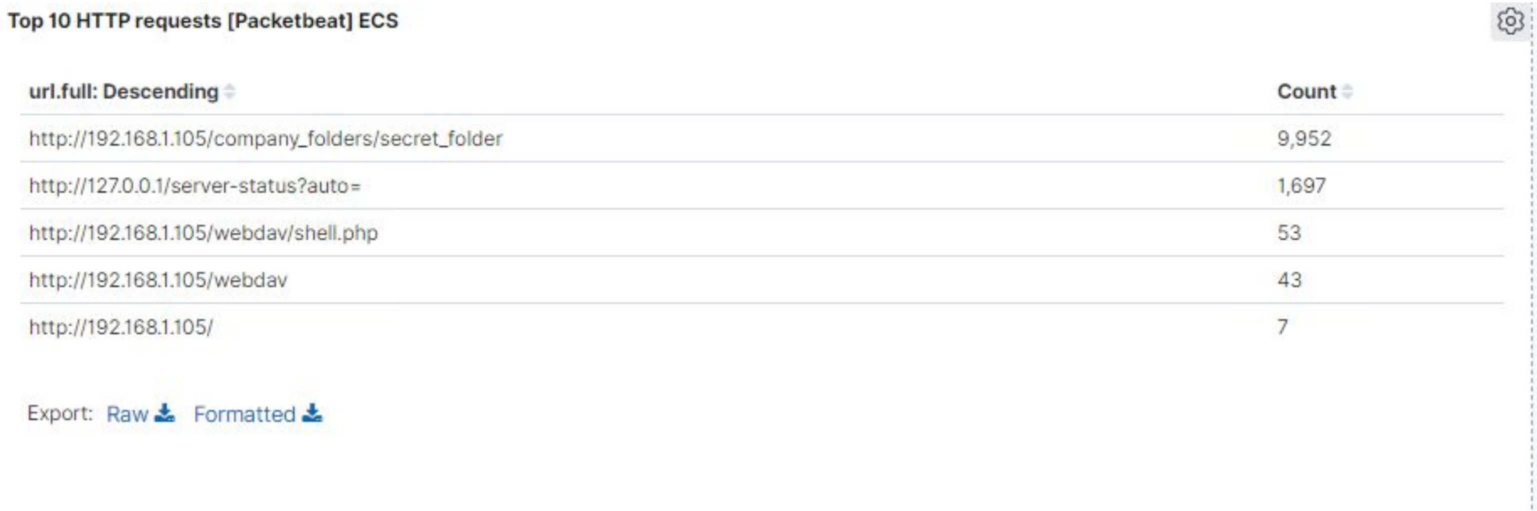


The port scan took place on 11/5/21 at 12:00PM and the first spike on the image on the right hand side from the IP 192.168.1.8.

Analysis: Finding the Request for the Hidden Directory

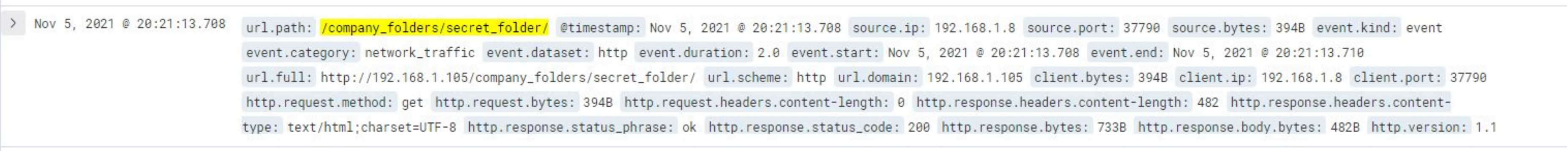
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,952
http://127.0.0.1/server-status?auto=	1,697
http://192.168.1.105/webdav/shell.php	53
http://192.168.1.105/webdav	43
http://192.168.1.105/	7



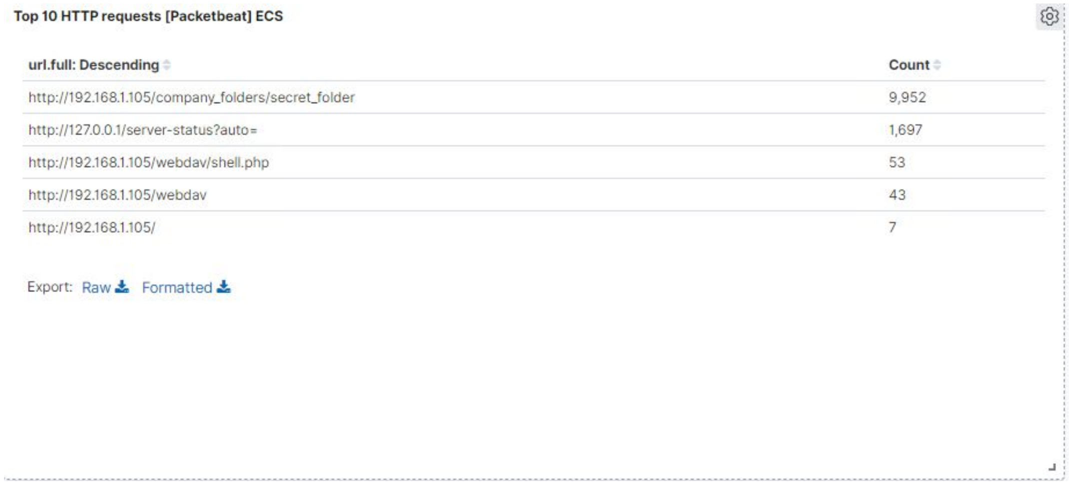
```
> Nov 5, 2021 @ 20:21:13.708   url.path: /company_folders/secret_folder/ @timestamp: Nov 5, 2021 @ 20:21:13.708 source.ip: 192.168.1.8 source.port: 37790 source.bytes: 394B event.kind: event
                               event.category: network_traffic event.dataset: http event.duration: 2.0 event.start: Nov 5, 2021 @ 20:21:13.708 event.end: Nov 5, 2021 @ 20:21:13.710
                               url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http url.domain: 192.168.1.105 client.bytes: 394B client.ip: 192.168.1.8 client.port: 37790
                               http.request.method: get http.request.bytes: 394B http.request.headers.content-length: 0 http.response.headers.content-length: 482 http.response.headers.content-
                               type: text/html;charset=UTF-8 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 733B http.response.body.bytes: 482B http.version: 1.1
```

The time the request occurred took place on Friday, November 5th at 8:21PM. The file requested is a secret folder and it contained PII including additional passwords and instructions for the attacker to exploit.

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

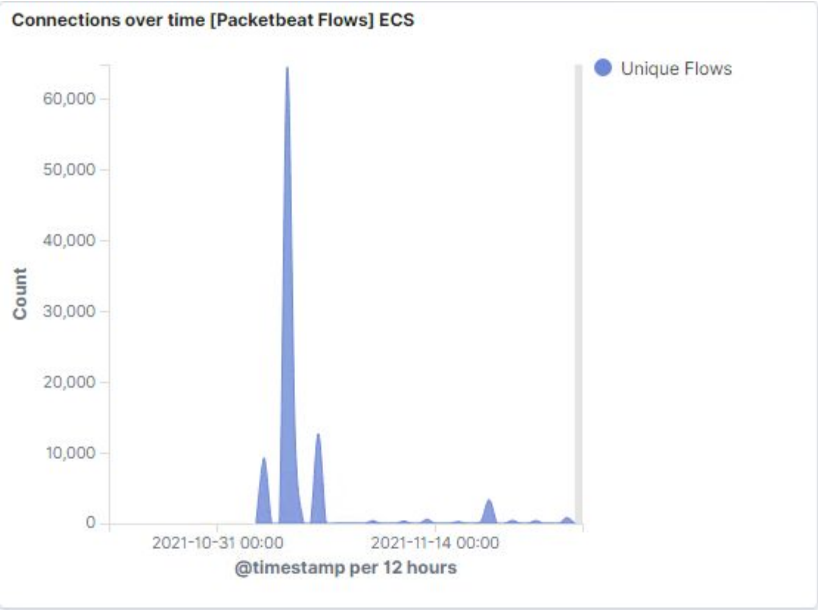
- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	9,952
http://127.0.0.1/server-status?auto=	1,697
http://192.168.1.105/webdav/shell.php	53
http://192.168.1.105/webdav	43
http://192.168.1.105/	7

Export: Raw Formatted



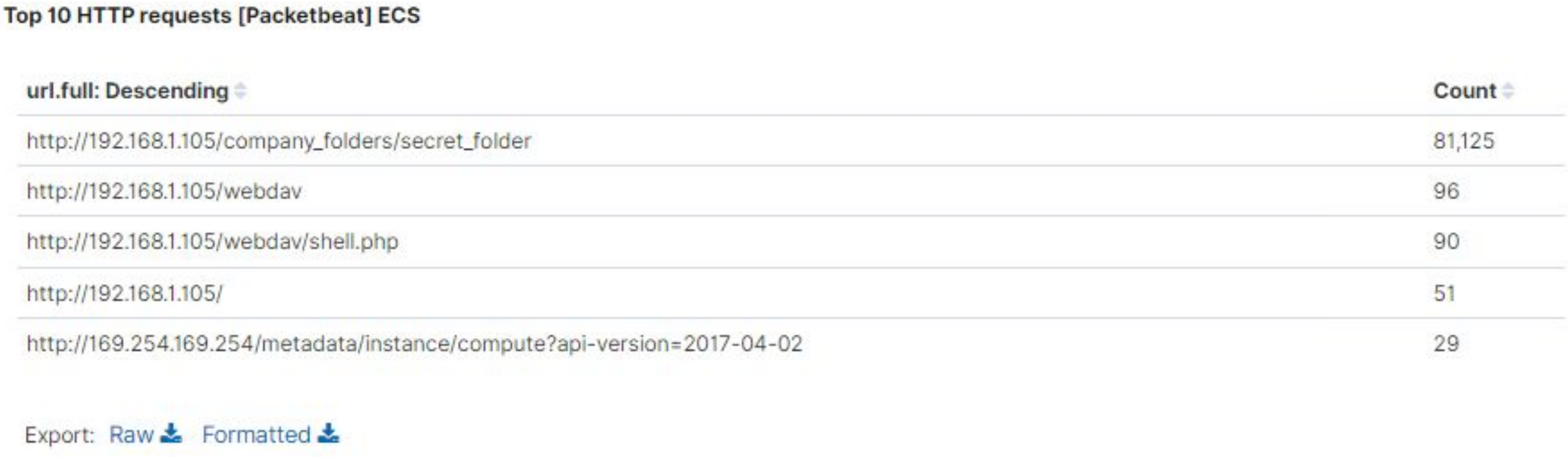
Connections over time [Packetbeat Flows] ECS

9,952 attacks were made in the Brute Force attack on the secret folder. 9,951 attempts were made before the attacker discovered the password.

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?
- Which files were requested?



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	81,125
http://192.168.1.105/webdav	96
http://192.168.1.105/webdav/shell.php	90
http://192.168.1.105/	51
http://169.254.169.254/metadata/instance/compute?api-version=2017-04-02	29

There were 96 requests made to the WebDAV directory. The file which was requested is the shell.php that was uploaded from the attacker.

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?

- An alert that triggers when a suspicious amount of port scans or ping request take place within a specified time frame

What threshold would you set to activate this alarm?

- Alert is triggered when ten or more port scan attempts or 75 ping requests are executed in one minute

System Hardening

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

- Enabling only necessary traffic to access trusted hosts.
- Configure firewalls to act upon alerts and thresholds that are defined to detect and block port scans in real time

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert that triggers when a certain amount of HTTP requests are sent to a Hidden Directory in a specified amount of time

What threshold would you set to activate this alarm?

- Alert is triggered if more than 100 HTTP requests to a Hidden Directory are counted within one minute

System Hardening

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

- Setup of an allow/deny list of approved IP addresses able to communicate with the host
- Keep folders in an external directory that contains ACL rules.
- By creating allow/deny lists, attackers will be denied due to their IP and won’t be able to access the hidden directory, especially if it’s located externally from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alert that triggers when a suspicious amount of login attempts takes place within a specified time frame

What threshold would you set to activate this alarm?

- If a user attempts 12 or more login attempts within a minute

System Hardening

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

- Creating and maintaining a strong password policy where complex passwords are required for access

Describe the solution. If possible, provide the required command line(s).

- Strong password policy that requires at least 12 characters, one uppercase, one lowercase, at least one number and special character.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm that triggers when the WebDAV server is accessed a certain amount of times within a specified time.

What threshold would you set to activate this alarm?

- Alarm will trigger if WebDAV server is accessed more than 15 times within the hour

System Hardening

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

- Create two factor authentication for gaining access to WebDAV.
- Providing 2 factor authorization prevents the attacker to gain access when they cannot retrieve the user’s second password generated from the login. This will also alarm the user of unauthorized access.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm that triggers when a certain amount of .php or .exe file is uploaded in a specified time frame

What threshold would you set to activate this alarm?

- Alarm triggers when 1 or more file upload attempts with extension .php, .bat and .exe every 30 minutes

System Hardening

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

- Creating an allow/deny list on specific file extensions and denying suspicious executable scripts.
- In this scenario, we would want to deny all files that contain extensions such as .php, .exe, .bat. These Configurations would be updated on ACLs.

The End