Capstone Engagement

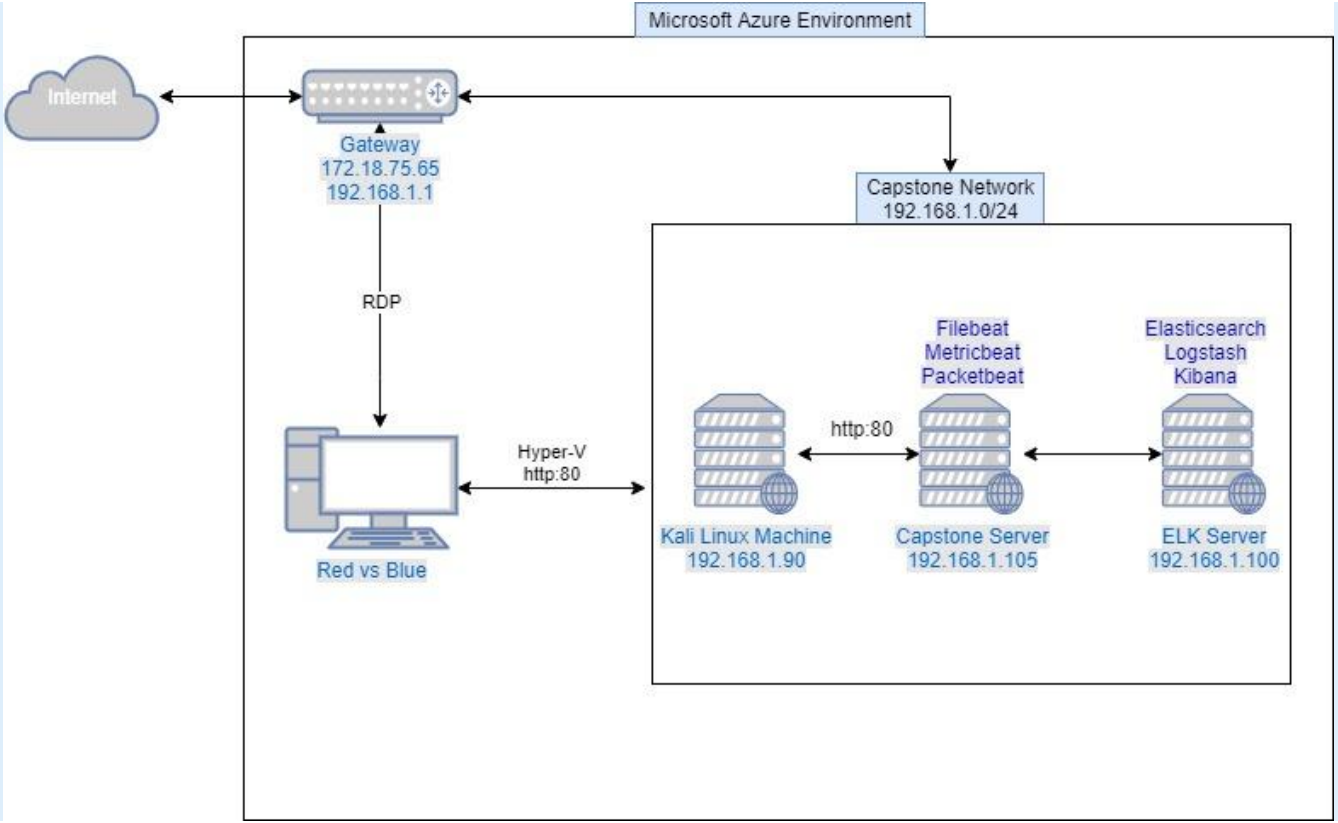
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.355.255.0
Gateway: 192.168.1.1

Machines
IPv4: 10.0.0.8
OS: Windows 10 Pro
Hostname: Red vs Blue

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali VM

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone VM

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK VM

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali Linux Client (VM)	192.168.1.90	-Penetration testing. -Attacking VM in this report.
ELK Server (VM)	192.168.1.100	- Public facing web server. - Run the Elasticsearch, Logstash, Kibana (ELK) server.
Capstone Server (VM)	192.168.1.105	-Company public facing server.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive data exposure OWASP A3:2017	*Secret_folder was referenced in public documentation. This included access information to the server.*	*Allowed unauthorized access to server files.*
Unauthorized File Upload	*Allows unauthorized users to upload files to the web server.*	*Malicious files can be uploaded which can include executables, PHP scripts.*
Remote Code Execution	*Allows attacker to run php files on remote server.*	*Attacker can gain access via reverse shell.*

Exploitation: Sensitive Data Exposure

01

Tools & Processes

Nmap used to discover topology.

FireFox to browse public file system.

Hydra used to brute force password.

02

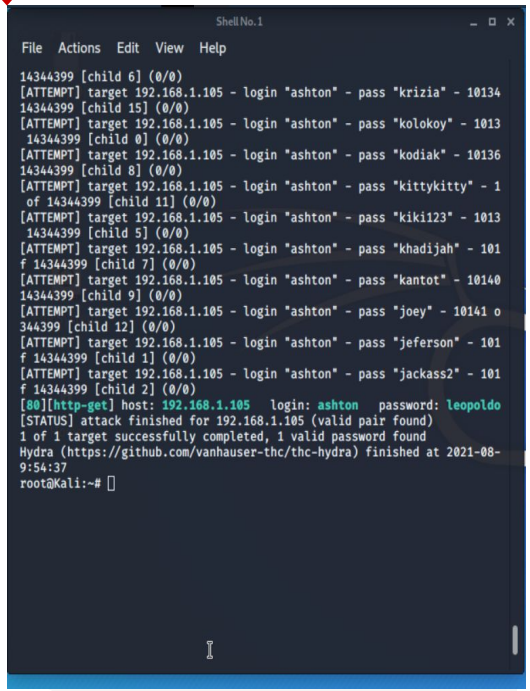
Achievements

Discovered *secret_folder* along with documentation on how to connect to company server.

Used Hydra to brute force credentials.

Accessed instructions to connect to corp_server with Ashton's credentials.

03



Exploitation: Unauthorized File Upload

01

Tools & Processes
Msfvenom was used to create a reverse shell (shell.php) for a linux system.

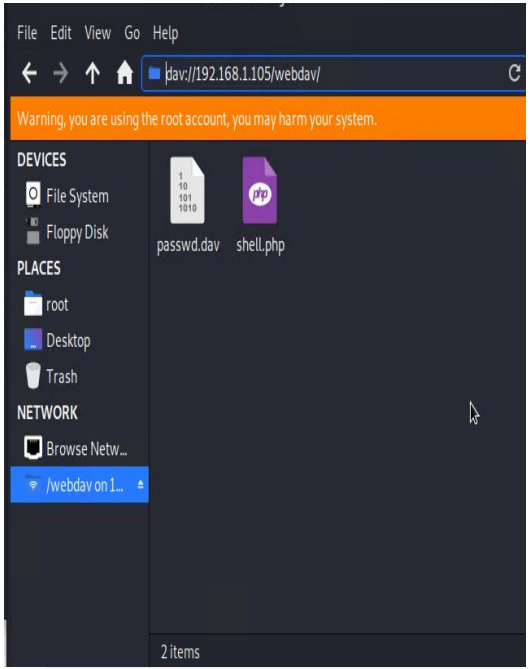
Webdav was used to access file system of web server with credentials that were brute forced.

02

Achievements
Shell.php was created with specific ports to contact the machine that would be listening.

The attacker then used webdav to upload shell.php to server.

03



Exploitation: Remote Code Execution

01

Tools & Processes

msfconsole was used to set a reverse shell payload.

Remote server was used to execute *shell.php* through *Firefox*.

Meterpreter was used to run the *shell* command.

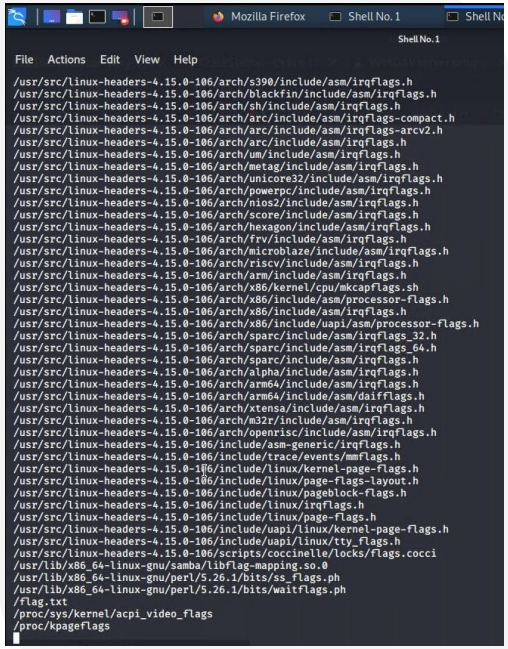
02

Achievements

Reverse shell was obtained by having attacking machine wait and listen for *shell.php* to be executed.

Once executed, meterpreter was used to open up a reverse shell giving the attacker access to web server file system.

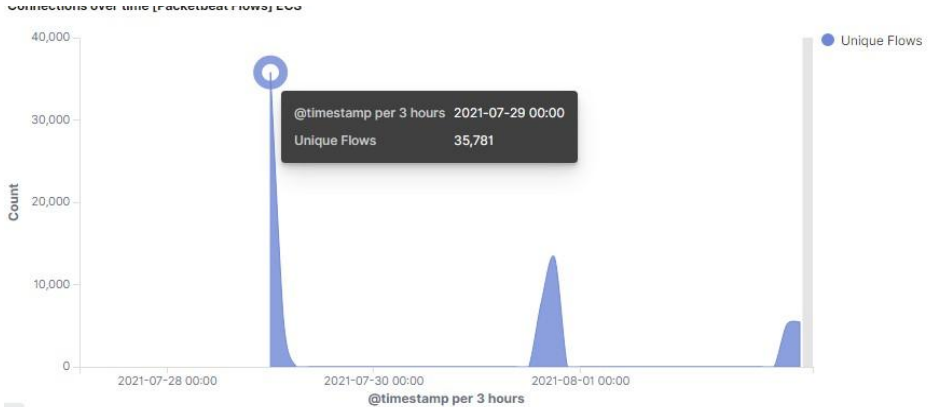
03

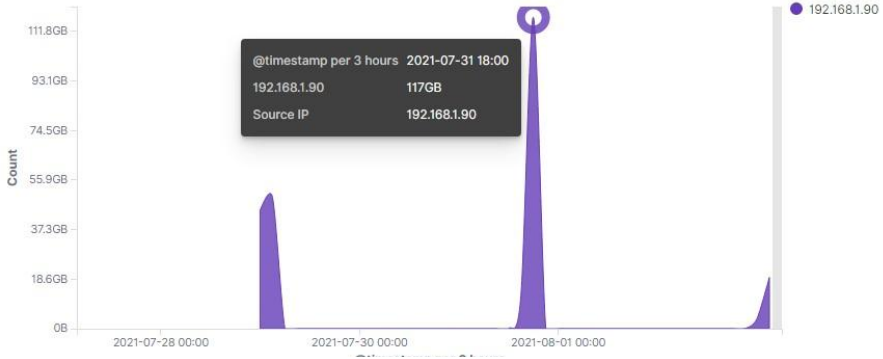


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





What time did the port scan occur?

- 00:00

How many packets were sent?

- 35,781

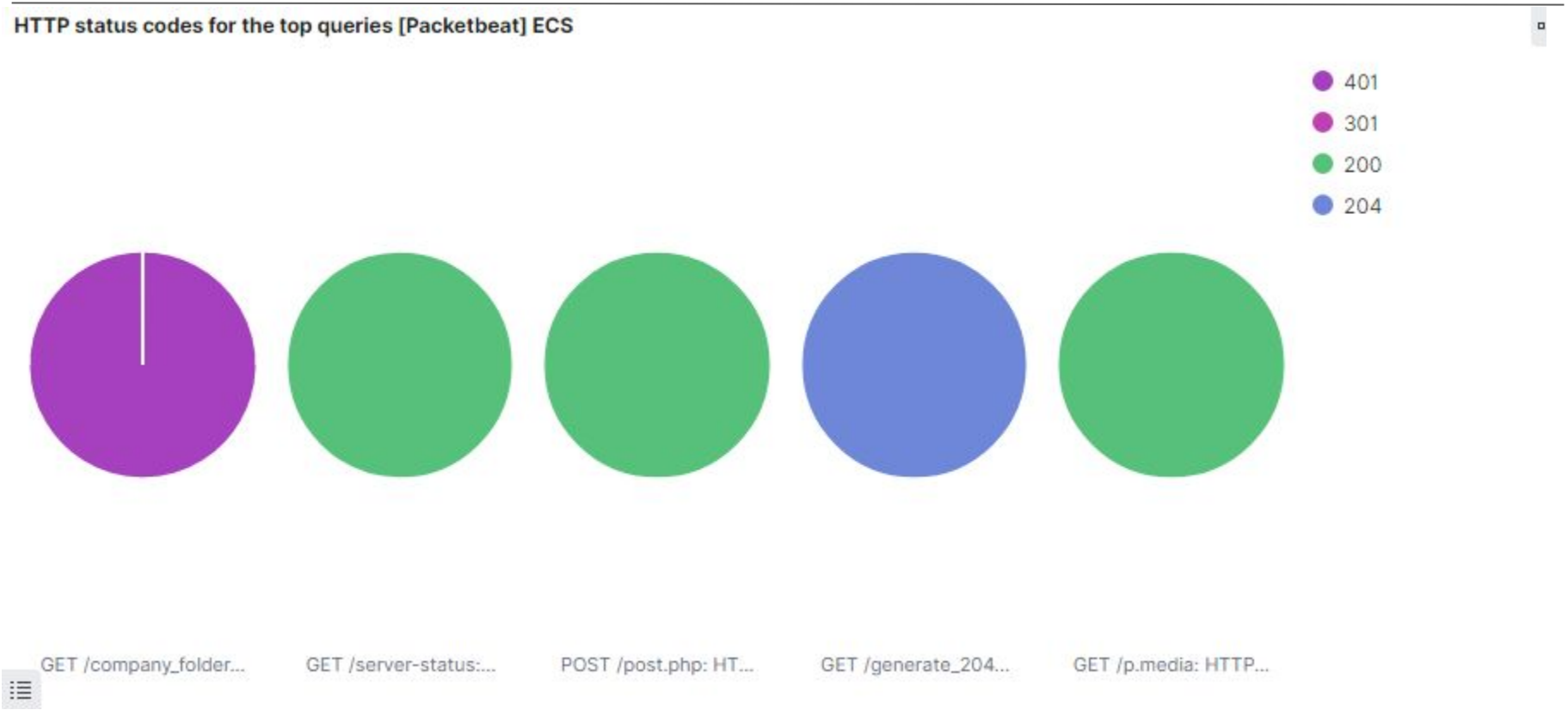
From which IP?

- 192.168.1.90

What indicates that this was a port scan?

- The victim machine responded back with 401 (Unauthorized), 301 (Moved Permanently), 200 (Ok) and 204 (No content) responses.

Analysis: Identifying the Port Scan Continued



Analysis: Uncovering the Brute Force Attack

Top 10 HTTP requests [Packetbeat] ECS

uri.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,219
http://127.0.0.1/server-status?auto=	1,547
http://snnmnkxdhflwgthqismb.com/post.php	245
http://www.gstatic.com/generate_204	126
http://ocsp.godaddy.com	63

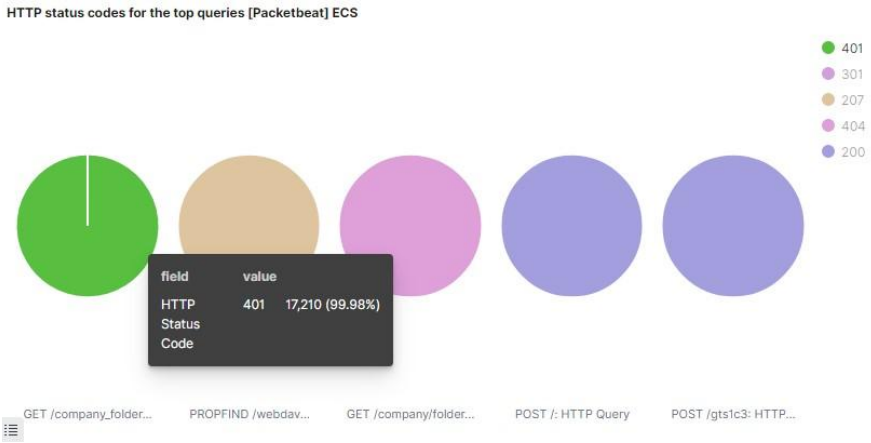
Export: Raw Formatted

server.ip	192.168.1.105
# server.port	80
# source.bytes	163B
source.ip	192.168.1.90
# source.port	42000
t status	Error
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder/
t url.path	/company_folders/secret_folder/
t url.scheme	http
t user_agent.original	Mozilla/4.0 (Hydra)

How many requests were in the attack?

- There were 17,219 total requests in the attack.

Analysis: Uncovering the Brute Force Attack Continued



Top 10 HTTP requests [Packetbeat] ECS

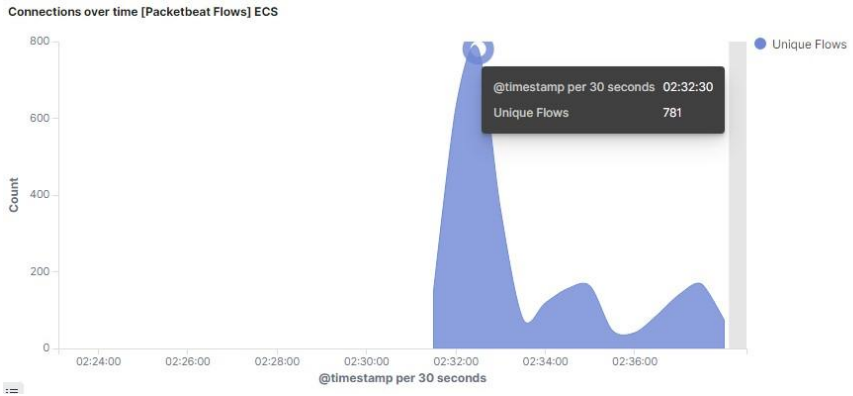
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,219
http://192.168.1.105/webdav	54
http://192.168.1.105/company/folders/secret_folder	32
http://192.168.1.105/webdav/shell.php	14
http://ocsp.pki.goog/gts1c3	12

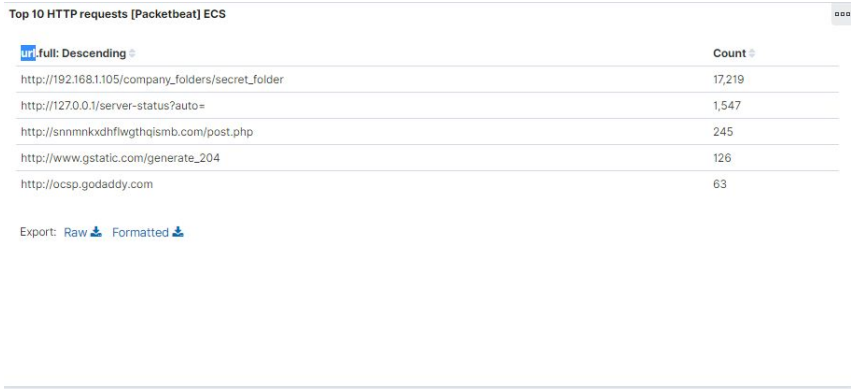
Export: Raw Formatted

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

- You can see that there were a total of 17,219 attempts and 17,210 of which showed status code 401 (Unauthorized) leaving a total of 9 successful logins.

Analysis: Finding the Request for the Hidden Directory





url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,219
http://127.0.0.1/server-status?auto=	1,547
http://snnmnkxdhflwgthqismb.com/post.php	245
http://www.gstatic.com/generate_204	126
http://ocsp.godaddy.com	63

What time did the request occur?

- 2:32

How many requests were made?

- 781

Which files were requested and what did they contain?

Top 3 hits requested:

- http://192.168.1.105/company_folder/secret_file
- http://127.0.0.1/server-status?auto=
- http://snnmnkxdhflwgthqismb.com/post.php

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,134
http://192.168.1.105/webdav	152
http://192.168.1.105/webdav/passwd.dav	20
http://192.168.1.105/webdav/shell.php	16
http://192.168.1.105/favicon.ico	14

How many requests were made to this directory?

- 152

Which files were requested?

- http://192.168.1.105/webdav/passwd.dav
- http://192.168.1.105/webdav/shell.php

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?

- We can create an alert whenever a number of ports are connected from a single origin over time and the alert can be sent sent either via email or text or both to the appropriate personnel.

System Hardening

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

- To mitigate port scans, we would implement both an Intrusion Detection System (IDS) and an Intrusion Prevention SyStem (IPS). An IDS can be configured to recognize a scanning attempt and the IPS can be configured to either alert or block the IP address of the attacker

Mitigation: Blocking the Port Scan Continued

Alarm

What threshold would you set to activate this alarm?

- We would set a threshold of 1 to set off the alarm.

System Hardening

Describe the solution. If possible, provide required command lines.

- An alert can be sent to the relevant personnel via email or text using tools such as SPLUNK when the threshold for the set number of port scans is reached.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- IDS Alarms can be set to notify of unauthorized access in real time and email.
- Correlation Alerts

What threshold would you set to activate this alarm?

- We would set the threshold to lock out at 20 unauthorized attempts.

System Hardening

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

- Firewalld configuration to allow only white-listed IP addresses
- Network traffic encryption

Mitigation: Preventing Brute Force Attacks

Alarm

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

- We can use certain tools like SPLUNK to send an email alert to notify the right people once a brute force attack is detected.

System Hardening

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

- We can limit logins to a specific IP address or range. We can also implement a CAPTCHA that would render automated bots ineffective.

.

Mitigation: Preventing Brute Force Attacks Continued

Alarm

What threshold would you set to activate this alarm?

- We would set the threshold to activate the brute force alarm at 5.

System Hardening

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

- By granting access only from a designated IP address, brute force attacker will find it harder to overcome that obstacle to gain access.
- Using a CAPTCHA has proved to be highly effective against bots since most of them do not use optical character recognition tools.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- We can set an alert that will be activated after a number of request are made that would hint at scanning. Tools such as splunk and Sumo Logic and be set up to send email alerts to the appropriate people.

What threshold would you set to activate this alarm?

- We can set a threshold of 3

System Hardening

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

- Limit the people that able to access the server via WebDav and implement MFA (Multi Factor Authentication)

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- IDS alarm should be set for any POST request as this can indicate a file upload.
- Set system so only certain files can be uploaded (documents/pictures/etc.) but not potentially harmful ones (exe/php/scripts).

What threshold would you set to activate this alarm?

- Alarm should activate when a potentially harmful file is updated.

System Hardening

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

- Only authorized users can be allowed to upload ANY file to the system.
- Uploads can be restricted to a non-public accessible part of the server.

the End