Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

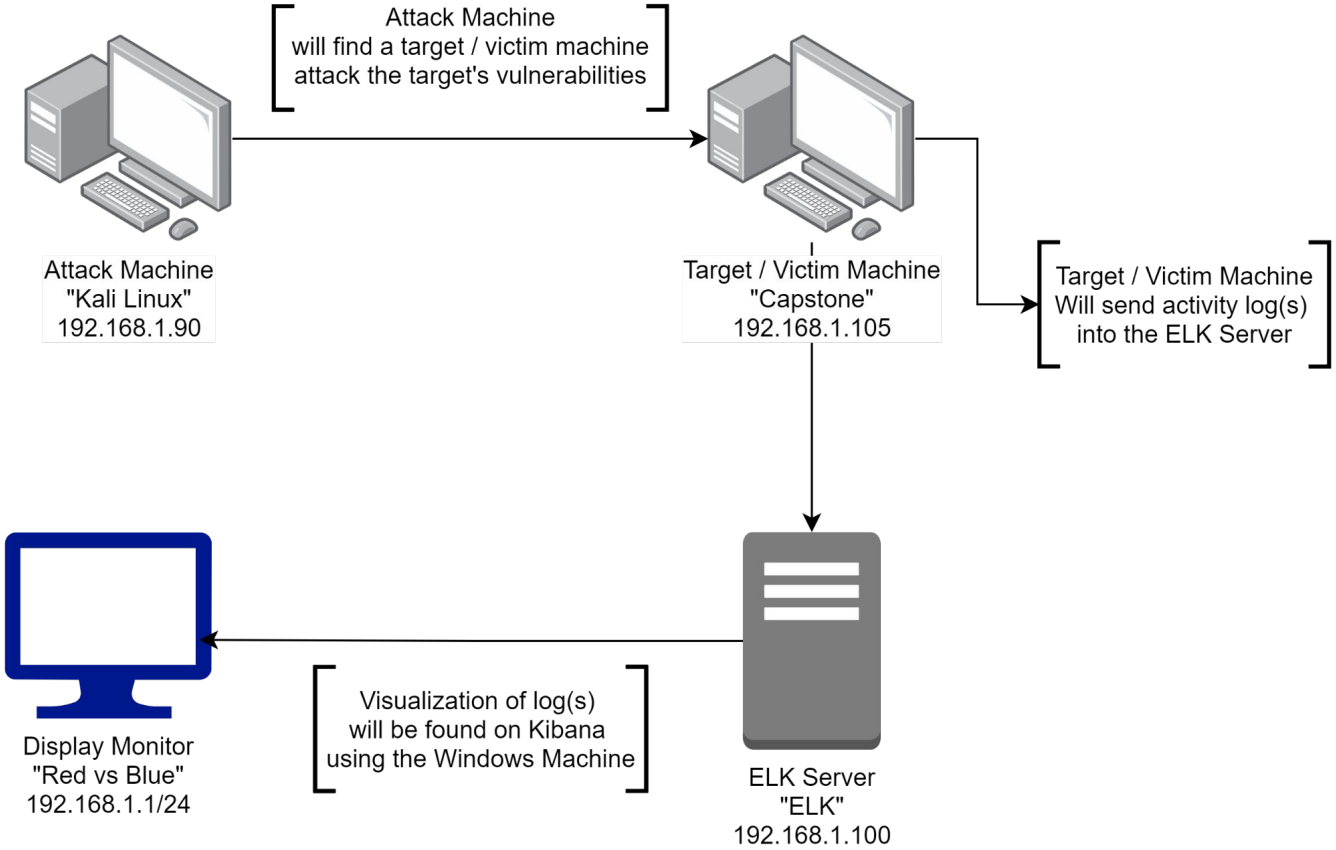
Julie Adams-Chatterley

Table of Contents

This document contains the following sections:

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 2.6.32
Hostname: kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs Blue - ML-REFVM

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue ML-REFVM	192.16.1.1	Windows virtual machine displays data log(s) in Kibana
Kali Linux	192.168.1.90	Attack virtual machine
ELK	192.168.1.100	Capturing log(s) data from Capstone “victim” virtual machine
Capstone	192.168.1.105	Victim virtual machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	*An open port can provide an entry point for an attacker to access sensitive info. which increases the risk of a data breach.*	*The open port 80 allowed the attacker to access a company directory and the files inside.*
Accessible Files	A web server, FTP server, etc often store data files in the “root” directory. The server’s users have permission to access these files.	The IP address was secured on the open port 80 using Firefox. The attacker viewed specific user info. regarding secret_folder.
Brute Force Password	Most common passwords can be obtained by using a brute force wordlist.	The attacker brute forced Ashton’s password (leopoldo), which allowed access to the secret_folder.
Hashed Password	Hashed passwords can be “cracked” using different tools: John the Ripper, md5 cracker, etc.	The attacker used online Crackstation to identify ryan’s password (linux4u).

Exploitation: Open Port 80

01

Tools & Processes

Used the **nmap** command to scan for any open ports and services on the network.

02

Achievements

Found an open port 80 on IP address 192.168.1.105. Through the open port 80 we gained access to a directory with sensitive data.

03

```
Nmap scan report for 192.168.1.105
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

Exploitation: Accessible Files

01

Tools & Processes

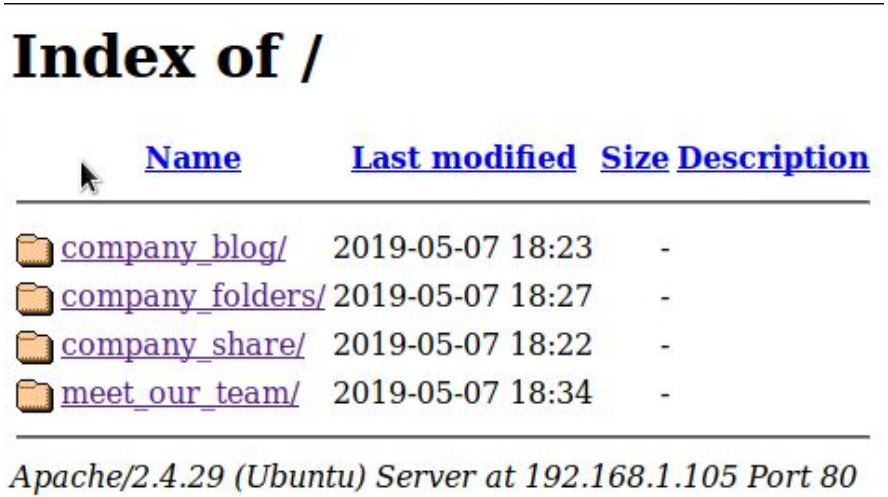
Using open port 80 to open the Firefox web browser to try and access a company directory.

02

Achievements

The IP address gave access to “Index of”: directory and files. The accessed files included user permissions and provided the exact user with access to the companies secret files location.

03




```
Ashton is 22 years young, with a masters degreee in aquatic
jousting. "Moving over to managing everyone's credit card and
security information has been terrifying. I can't believe that they
have me managing the company_folders/secret_folder! I really
shouldn't be here" We look forward to working more with Ashton in
the future!
```

Exploitation: Brute Force Password

01

Tools & Processes

We used **Hydra** to forcibly access ashton's password

02

Achievements

The user's password was exploited and granted user shell access into the victim machine. We are now able to navigate to the secret files.

03

```
server1:~$ locate secret_folder
w/html/company_folders/secret_folder
w/html/company_folders/secret_folder/.htaccess
w/html/company_folders/secret_folder/.htpasswd
w/html/company_folders/secret_folder/connect_to_corp_server
server1:~$ cd /var/www/html/company_folders/secret_folder/
server1:/var/www/html/company_folders/secret_folder$ ls
_to_corp_server
server1:/var/www/html/company_folders/secret_folder$ cat connect_to_
rver
l Note

r to connect to our companies webdav server I need to use ryan's acc
ash:d7dad0a5cd7c8376eeb50d69b[ccd352)

ed to open the folder on the left hand bar
ed to click "Other Locations"
ed to type "dav://172.16.84.205/webdav/"
ll be prompted for my user (but i'll use ryans account) and password
n click and drag files into the share and reload my browser
```

```
[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 2021-07-20 2
```

Exploitation: Hashed Password

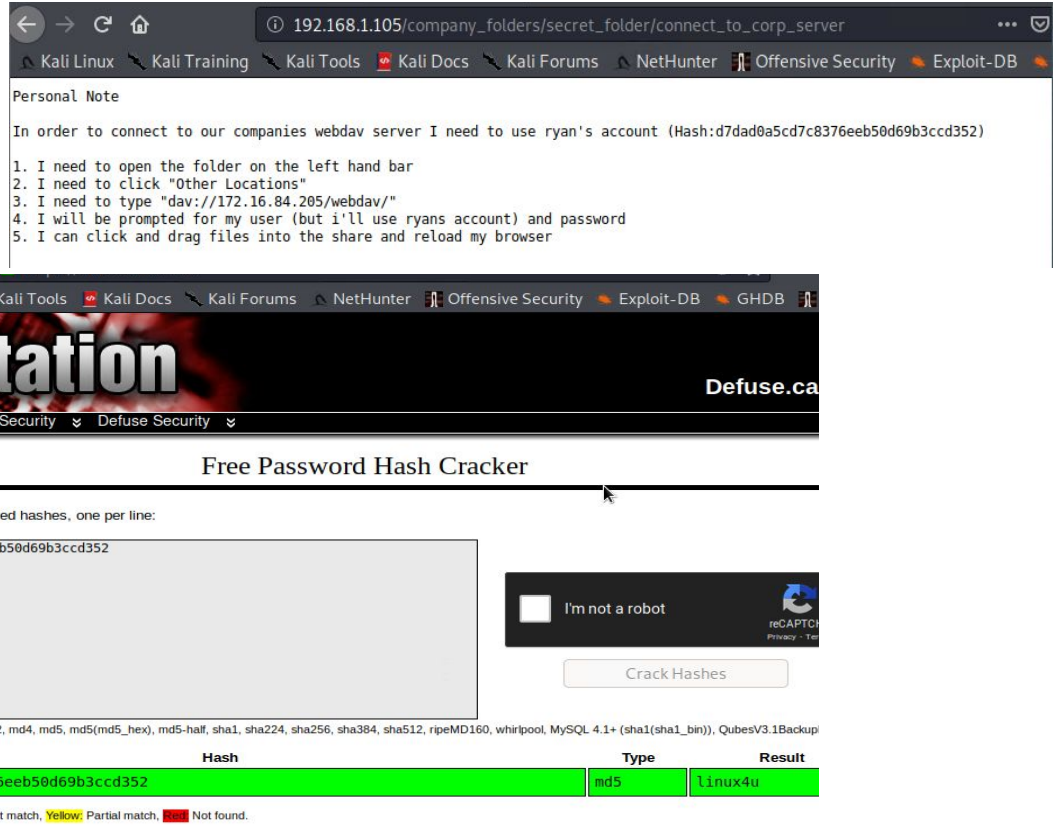
01

Tools & Processes
Used website crackstation.net to “unhash” ryan’s password

02

Achievements
Ryan’s password granted access to the company’s system. By using the webdav directory, the attacker uploaded a reverse shell.

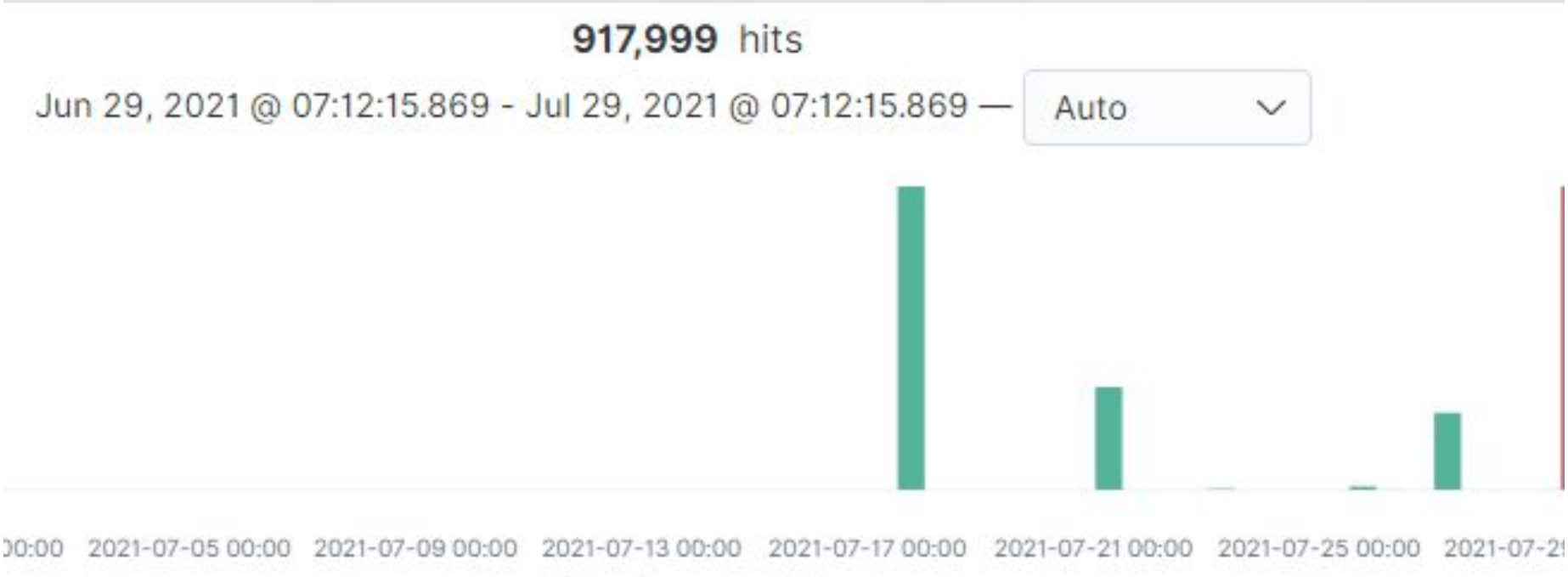
03



Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan performed by 192.168.1.90 occurred on Jul 27 2021 @ 05:28:45
- 917,999 hits were sent from 192.168.1.90
- Multiple ports requested at the same time are indicative of a port scan

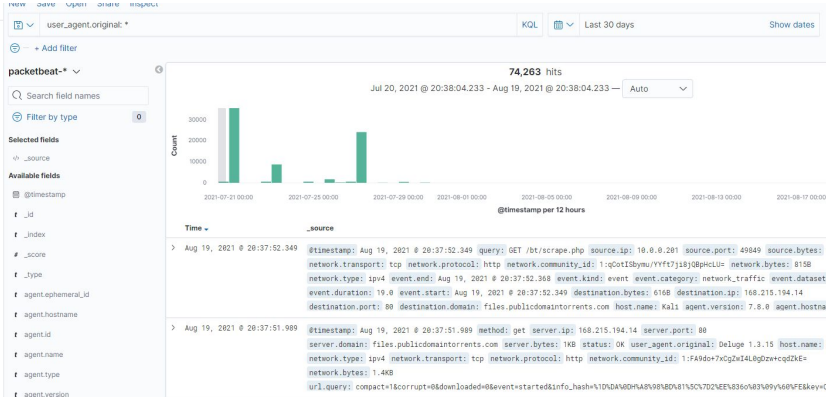


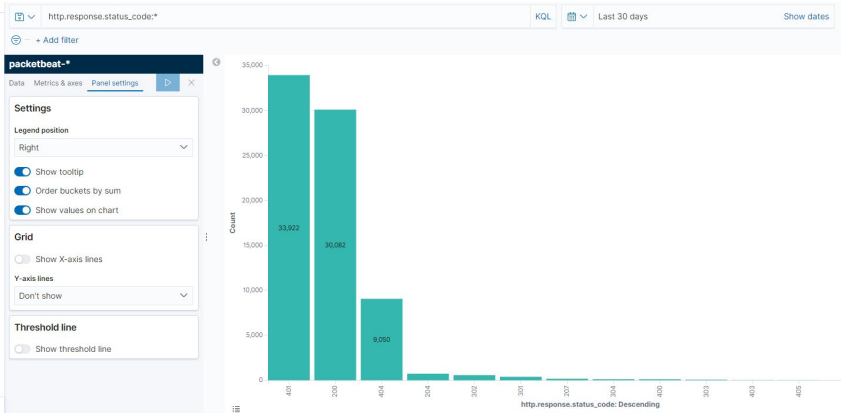
Analysis: Finding the Request for the Hidden Directory

- The 16,795 requests occurred on Jul 29, 2021 @ 07:17:55
- 16,795 requests were made
- connect_to_corp_server file was requested
- Contains information on connecting to the WedDav directory

Analysis: Uncovering the Brute Force Attack

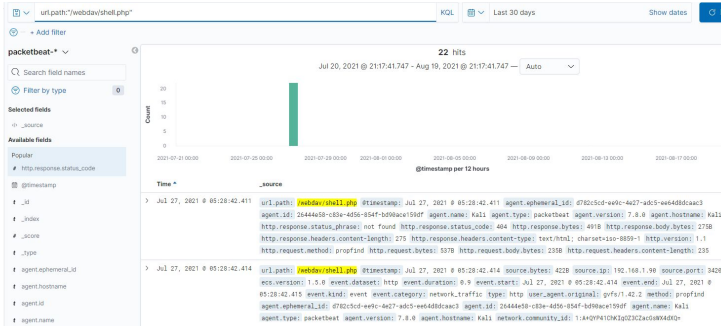
- 75,232 requests were made during the attack
- 33,922 requests were made from the attacker's IP address (192.168.1.90) before the password was discovered
- Password discovered Jul 20, 2021 @ 23:31:57

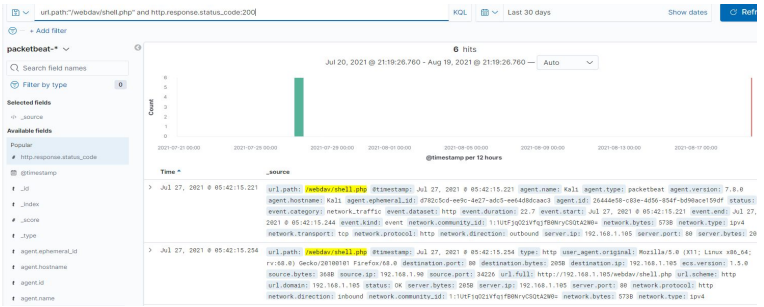


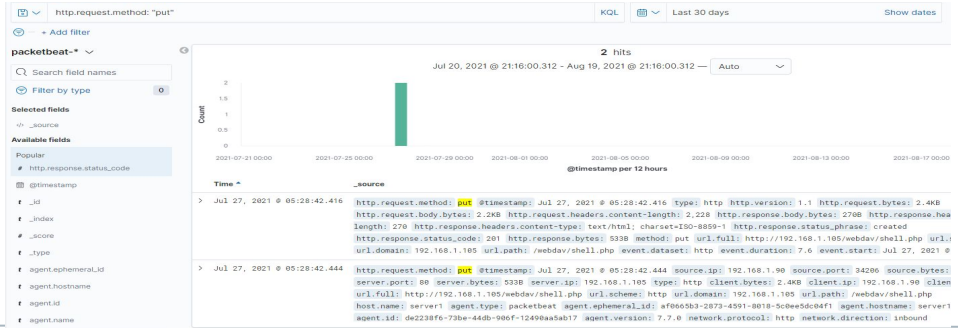


Analysis: Finding the WebDAV Connection

- 22 requests were made to the WebDav directory
- The shell.php was uploaded from the attacker machine on Jul 21, 2021 @ 05:28:42







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?

- Firewall Port Scan Alert

What threshold would you set to activate this alarm?

- Same remote source with up to 10 different port numbers in 5000 microseconds (0.005 seconds)
- All additional packets from the remote source will be denied.

System Hardening

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

- Install a Firewall to prevent unauthorized access to network.
- TCP Wrappers will permit or deny access based on IP address or domain name.

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

- ufw allow in from <subnet range>
- nano /etc/hosts.allow vsftpd : <IP address> or <domain name>
- nano /etc/hosts.deny vsftpd : ALL

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Non-Admin Attempted Access Alert
  - Triggered when a non-admin user attempts to access the specified directory.
- Any Attempted Access Alert
  - Triggered by any machine attempts to access the specified directory.

What threshold would you set to activate this alarm?

- For both, Threshold is more that 1 attempt.

System Hardening

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

- Remove the specified directory from a web server with an open port and place on an offline server.

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

- rm -i ../company_files
- mv -i ../company_files >>
  - Using “-i” ensures correct directory and/or files are changed.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Login Attempt Limit Reached Alert
- 401 Unauthorized HTTP Alert
- User Agent=Hydra Alarm

What threshold would you set to activate this alarm?

- 7 login attempts :: user locked out 30 min.
- 401 Alarm: Starting threshold is 10 attempts in one hour (will refine over time.
- “User_agent”: threshold is 1 or more attempts.

System Hardening

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

- Limit Login Attempts to 7 per user, lockout for 30 minutes.
- 401 alert :: server automatically drops traffic from the IP address for 30 minutes.

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

- Display number of attempts and lockout time to user. Once 7 attempts have occurred a lockout page will be displayed.
- User_agent original=hydra

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Unauthorized Machine Access Alert
  - Alerts anytime this directory is accessed by an unauthorized machine.

What threshold would you set to activate this alarm?

- Set threshold at 1 attempt

System Hardening

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

- Block web interface connection to this directory and files
- Connection to this directory and files restricted to specific machine or IP address.

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

- Nano /etc/httpd/conf/http.conf
- /var/www/webdav/
  - Allow <IP address>
  - Deny ALL

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Unauthorized User POST, PUT Upload Alert
- Unauthorized User Upload .php, or .txt files

What threshold would you set to activate this alarm?

- Any attempt where POST/PUT or .php/.txt command is made to sensitive directory or file from an unauthorized IP address

System Hardening

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

- Disable users upload permissions through the web interface.
- Allow uploading by specific users by IP address.

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

- Nano /etc/httpd/conf/httpd.conf
- /var/www/webdav
  - Allow <IP address>
  - Deny ALL


The End