Capstone Engagement

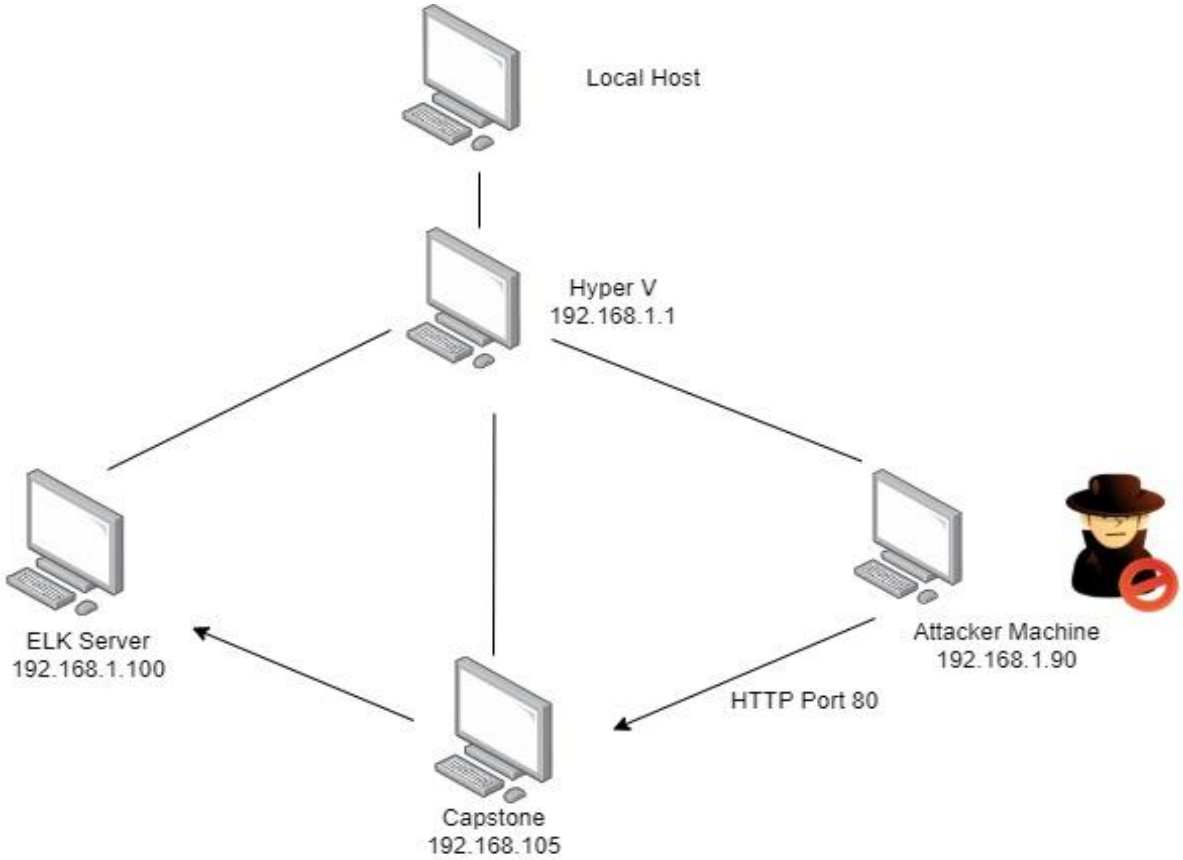
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address
Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.1
OS: WINDOWS
Hostname: HYPER V

IPv4:192.168.1.100
OS: LINUX
Hostname: ELK

IPv4:192.168.1.105
OS: LINUX
Hostname: CAPSTONE

IPv4:192.168.1.90
OS: KALI LINUX
Hostname:KALI

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker machine. Used to find vulnerabilities
Capstone	192.168.1.105	Victim machine. Web hosting machine using apache
ELK Server	192.168.1.100	Used to collect logs/activity on Victim machine
Hyper V Manager	192.168.1.1	Hosts entire network.

Vulnerability Assessment

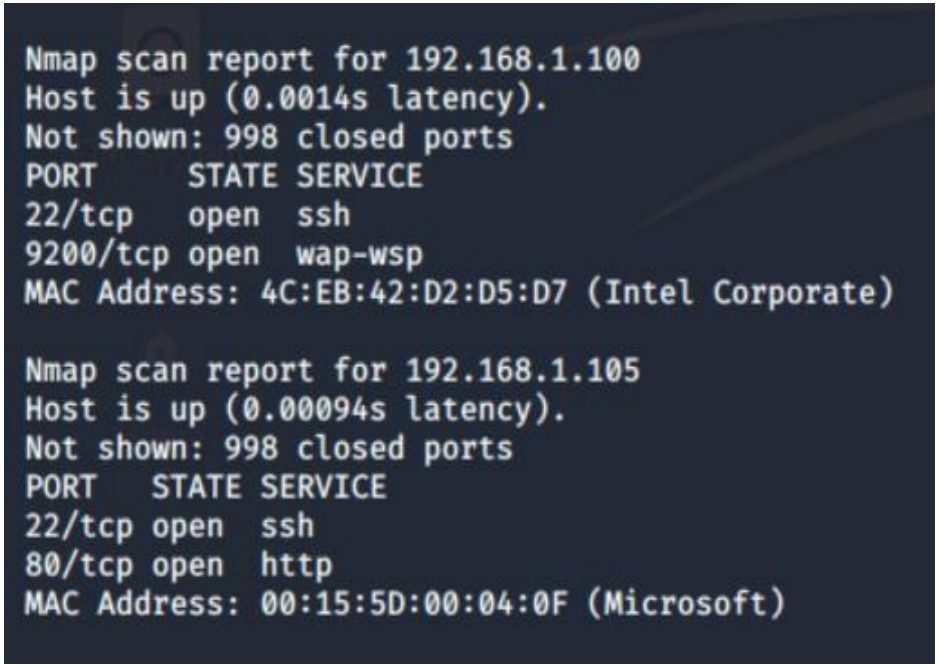
The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2019-6579	*Port 80 is left open for traffic.*	*This allows the attacker to execute system commands with administrative privileges*
Improper Restriction of Excess Authentication Attempts(CVE-2020-14494 / CWE-307)	This does not block out the amount of failed password attempts in short period of time.	This leave the system vulnerable to Brute Force attacks.
Use of Password with Insufficient Computational Effort (CWE-916)	The software generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.	The password can easily be decrypted using john the ripper or crackstation.net

Exploitation: CVE-2019-6579

1st step was running an nmap scan.
Command:
Nmap 192.168.1.*

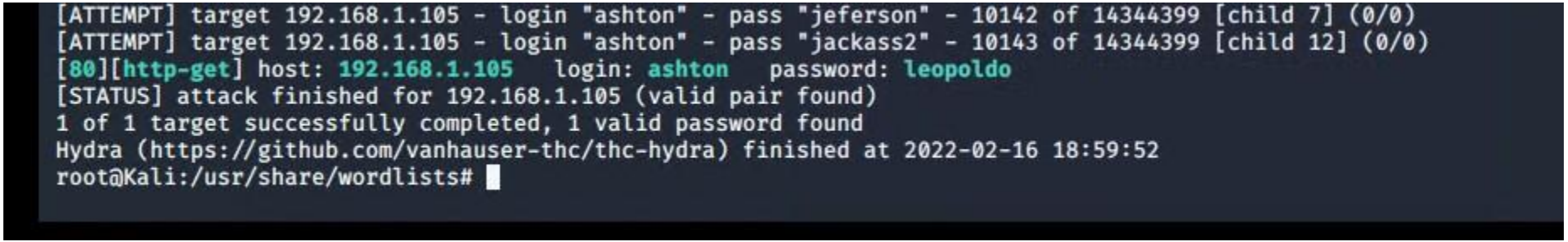
Achievements
By running the scan, was able to determine port 22 and port 80 on victim machine was open.



Exploitation: Improper Restriction of Excess Authentication Attempts(CVE-2020-14494 / CWE-307)

Used Hydra along with wordlist “rockyou.txt” to brute force to gain Ashton’s password

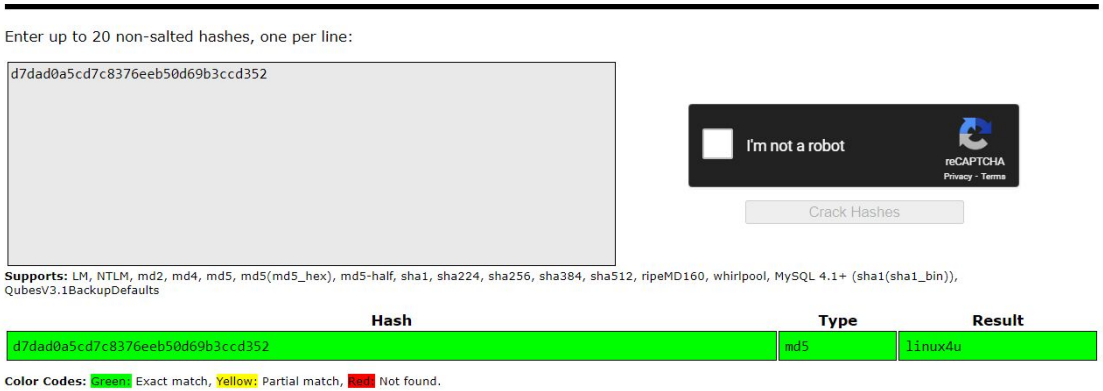
Command: hydra -l ashton - P usr/share/wordlists/rockyou.txt s- 80 -vV 192.168.1.105 http-get /company_folders/secret_folder



Exploitation: Use of Password with Insufficient Computational Effort (CWE-916)

Ryan's hashed password existed within the connect to connect_to_corp_server folder within the secret folder. copy/pasted the hashed password in crackstation.net to achieve ryan's password

By pasting the hashed password within crackstation was able to achieve Ryan's password.

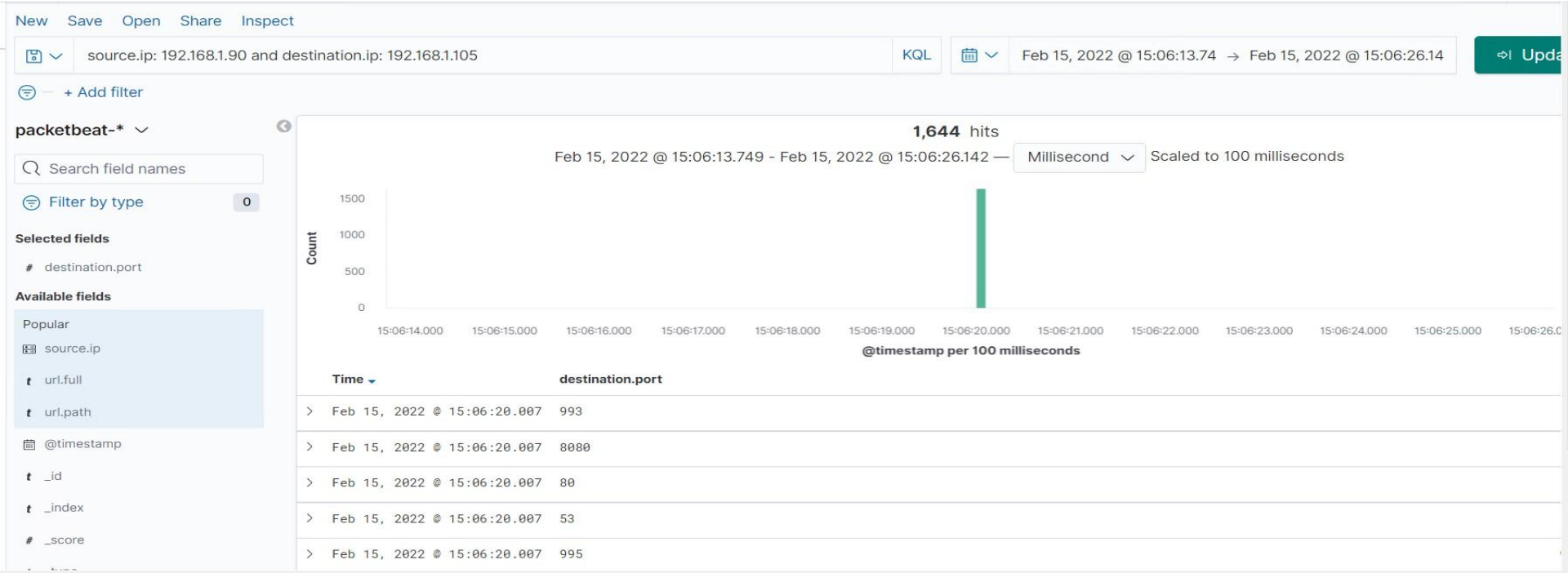


Blue Team
Log Analysis and Attack Characterization

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.

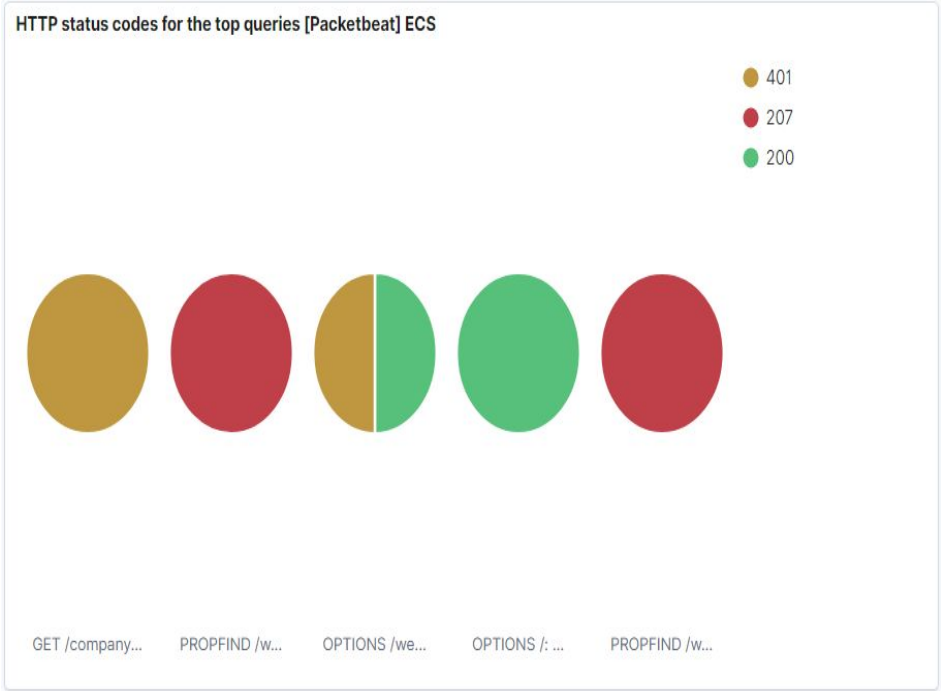
- The scan was performed at 15:06:00-15:06:30
- 1644 hits were sent from IP 192.168.1.90
- The Port scan is indicated by the different ports listed below



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.

- Requests were made at 15:15 approx. 16, 715 requests were made
- Access was requested to the secret_folder. This folder contains instructions to access the corp server



Top 10 HTTP requests [Packetbeat] ECS

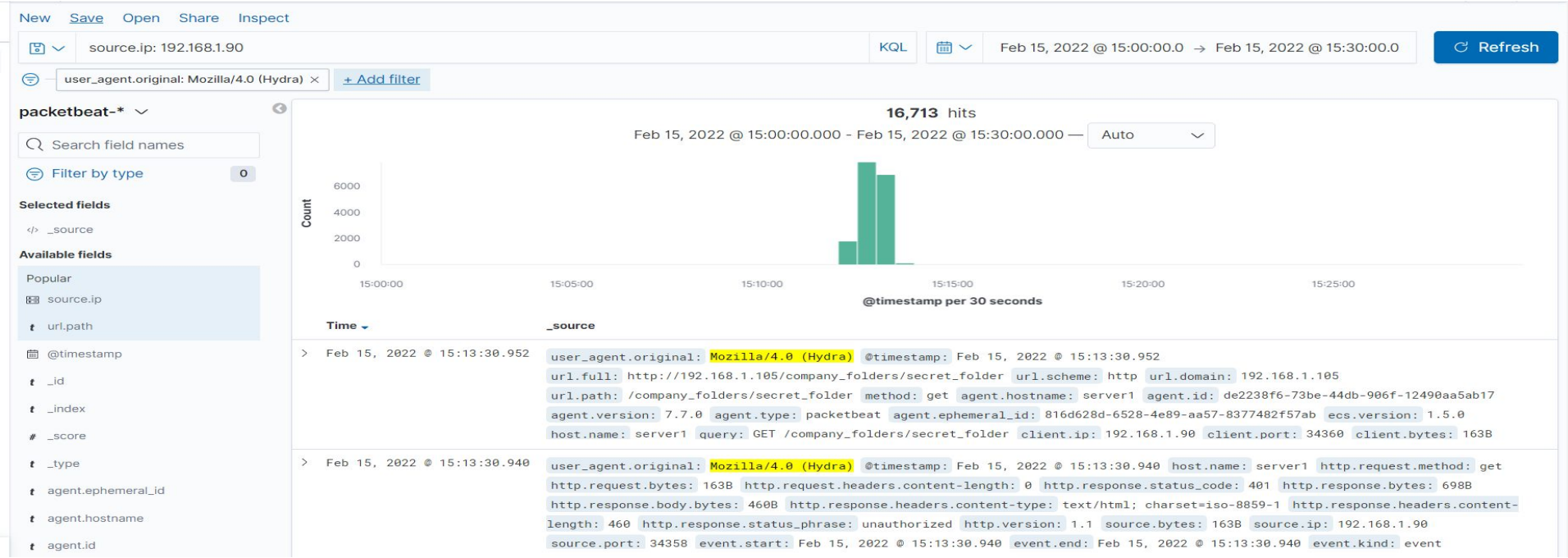
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,715
http://127.0.0.1/server-status?auto=	557
http://192.168.1.105/webdav	20
http://192.168.1.105/	4
http://192.168.1.105/webdav/shell1.php	4

Export: Raw Formatted

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.

- There was a total 16, 713 requests were made in this attack.



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.

- There was a total of 20 requests made to the webdav directory
- The files that were requested in the directory were shell1.php as well as passwd.dav

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,715
http://127.0.0.1/server-status?auto=	557
http://192.168.1.105/webdav	20
http://192.168.1.105/	4
http://192.168.1.105/webdav/shell1.php	4

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 if there is a significant amount of scan of open ports in a very short period of time.

What threshold would you set to activate this alarm?

System Hardening

What configurations can be set on the host to mitigate port scans? Close all ports that are accessible to the internet.
Implement firewall rules

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Set an alarm if the secret folder is accessed.

What threshold would you set to activate this alarm? The threshold should be 0. Anything secret should not be available on the internet

System Hardening

What configuration can be set on the host to block unwanted access?
Remove the hidden secret_folder from the webpage and secure the file offline.

Can implement 2 factor authentication to access the folder.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set an alarm for error code 401 in short period of time.

What threshold would you set to activate this alarm? 10 401 errors within 30 seconds.

System Hardening

What configuration can be set on the host to block brute force attacks?
Account gets locked out after 5 failed log in attempts
2 factor authentication
Password complexity

Mitigation: Detecting the WebDAV Connection

Alarm

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

Alerts should be triggered anytime a foreign IP is trying to access these folders

What threshold would you set to activate this alarm? The threshold for this alarm should be 1.

System Hardening

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

Restrict the IPs that can access this directory.

Implement 2 factor authentication

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Set alerts for any .php or .exe files that are being uploaded to server.
Restrict access to certain IP addresses.
Send alert if foreign IP address is accessing

What threshold would you set to activate this alarm? The threshold should be 1, before alert is triggered.

System Hardening

Remove the ability to upload any files to directory via the web.


The End