CAPSTONE ENGAGEMENT

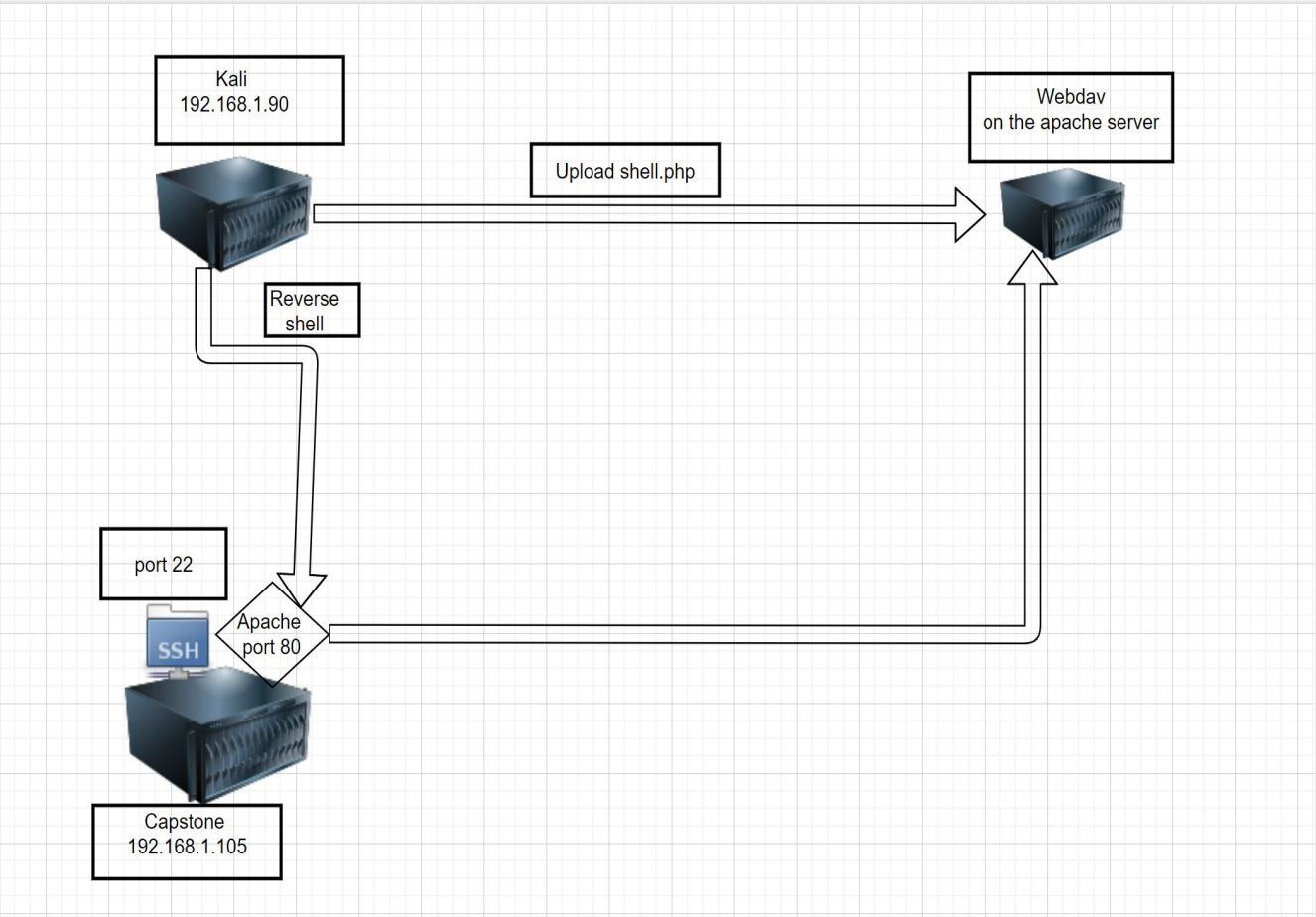
ASSESSMENT, ANALYSIS AND HARDENING OF VULNERABLE SYSTEM

TABLE OF CONTENTS

THIS DOCUMENT CONTAINS THE FOLLOWING SECTIONS:

NETWORK TOPOLOGY

NETWORK TOPOLOGY



Network:
IP Address range: 192.168.1.0/24
Netmask Gateway:

Machines:
IP address:
Operating system (OS):

IP address: 192.168.1.90
Hostname: Kali
OS: Linux

IP address: 192.168.1.105
Hostname: Capstone
OS: Linux

IP address: 192.168.1.100
Hostname: ELK
OS: Linux

RED TEAM
SECURITY ASSESSMENT

RECON: DESCRIBING THE TARGET

Hostname	IP Address	Role on Network
Kali	192.168.1.90	This is the VM for penetrating testing
Capstone	192.168.1.105	This VM is for us to attack by reverse shell into it.
ELK	192.168.1.100	This is the Kibana server. It manages to monitor systems and metric logs on 192.168.1.105

VULNERABILITY ASSESSMENT

THE ASSESSMENT UNCOVERED THE FOLLOWING CRITICAL VULNERABILITIES IN THE TARGET:

Vulnerability	Description	Impact
Port 4444 is for uploading the PHP reverse shell and the port is open	Port 4444 allowed uploading of the PHP reverse shell	The PHP reverse shell was loaded onto the browse network and uploaded
The capstone VM allowed a brute force attack with Hydra. This created an unauthorized 401	Allowed the Brute force attack with Hydra	Found and obtained the password file to login to the network system
In the Capstone machine, the password folder and the secret folder was hidden in the server	In the server the password folder and secret folder was revealed	The password and secret folder were obtained and was used to login

EXPLOITATION: [NAME OF FIRST VULNERABILITY]

01

TOOLS & PROCESSES

HOW DID YOU EXPLOIT THE VULNERABILITY? WHICH TOOL (NMAP, ETC.) OR TECHNIQUES (XSS, ETC.) DID YOU USE?

- METASPLOIT
- MSVENOM

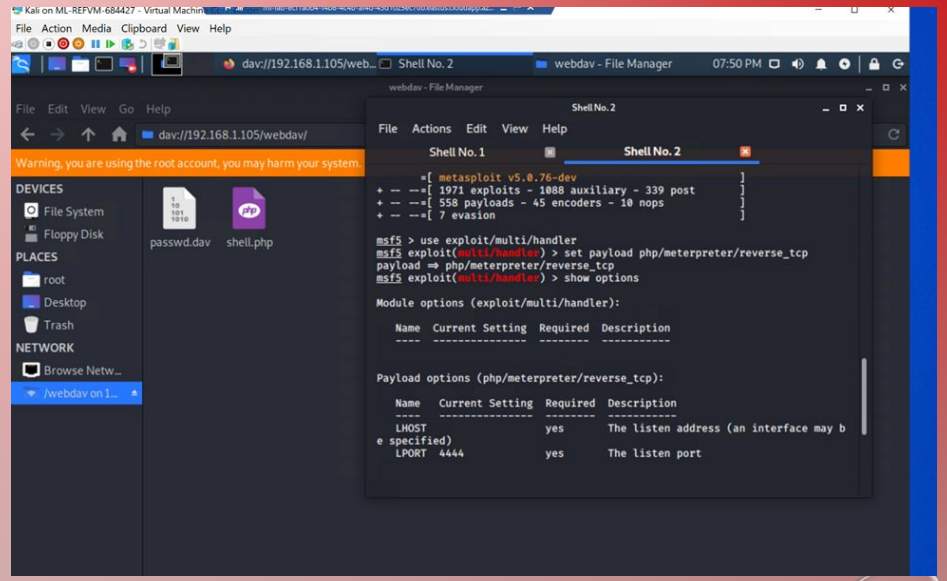
02

ACHIEVEMENTS

WHAT DID THE EXPLOIT ACHIEVE? FOR EXAMPLE: DID IT GRANT YOU A USER SHELL, ROOT ACCESS, ETC.?

- UPLOADED A PHP REVERSE SHELL PAYLOAD
- SETUP A LISTENER

03



EXPLOITATION: [NAME OF SECOND VULNERABILITY]

01

TOOLS & PROCESSES

HOW DID YOU EXPLOIT THE VULNERABILITY?

- I USED HYDRA

WHICH TOOL (NMAP, ETC.) OR TECHNIQUES (XSS, ETC.) DID YOU USE?

- JOHN THE RIPPER

AND

- HTTPS://CRACKINGSTATION.NET

02

ACHIEVEMENTS

WHAT DID THE EXPLOIT ACHIEVE? FOR EXAMPLE: DID IT GRANT YOU A USER SHELL, ROOT ACCESS, ETC.?

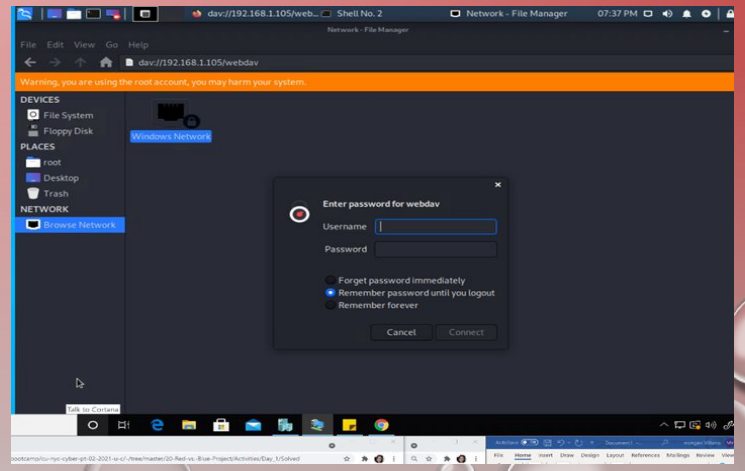
- THE EXPLOIT HELPED OBTAIN THE PASSWORD FOR THE HIDDEN DIRECTORY WHICH WAS EXPLOITED BY A BRUTE FORCE ATTACK
- IT ALSO HELPED LOGGING IN TO CONNECT TO THE SECRET FOLDER.
- FINALLY, HELPED FIND INSTRUCTIONS TO CONNECT TO WEBDAV DIRECTORY. THIS HELPED OBTAIN THE USERNAME AND HASHED PASSWORD

03

COMMANDS:

HYDRA -L ASHTON -P /USR/SHARE/WORDLISTS/ROCKYOU.TXT -S 80 -F -VV 192.168.1.105 HTTP-GET /COMPANY_FOLDERS/SECRET_FOLDER

1. OPEN FILE SYSTEM
2. BROWSE SYSTEM
3. GO TO BROWSE NETWORK THEN TYPE DAV://192.168.1.105/WEBDAV



EXPLOITATION: [NAME OF THIRD VULNERABILITY]

01

TOOLS & PROCESSES

HOW DID YOU EXPLOIT THE VULNERABILITY? WHICH TOOL (NMAP, ETC.) OR TECHNIQUES (XSS, ETC.) DID YOU USE?

HTTPS://CRACKINGSTATION.NET

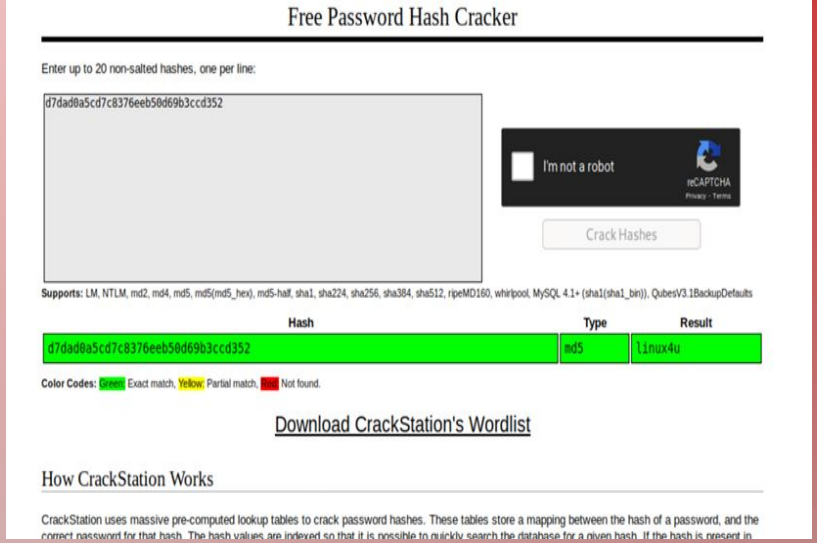
02

ACHIEVEMENTS

WHAT DID THE EXPLOIT ACHIEVE? FOR EXAMPLE: DID IT GRANT YOU A USER SHELL, ROOT ACCESS, ETC.?

- CRACKED THE GIVEN HASHES TO OBTAIN THE PASSWORD

03



USERNAME: RYAN

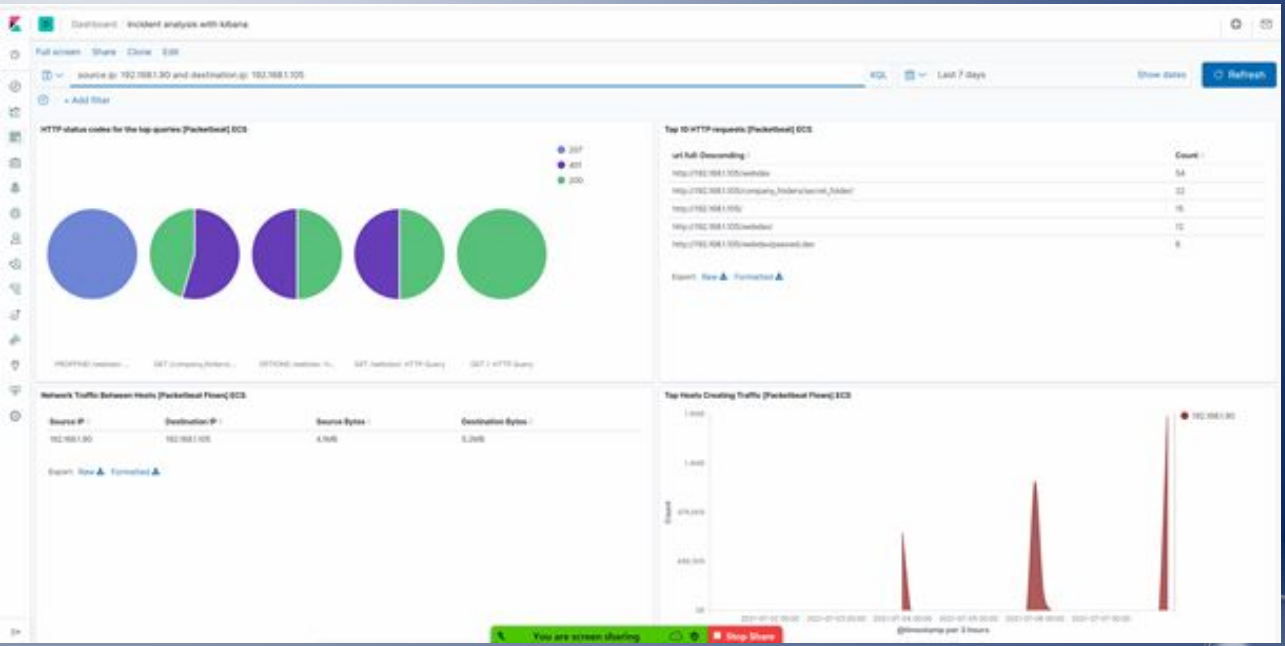
PASSWORD: LINUX4U

BLUE TEAM
LOGIN ANALYSIS AND ATTACK CHARACTERIZATION

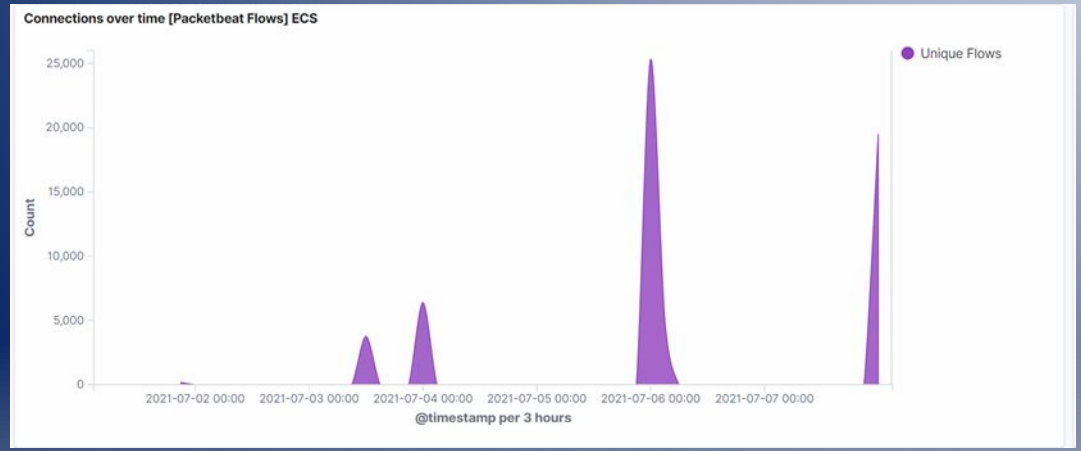
ANALYSIS: IDENTIFYING THE PORT SCAN

- 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

On the dashboard you can see the HTTP error codes panel



We can see that a connection spike in the connection over time [packetbeat flows] ECS



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.
  - ANSWER THE FOLLOWING QUESTIONS IN BULLET POINTS UNDER THE SCREENSHOT IF SPACE ALLOWS. OTHERWISE, ADD THE ANSWERS TO SPEAKER NOTES.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	54
http://192.168.1.105/company_folders/secret_folder/	22
http://192.168.1.105/	15
http://192.168.1.105/webdav/	12
http://192.168.1.105/webdav/passwd.dav	6

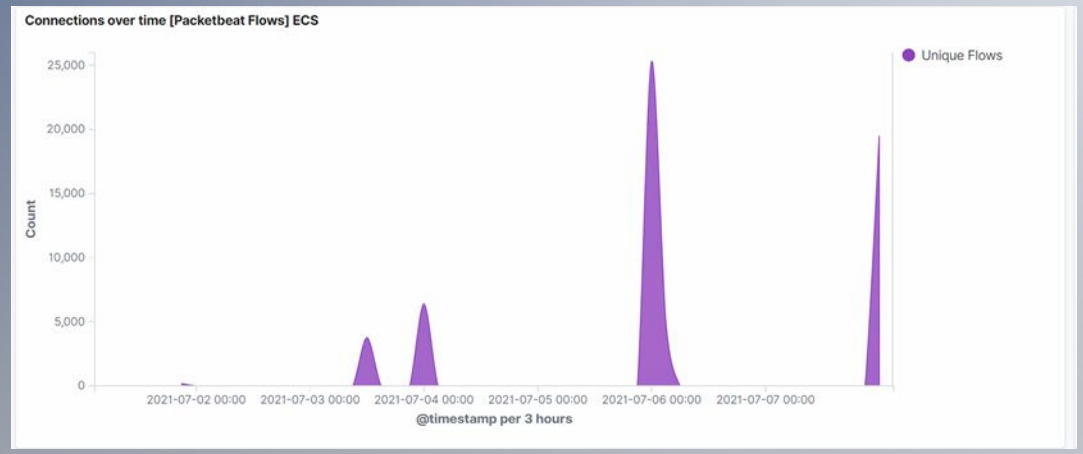
Export: Raw Formatted

On the dashboard that was created, this is a look at your top 10 HTTP requests

Here you can see that this folder had been requested 54 times

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?



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	6
http://192.168.1.105/webdav/	12
http://192.168.1.105/	15
http://192.168.1.105/company_folders/secret_folder/	22
http://192.168.1.105/webdav	54

Export: Raw Formatted

- there is a spike min the traffic to the server and error codes
- There was also a connections in the connection overtime [packet flows] ECS

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?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	6
http://192.168.1.105/webdav/	12
http://192.168.1.105/	15
http://192.168.1.105/company_folders/secret_folder/	22
http://192.168.1.105/webdav	54

Export: Raw Formatted

- It is observed that the shell.php file is in the WebDAV directory on the top 10 HTTP requests
- Command: **source. Ip: 192.168.1.1o05 and destination port 4444**

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?
  - YOU CAN SET AN ALERT FOR THE HTTP STATUS CODES AS 401. (UNAUTHORIZED ERROR)
- WHAT THRESHOLD WOULD YOU SET TO ACTIVATE THIS ALARM?
  - CRITICAL

SYSTEM HARDENING

- WHAT CONFIGURATIONS CAN BE SET ON THE HOST TO MITIGATE PORT SCANS?
  - YOU CAN SET A THRESHOLD FOR THE CONNECTION IN THE SPIKE OVER TIME.

MITIGATION: PREVENTING BRUTE FORCE ATTACK

ALARM

- WHAT KIND OF ALARM CAN BE SET TO DETECT FUTURE BRUTE FORCE ATTACKS?
- YOU CAN SET AN ALERT OF 401 UNAUTHORIZED IS RETURNED FOR ANY UNKNOWN PASSWORDS OVER A CERTAIN THRESHOLD. THIS WILL PUSH OUT ALL THE UNWANTED ATTACKS.
- WHAT THRESHOLD WOULD YOU SET TO ACTIVATE THIS ALARM?
    - 5

SYSTEM HARDENING

- WHAT CONFIGURATION CAN BE SET ON THE HOST TO BLOCK BRUTE FORCE ATTACKS?
    - AFTER 5, THE ALARM THAT WAS SET (401 UNAUTHORIZED) CODES, WOULD DROP THE IP ADDRESS FOR A CERTAIN TIME PERIOD TO MAKE SURE EVERYTHING IS SECURE. IT MIGHT TELL YOU TO RESET YOUR PASSWORD AND DO 2 STEP AUTHENTICATION
- DESCRIBE THE SOLUTION. IF POSSIBLE, PROVIDE THE REQUIRED COMMAND LINE(S).

MITIGATION: DETECTING THE WEBDAV CONNECTION

ALARM

- WHAT KIND OF ALARM CAN BE SET TO DETECT FUTURE ACCESS TO THIS DIRECTORY?
  - YOU CAN CREATE AN ALARM THAT IF SOMEONE ACCESSES IT FROM A RANDOM MACHINE NOT THE MACHINE IT IS SUPPOSED TO RUN ON THE ALERT WOULD GO OFF.
- WHAT THRESHOLD WOULD YOU SET TO ACTIVATE THIS ALARM?
  - MODERATE

SYSTEM HARDENING

- WHAT CONFIGURATION CAN BE SET ON THE HOST TO CONTROL ACCESS?
  - THE ONLY MACHINE THAT SHOULD HAVE ACCESS TO THE FOLDER IS THE HOST MACHINE THAT IT WAS ORIGINALLY LOCATED ON, WHICH MEANS THAT YOU HAVE TO CREATE A FIREWALL RULE. THIS FOLDER SHOULD NOT BE ABLE TO BE OBTAINED BY ANOTHER MACHINE.
- DESCRIBE THE SOLUTION. IF POSSIBLE, PROVIDE THE REQUIRED COMMAND LINE(S).

MITIGATION: IDENTIFYING REVERSE SHELL UPLOADS

ALARM

- WHAT KIND OF ALARM CAN BE SET TO DETECT FUTURE FILE UPLOADS?
  - CREATE AN ALARM FOR ANY TRAFFIC THAT IS TRYING TO GO THROUGH PORT 4444. BECAUSE THIS WAS ONE OF THE VULNERABILITIES WE HAD IN THE PROJECT.
  - IF ANY FILE IS UPLOADED SUCH AS (.PHP FILE) MAKE SURE AN ALERT POPS-UP TO MAKE SURE THAT IT IS SAFE OR NOT.
- WHAT THRESHOLD WOULD YOU SET TO ACTIVATE THIS ALARM?
  - MODERATE

SYSTEM HARDENING

- WHAT CONFIGURATION CAN BE SET ON THE HOST TO BLOCK FILE UPLOADS?
  - YOU CAN HAVE A FILE TYPE VERIFICATION OR RESTRICT SPECIFIC FILE EXTENSIONS. THIS CAN BE ACCESSED ONLY BY ADMINISTRATOR-APPROVED PROGRAMS.
  - YOU CAN ALSO HAVE AN ERROR MESSAGE
- DESCRIBE THE SOLUTION. IF POSSIBLE, PROVIDE THE REQUIRED COMMAND LINE.

The End