Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

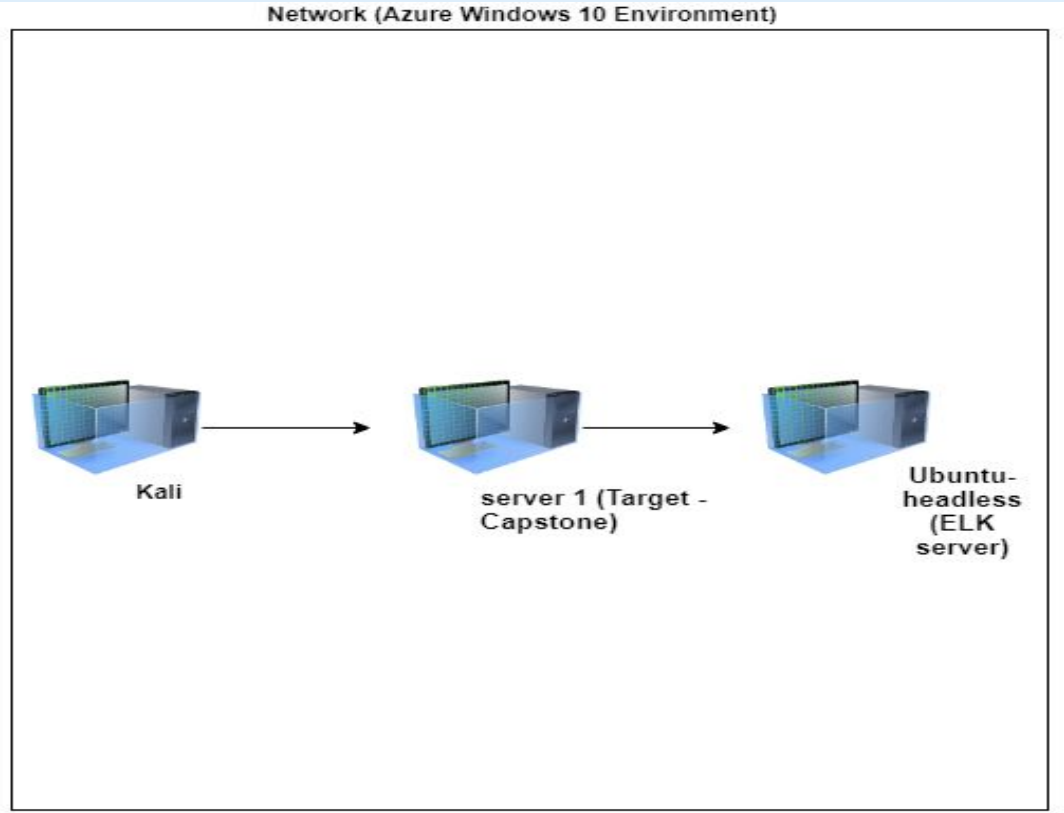
John Schmidt

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.0.1/24
Netmask: 255.255.255.240
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.8
OS: Kali
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.3
Hostname: Ubuntu-headless (ELK server)

IPv4: 192.168.1.105
OS: Linux
Hostname: server 1 (Target - Capstone)

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.8	Attack machine
Ubuntu-headless (ELK server)	192.168.1.100	Network log recording
server 1 (Target - Capstone)	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory List	The directory list is visible via browser even though some directories required some authentication.	The directory list in general was not protected, opening the door for eventual shell.php execution.
Weak Password, weak hash	Vulnerability allowed for access via brute force attack. Also, posting the hash within secret folders.	Allows for attackers to crack the password with brute force text lists.
Reverse Shell Attack	This attack used a lister the client, attacker machine. The target executed the connection. Helps get around firewalls.	Enabled shell.php to be linked together for shell creation if executed from target directory

Exploitation: Directory List

01

Tools & Processes

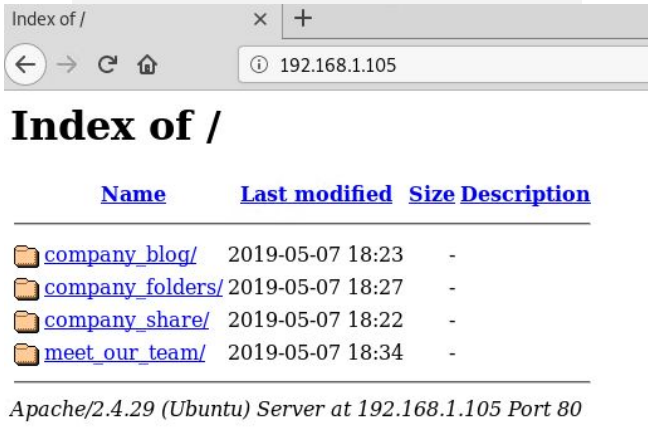
After a port scan, some of the files and directories could be accessed from the browser. The text files gave hints to the secret folder which was password protected. After cracking the password, instructions and a hash were found for connecting to the server. The hash was decoded and connection information found.

02

Achievements

Access was granted to the file directories, allowing for shell.php to be uploaded remotely after hash decryption via shared folder.

03



Exploitation: Weak Password, weak hash

01

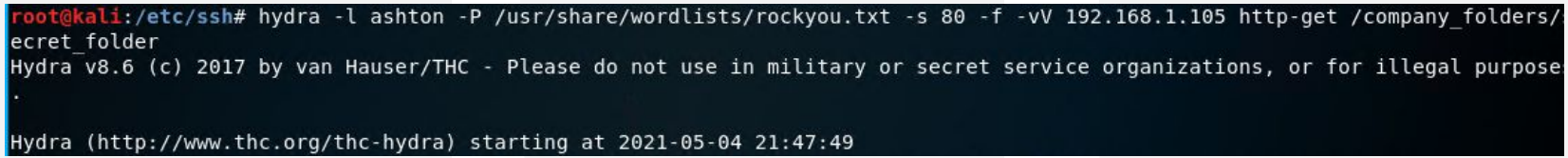
Tools & Processes
Hydra brute force attack was used with wordlist rockyou.txt. The target was set to the secret_folder and the process began.

02

Achievements
After about 10,000 attempts, the password was cracked which paved the way for a reverse shell to be set up along with a shell.php upload which would provide shell access to the target machine.

03

Illustration shows the initiation of hydra brute force attack.



Exploitation: Reverse Shell Attack

01

Tools & Processes

Used reverse shell to gain access to target remotely. Listener port and target ip were set.

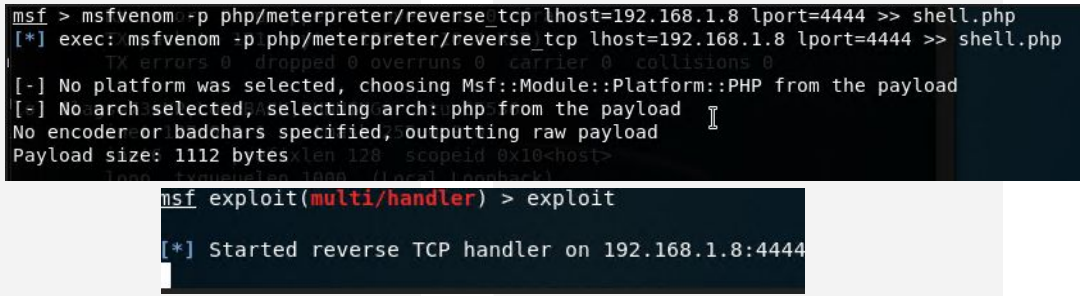
02

Achievements

When shell.php was executed, a shell session could be established, enabling full directory access.

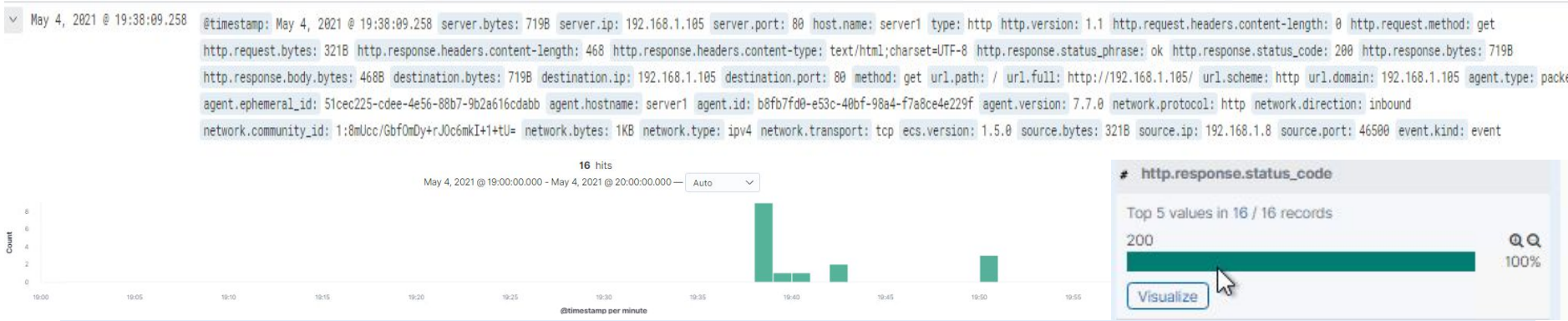
03

Illustration shows exploit waiting for shell.php execution for meterpreter, shell session. After obtaining root access password, msfvenom was used to execute the payload



Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The port scan began at 19:38 on May 4, 2021. There were 16 total packets for the port scan from source_ip:192.168.1.8 to destination.ip: 192.168.1.105 (Target machine). The indication of a port scan would be the timeline before the attack began as well as the status code 200 as the port scan was successful.

Analysis: Finding the Request for the Hidden Directory

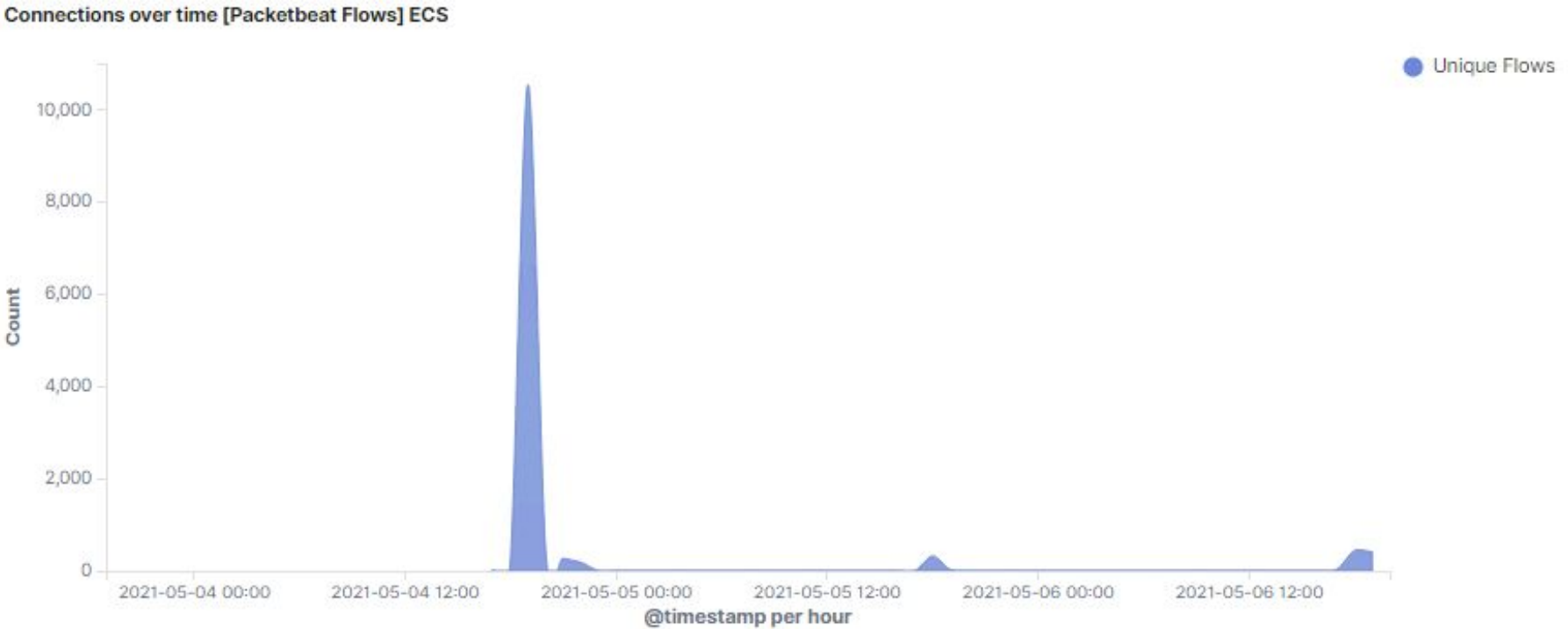
- The request began at 19:30 on May 4, 2021, with 10,018 requests for secret_folder. _doc files were requested. The files contained data.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,018
http://127.0.0.1/server-status?auto=	1,117
http://192.168.1.105/webdav/passwd.dav	20
http://192.168.1.105/webdav	11
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	8

Analysis: Uncovering the Brute Force Attack

- 10,537 total requests.
- 10,536 requests before the password was discovered.



Analysis: Finding the WebDAV Connection

- 15 requests were made to the directory 192.168.1.105/webdav
- Text files were requested.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	252
http://192.168.1.105/webdav	15
http://192.168.1.105/webdav/shell.php	4
http://192.168.1.105/	2
http://192.168.1.105/webdav/	2

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Create an alarm that will alert anytime a scan occurs.

System Hardening

- Close ports, utilize a firewall.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alarm could be set that goes off for any machine that attempts to access that particular directory or file.

System Hardening

- The directory could be moved from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

- Anytime a large number of requests come in at small time intervals. A threshold could be set based on the average traffic compared to the brute force attack sample size of about 10,000. Setting the threshold at 100 would help to identify repeated failed login attempts.

System Hardening

- Close ports that would allow such activity. Port 22 as well as port 80, in this case.
- Create complex passwords.

Mitigation: Detecting the WebDAV Connection

Alarm

- An alarm that goes off if there are any attempts to access the directory or file.

System Hardening

- Remove the file or directory from the server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set an alert for traffic over port 4444 and set alerts for any .php file types being uploaded.

System Hardening

- Uploads should require authorization.
- The server should implement an upload filter and disallow any executable file downloads.
- Disable ssh by commenting out Port 22 in the sshd_config file.


The End