Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

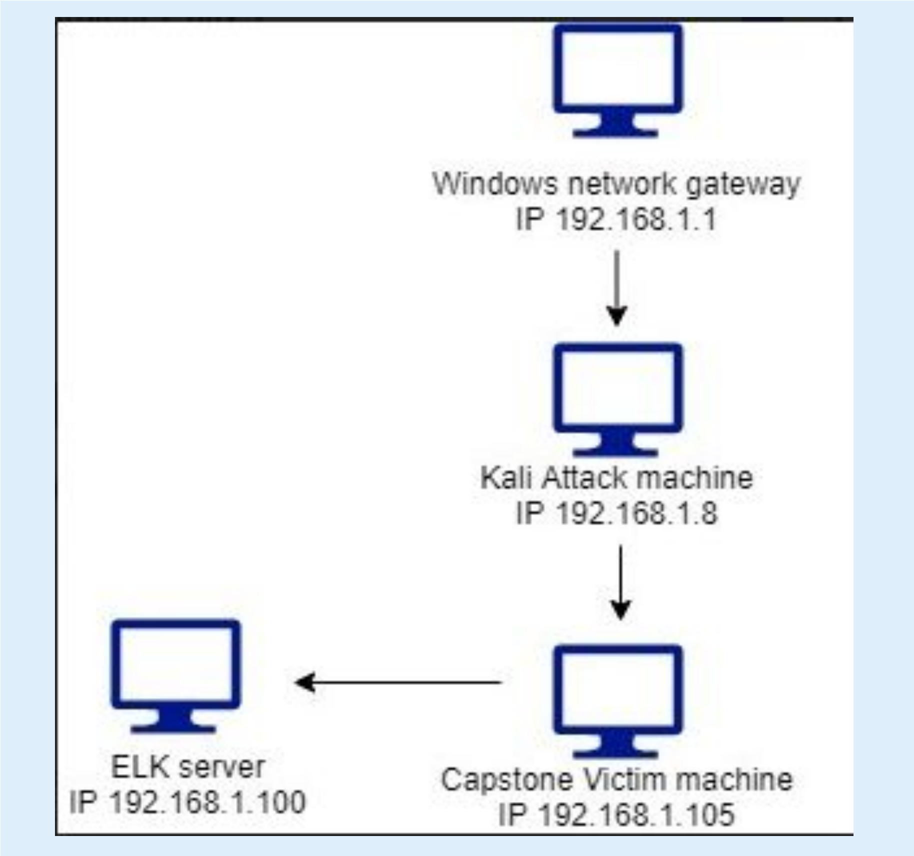
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

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 XP
Hostname: gateway

IPv4:192.168.1.100
OS:Linux 3.2 - 4.9
Hostname: ELK

IPv4:192.168.1.105
OS: Linux 3.2-4.9
Hostname: Capstone

IPv4:192.168.1.8
OS:Linux 3.7 - 3.10
Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
gateway	192.168.1.1	Jumpbox/Hypervisor
ELK	192.168.1.100	ELK stack
Capstone	192.168.1.105	webserver/victim
Kali	192.168.1.8	Attacker computer

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive data exposure	The name of the secret_folder was left in full view in documents easily accessible by the public.	This allowed for an attacker to try a brute force attack on the secret_folder login with usernames that were easily found.
Credential stuffing	Brute forcing a password	The password for ashton was brute forced to allow access to the secret_folder
Sensitive data exposure	Password hashes exposed	The password hash for Ryan was found and cracked, allowing access to the webserver.
LFI vulnerability	Shell.php was uploaded to webserver	The script was ran to open a reverse shell on the attack computer.

Exploitation: Brute force attack for credentials

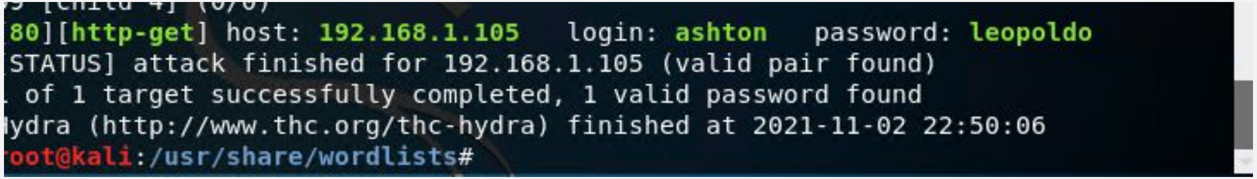
01

Tools & Processes
A brute force attack was used with Hydra to find the password for user “ashton”.

02

Achievements
This allowed us access into the secret_folder on the web server.

03



```
)5 [child 4] (0/0)
80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
STATUS] attack finished for 192.168.1.105 (valid pair found)
 of 1 target successfully completed, 1 valid password found
ydra (http://www.thc.org/thc-hydra) finished at 2021-11-02 22:50:06
oot@kali:/usr/share/wordlists#
```

Exploitation: Cracking a password hash

01

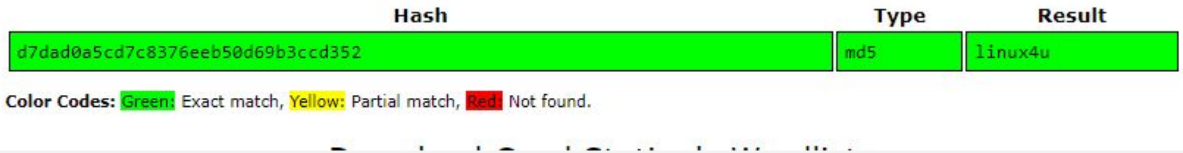
Tools & Processes
Located in the secret_folder there was a password hash for user “ryan”. This hash was cracked using crackstation.net

02

Achievements
This password and username combination gained us access to the /webdav page.

03

This screen shot shows the found hash, and the password.



Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Exploitation: Uploading and running exploit

01

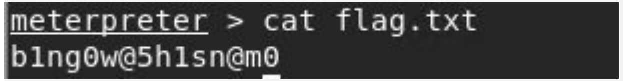
Tools & Processes
With access to the /webdav server, I was able to create a PHP reverse shell payload using Msfvenom. This script was uploaded to the webserver, and then ran. Creating a reverse shell on the web server.

02

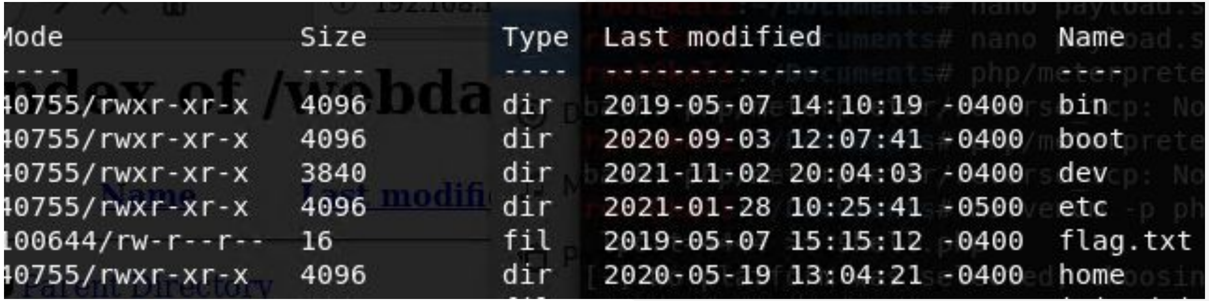
Achievements
This exploit granted me access to the server via a meterpreter session. I was then able to find the flag file on the server located in the root directory.

03

This screen shot shows the files located in the root directory, and the flag from the flag.txt file.



```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
```



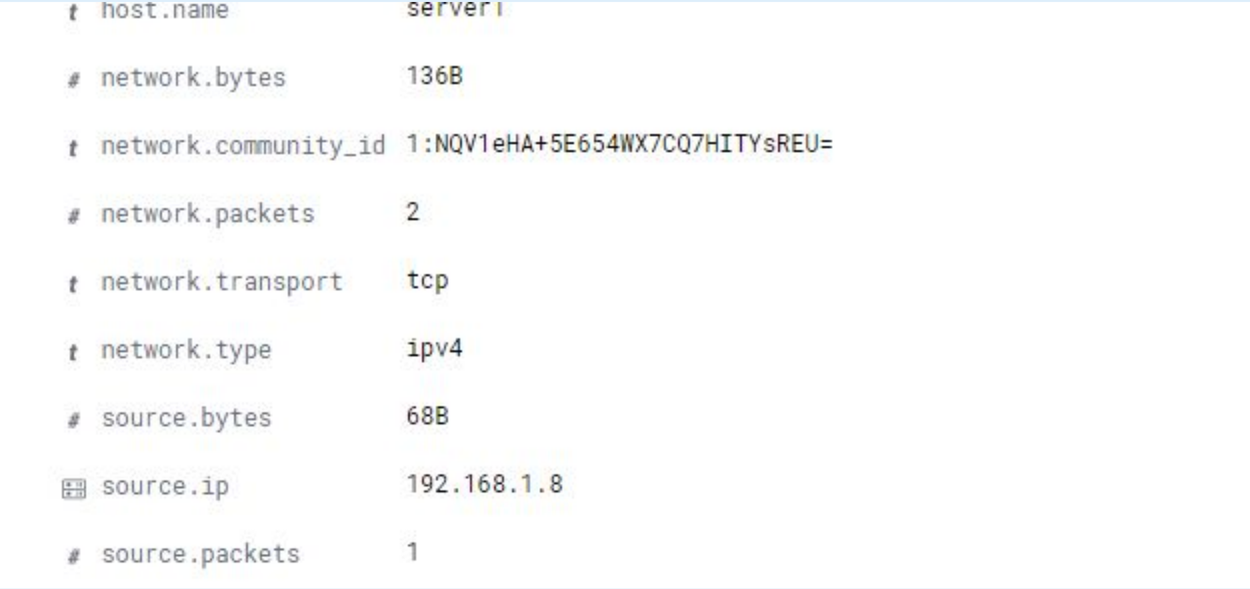
```
Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40755/rwxr-xr-x   4096       dir   2019-05-07 14:10:19 -0400  bin
40755/rwxr-xr-x   4096       dir   2020-09-03 12:07:41 -0400  boot
40755/rwxr-xr-x   3840       dir   2021-11-02 20:04:03 -0400  dev
40755/rwxr-xr-x   4096       dir   2021-01-28 10:25:41 -0500  etc
100644/rw-r--r--  16         fil   2019-05-07 15:15:12 -0400  flag.txt
40755/rwxr-xr-x   4096       dir   2020-05-19 13:04:21 -0400  home
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

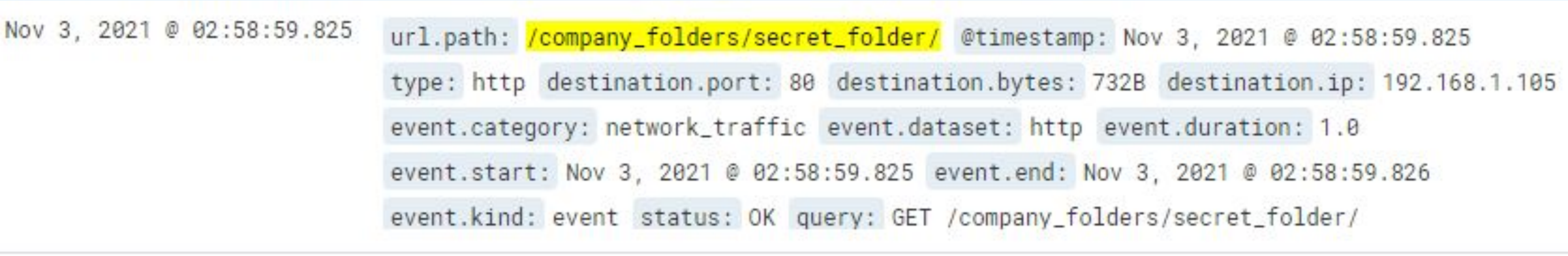
- What time did the port scan occur? 1:29am
- How many packets were sent, and from which IP? 28,120 packets from 192.168.1.8
- What indicates that this was a port scan? All ports were sent a packet in a short amount of time.



```
t  host.name              server1
#  network.bytes          136B
t  network.community_id   1:NQV1eHA+5E654WX7CQ7HITYsREU=
#  network.packets        2
t  network.transport      tcp
t  network.type           ipv4
#  source.bytes           68B
   source.ip              192.168.1.8
#  source.packets         1
```

Analysis: Finding the Request for the Hidden Directory

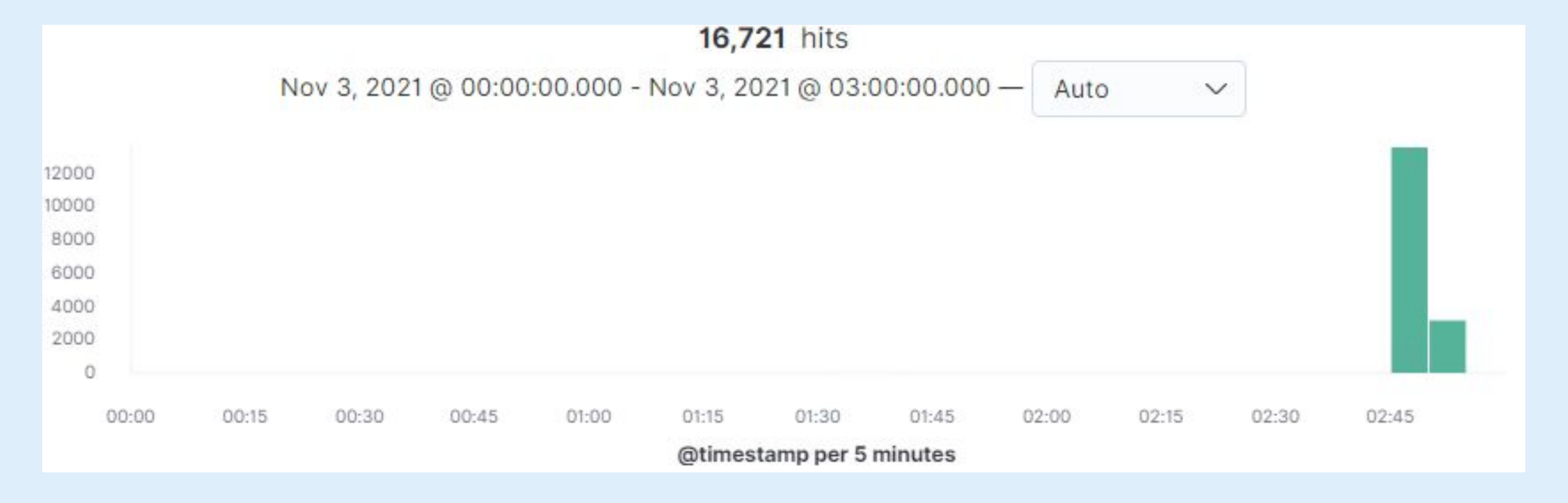
- What time did the request occur? 2:58am
- How many requests were made? 16,721
- Which files were requested? The files requested were connect_to_corp_server
- What did they contain? It contained the password hash for Ryan, as well as instructions on connecting to the server



```
Nov 3, 2021 @ 02:58:59.825   url.path: /company_folders/secret_folder/ @timestamp: Nov 3, 2021 @ 02:58:59.825
                             type: http destination.port: 80 destination.bytes: 732B destination.ip: 192.168.1.105
                             event.category: network_traffic event.dataset: http event.duration: 1.0
                             event.start: Nov 3, 2021 @ 02:58:59.825 event.end: Nov 3, 2021 @ 02:58:59.826
                             event.kind: event status: OK query: GET /company_folders/secret_folder/
```

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 16,721
- How many requests had been made before the attacker discovered the password? 10,143



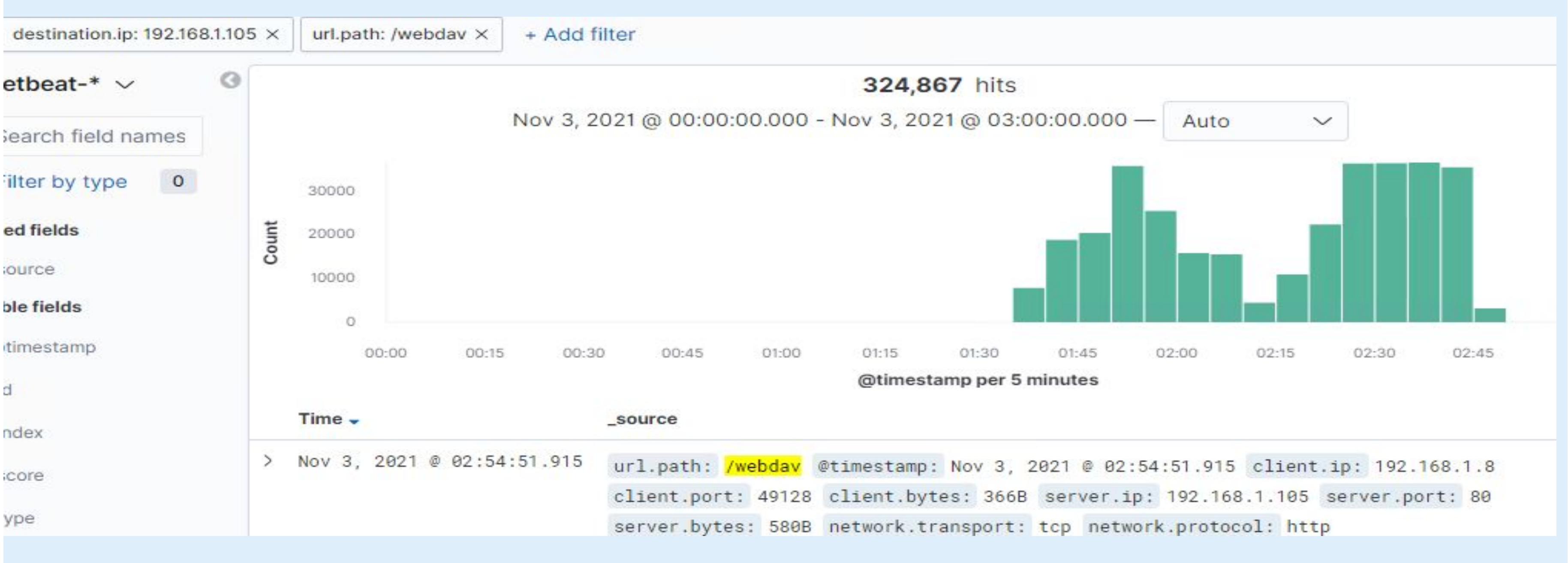
16,721 hits

Nov 3, 2021 @ 00:00:00.000 - Nov 3, 2021 @ 03:00:00.000 — Auto

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? 324,867
- Which files were requested? Passwd.dav, as well as uploading the shell.php file



destination.ip: 192.168.1.105 ✕ | url.path: /webdav ✕ | + Add filter

etbeat-*

earch field names

ilter by type 0

ed fields

ource

ble fields

timestamp

d

ndex

core

ype

324,867 hits

Nov 3, 2021 @ 00:00:00.000 - Nov 3, 2021 @ 03:00:00.000 — Auto

Time	_source
> Nov 3, 2021 @ 02:54:51.915	url.path: /webdav @timestamp: Nov 3, 2021 @ 02:54:51.915 client.ip: 192.168.1.8 client.port: 49128 client.bytes: 366B server.ip: 192.168.1.105 server.port: 80 server.bytes: 580B network.transport: tcp network.protocol: http

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Create an alarm to detect excessive SYN requests, or UDP scans.

Set the threshold at 10 requests within 5 seconds from the same IP address.

System Hardening

Close all unnecessary ports. Make sure all open ports don’t have vulnerabilities, and patch the vulnerabilities that are found

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set alarm for URL paths that are not publicly accessible, and not coming from a whitelisted IP address.
The threshold for this should be 1.

System Hardening

No webpages should have information, or links to a webpage that is not publicly accessible.

Sterlize all public webpages for links to all hidden webpages. All hidden webpages need only be accessible with proper 2 factor authentication.

Mitigation: Preventing Brute Force Attacks

Alarm

Set alarm for excessive failed login attempts. A threshold of 5 failed logins with a lockout period of 30 minutes would be sufficient.

System Hardening

2 factor authentication would be most beneficial, but a lockout period after a threshold is met would help prevent brute force attacks as well.

Mitigation: Detecting the WebDAV Connection

Alarm

An alarm for non-whitelisted IP addresses successfully logging in to the WebDAV server.

The threshold for this alarm should be 1. So anybody not on the whitelist would alert the SOC if they successfully logged in.

System Hardening

Whitelist known IP addresses of employees who need access to the WebDAV server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alarm can be set for any file uploaded to the server and who uploaded it. If a malicious file is uploaded, antivirus software can stop it and the IP address can be blacklisted .

System Hardening

Antivirus should be ran on all files once uploaded to the server. This would prevent malicious files being uploaded and ran.

The End