Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

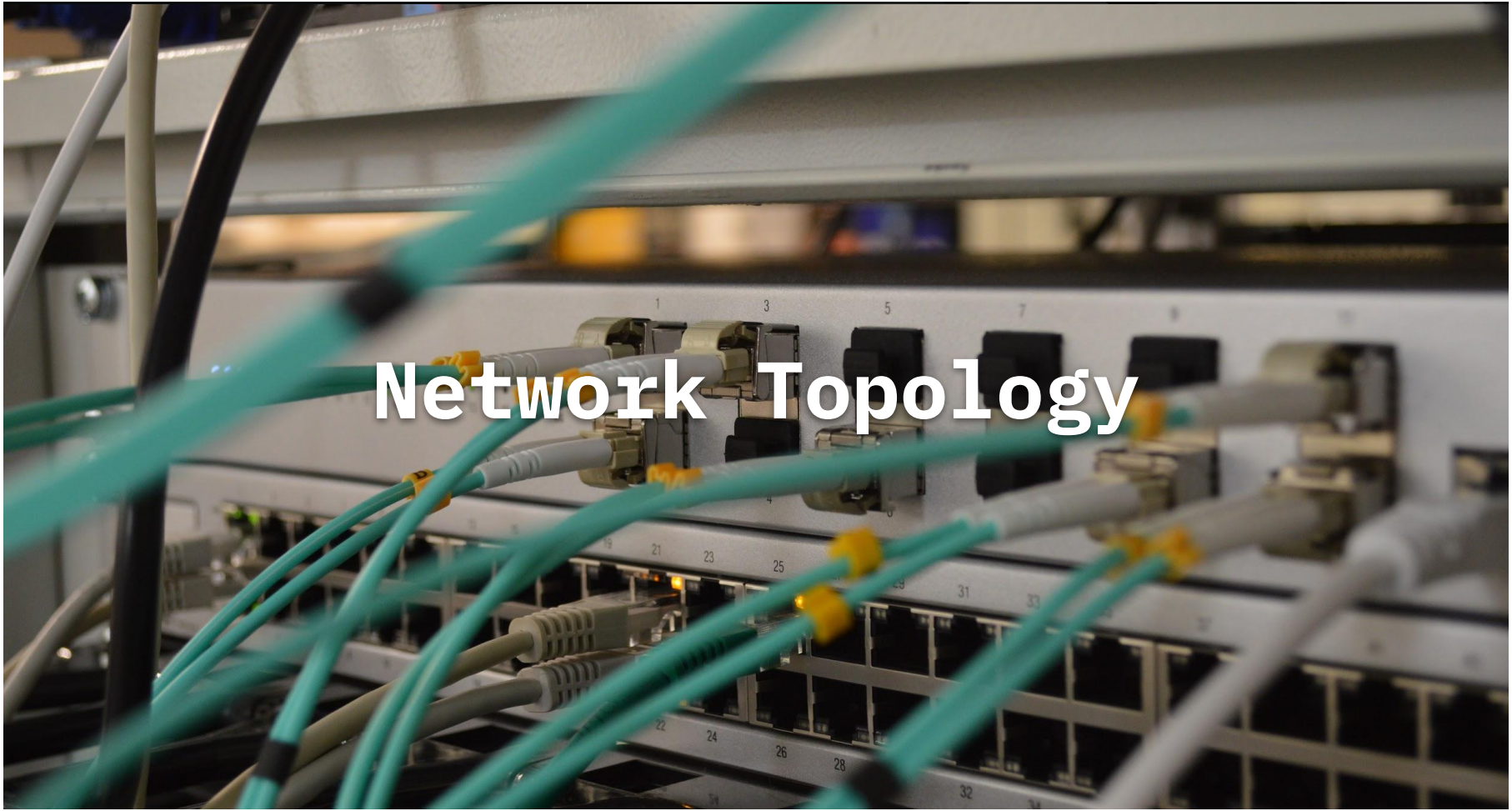
Josh Brnak

August 2020

Project Overview

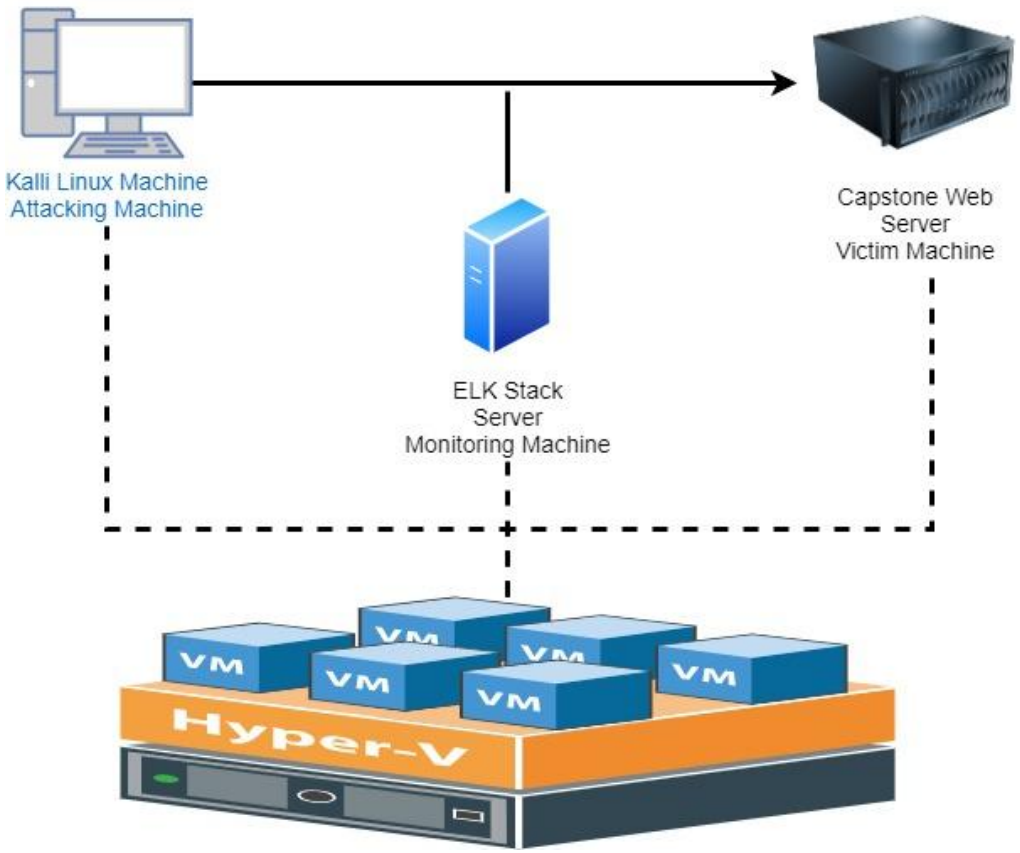
- Red Team - Blue Team Exercise
- Red Team - Identify and Exploit Vulnerabilities On the Victim Machine (Capstone Server)
- Blue Team - Monitor Network Traffic To Characterize Red Team Attack
- Blue Team - Propose Monitoring and Alarms To Mitigate Red Team Attack

Table of Contents



Network Topology

Network Topology



Network
Address Range:
192.168.1.1/24

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname:Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V

Red Team
Capstone Security Assessment

Vulnerability/Exploit Assessment

The assessment uncovered the following critical vulnerabilities and exploits in the target:

Vulnerability/Exploit	Description	Impact
Port Scan	Scans ports of the victim machine	Provides the hacker the ability to see what ports are open on the victim machine to exploit
Human Element	Human element puts information important to the hacker in public domains	Allows the hacker to obtain important information used to gain access to the system
Brute Force Attack	Brute force finds the password protecting sensitive files	Sensitive files protected by the password can be obtained
Hash Protected User Password	An encrypted user password was able to be decrypted	Allows the hacker to log in to the sensitive WebDAV directory
Reverse Shell Script Uploading to Company Server	Malicious files can be uploaded to the server	Malicious files can be used for attacker to gain access to sensitive information

Recon: Describing the Target

Nmap scan identified the following hosts on the network 192.168.1.1/24

Hostname	IP Address	Role on Network
Hyper-V Manager	192.168.1.1	Terminal Services
Kali	192.168.1.90	Attacking Machine
Capstone	192.168.1.105	Victim Machine
ELK	192.168.1.100	Monitoring Machine

Exploitation: Port Scan

01

Tools & Processes

Used Kali Linux to run a port scan on the victim machine

02

Achievements

Was able to identify that the victim machine had an open HTTP port with which to possibly exploit

03

```
Nmap scan report for cap_machine (192.168.1.105)
Host is up (0.00047s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

Exploitation: Human Factor

01

Tools & Processes

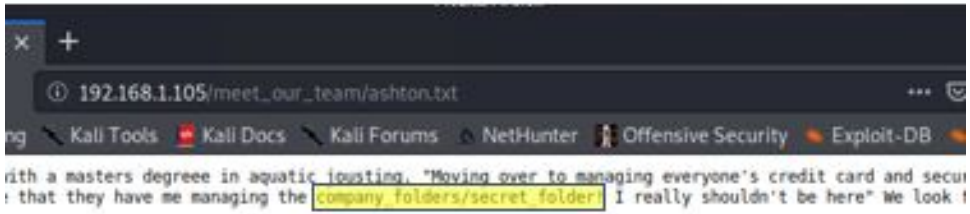
Navigated through victim system looking for human errors to exploit

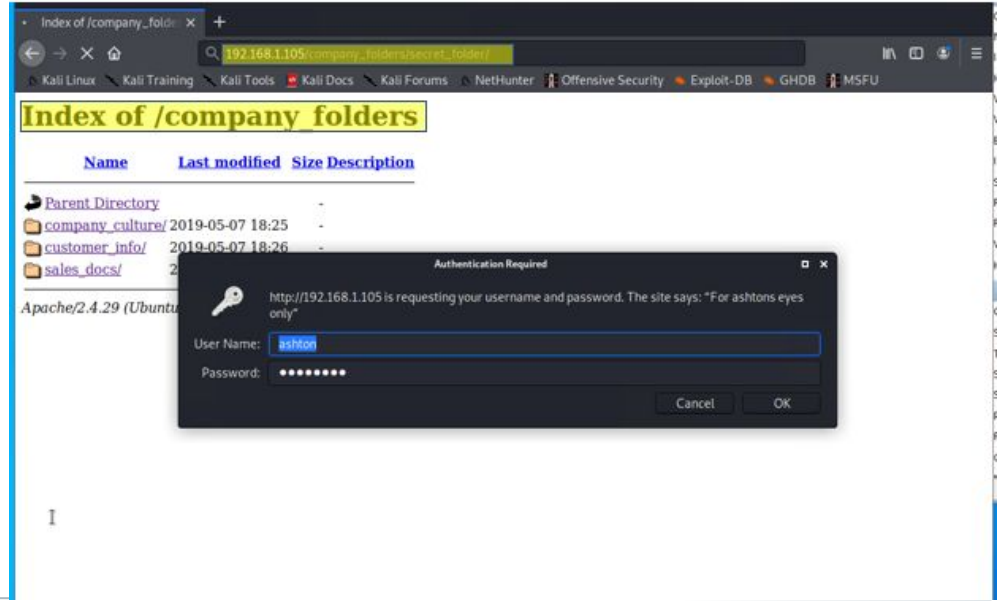
02

Achievements

Found clues to user login information and the location of a secret folder used to gain access to sensitive information

03





Exploitation: Brute Force Attack

01

Tools & Processes

Used a tool in Kali Linux (Hydra) to brute force crack a user password

02

Achievements

Gave us access to password protected company folders containing directions to access the company server

03

- The command line syntax to use hydra is:

hydra -l <password_username> -P <wordlist> -s <Port> -f -vV <victim_ip_address> http-get <path_to_directory_on_victim_machine>

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 3] (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 2020-08-14 17:39:24
root@Kali:~#
```

Exploitation: Hash Protected User Password

01

Tools & Processes

Able to use the tool CrackStation to decrypt a hashed password

02

Achievements

Obtained the password needed to log in to the company server

03

Exploitation: Reverse Shell Script Upload

01

Tools & Processes

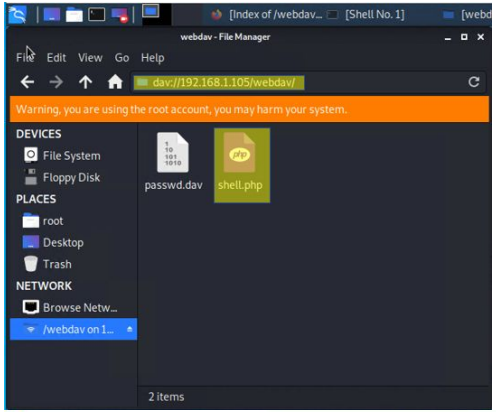
Uploaded a reverse shell script onto company server

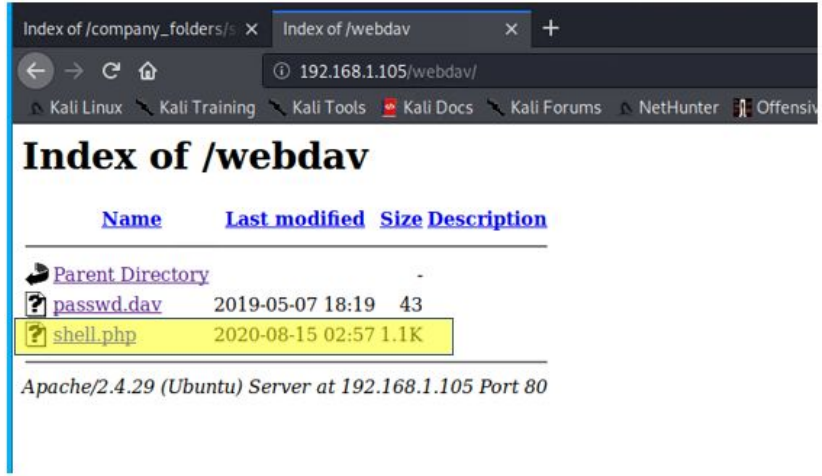
02

Achievements

When shell script is ran access to the victim machine is given to attacker

03





Blue Team

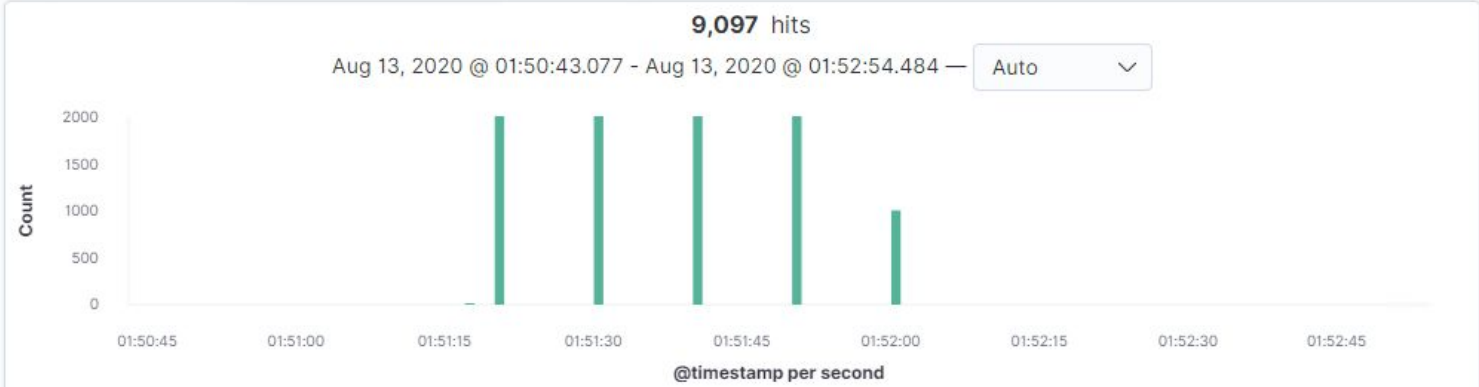
Log Analysis and Attack Characterization

Evidence of Attack in Logs

Attack Description	Evidence
Port Scan	Large volume of activity from attacking machine to many different ports
Access to Secret Folder	Shown in the url path
Brute Force Attack	Large volume of failed HTTP requests from Mozilla (Hydra)
Access to WebDAV Directory On Capstone Server	Shown in url path
Reverse PHP Shell	Traffic to reverse shell /webdav/shell.php

Analysis: Identifying the Port Scan

- Port Scan occurred at 01:51:17:449
- 9,097 packets were sent from 192.168.1.90
- Packets were sent from varying ports indicating a port scan



Time	_source
Aug 13, 2020 @ 01:51:17.449	@timestamp: Aug 13, 2020 @ 01:51:17.449 client.port: 53550 client.bytes: 18B client.ip: 192.168.1.90 status: OK http.request.bytes: 18B http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 1.4KB http.response.headers.content-length: 1,389 http.response.headers.content-type: text/html;charset=UTF-8 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 1.5KB http.version: 1.0 type: http

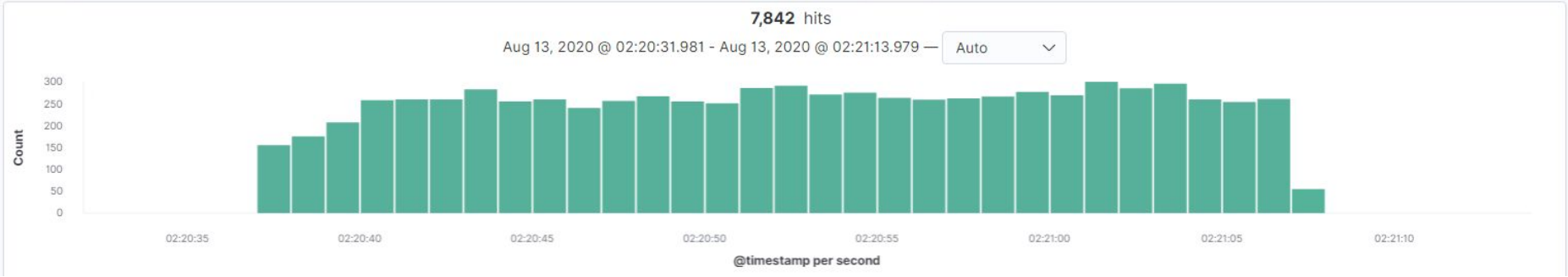
Analysis: Finding the Request for the Hidden Directory

- Request occurred 01:59:49:132 on August 13
- 6 requests are seen being made
- Trying to access secret_folder with instructions to connect to corporate server

Analysis: Uncovering the Brute Force Attack

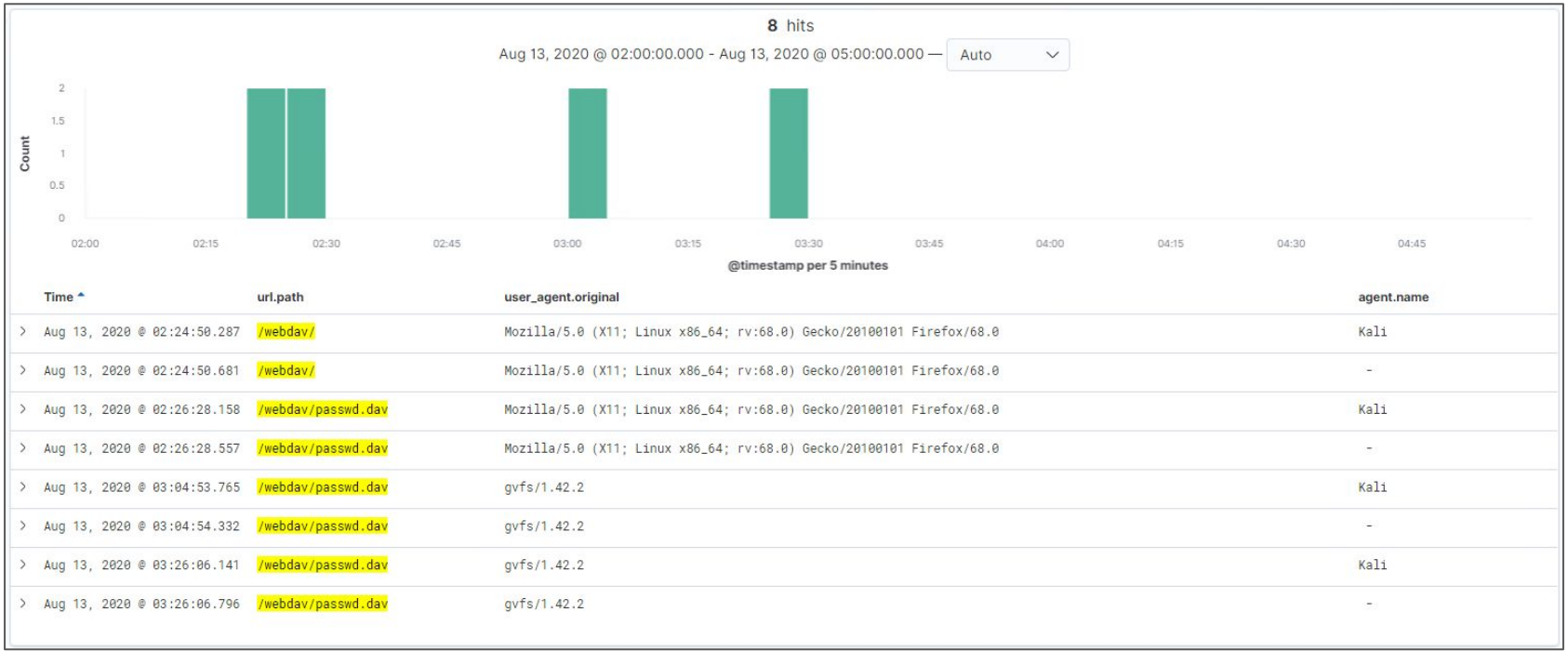
- 7,842 attempts were made in the brute force attack
- Brute force attack indicated by large number of failed HTTP requests by same source
- User agent shows brute force attack tool (Hydra)

Time	agent.type	user_agent.original	source.port
Aug 13, 2020 @ 02:22:01.312	packetbeat	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	54740
Aug 13, 2020 @ 02:22:00.928	packetbeat	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	54740
Aug 13, 2020 @ 02:21:07.379	packetbeat	Mozilla/4.0 (Hydra)	54730
Aug 13, 2020 @ 02:21:07.379	packetbeat	Mozilla/4.0 (Hydra)	54732



Analysis: Finding the WebDAV Connection

- 8 requests were made to the /webdav directory.
- The passwd.dav file was trying to be accessed



Time	url.path	user_agent.original	agent.name
Aug 13, 2020 @ 02:24:50.287	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	Kali
Aug 13, 2020 @ 02:24:50.681	/webdav/	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	-
Aug 13, 2020 @ 02:26:28.158	/webdav/passwd.dav	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	Kali
Aug 13, 2020 @ 02:26:28.557	/webdav/passwd.dav	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	-
Aug 13, 2020 @ 03:04:53.765	/webdav/passwd.dav	gvfs/1.42.2	Kali
Aug 13, 2020 @ 03:04:54.332	/webdav/passwd.dav	gvfs/1.42.2	-
Aug 13, 2020 @ 03:26:06.141	/webdav/passwd.dav	gvfs/1.42.2	Kali
Aug 13, 2020 @ 03:26:06.796	/webdav/passwd.dav	gvfs/1.42.2	-

Analysis: Finding the Reverse Shell Script

- Traffic to shell.php on WebDAV server from attacking machine

/webdav/shell.php	gvfs/1.42.2	-	192.168.1.90	server1
/webdav/shell.php	gvfs/1.42.2	-	192.168.1.90	server1
/webdav/shell.php	gvfs/1.42.2	-	192.168.1.90	server1
/webdav/shell.php	gvfs/1.42.2	-	192.168.1.90	server1
/webdav/shell.php	gvfs/1.42.2	Kali	192.168.1.90	Kali
/webdav/shell.php	gvfs/1.42.2	Kali	192.168.1.90	Kali
/webdav/shell.php	gvfs/1.42.2	Kali	192.168.1.90	Kali
/webdav/shell.php	gvfs/1.42.2	Kali	192.168.1.90	Kali
/webdav/shell.php	gvfs/1.42.2	-	192.168.1.90	server1
/webdav/shell.php	gvfs/1.42.2	-	192.168.1.90	server1
/webdav/shell.php	gvfs/1.42.2	Kali	192.168.1.90	Kali
/webdav/shell.php	gvfs/1.42.2	Kali	192.168.1.90	Kali

Blue Team

Monitoring, Alarms and Mitigation

Mitigation: Port Scan

Alarm

Monitor source IP, source port, packet count, http request status’

Set alarm to notify if the number of requests from the same host exceeds a certain threshold

Set threshold of 1 attempt per second

System Hardening

Restrict access to Capstone server to employees only thus blocking potential port scans from outside hosts

Patch firewall to allow only desired hosts access to system

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set alarm for when there is traffic to secret_folder directory from outside the company

Set alarm to activate after one attempt to access secret folder from outside the company network

Monitor url path, source IP, and source port, for traffic to secret_folder

System Hardening

Eliminate information on system that hints at login information

Reduce human error component. Educate employees about what type of information to not put in public forums

Patch firewall to whitelist company users and blacklist all others from access to secret_folder

Mitigation: Preventing Brute Force Attacks

Alarm

Set alarm to notify when a certain threshold of attempted failed logins occurs

Set alarm to notify when threshold of 1 failed attempt per second occurs

Monitor source IP, source port, http request code, url path, user agent,

System Hardening

Establish an account lockout policy to minimize the number of attempts that can be made to log in.

The victim machine has a linux OS so tools such as PAM and pam_tally2 can be used to set the lockout policy

Whitelist or blacklist IP's that can access the secret_folder and are able to attempt to log in

Set up white or black lists in firewall

Mitigation: Detecting the WebDAV Connection

Alarm

Set alarm to notify if a host outside of the company is trying to access the WebDAV directory

Monitor source IP, source port, url path

System Hardening

Whitelist or blacklist users able to connect to the WebDav directory

Set-up firewall on server with whitelist or blacklist IP's

Eliminate human component of storing a hash protected password easily decrypted

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Alerts should be sent notifying of all/any file upload activity
- Alerts sent for any outside IP address requesting access

System Hardening

- Limit file upload access to a list of approved IP address (whitelist)
- Internal audits to ensure that sensitive data/information is not on the website

the End