Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Tristen Maetzold

Table of Contents

This document contains the following sections:

01 **Network Topology**

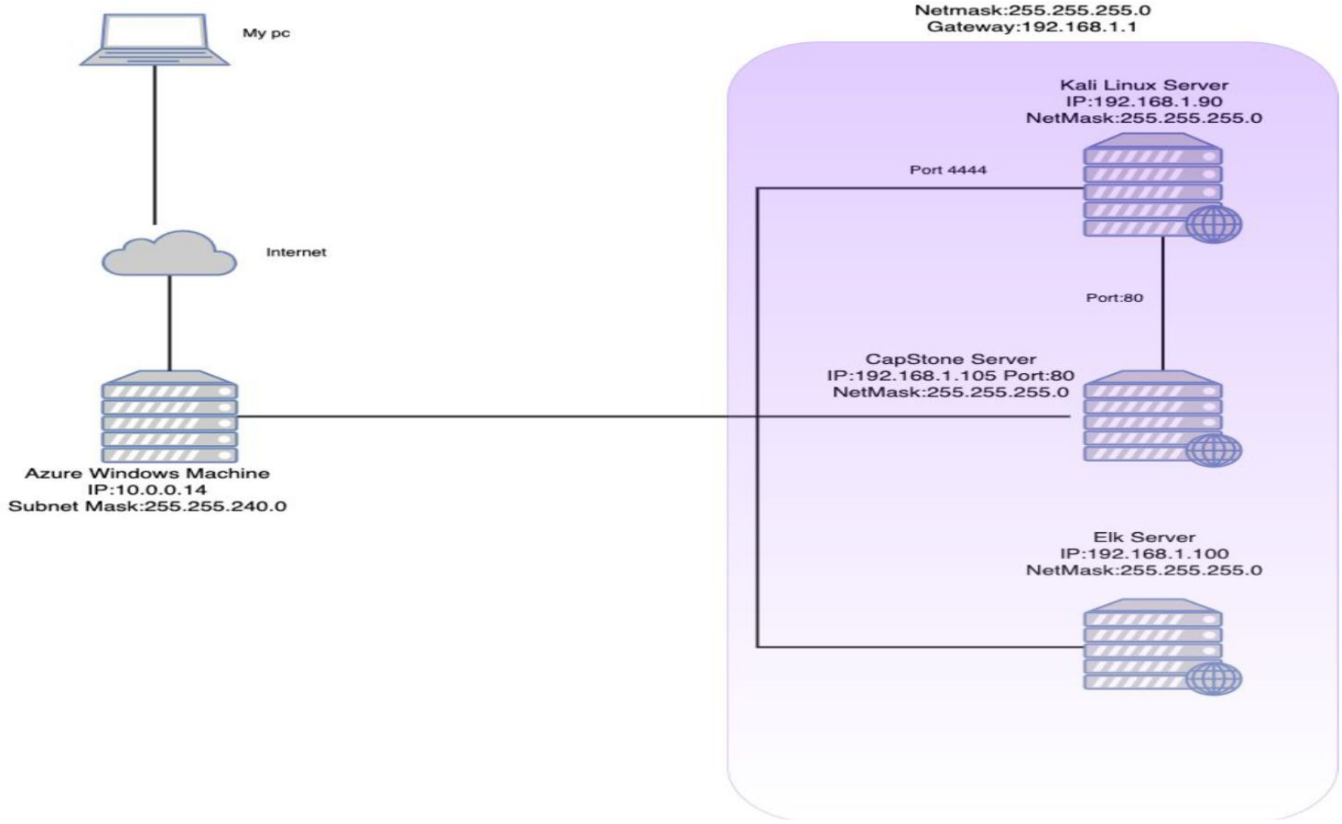
02 **Red Team**: Security Assessment

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: 192.167.1.90
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: ML-RFVM-68
4424 **Azure**

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacking Machine
Capstone	192.168.1.105	Defending Machine
ELK	192.168.1.100	Network Monitor (Kibana)
Hyper V Manager	192.168.1.1	Virtual Machine Host

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (1l)	Information is disclosed that the recipient is not mean to receive.	Found the ‘secret_folder’
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (II)	Information is disclosed that the recipient is not mean to receive.	Brute force password for ‘secret_folder’
CWE-434: Unrestricted Upload of File with Dangerous Type	Arbitrary code execution is possible if the uploaded file is interpreted and executed as code.	Allows me to upload php reverse shell to webdav share.
OWASP A02:2021 - Cryptographic Failures	Deprecated hash functions (e.g. MD5 or SHA1) are in use	Able to unhash passwords and get credentials
OWASP A05:2021 - Security Misconfiguration	Missing appropriate security hardening across any part of application stack.	SSH allows password authentication.

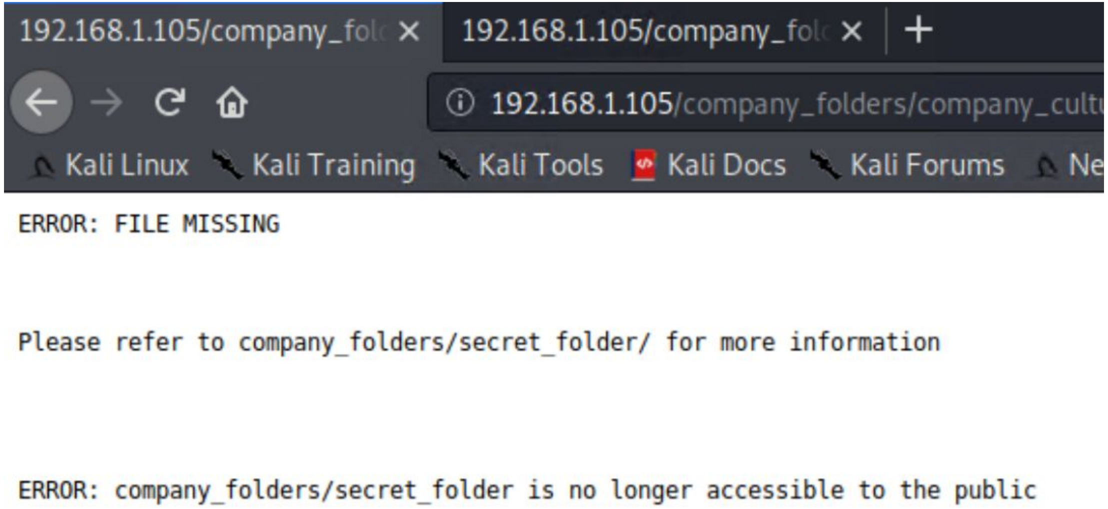
Exploitation: Learning of ‘Secret_Folder’

01

Tools & Processes
Sleuthing through 192.168.1.105 on a web browser.

02

Achievements
company_folders/secret_folder/ exists


192.168.1.105/company_fol
192.168.1.105/company_fol
192.168.1.105/company_folders/company_cultu
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
Ne

```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


ERROR: company_folders/secret_folder is no longer accessible to the public
```

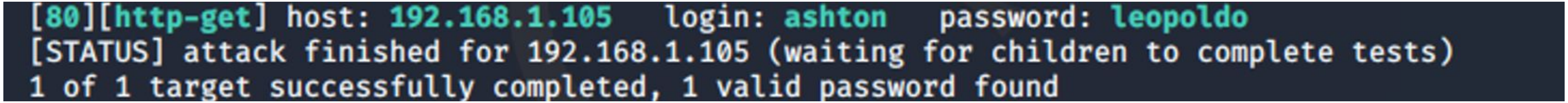
Exploitation: Hydra Brute Forcing

01

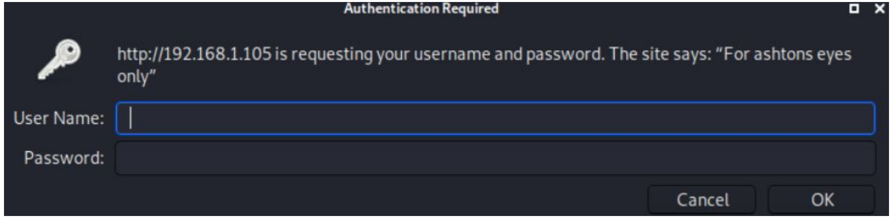
Tools & Processes
Use the ‘Hydra’ tool to find the password.

02

Achievements
Found Ashton’s credentials and signed in.



```
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
```

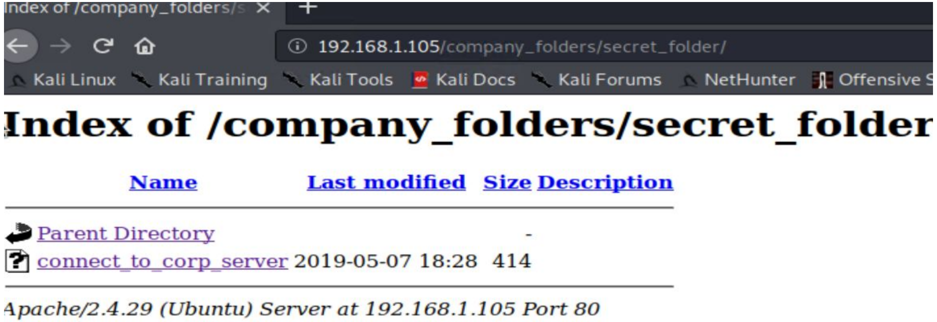


Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name:

Password:



Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

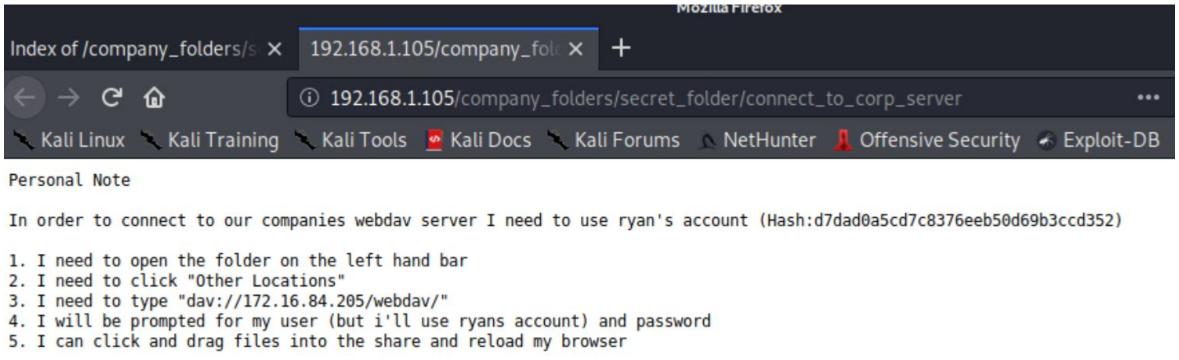
Exploitation: Instructions Located for webdav

01

Tools & Processes
Signed into the /secret_folder/ using credentials from Hydra.

02

Achievements
Retrieved webdav instructions.


Mozilla Firefox
Index of /company_folders/s
192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

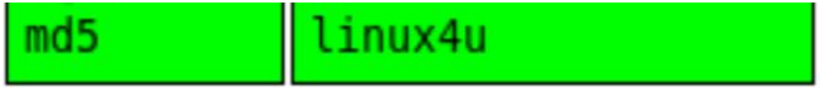
Exploitation: Crack the Hash

01

Tools & Processes
Cracked the hash found in 'secret_folder' using a website called crackstation.net found by googling 'Hash Cracking website'.

02

Achievements
Acquired Ryan's password.

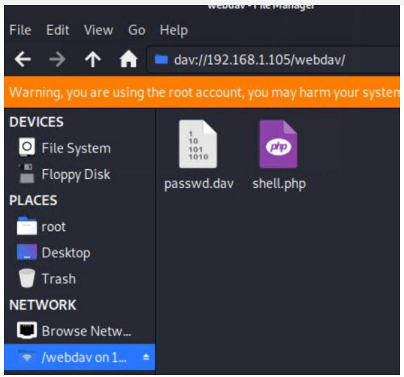


md5	linux4u

Exploitation: Reverse Shell Delivery

01

Tools & Processes
Utilized msfvenom to create a reverse shell, and uploaded it via webdav. This shell connects back to the **Kali** machine.



dav://192.168.1.105/webdav/

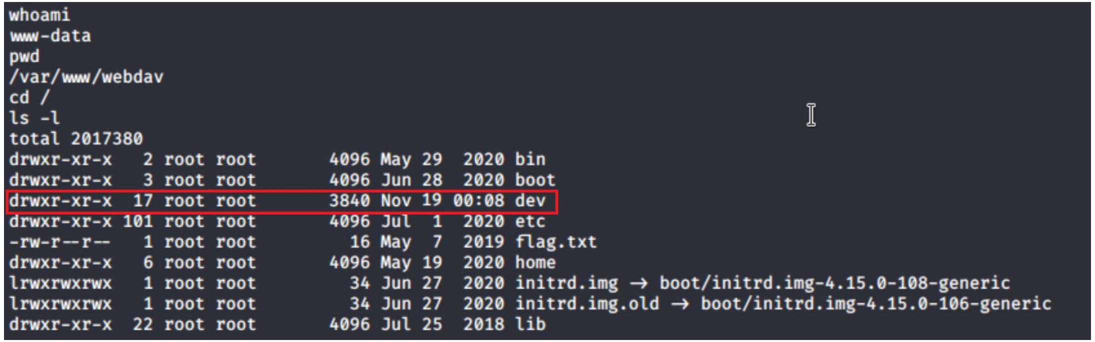
Warning, you are using the root account, you may harm your systen

passwd.dav

shell.php

02

Achievements
I can now execute commands on the system.

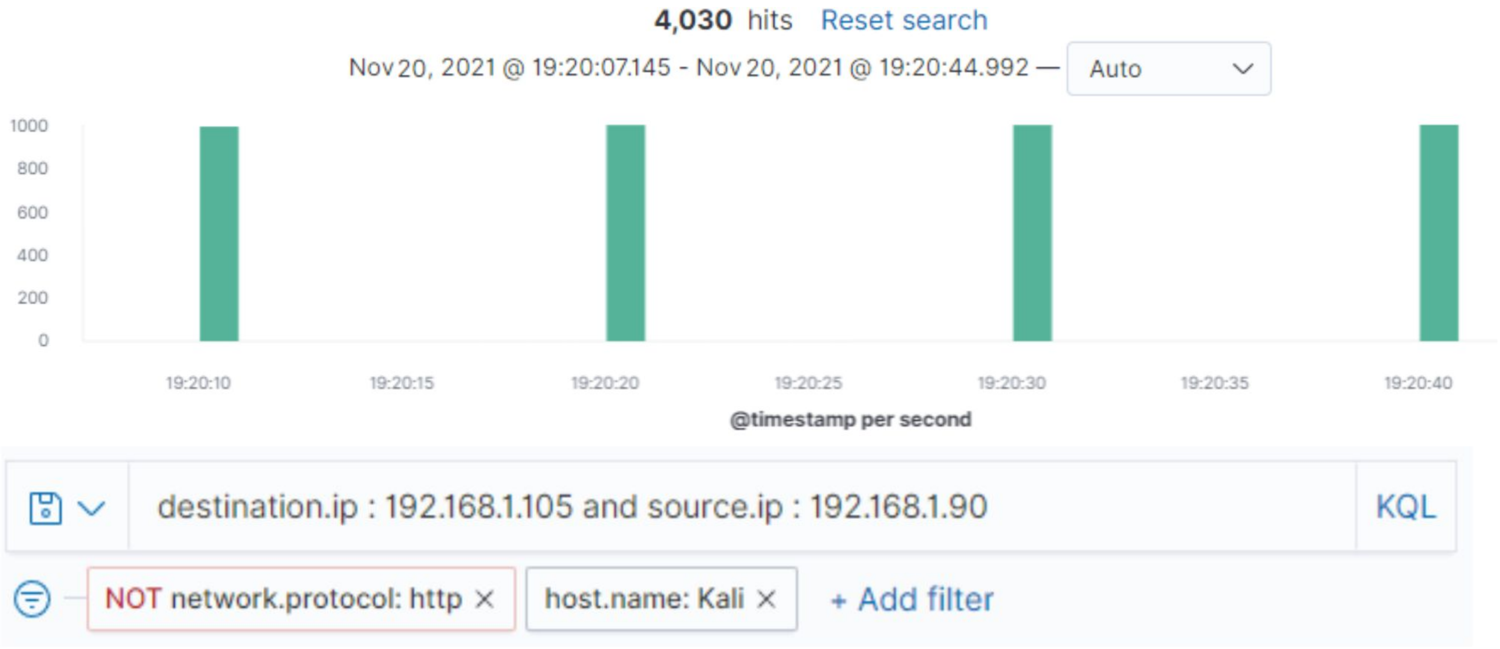


```
whoami
www-data
pwd
/var/www/webdav
cd /
ls -l
total 2017380
drwxr-xr-x   2 root root       4096 May 29  2020 bin
drwxr-xr-x   3 root root       4096 Jun 28  2020 boot
drwxr-xr-x  17 root root       3840 Nov 19 00:08 dev
drwxr-xr-x 101 root root       4096 Jul  1  2020 etc
-rw-r--r--   1 root root         16 May  7  2019 flag.txt
drwxr-xr-x   6 root root       4096 May 19  2020 home
lrwxrwxrwx   1 root root         34 Jun 27  2020 initrd.img → boot/initrd.img-4.15.0-108-generic
lrwxrwxrwx   1 root root         34 Jun 27  2020 initrd.img.old → boot/initrd.img-4.15.0-106-generic
drwxr-xr-x  22 root root       4096 Jul 25  2018 lib
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



4,030 hits

Nov 20, 2021 @ 19:20:07.145 - Nov 20, 2021 @ 19:20:44.992 — Auto

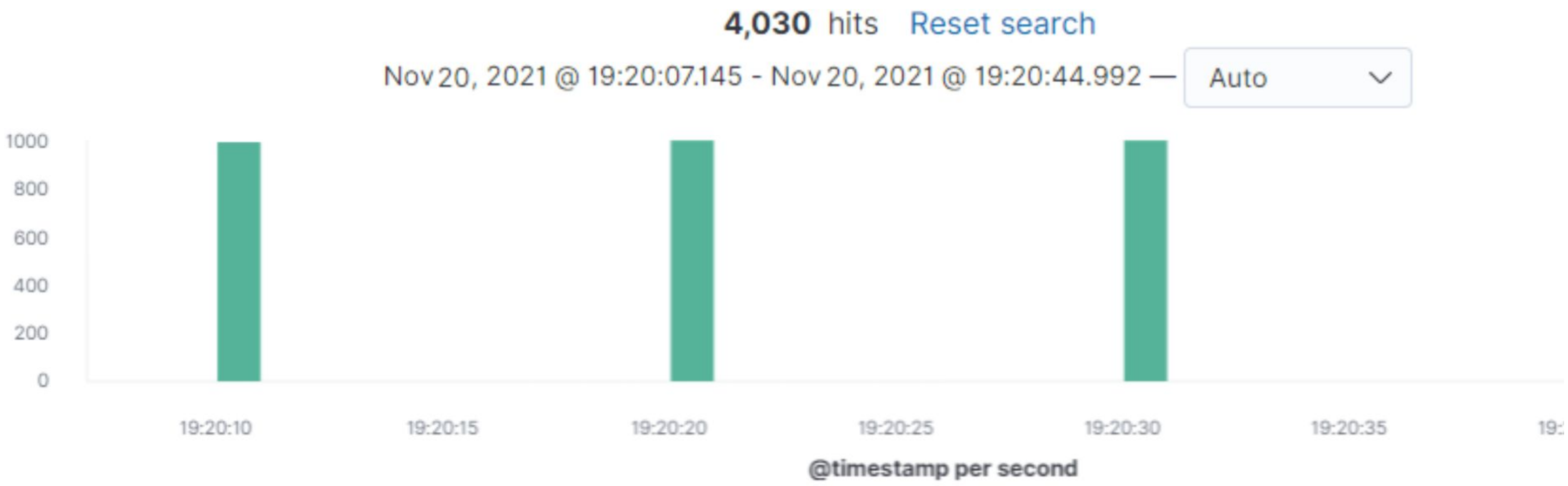
destination.ip : 192.168.1.105 and source.ip : 192.168.1.90

NOT network.protocol: http

host.name: Kali

- 4 scans occurred between 19:20:10-19:20:40
- 4030 packets were sent from 192.168.1.90
- Only common ports are scanned with a single packet (Syn)

Analysis: Finding the Request for the Hidden Directory

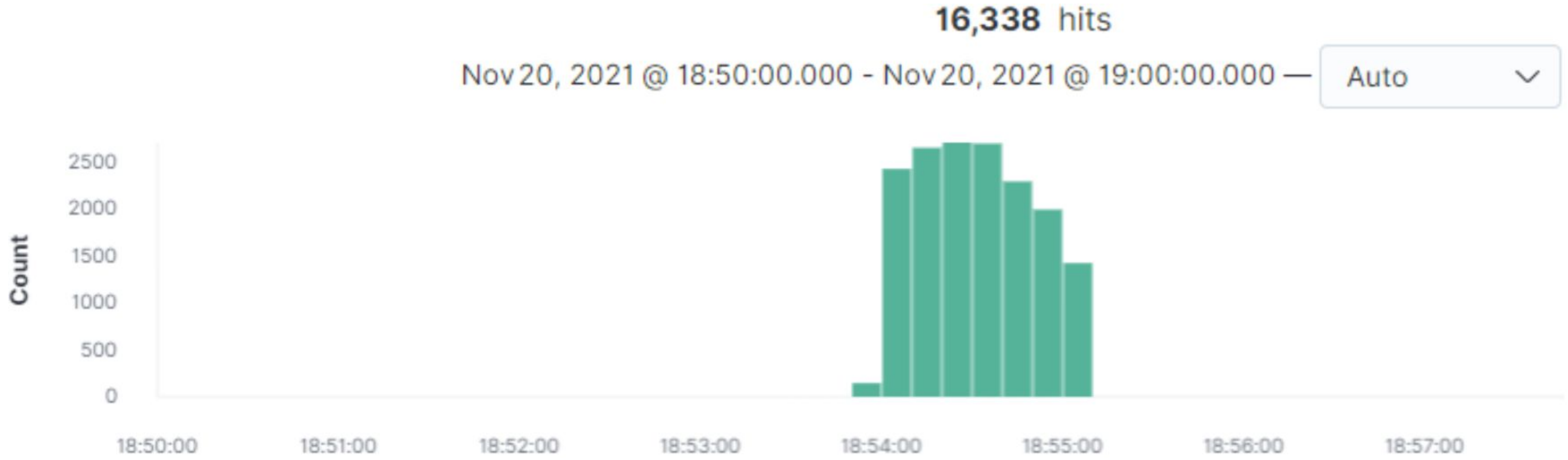


4,030 hits Reset search

Nov 20, 2021 @ 19:20:07.145 - Nov 20, 2021 @ 19:20:44.992 — Auto

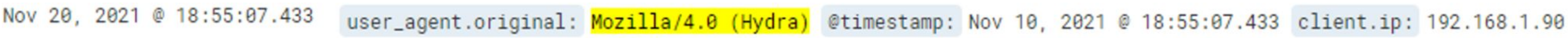
- Two requests were made between 18:55 and 19:05
- They requested **secret_folder/connect_to_corp_server.**
    - This folder contains ‘webdav’ instructions.

Analysis: Uncovering the Brute Force Attack



16,338 hits

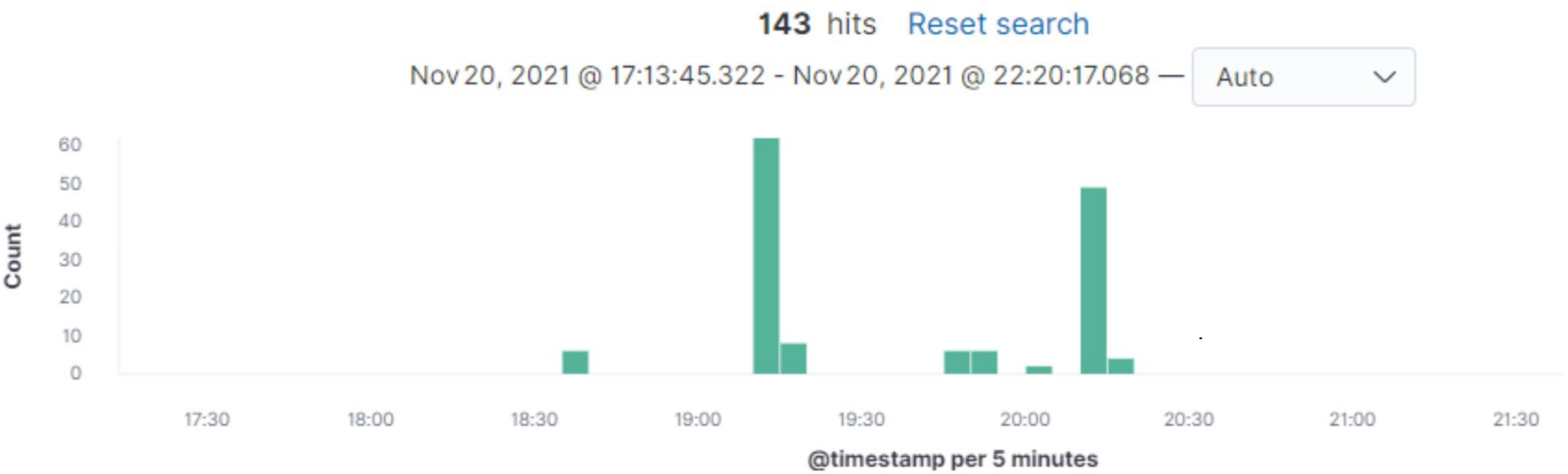
Nov 20, 2021 @ 18:50:00.000 - Nov 20, 2021 @ 19:00:00.000 — Auto



```
Nov 20, 2021 @ 18:55:07.433   user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Nov 10, 2021 @ 18:55:07.433 client.ip: 192.168.1.90
```

- 16,338 attempts before the password was discovered.

Analysis: Finding the WebDAV Connection



143 hits Reset search

Nov 20, 2021 @ 17:13:45.322 - Nov 20, 2021 @ 22:20:17.068 — Auto

Directory	/webdav	/webdav/passw.dav	/webdav/shell.php	/webdavv
Requests	95	34	13	1

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An alert that triggers when many scans occur over a short period of time

- 8 scans in 1 minute

System Hardening

- Firewall rules that only allow intranet access
- Differentiate between external and internal traffic

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Alert if ‘secret_folder’ has connection attempts from someone not on the whitelist

- The alarm should trigger immediately for sensitive data.

System Hardening

- Apache **mod_authz_host** that **Require ‘ip’** for file access to whitelisted OU’s.

Mitigation: Preventing Brute Force Attacks

Alarm

- Monitor the number of 401 errors occurring.

- I recommend that the alarm triggers after 50 errors in 1 minute as these attacks happen rapidly .

System Hardening

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

- Adding a Captcha, or any anti-bot measures.

- Adding a delay to password processing to slow down the process slightly; 1-3 second delay.

Mitigation: Detecting the WebDAV Connection

Alarm

- Alert when the number of connection attempts to the webDAV exceeds a threshold

- 5 connection attempts a minute

System Hardening

- Whitelist remote access IP’s

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Alert triggers whenever a source attempts to upload a PHP or other executable to the server
- This should trigger immediately

System Hardening

- Deny all PHP or other executable files from being uploaded

or

- Encrypt PHP or other executables on upload for examination; Lock them away so we can find more identifiers from the attacker

The End