# Capstone Engagement

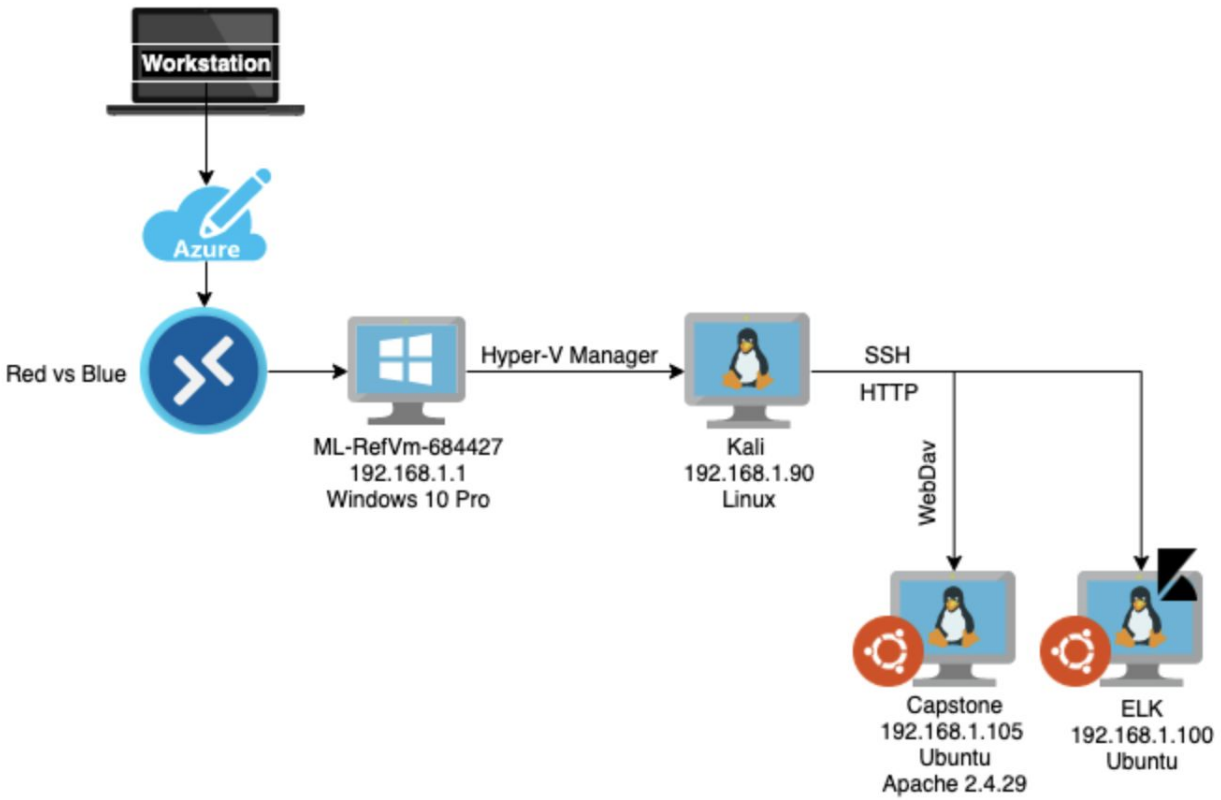
## Assessment, Analysis, and Hardening of a Vulnerable System

# Table of Contents

This document contains the following sections:

# Network Topology

# Network Topology




**Network**
Address Range:255
Netmask:255.255.255
Gateway:10.0.0.1

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

IPv4: 192.168.1.105
OS: Ubuntu Linux
Hostname:Capstone

IPv4: 192.168.1.100
OS: Ubuntu Linux
Hostname:ELK

IPv4: 192.168.1.90
OS: Kali Linux
Hostname:Kali

# Red Team

Security Assessment

# Recon: Describing the Target

## Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| ML-RefVm-684427 | 192.168.1.1 | Host |
| ELK | 192.168.1.100 | Elk server |
| Capstone | 192.168.1.105 | Target |
| Kali | 192.168.1.90 | Pen test machine |

# Vulnerability Assessment

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

| Vulnerability | Description | Impact |
|---|---|---|
| *HTTP* | *Unsecure protocol that handles communications between web servers and browsers.* | *Loss of data, browser hijacking, session hijacking, xxs, sensitive data exposure, etc.* |
| SSH | OpenSSH using port 22 that can be used to remotely log into a machine. | Access to data, loss of data, access to administrator, full machine access, etc. |
| WebDav | "WebDAV is an industry standard extension to the HTTP specification that adds a capability for authorized users to remotely add and manage the content of a web server." | Connect to a server and add an exploit for example, shell.php. |
| reverse_tcp | Server(target) initiates a connection to host(attacker). | Allows the attacker machine to listen for a connection to the target to take control of the device and pass commands. |

# Exploitation: HTTP

01

**Tools & Processes**

- Nmap service and version scan on Target's IP address.
- Mozilla Firefox address bar, input Target's IP address.

02

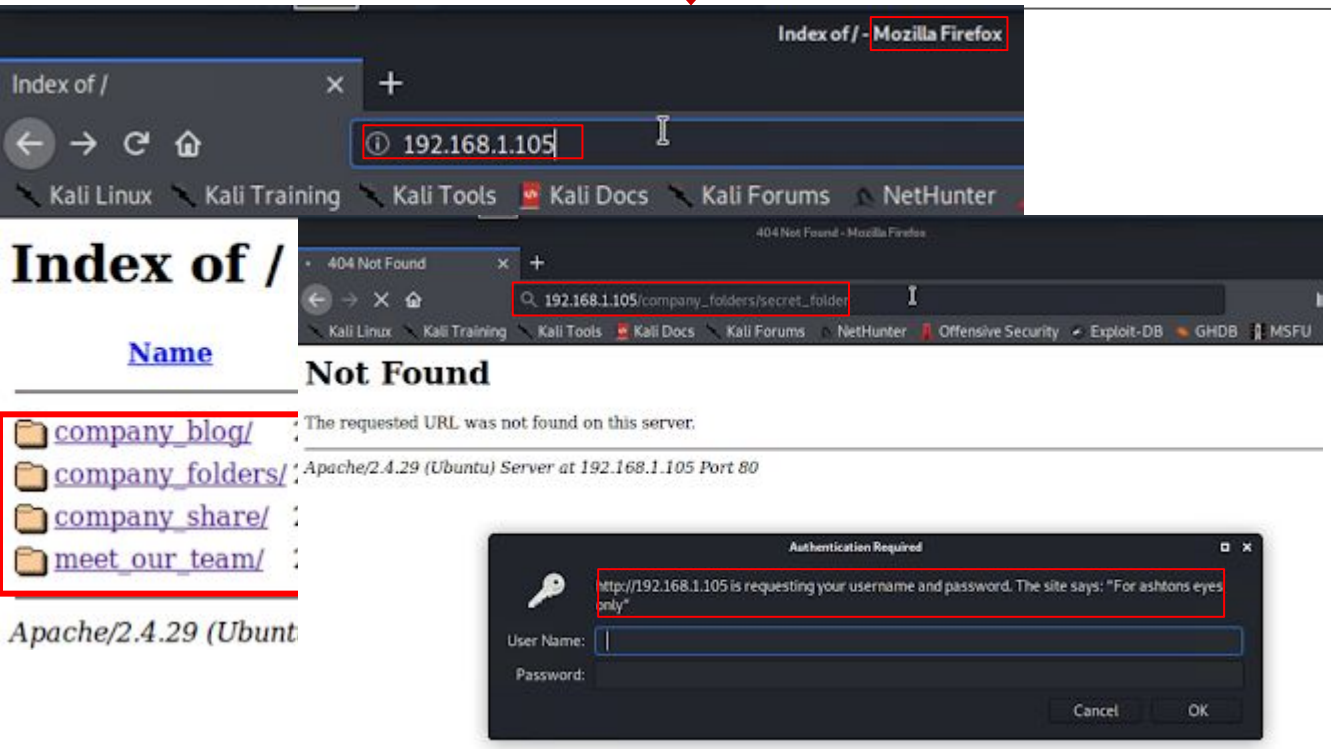
**Achievements**

- Gained access to the Target's directories.
  - Reviewed each file
- Located a hidden directory.
- Gained access to multiple user credentials using a brute force attack.

03

```
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) a
Nmap scan report for 192.168.1.105
Host is up (0.00070s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
```

# Exploitation: HTTP 03 Continued...




User Name: **ashton**
Password: **leopoldo**

- Hidden directory,

**/company_folders/secret_folder**

- Terminal command:

**hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder**

Syntax: hydra -l username -P wordlist -s port -f -vV target_ip_address http-get secret_directory_path

# Exploitation: HTTP 03 Continued...

Index of /company_folders/secret_fo

Index of /company_folders/s

192.168.1.105/company_folders/secret_folder/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHun

## Index of /company_folders/secret

| 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*

Mozilla Firefox

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

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

https://crackstation.net

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Expl Show history MSFU

CrackStation

Defuse.ca

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

d7dad0a5cd7c8376eeb50d69b3ccd352

I'm not a robot reCAPTCHA

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.

User Name: **ryan**
Password: **linux4u**

# Exploitation: SSH

01

**Tools & Processes**

- Nmap service and version scan on Target's IP address.
  - OpenSSH
- HTTP exploit provided me with usernames and passwords

02

**Achievements**

- Successfully remotely logged into Target.

03

- Command Line::

**nmap -sV 192.168.1.105**

**ssh ashton@192.168.1.105**
*ashton@192.168.1.105's password:* **leopoldo**
*ashton@server:*

**ssh ryan@192.168.1.105**
*ryan@192.168.1.105's password:* **linux4u**
*ryan@server:*

# Exploitation: WebDav

01

**Tools & Processes**

- HTTP exploit provided me with usernames and passwords
- Network-File Manager

02

**Achievements**

- Successfully connected to the server via WebDav and planted a reverse shell into the directory.

03

- Network-File Manager address bar input:

**dav://192.168.1.105/webdav**

- Entered credentials,

Username: **ryan**
Password: **linux4u**

# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

**20,123** hits

Jan 14, 2021 @ 02:00:00.000 - Jan 14, 2021 @ 02:30:00.000 — Auto

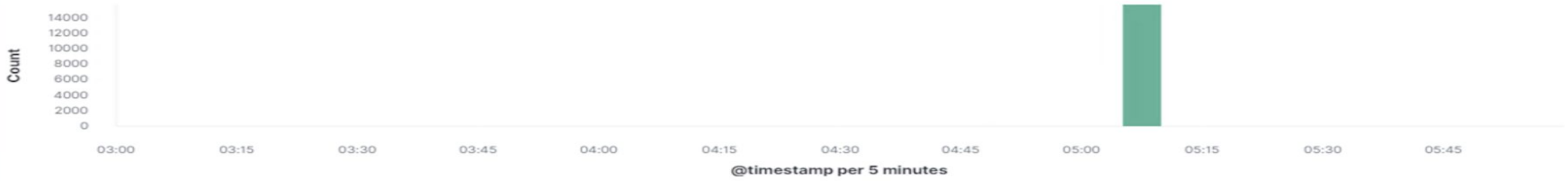

| Time | source.ip | source.port | destination.ip | destination.port |
|---|---|---|---|---|
| Jan 14, 2021 @ 02:30:00.000 | 192.168.1.90 | 52202 | 192.168.1.105 | 22 |
| Jan 14, 2021 @ 02:29:50.009 | 192.168.1.90 | 34814 | 192.168.1.100 | 9200 |
| Jan 14, 2021 @ 02:29:50.009 | 192.168.1.90 | 52202 | 192.168.1.105 | 22 |
| Jan 14, 2021 @ 02:29:50.000 | 192.168.1.90 | 52202 | 192.168.1.105 | 22 |
| Jan 14, 2021 @ 02:29:40.009 | 192.168.1.90 | 55002 | 192.168.1.105 | 80 |
| Jan 14, 2021 @ 02:29:40.009 | 192.168.1.90 | 55004 | 192.168.1.105 | 80 |
| Jan 14, 2021 @ 02:29:40.009 | 192.168.1.90 | 55006 | 192.168.1.105 | 80 |
| Jan 14, 2021 @ 02:29:40.009 | 192.168.1.90 | 34814 | 192.168.1.100 | 9200 |
| Jan 14, 2021 @ 02:29:40.009 | 192.168.1.90 | 52202 | 192.168.1.105 | 22 |
| Jan 14, 2021 @ 02:29:40.000 | 192.168.1.90 | 52202 | 192.168.1.105 | 22 |
| Jan 14, 2021 @ 02:29:40.000 | 192.168.1.90 | 55002 | 192.168.1.105 | 80 |
| Jan 14, 2021 @ 02:29:40.000 | 192.168.1.90 | 55004 | 192.168.1.105 | 80 |
| Jan 14, 2021 @ 02:29:40.000 | 192.168.1.90 | 55006 | 192.168.1.105 | 80 |
| Jan 14, 2021 @ 02:29:30.009 | 192.168.1.90 | 55002 | 192.168.1.105 | 80 |

- What time did the port scan occur? 02:00
- How many packets were sent, and from which IP?
  20,123 hits
- What indicates that this was a port scan? Source ip was hitting multiple ports in a short time frame

# Analysis: Finding the Request for the Hidden Directory

**15,687** hits

Jan 16, 2021 @ 03:00:00.000 - Jan 16, 2021 @ 06:00:00.000 — Auto



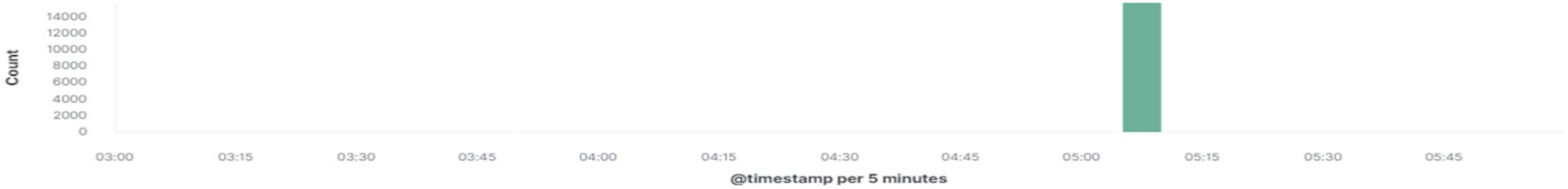

| Time | _source |
|---|---|
| > Jan 16, 2021 @ 05:13:49.237 | url.domain: 192.168.1.105 url.path: /company_folders/secret_folder @timestamp: Jan 16, 2021 @ 05:13:49.237 http.request.bytes: 385B http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 338B http.response.headers.content-length: 338 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: moved permanently http.response.status_code: 301 http.response.bytes: 626B http.version: 1.1 event.duration: 0.6 event.start: Jan 16, 2021 @ 05:13:49.237 event.end: Jan 16, 2021 @ 05:13:49.237 event.kind: event |
| > Jan 16, 2021 @ 05:13:49.212 | url.path: /company_folders/secret_folder url.domain: 192.168.1.105 @timestamp: Jan 16, 2021 @ 05:13:49.212 type: http method: get query: GET /company_folders/secret_folder host.name: Kali user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: daa55f0c-419a-4569-be13-df2a72fedc50 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali http.request.method: get http.request.bytes: 385B http.request.headers.content-length: 0 http.response.status_phrase: moved |
| > Jan 16, 2021 @ 05:06:35.480 | url.domain: 192.168.1.105 url.path: /company_folders/secret_folder @timestamp: Jan 16, 2021 @ 05:06:35.480 user_agent.original: Mozilla/4.0 (Hydra) query: GET /company_folders/secret_folder network.community_id: 1:ffEP8yAfokOtRUTdQBMV2P4PQfQ= network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound url.full: http://192.168.1.105/company_folders/secret_folder |

- What time did the request occur? 03:00
- How many requests were made? 15, 687 hits
- Which files were requested? /company_folders/secret_folder
- What did they contain? User ryan's password hash and instructions on how to connect to WebDav

# Analysis: Uncovering the Brute Force Attack

**15,683** hits

Jan 16, 2021 @ 03:00:00.000 - Jan 16, 2021 @ 06:00:00.000 — Auto



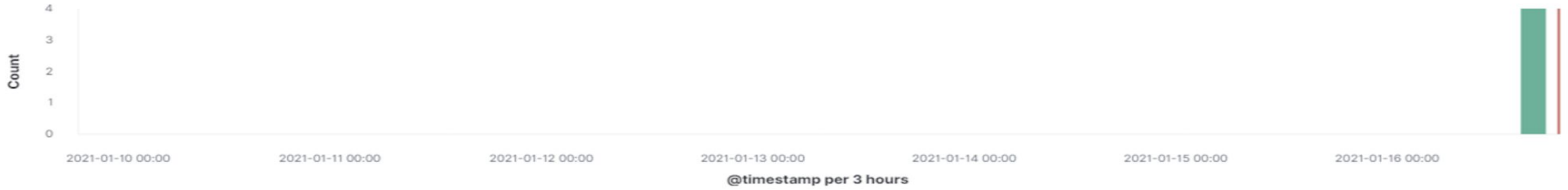

| Time | _source |
|---|---|
| > Jan 16, 2021 @ 05:06:35.480 | user_agent.original: Mozilla/4.0 (Hydra) url.domain: 192.168.1.105 @timestamp: Jan 16, 2021 @ 05:06:35.480 query: GET /company_folders/secret_folder network.community_id: 1:ffEP8yAfokOtRUTdQBMV2P4PQfQ= network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http method: get type: http server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B agent.hostname: server1 agent.id: de2238f6-73be-44db-906f- |
| > Jan 16, 2021 @ 05:06:35.470 | url.domain: 192.168.1.105 user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 16, 2021 @ 05:06:35.470 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 159B type: http query: GET /company_folders/secret_folder |
| > Jan 16, 2021 @ 05:06:35.460 | url.domain: 192.168.1.105 user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 16, 2021 @ 05:06:35.460 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http destination.bytes: 698B destination.ip: 192.168.1.105 destination.port: 80 server.ip: 192.168.1.105 server.port: 80 |

- How many requests were made in the attack? 15, 683 hits
- How many requests had been made before the attacker discovered the password? 15, 681

# Analysis: Finding the WebDAV Connection

**4** hits

Jan 9, 2021 @ 19:22:57.513 - Jan 16, 2021 @ 19:22:57.514 — Auto




| Time | _source |
|---|---|
| Jan 16, 2021 @ 17:36:17.114 | url.domain: 192.168.1.105 query: GET /webdav/passwd.dav @timestamp: Jan 16, 2021 @ 17:36:17.114 url.full: http://192.168.1.105/webdav/passwd.dav url.scheme: http url.path: /webdav/passwd.dav server.bytes: 301B server.ip: 192.168.1.105 server.port: 80 network.protocol: http network.direction: inbound network.community_id: 1:Oj5xHb80azAUYNzGVOLKQJfCqvY= network.bytes: 709B network.type: ipv4 network.transport: tcp agent.ephemeral_id: 09b64d0f-931f-426e-830e-28db4c81d905 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat host.name: server1 ecs.version: 1.5.0 client.bytes: 408B |
| Jan 16, 2021 @ 17:36:16.981 | url.domain: 192.168.1.105 query: GET /webdav/passwd.dav @timestamp: Jan 16, 2021 @ 17:36:16.981 status: OK network.community_id: 1:Oj5xHb80azAUYNzGVOLKQJfCqvY= network.bytes: 709B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound method: get url.scheme: http url.path: /webdav/passwd.dav url.full: http://192.168.1.105/webdav/passwd.dav source.ip: 192.168.1.90 source.port: 43342 source.bytes: 408B destination.port: 80 destination.bytes: 301B destination.ip: 192.168.1.105 ecs.version: 1.5.0 host.name: Kali server.ip: 192.168.1.105 server.port: 80 server.bytes: 301B type: http event.end: Jan 16, 2021 @ |
| Jan 16, 2021 @ 17:34:53.308 | url.domain: 192.168.1.105 query: GET /webdav/shell.php @timestamp: Jan 16, 2021 @ 17:34:53.308 error.message: Unmatched request http.version: 1.1 http.request.bytes: 209B http.request.headers.content-length: 0 http.request.method: get event.category: network_traffic event.dataset: http event.start: Jan 16, 2021 @ 17:34:53.308 event.kind: event type: http network.transport: tcp network.protocol: http |

get

- How many requests were made to this directory? 4 hits
- Which files were requested? shell.php

# 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?

- Create a rule to alert when there are consecutive ports scans or ping request.

What threshold would you set to activate this alarm?

- 10 port scans in one minute or 100 consecutive ping request.

## System Hardening

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

- Install firewall
- TCP Wrappers
- Uncover Holes in the network

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

- Block pings and ICMP requests
- Add a rich rule to block the servers IP addresses or domains
- Run a port scan and close unused ports.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

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

- Create an alert when Hidden Directory is requested from a non whitelisted IP

What threshold would you set to activate this alarm?

- 5

## System Hardening

- Create a firewall rule to only allow IP addresses 192.168.1.1 and 192.168.1.105 to access port 80
- Use port 443 instead of 80
- Remove all existence of a hidden directory from the website

# Mitigation: Preventing Brute Force Attacks

## Alarm

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

- Create a rule to detect Hydra

What threshold would you set to activate this alarm?

- 3 failed login attempts

## System Hardening

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

- Enforce the use of strong passwords
- Use multifactor
- Lockout policy

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

- Lock accounts after several failed login attempts and then unlock it as the administrator
- Use multiple factors to authenticate identity and grant access to accounts
- force users to define long and complex passwords. You should also enforce periodical password changes

# Mitigation: Detecting the WebDAV Connection

## Alarm

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

- Create an when unauthorized IP address attempts to access the tool

What threshold would you set to activate this alarm?

- 5

## System Hardening

- Set up alert source.ip : (not <whitelisted IP> or <whitelisted IP>)
- If you do not use this extension, you should disable it
- Patch/Repair the vulnerability

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

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

- Create a alert for http.request.method : “put” and source : (not 192.168.1.105 or 192.168.1.1)

What threshold would you set to activate this alarm?

- 5

## System Hardening

- “lock down outgoing connectivity to allow only specific remote IP addresses and ports for the required services”

# the End