# Capstone Engagement

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

By John Sowers

# Table of Contents

This document contains the following sections:

01 **Network Topology**

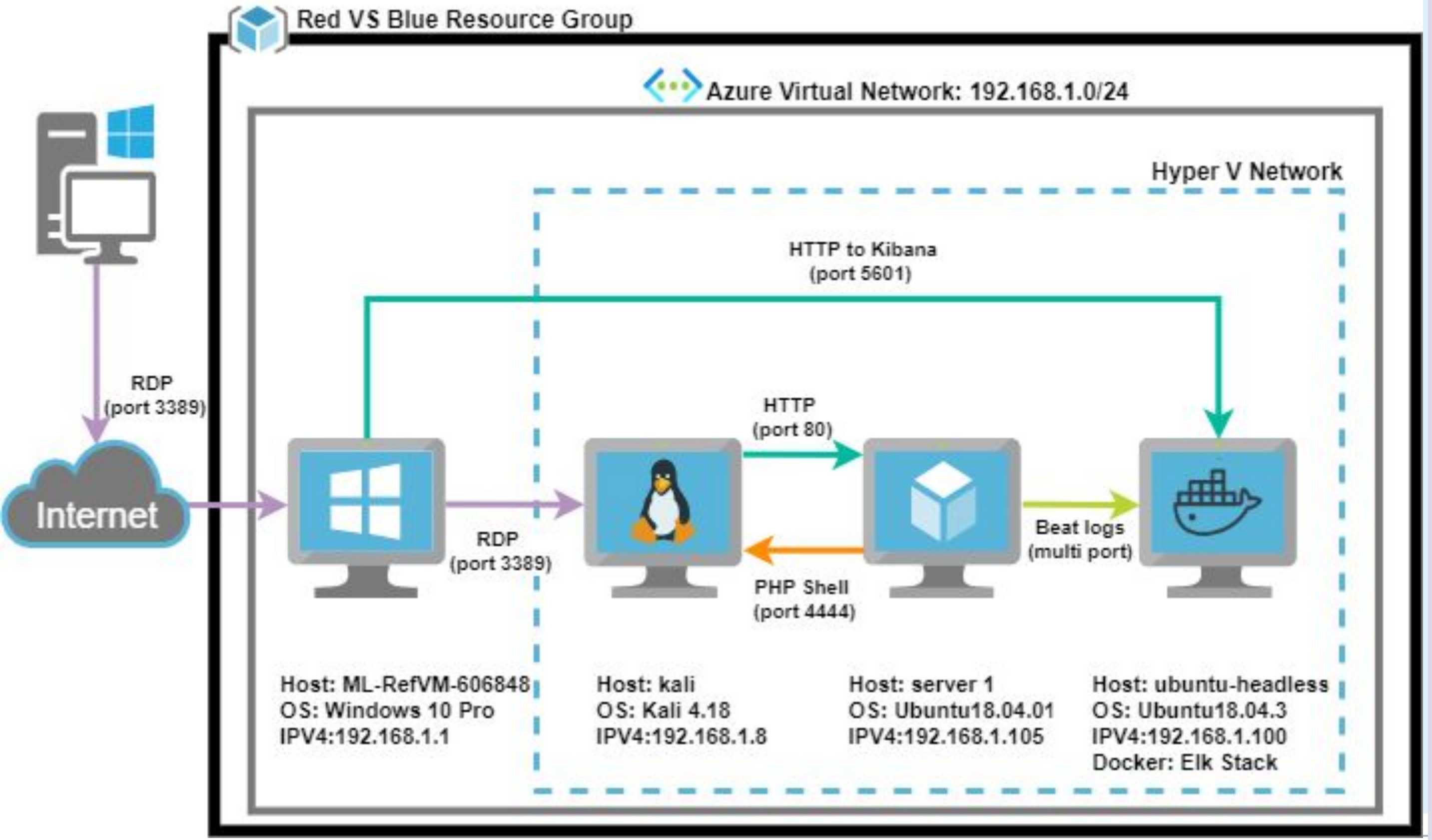
02 **Red Team**: Security Assessment

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: 192.168.1.1
OS: Windows 10 Pro
Hostname: ML-RefVM-606848

IPv4: 192.168.1.100
OS: Ubuntu 18.04.3
Hostname: ubuntu-headless (ELK)

IPv4: 192.168.1.05
OS: Ubuntu 18.04.01
Hostname: server1 (Capstone)

IPv4:192.168.1.8
OS: Kali 4.18.0
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-606848 | 192.168.1.1 | **Host server**<br>Windows Hyper-V Manager Virtual Server (hosts 3 machines below)<br>- Network Gateway<br>- RDP interface |
| ubuntu-headless | 192.168.1.100 | **Log server - ELK stack**<br>Aggregate system logs for analysis |
| server1 | 192.168.1.105 | **Target web server**<br>Capstone Corporate server being accessed and tested. |
| Kali | 192.168.1.8 | **Attacker machine**<br>Used to find vulnerabilities. |

# Vulnerability Assessment

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

| Vulnerability | Description | Impact |
|---|---|---|
| Brute force: Hydra over HTTP-GET | Finds passwords when provided with an IP address, user name, and word list | A brute force vulnerability allows attackers to gain access to employee only information |
| Meterpreter shell: Reverse TCP via PHP script | Run a php script through the browser to gain meterpreter access to a compromised system | Allow an attacker to explore the target machine and execute code |
| Employee security practices | Poor knowledge or adherence of security best practices by employees | Exposed sensitive information and login requirements leading to exploitation of the server |

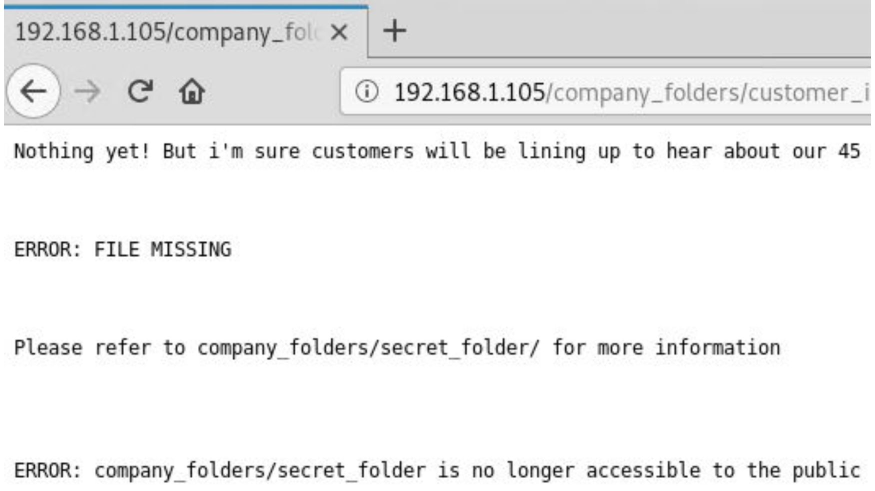
# Exploitation: Brute Force: Hydra over HTTP-GET

**Tools & Processes**

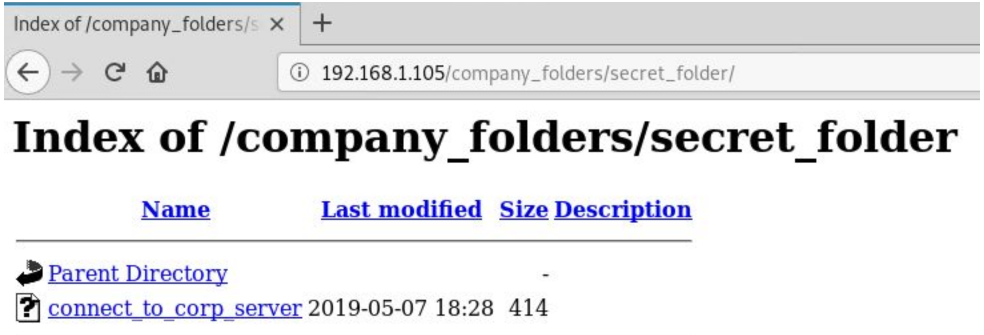
Exploring the web page revealed the existence of “/secret_folder”. Using the employee names as usernames Hydra was able to guess a password which allowed the attacker to login to the web page as an employee.

**Achievements**

This granted access to the secret_folder and all of its content, as well as other sensitive information about customers customer


192.168.1.105/company_fol
192.168.1.105/company_folders/customer_i

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45


ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information



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


Index of /company_folders/s
192.168.1.105/company_folders/secret_folder/

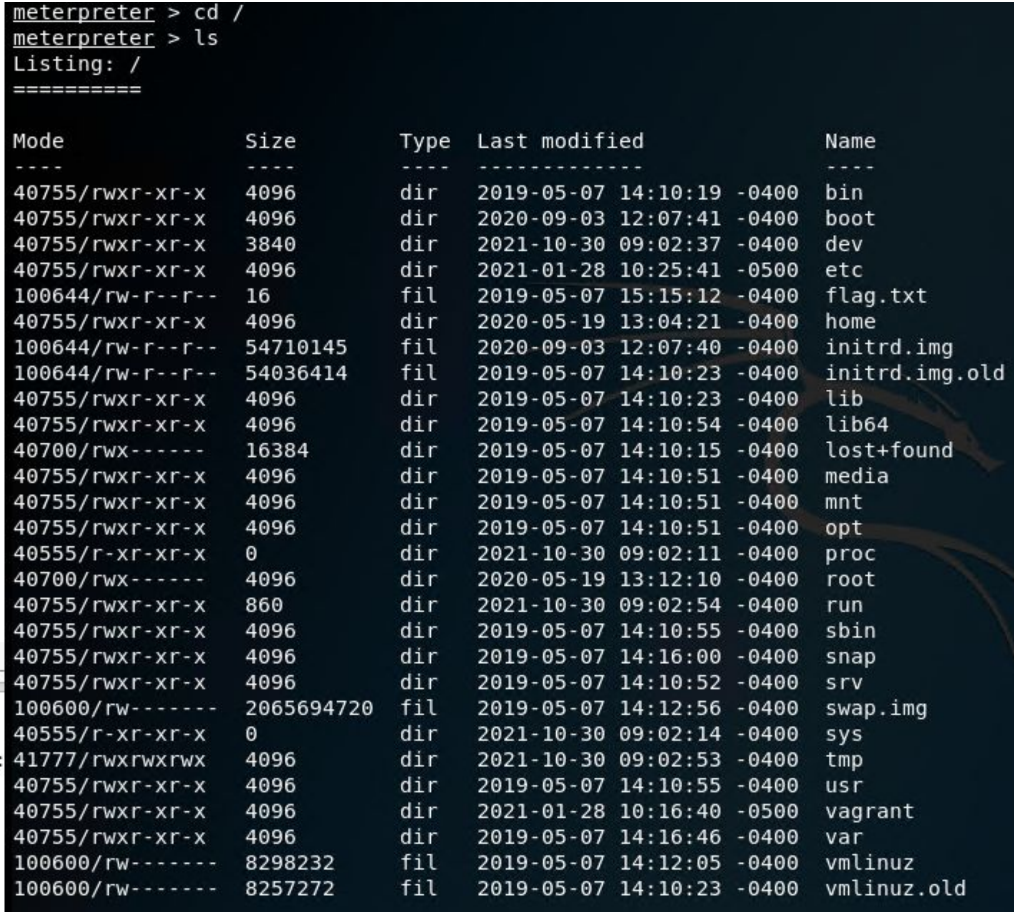
## Index of /company_folders/secret_folder

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| connect_to_corp_server | 2019-05-07 18:28 | 414 | |

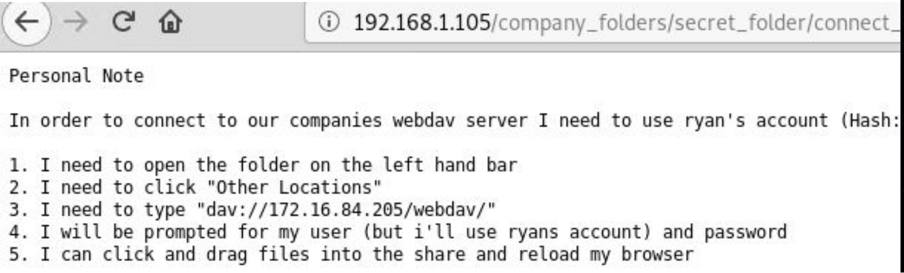
# Exploitation: Meterpreter shell: Reverse TCP via PHP script

**Tools & Processes**
After gaining access to the secret_folder instructions were given to log onto a Webdav server. From there the attacker uploaded a php script that would enable a meterpreter shell to interact with the web server

**Achievements**
This gave the attacker the ability to explore the web server’s entire folder structure and download sensitive files.



```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:19 -0400  bin
40755/rwxr-xr-x   4096        dir   2020-09-03 12:07:41 -0400  boot
40755/rwxr-xr-x   3840        dir   2021-10-30 09:02:37 -0400  dev
40755/rwxr-xr-x   4096        dir   2021-01-28 10:25:41 -0500  etc
100644/rw-r--r--  16          fil   2019-05-07 15:15:12 -0400  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 13:04:21 -0400  home
100644/rw-r--r--  54710145    fil   2020-09-03 12:07:40 -0400  initrd.img
100644/rw-r--r--  54036414    fil   2019-05-07 14:10:23 -0400  initrd.img.old
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:23 -0400  lib
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:54 -0400  lib64
40700/rwx------   16384       dir   2019-05-07 14:10:15 -0400  lost+found
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  media
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  mnt
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  opt
40555/r-xr-xr-x   0           dir   2021-10-30 09:02:11 -0400  proc
40700/rwx------   4096        dir   2020-05-19 13:12:10 -0400  root
40755/rwxr-xr-x   860         dir   2021-10-30 09:02:54 -0400  run
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:55 -0400  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 14:16:00 -0400  snap
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:52 -0400  srv
100600/rw-------  2065694720  fil   2019-05-07 14:12:56 -0400  swap.img
40555/r-xr-xr-x   0           dir   2021-10-30 09:02:14 -0400  sys
41777/rwxrwxrwx   4096        dir   2021-10-30 09:02:53 -0400  tmp
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:55 -0400  usr
40755/rwxr-xr-x   4096        dir   2021-01-28 10:16:40 -0500  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 14:16:46 -0400  var
100600/rw-------  8298232     fil   2019-05-07 14:12:05 -0400  vmlinuz
100600/rw-------  8257272     fil   2019-05-07 14:10:23 -0400  vmlinuz.old
```



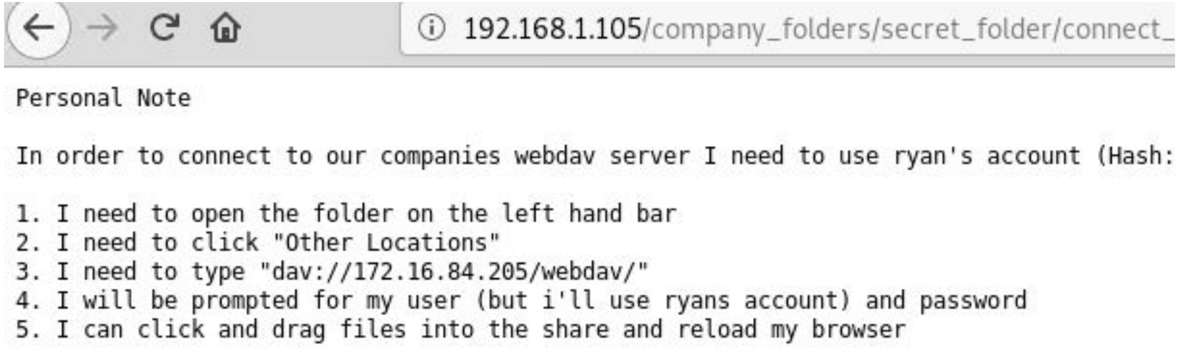
192.168.1.105/company_folders/secret_folder/connect_

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:

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: Employee security practices

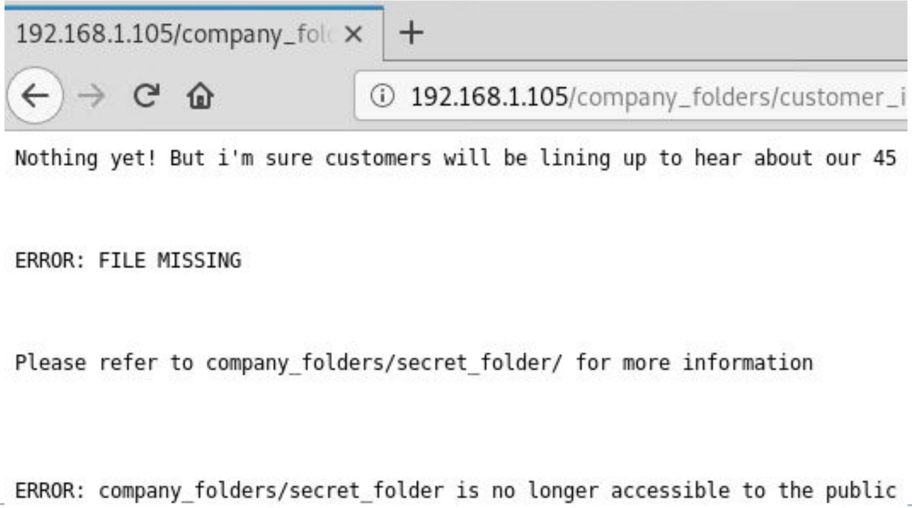
**Tools & Processes**
The information left by employee's poor security practices were key in compromising this system.. Leaving login instructions, hashes, and references to hidden folders on the web server made exploiting this machine quick and relatively easy.

**Achievements**
The combination of all the information exposed by employees led to a full compromise of the web server.



192.168.1.105/company_folders/secret_folder/connect_

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:

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
```



192.168.1.105/company_fol

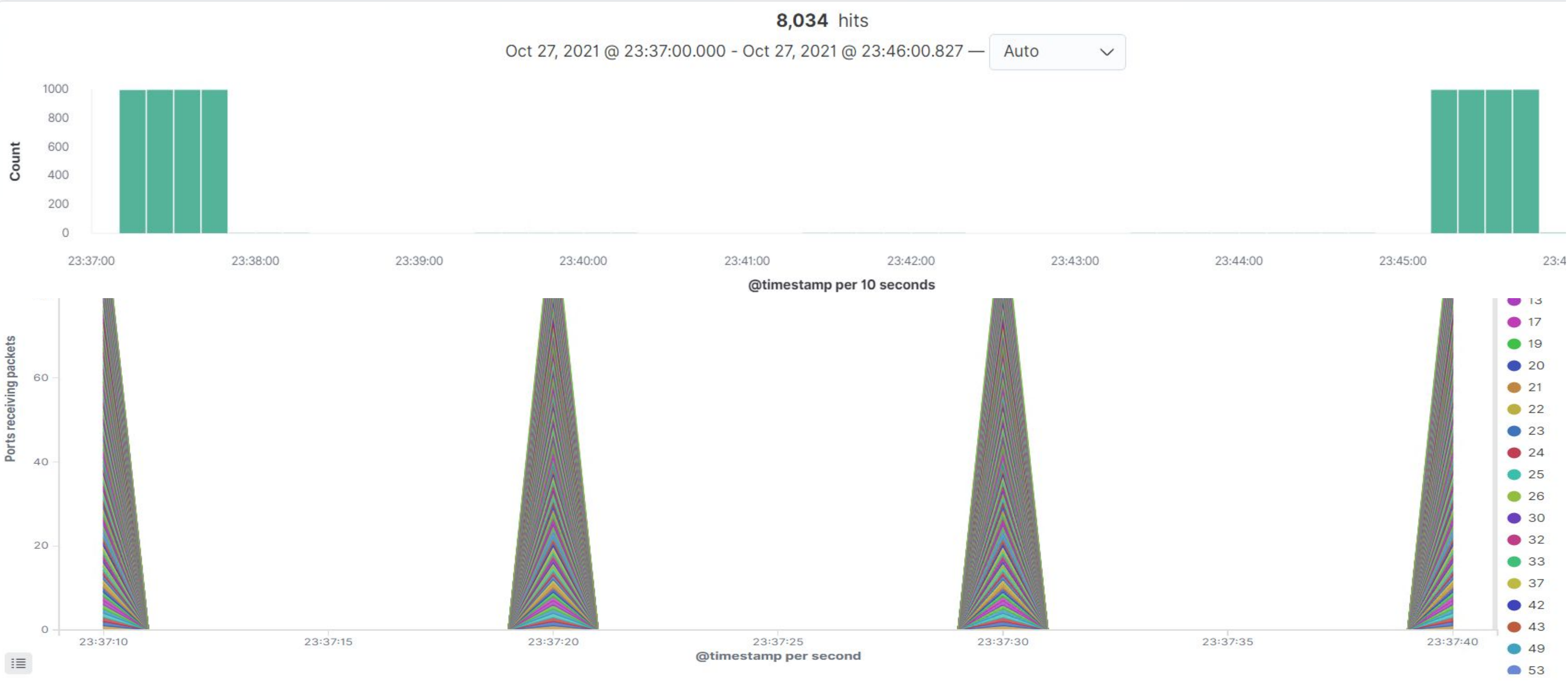
192.168.1.105/company_folders/customer_i

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45


ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


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

# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan



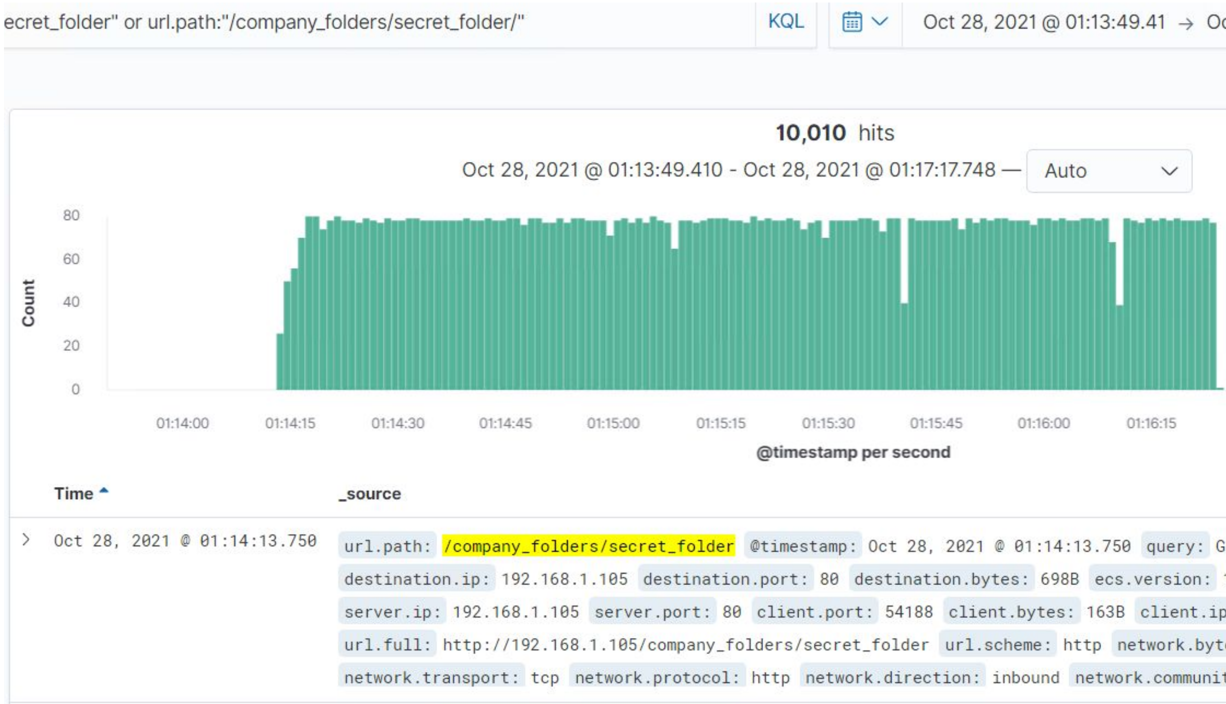
**8,034** hits

Oct 27, 2021 @ 23:37:00.000 - Oct 27, 2021 @ 23:46:00.827 — Auto

- Two port scans can be seen around 23:37 and 23:45.
- Each scan consisted of about 4000 packets all coming from the IP address 192.168.1.8

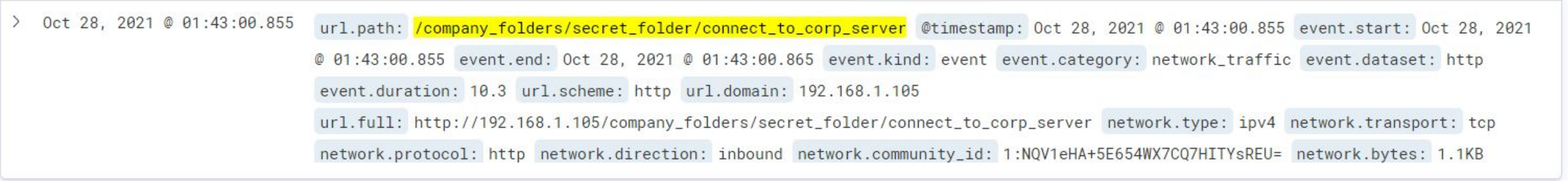
# Analysis: Finding the Request for the Hidden Directory

- The first request to the hidden directory was made at 01:14 on October 28, 2021. A file was not actually requested until 01:43.
- After the initial request thousands of attempts were made to access the directory.
- After the attacker obtained the correct login credentials the only file they accessed was connect_to_corp_server
- This file contained a personal reminder of how to login to the Webdav server



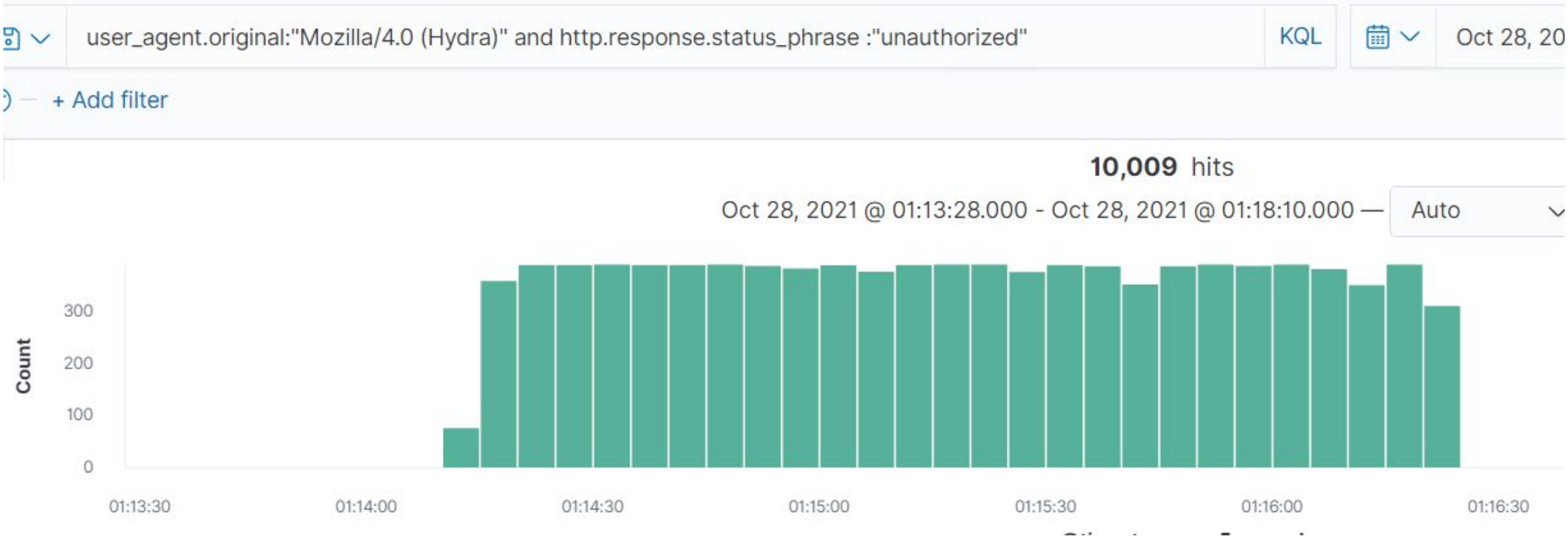
ecret_folder" or url.path:"/company_folders/secret_folder/"

```
Time ▲                        _source
> Oct 28, 2021 @ 01:14:13.750  url.path: /company_folders/secret_folder @timestamp: Oct 28, 2021 @ 01:14:13.750 query: G
                               destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B ecs.version:
                               server.ip: 192.168.1.105 server.port: 80 client.port: 54188 client.bytes: 163B client.ip
                               url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http network.byt
                               network.transport: tcp network.protocol: http network.direction: inbound network.communit
```



```
> Oct 28, 2021 @ 01:43:00.855  url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Oct 28, 2021 @ 01:43:00.855 event.start: Oct 28, 2021
                               @ 01:43:00.855 event.end: Oct 28, 2021 @ 01:43:00.865 event.kind: event event.category: network_traffic event.dataset: http
                               event.duration: 10.3 url.scheme: http url.domain: 192.168.1.105
                               url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server network.type: ipv4 network.transport: tcp
                               network.protocol: http network.direction: inbound network.community_id: 1:NQV1eHA+5E654WX7CQ7HITYsREU= network.bytes: 1.1KB
```

# Analysis: Uncovering the Brute Force Attack



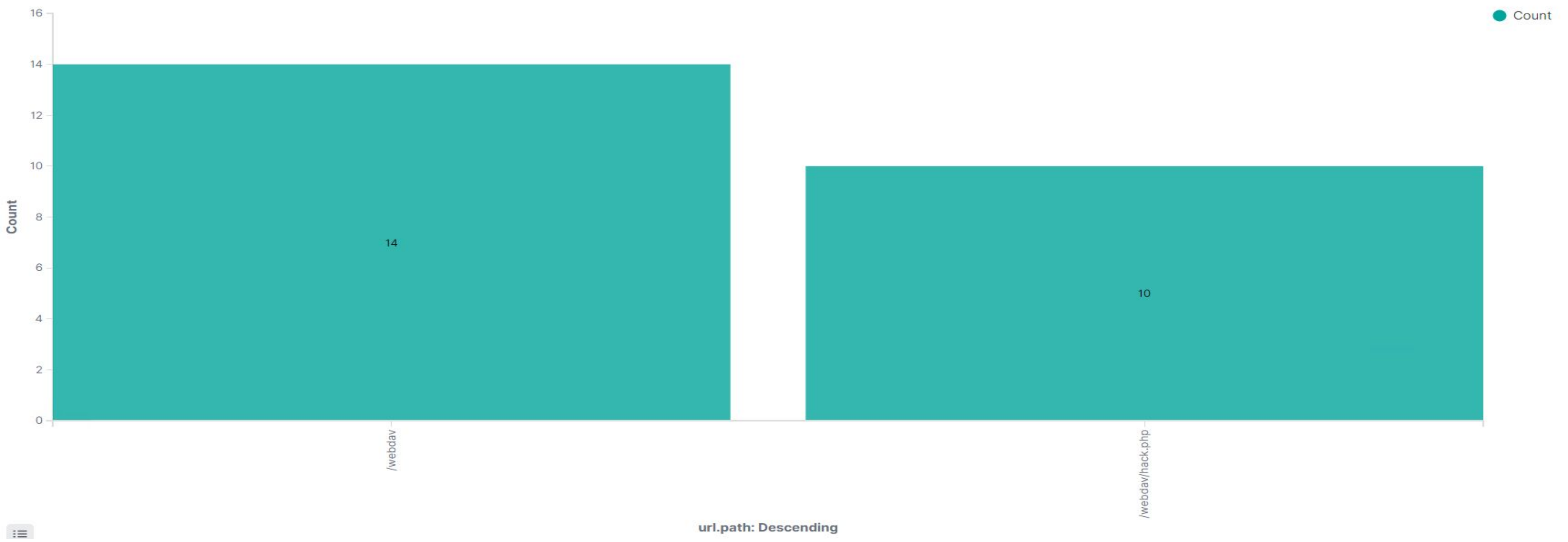
user_agent.original:"Mozilla/4.0 (Hydra)" and http.response.status_phrase :"unauthorized"

**10,009** hits

Oct 28, 2021 @ 01:13:28.000 - Oct 28, 2021 @ 01:18:10.000 — Auto

- Noting the user agent that was making a majority of the requests to the “secret_folder” we can filter by request made from Mozilla/4.0 (Hydra) and see how many failed or “unauthorized” status were returned
- There were 10,009 failed attempts to access the “secret_folder”

# Analysis: Finding the WebDAV Connection



- There were 24 total requests made to /webdav
- The only file requested from /webdav was “hack.php”, which was requested 10 times
- This indicates this file was used to run code within the web server from a browser

# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

An alarm for a port scan could be activated when:

- Numerous TCP port requests are sent from a single IP address
- Requests occur within a small time frame, less than 30 seconds apart

I would set the threshold of 10 scans to any port from a single IP address within 1 second to avoid any false positives.

## System Hardening

In this scenario it might be best configure the firewall to "block all" by default and whitelist only ports that are meant to be used. This could include ports 80 (http/webdav), 443 (https), 22 (ssh, assuming it is configured properly).

If the correct firewall settings are applied an attacker will not be able to tell if the ports are simply being blocked, or closed which could force them to use more time or a more conspicuous type of scan for reconnaissance.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

An alarm could be set to trigger on:

- **url.path : “/company_folders/secret_folder”**
- **and http.response.status_phrase : “unauthorized”**
- **or http.response.status_code : “401”**

Since I cannot determine a baseline for login attempts (I do not have fake logs including legitimate login attempts) I would set the threshold to 6-7 failed login attempts before sending an alarm.

## System Hardening

One way to prevent unauthorized logins to the hidden directory would be to only allow logins through a VPN or whitelisted IP address.

Another method would be to implement more rigorous password requirements such as:

- Maximum password age
- Minimum password complexity
- Deny password reuse
- Multifactor Authentication

Finally the secret_file could be removed completely from the public server and only be accessible from the local network.

# Mitigation: Preventing Brute Force Attacks

## Alarm

An alarm can be triggered when an event matches the following:

- **http.response.status_phrase : ”unauthorized”**
- **or http.response.status_code : “401”**

This alert does not need a specific url.path like we have for the secret_folder. This distinction will be important for determining the severity of the threat.

Without a baseline for login failures I would start at triggering the alert with 10 failures in an hour and adjust from there.

## System Hardening

One method would be to implement more rigorous password as with blocking requests for the hidden directory with the following rules:

- Maximum password age
- Minimum password complexity
- Deny password reuse
- Multifactor Authentication

Additionally IP address that are triggering the alarm could be temporarily blocked to prevent them from continuing an attack.

# Mitigation: Detecting the WebDAV Connection

## Alarm

An alarm for detecting WebDAV Connections could be quite simple with only the following required:

- **url.path=/webdav/***

The threshold is what could make this alarm more complicated. You could set the alarm to look for non-whitelisted IP addresses with a rule similar to:

- **not source.ip:”192.169.1.100”**

This way authorized access will not set of the alarm.

## System Hardening

On the host system it would also be beneficial to implement an IP whitelist to ensure only authorized users can access WebDav.

As with the “secret_folder” if it must be accessible from the internet restricting WAN access to VPN only would also be a viable solution. This would change the required rules for the alarm to function properly.

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

An alarm could be set with the following filters:

- **http.request.method : "put"**
- **and url.path : ”/webdav/*.php”**

This alarm does not need a threshold and should be triggered any time this activity is detected.

## System Hardening

Several methods can be used to prevent this type of attack.

- Block “PUT” http methods that contain the file extension “.php”
- Do not allow the web server to run .php scripts since they are the main method used for starting reverse shells.
- Implement a firewall rule preventing the web server from sending traffic outside of the LAN.