CAPSTONE ENGAGEMENT

ASSESSMENT, ANALYSIS, AND HARDENING OF A VULNERABLE SYSTEM

PRESENTED BY JENNIFER ZINN

TABLE OF CONTENTS

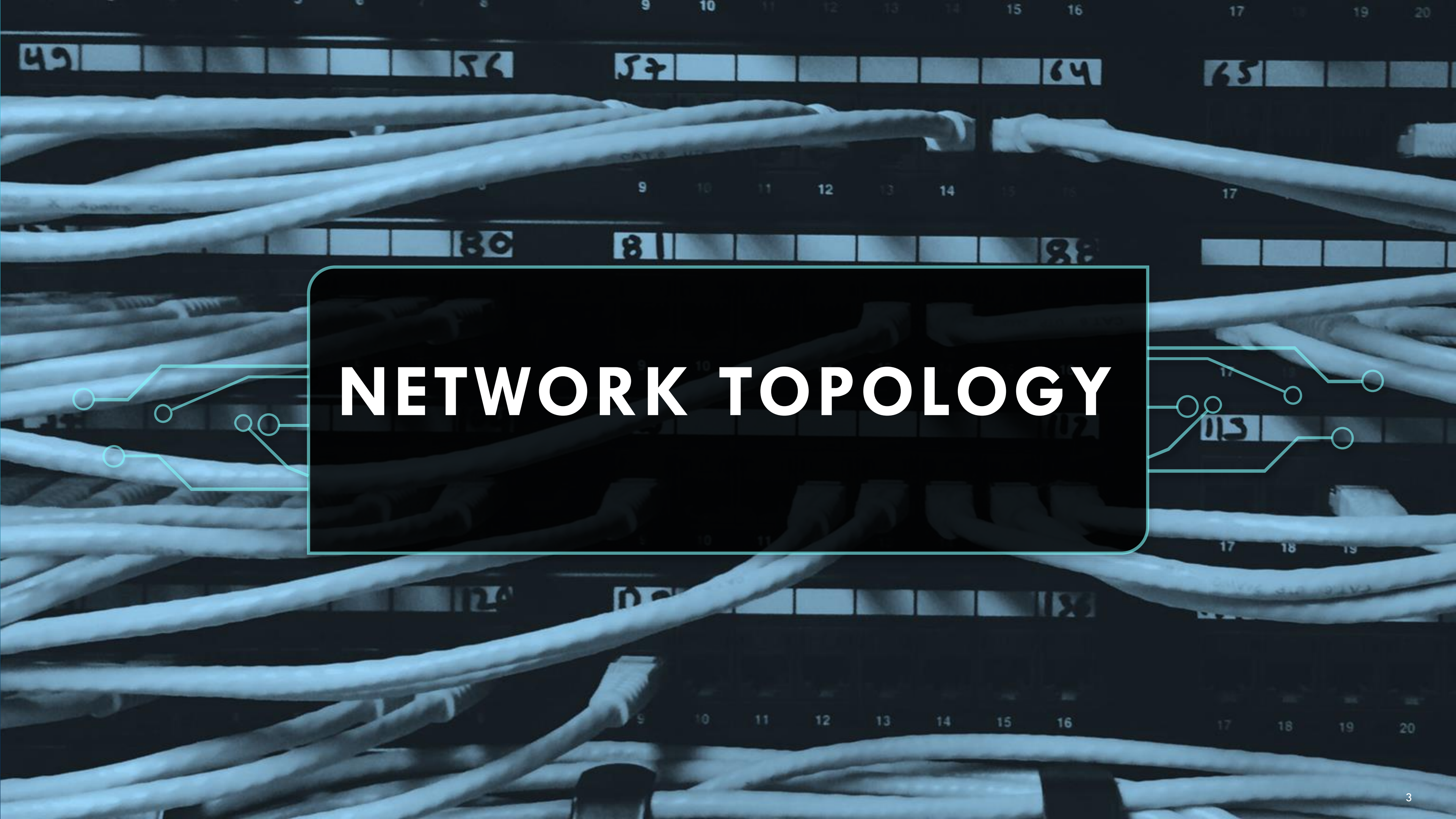
This document contains the following sections:

01 **Network Topology**

02 **Red Team**: Security Assessment

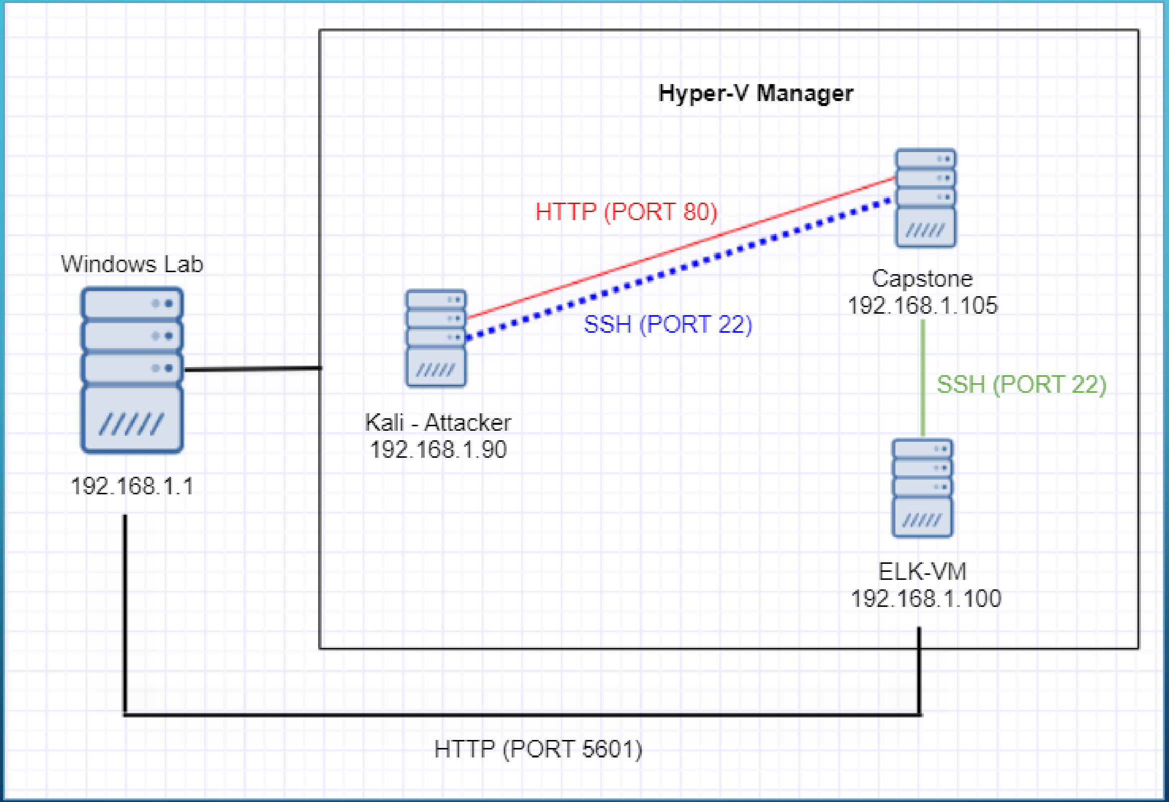
03 **Blue Team**: Log Analysis and Attack Characterization

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: 192.168.1.1
OS: Windows 10
Hostname: Windows Lab

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu Linux
Hostname: Capstone

This Photo by Unknown Author is licensed under CC BY-NC-ND

RED TEAM SECURITY ASSESSMENT

RECON: DESCRIBING THE TARGET

The following hosts were identified on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Red Team offensive attack machine
Capstone	192.168.1.105	Vulnerable VM web server
ELK	192.168.1.100	Kibana for Incident Analysis
Windows Lab	192.168.1.1	Hyper-V VM manager

VULNERABILITY ASSESSMENT

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2018-15919 - OpenSSH 7.6p1	Tool for remote login with the SSH protocol.	Could be used by attackers to remotely connect and execute commands on the victim computer.
Apache httpd 2.4.29 PHP Exploit	PHP exploit allows the attacker access to the web server.	Allows attackers to gain full access to sensitive information and the ability to execute commands.
WebDav	Protocol that allows users to remotely collaborate and edit content on the web.	A reverse shell can be uploaded and compromise the server by allowing remote access.

EXPLOITATION: OPENSSH 7.6P1

Recon:

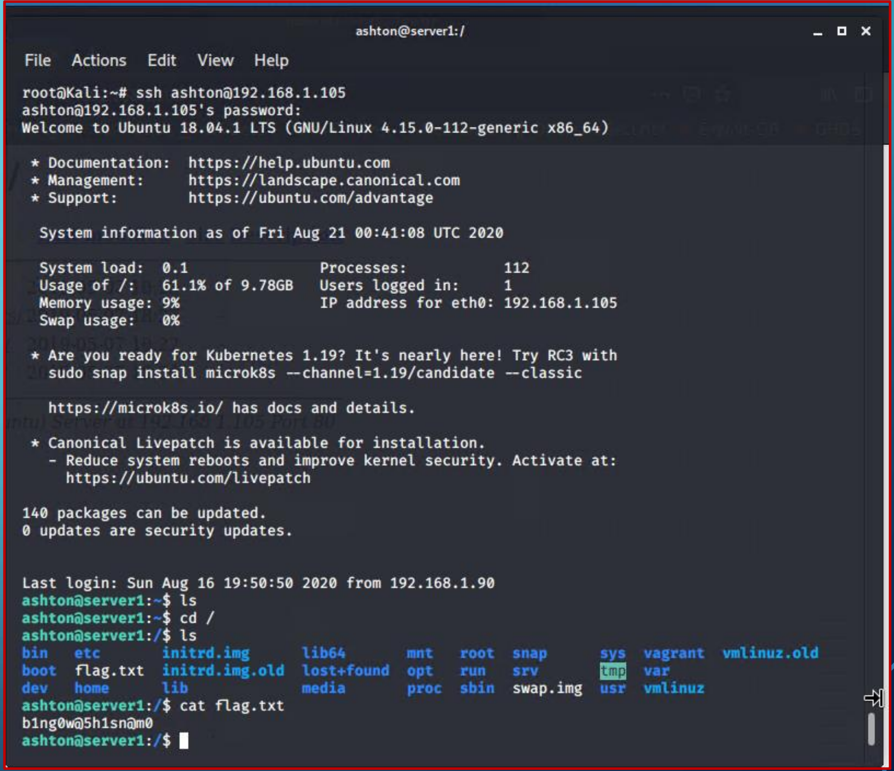
By exploring the Capstone web server using a web browser, a secret_file was found within company_folders. This file is managed by Ashton.

Process:

Ashton's password was cracked using a Brute Force Attack (specifically, Hydra). Using the command line in Kali, access was gained by using the SSH protocol with Ashton's username and password to remotely connect to the web server.

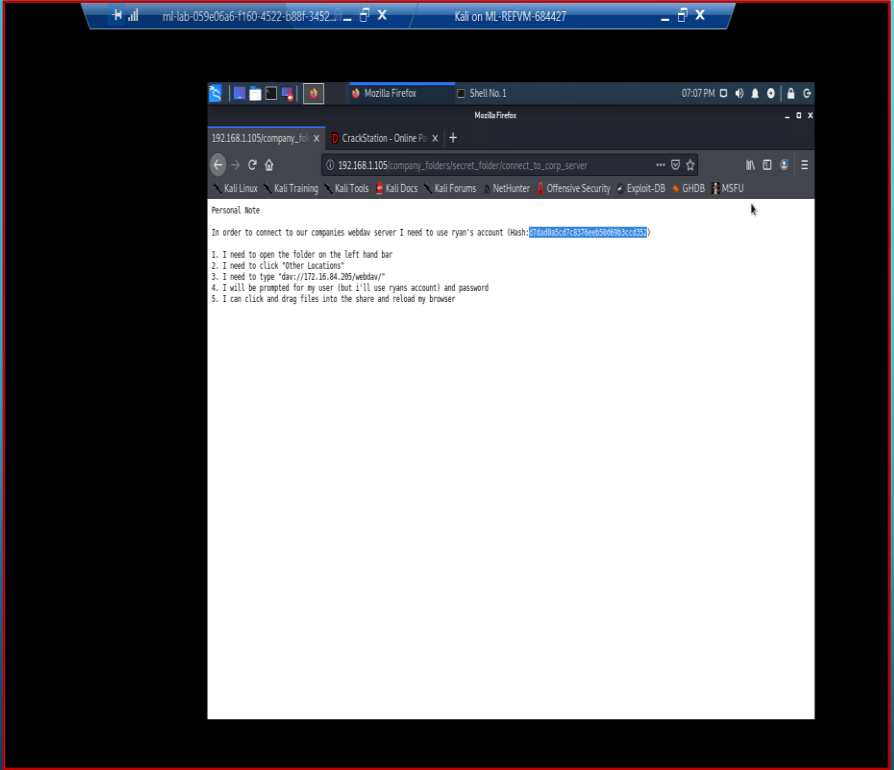
Achievements:

It allowed exploration of folders including the root folder where a sensitive file called flag.txt was located. It can also be used to execute commands.



```
root@Kali:~# ssh ashton@192.168.1.105
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Aug 21 00:41:08 UTC 2020

  System load:  0.1               Processes:           112
  Usage of /:   61.1% of 9.78GB   Users logged in:     1
  Memory usage: 9%                IP address for eth0: 192.168.1.105
  Swap usage:   0%

 * Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
   sudo snap install microk8s --channel=1.19/candidate --classic

   https://microk8s.io/ has docs and details.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

140 packages can be updated.
0 updates are security updates.


Last login: Sun Aug 16 19:50:50 2020 from 192.168.1.90
ashton@server1:~$ ls
ashton@server1:~$ cd /
ashton@server1:/$ ls
bin   etc       initrd.img      lib64       mnt   root  snap      sys  vagrant  vmlinuz.old
boot  flag.txt  initrd.img.old  lost+found  opt   run   srv       tmp  var
dev   home      lib             media       proc  sbin  swap.img  usr  vmlinuz
ashton@server1:/$ cat flag.txt
b1ng0w@5h1sn@m0
ashton@server1:/$ 
```

EXPLOITATION: APACHE HTTPD 2.4.29



```
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
```

Process:

Ashton's password was cracked using a Brute Force Attack. With Ashton's username and password, logged into the secret_folder on the Capstone web server using a web browser.

Achievements:

Ability to access secret_file and find unsecured instructions on how to access the Capstone web server using the WebDAV protocol, including Ryan's password hash. This protocol is vulnerable to a PHP reverse shell payload.

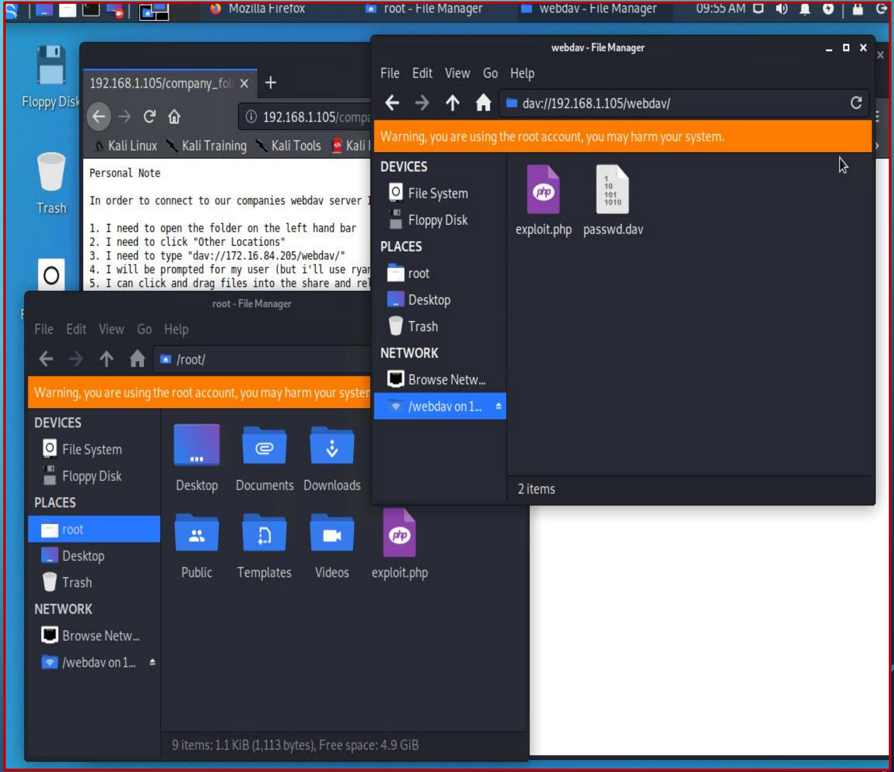
EXPLOITATION: WEBDAV

Process:

A PHP reverse shell payload was created using MSFvenom. Using CrackStation, Ryan's password hash was cracked revealing his password. Kali File Manager was used to drag and drop the payload onto the victim web server using Ryan's credentials and the WebDAV protocol.

Achievements:

Ability to establish a reverse shell after uploading and opening the PHP payload on the victim system. The payload opened a listener on port 4444. Using Metasploit, the PHP reverse shell exploit was used to allow remote connection to the web server and explore folders, including the root folder.

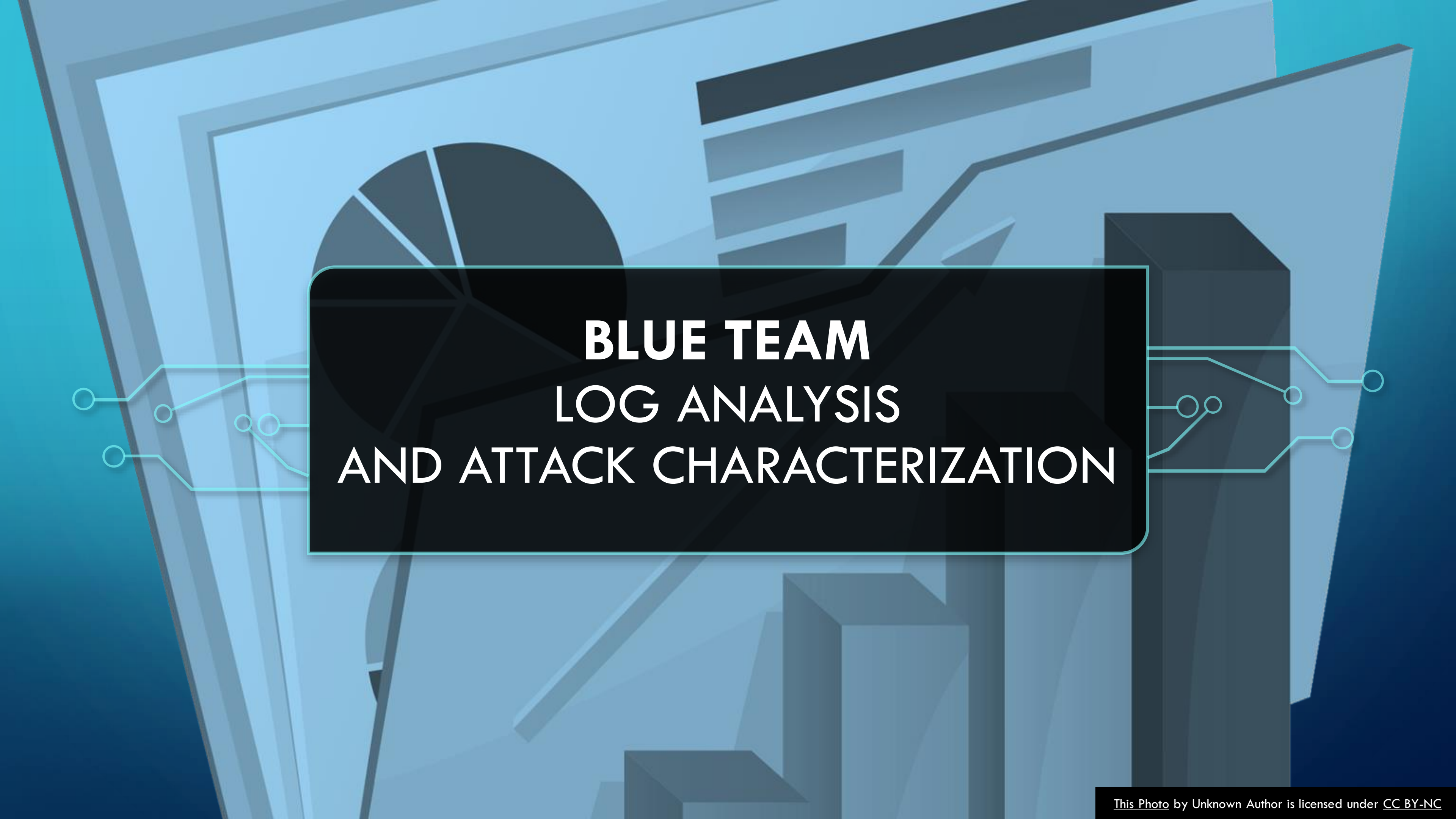


```
Personal Note

In order to connect to our companies webdav server I

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 rya
5. I can click and drag files into the share and rel
```

Warning, you are using the root account, you may harm your system.

Warning, you are using the root account, you may harm your syster

9 items: 1.1 KiB (1,113 bytes), Free space: 4.9 GiB

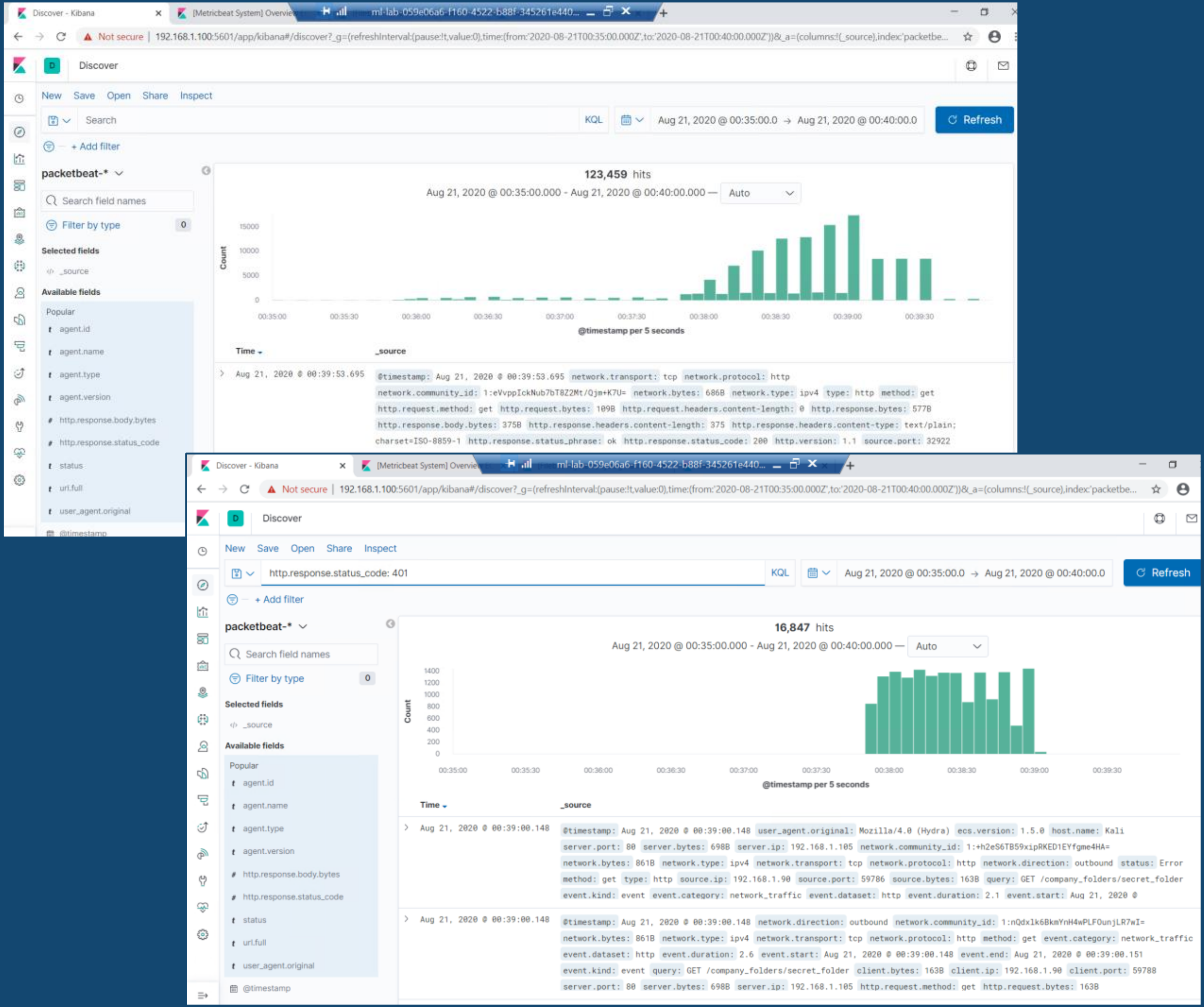


BLUE TEAM
LOG ANALYSIS
AND ATTACK CHARACTERIZATION

ANALYSIS: IDENTIFYING THE OFFENSIVE TRAFFIC

Traffic between the attacker Kali and Capstone victim web server took place between 12:35 and 12:40 on August 21st. There were 123,459 responses.

The Blue Team is most concerned with http status code 401 which indicates unauthorized access.



192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-08-21T00:35:00.000Z',to:'2020-08-21T00:40:00.000Z'))&_a=(columns:!(_source),index:'packetbe...

Search

Aug 21, 2020 @ 00:35:00.0 → Aug 21, 2020 @ 00:40:00.0

123,459 hits

Aug 21, 2020 @ 00:35:00.000 - Aug 21, 2020 @ 00:40:00.000 —

```
Aug 21, 2020 @ 00:39:53.695   @timestamp: Aug 21, 2020 @ 00:39:53.695 network.transport: tcp network.protocol: http
                              network.community_id: 1:eVvppIckNub7bT8Z2Mt/Qjm+K7U= network.bytes: 686B network.type: ipv4 type: http method: get
                              http.request.method: get http.request.bytes: 109B http.request.headers.content-length: 0 http.response.bytes: 577B
                              http.response.body.bytes: 375B http.response.headers.content-length: 375 http.response.headers.content-type: text/plain;
                              charset=ISO-8859-1 http.response.status_phrase: ok http.response.status_code: 200 http.version: 1.1 source.port: 32922
```

http.response.status_code: 401

Aug 21, 2020 @ 00:35:00.0 → Aug 21, 2020 @ 00:40:00.0

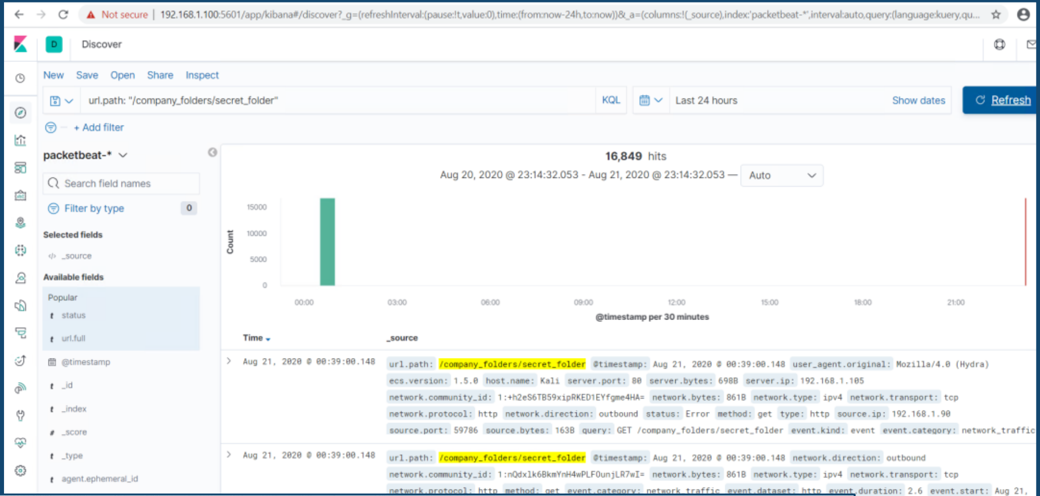
16,847 hits

Aug 21, 2020 @ 00:35:00.000 - Aug 21, 2020 @ 00:40:00.000 —

```
Aug 21, 2020 @ 00:39:00.148   @timestamp: Aug 21, 2020 @ 00:39:00.148 user_agent.original: Mozilla/4.0 (Hydra) ecs.version: 1.5.0 host.name: Kali
                              server.port: 80 server.bytes: 698B server.ip: 192.168.1.105 network.community_id: 1:+h2eS6TB59xipRKED1EYfgme4HA=
                              network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound status: Error
                              method: get type: http source.ip: 192.168.1.90 source.port: 59786 source.bytes: 163B query: GET /company_folders/secret_folder
                              event.kind: event event.category: network_traffic event.dataset: http event.duration: 2.1 event.start: Aug 21, 2020 @

Aug 21, 2020 @ 00:39:00.148   @timestamp: Aug 21, 2020 @ 00:39:00.148 network.direction: outbound network.community_id: 1:nQdxlk6BkmYnH4wPLFOunjLR7wI=
                              network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http method: get event.category: network_traffic
                              event.dataset: http event.duration: 2.6 event.start: Aug 21, 2020 @ 00:39:00.148 event.end: Aug 21, 2020 @ 00:39:00.151
                              event.kind: event query: GET /company_folders/secret_folder client.bytes: 163B client.ip: 192.168.1.90 client.port: 59788
                              server.port: 80 server.bytes: 698B server.ip: 192.168.1.105 http.request.method: get http.request.bytes: 163B
```

ANALYSIS: FINDING THE REQUEST FOR THE HIDDEN DIRECTORY

The hidden directory “secret_folder” was accessed 16,849 times around 12:39. The IP address the requests were coming from is 192.168.1.90.
It contained a file called “connect_to_corp_server” which was accessed 2 times.

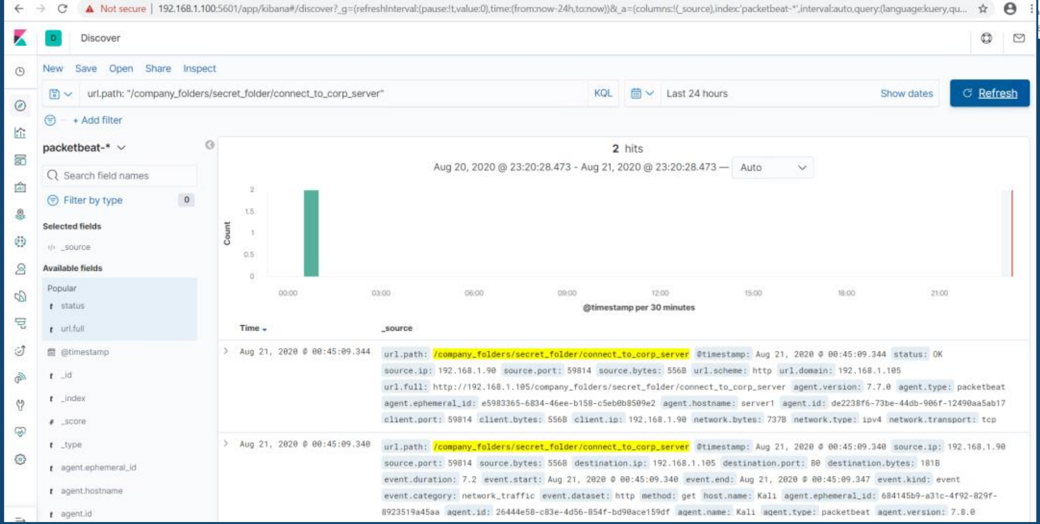


url.path: "/company_folders/secret_folder"

16,849 hits

Aug 20, 2020 @ 23:14:32.053 - Aug 21, 2020 @ 23:14:32.053 —

```
Aug 21, 2020 @ 00:39:00.148   url.path: /company_folders/secret_folder @timestamp: Aug 21, 2020 @ 00:39:00.148 user_agent.original: Mozilla/4.0 (Hydra)
                              ecs.version: 1.5.0 host.name: Kali server.port: 80 server.bytes: 698B server.ip: 192.168.1.105
                              network.community_id: 1:+h2eS6TB59xipRKED1EYfgme4HA= network.bytes: 861B network.type: ipv4 network.transport: tcp
                              network.protocol: http network.direction: outbound status: Error method: get type: http source.ip: 192.168.1.90
                              source.port: 59786 source.bytes: 163B query: GET /company_folders/secret_folder event.kind: event event.category: network_traffic

Aug 21, 2020 @ 00:39:00.148   url.path: /company_folders/secret_folder @timestamp: Aug 21, 2020 @ 00:39:00.148 network.direction: outbound
                              network.community_id: 1:nQdx1k6BkmYnH4wPLFOunjLR7wI= network.bytes: 861B network.type: ipv4 network.transport: tcp
                              network.protocol: http method: get event.category: network_traffic event.dataset: http event.duration: 2.6 event.start: Aug 21,
                              ny_folders/secret_folder
                              698B server.ip: 192.168.1.105
```



url.path: "/company_folders/secret_folder/connect_to_corp_server"

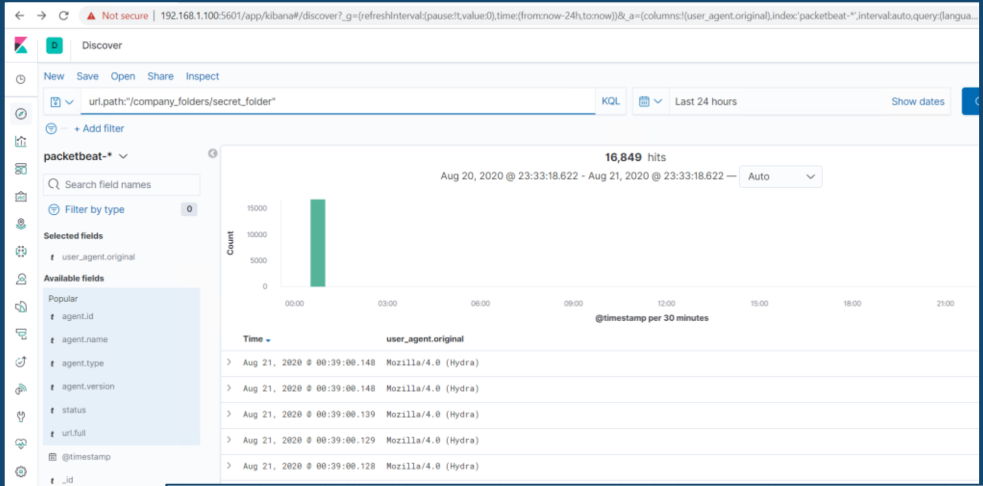
2 hits

Aug 20, 2020 @ 23:20:28.473 - Aug 21, 2020 @ 23:20:28.473 —

```
Aug 21, 2020 @ 00:45:09.344   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Aug 21, 2020 @ 00:45:09.344 status: OK
                              source.ip: 192.168.1.90 source.port: 59814 source.bytes: 556B url.scheme: http url.domain: 192.168.1.105
                              url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server agent.version: 7.7.0 agent.type: packetbeat
                              agent.ephemeral_id: e5983365-6834-46ee-b158-c5eb0b8509e2 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17
                              client.port: 59814 client.bytes: 556B client.ip: 192.168.1.90 network.bytes: 737B network.type: ipv4 network.transport: tcp

Aug 21, 2020 @ 00:45:09.340   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Aug 21, 2020 @ 00:45:09.340 source.ip: 192.168.1.90
                              source.port: 59814 source.bytes: 556B destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 181B
                              event.duration: 7.2 event.start: Aug 21, 2020 @ 00:45:09.340 event.end: Aug 21, 2020 @ 00:45:09.347 event.kind: event
                              event.category: network_traffic event.dataset: http method: get host.name: Kali agent.ephemeral_id: 684145b9-a31c-4f92-829f-
                              8923519a45aa agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0
```

ANALYSIS: UNCOVERING THE BRUTE FORCE ATTACK

There were 16,849 packet requests made by a Brute Force Attack (specifically, Hydra). The http response code 301 indicates a successful discovery of the correct password and was redirected to another web page.



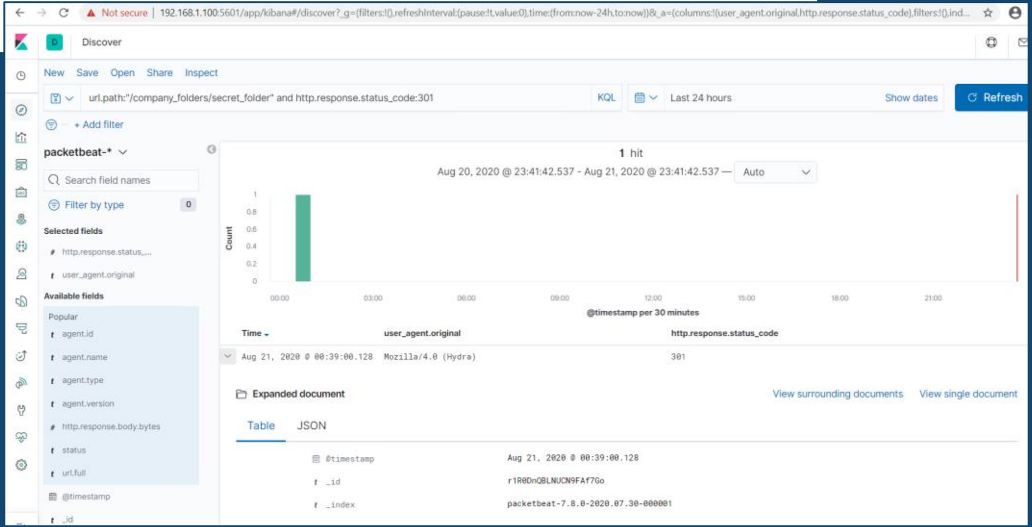
192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(user_agent.original),index:'packetbeat-*',interval:auto,query:(langua...

url.path:"/company_folders/secret_folder"

16,849 hits

Aug 20, 2020 @ 23:33:18.622 - Aug 21, 2020 @ 23:33:18.622 —

Time	user_agent.original
Aug 21, 2020 @ 00:39:00.148	Mozilla/4.0 (Hydra)
Aug 21, 2020 @ 00:39:00.148	Mozilla/4.0 (Hydra)
Aug 21, 2020 @ 00:39:00.139	Mozilla/4.0 (Hydra)
Aug 21, 2020 @ 00:39:00.129	Mozilla/4.0 (Hydra)
Aug 21, 2020 @ 00:39:00.128	Mozilla/4.0 (Hydra)



192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(user_agent.original,http.response.status_code),filters:!(),ind...

url.path:"/company_folders/secret_folder" and http.response.status_code:301

1 hit

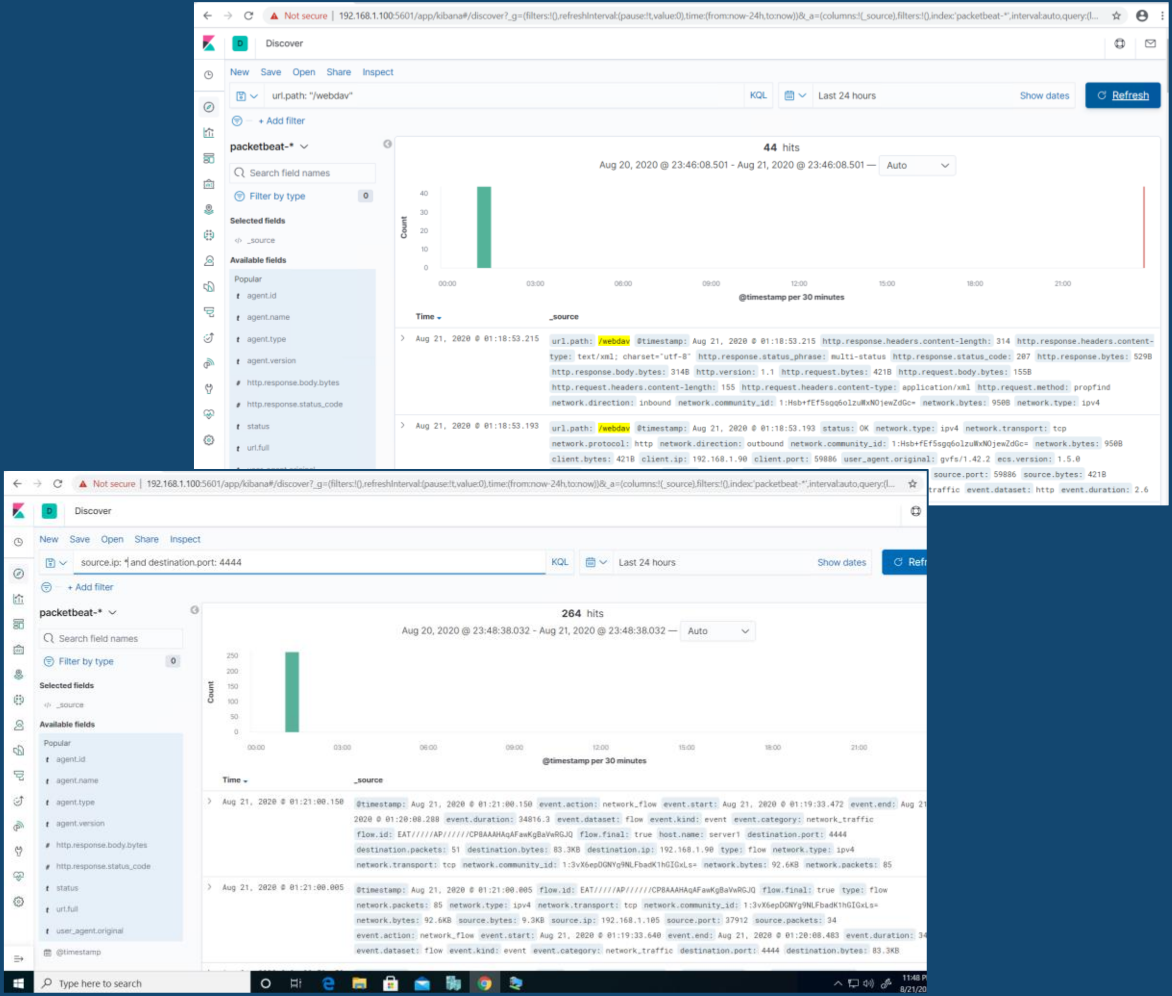
Aug 20, 2020 @ 23:41:42.537 - Aug 21, 2020 @ 23:41:42.537 —

Time	user_agent.original	http.response.status_code
Aug 21, 2020 @ 00:39:00.128	Mozilla/4.0 (Hydra)	301

@timestamp	Aug 21, 2020 @ 00:39:00.128
_id	r1R0DnQBLNUCN9FAf7Go
_index	packetbeat-7.8.0-2020.07.30-000001

ANALYSIS: FINDING THE WEBDAV CONNECTION

There were 44 hits to the WebDAV connection where the files exploit.php and passwd.dav were requested. The PHP reverse shell was uploaded to start a Metepreter shell session.



url.path: "/webdav"

44 hits

Aug 20, 2020 @ 23:46:08.501 - Aug 21, 2020 @ 23:46:08.501

```
Aug 21, 2020 @ 01:18:53.215   url.path: /webdav @timestamp: Aug 21, 2020 @ 01:18:53.215 http.response.headers.content-length: 314 http.response.headers.content-
                              type: text/xml; charset="utf-8" http.response.status_phrase: multi-status http.response.status_code: 207 http.response.bytes: 529B
                              http.response.body.bytes: 314B http.version: 1.1 http.request.bytes: 421B http.request.body.bytes: 155B
                              http.request.headers.content-length: 155 http.request.headers.content-type: application/xml http.request.method: propfind
                              network.direction: inbound network.community_id: 1:Hsb+fEf5sgq6olzuWxNOjewZdGc= network.bytes: 950B network.type: ipv4

Aug 21, 2020 @ 01:18:53.193   url.path: /webdav @timestamp: Aug 21, 2020 @ 01:18:53.193 status: OK network.type: ipv4 network.transport: tcp
                              network.protocol: http network.direction: outbound network.community_id: 1:Hsb+fEf5sgq6olzuWxNOjewZdGc= network.bytes: 950B
                              client.bytes: 421B client.ip: 192.168.1.90 client.port: 59886 user_agent.original: gvfs/1.42.2 ecs.version: 1.5.0
                              source.port: 59886 source.bytes: 421B
                              traffic event.dataset: http event.duration: 2.6
```

source.ip: * and destination.port: 4444

264 hits

Aug 20, 2020 @ 23:48:38.032 - Aug 21, 2020 @ 23:48:38.032

```
Aug 21, 2020 @ 01:21:00.150   @timestamp: Aug 21, 2020 @ 01:21:00.150 event.action: network_flow event.start: Aug 21, 2020 @ 01:19:33.472 event.end: Aug 21
                              2020 @ 01:20:08.288 event.duration: 34816.3 event.dataset: flow event.kind: event event.category: network_traffic
                              flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRGJQ flow.final: true host.name: server1 destination.port: 4444
                              destination.packets: 51 destination.bytes: 83.3KB destination.ip: 192.168.1.90 type: flow network.type: ipv4
                              network.transport: tcp network.community_id: 1:3vX6epDGNYg9NLFbadK1hGIGxLs= network.bytes: 92.6KB network.packets: 85

Aug 21, 2020 @ 01:21:00.005   @timestamp: Aug 21, 2020 @ 01:21:00.005 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRGJQ flow.final: true type: flow
                              network.packets: 85 network.type: ipv4 network.transport: tcp network.community_id: 1:3vX6epDGNYg9NLFbadK1hGIGxLs=
                              network.bytes: 92.6KB source.bytes: 9.3KB source.ip: 192.168.1.105 source.port: 37912 source.packets: 34
                              event.action: network_flow event.start: Aug 21, 2020 @ 01:19:33.640 event.end: Aug 21, 2020 @ 01:20:08.483 event.duration: 34
                              event.dataset: flow event.kind: event event.category: network_traffic destination.port: 4444 destination.bytes: 83.3KB
```

This Photo by Unknown Author is licensed under CC BY-SA

BLUE TEAM PROPOSED ALARMS AND MITIGATION STRATEGIES

MITIGATION:
BLOCKING OFFENSIVE TRAFFIC

ALERT

- Alert if a large amount of traffic occurs in a short time from a single source IP that targets multiple ports.
- 10 port scans in one minute or 100 consecutive ping (ICMP) requests.

SYSTEM HARDENING

- Enable only the traffic you need to access internal hosts and deny everything else.
- Configure firewalls to look for malicious behavior and have rules in place to cut off attacks if a certain threshold is reached.

MITIGATION:
FINDING THE REQUEST FOR THE HIDDEN DIRECTORY

ALERT

- Alert if there are requests for the hidden directory from an unauthorized user.
- By whitelisting authorized users, the hidden directory will have limited access.

SYSTEM HARDENING

- Stronger usernames and password requirements for users that have access to the hidden directory.
- Create a whitelist for authorized IP addresses.
- Make the folder private by changing permissions.

MITIGATION:
PREVENTING BRUTE FORCE ATTACKS

ALERT

- Alert if there are many failed logins from the same IP address and/or logins for a single account from many different IP addresses.
- Alert if there are any Hydra attempts.

SYSTEM HARDENING

- More secure password requirements.
- Limiting the number of attempts that a password can be tried.
- Locking accounts out after unsuccessful login attempts.
- Using CAPTCHA
  (human vs machine input)

MITIGATION:
DETECTING THE WEBDAV CONNECTION

ALERT

- Alert if requests are made from port 4444.
- Alert if a PHP file is uploaded using the WebDAV protocol.

SYSTEM HARDENING

- Avoid storing instructions for accessing the server that can be accessed by a web browser.
- Make sure software patches are up-to-date.
- Disable WebDAV or make sure it's configured correctly.

MITIGATION:
IDENTIFYING REVERSE SHELL UPLOADS

ALERT

- Alert if invalid file types are uploaded to the web server.
- Alert if any port is open.
- Alert on any traffic that is not expected.

SYSTEM HARDENING

- Store uploaded files in a location not accessible from the web.
- Manage privileges of all users to control access to sensitive files.
- Define valid types of files that the users should be allowed to upload.

THE END

ANY QUESTIONS?