Capstone Engagement Assessment, Analysis, and Hardening of a Vulnerable System

Presented by : Nauman Jaliawala

Table of Contents

This document contains the following sections:

01 **Network Topology**

02 **Red Team**: Security Assessment

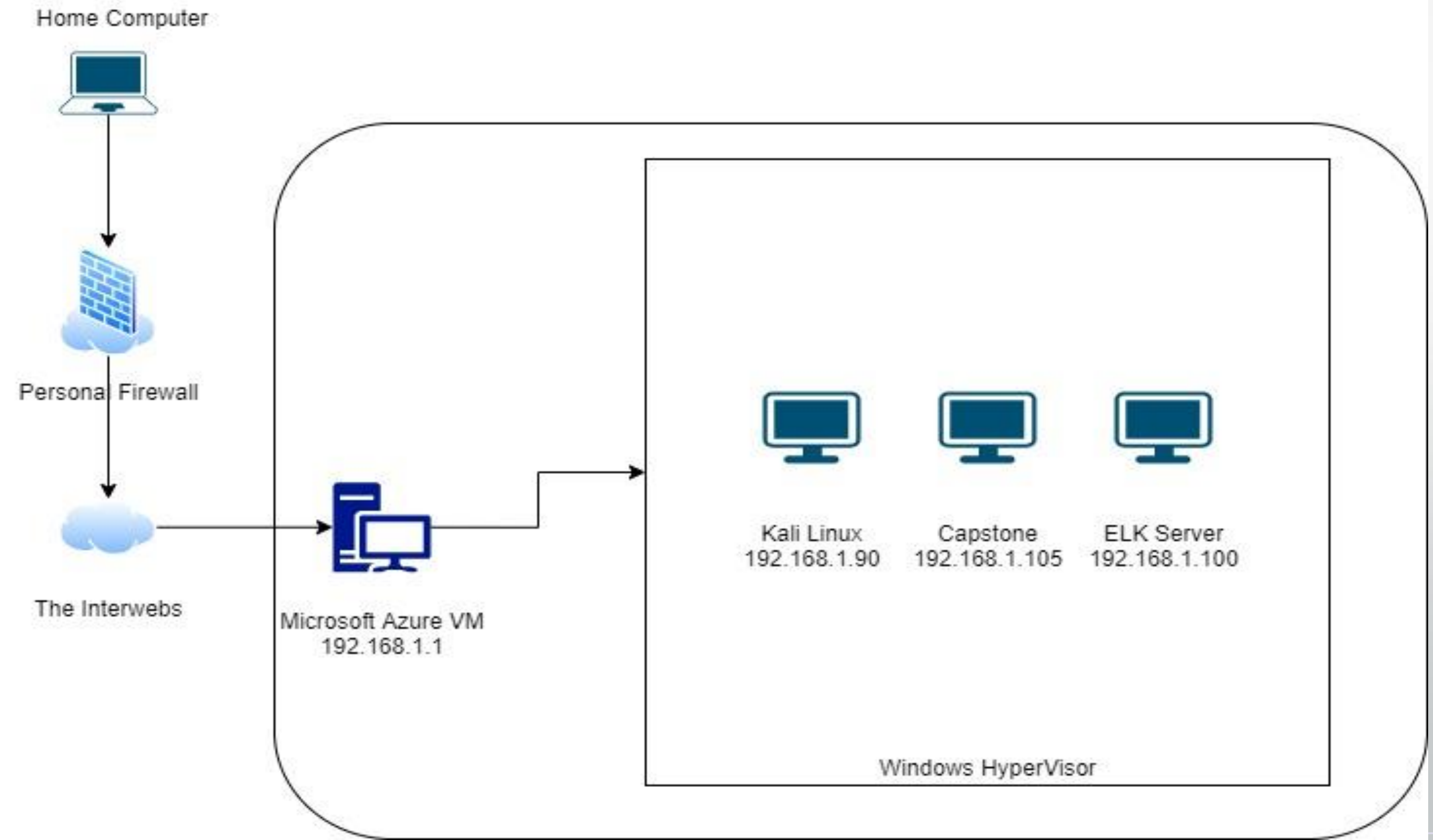
03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology

Azure Environment



Personal public IP withheld for obvious reasons. Connection to Microsoft servers to remote connect to Azure Labs virtual machine. Through hypervisor connection is established to additional virtual machines located at internal IP addresses list in diagram.

Red Team Security Assessment

Attack Phase

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	Microsoft Windows 10 Server
Kali	192.168.1.90	Kali Linux VM
ELK	192.168.1.100	ELK server VM
Capstone	192.168.1.105	Ubuntu Linux VM

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
NMAP port scanning enabled	Ability to scan without limitation or blocks in place allows high level of recon capability	Ability to identify not only ports but type of server and services as well as versions to aid in recon
Hydra Brute force without limitation	Although noisy it is possible to endlessly scan the webserver to gain as many credentials as possible	The impact of being able to brute force a server endlessly is self explanatory; especially if proper alerts are not in play
Easily cracked hashes with weak passwords	Readily available wordlists can crack the weak hashes used by personnel	It only takes one weak password to gain access and allow time to sniff out administrative control

Exploitation: [Recon with NMAP]

01

Tools & Processes

–Detailed NMAP scan of the Capstone virtual machine showed open ports on 22 and 80.
22 did not seem like a viable target so 80 was chosen as there would have been more vulnerabilities to gain access.

02

Achievements

–With the information gathered from allowed scanning we were able to determine type of server and operating system information in order to determine best course of action to attack.

03

Nmap –Pn –sC –sV –p-–open 192.168.1.0/24 –oA lab

Exploitation: [HYDRA – webserver brute force]

01

Tools & Processes

–HYDRA was used to brute force access to admin account as no security measure prevented this action.

02

Achievements

–HYDRA allowed access to webserver secret folder which in turn provided information we can then use to gain additional access to achieve our goal

03

Hydra –l ashton –P /usr/share/wordlists/rockyou.txt 192.168.1.105 http-get /company_folders/secret_folder

Exploitation: [Weak hash easily cracked with John]

01

Tools & Processes

–John was used to crack simple hash found on webserver secret folder

02

Achievements

–John provided access to network share for webserver where malicious payload was delivered to exploit the webserver. This exploit provided us with a shell to capture the flag

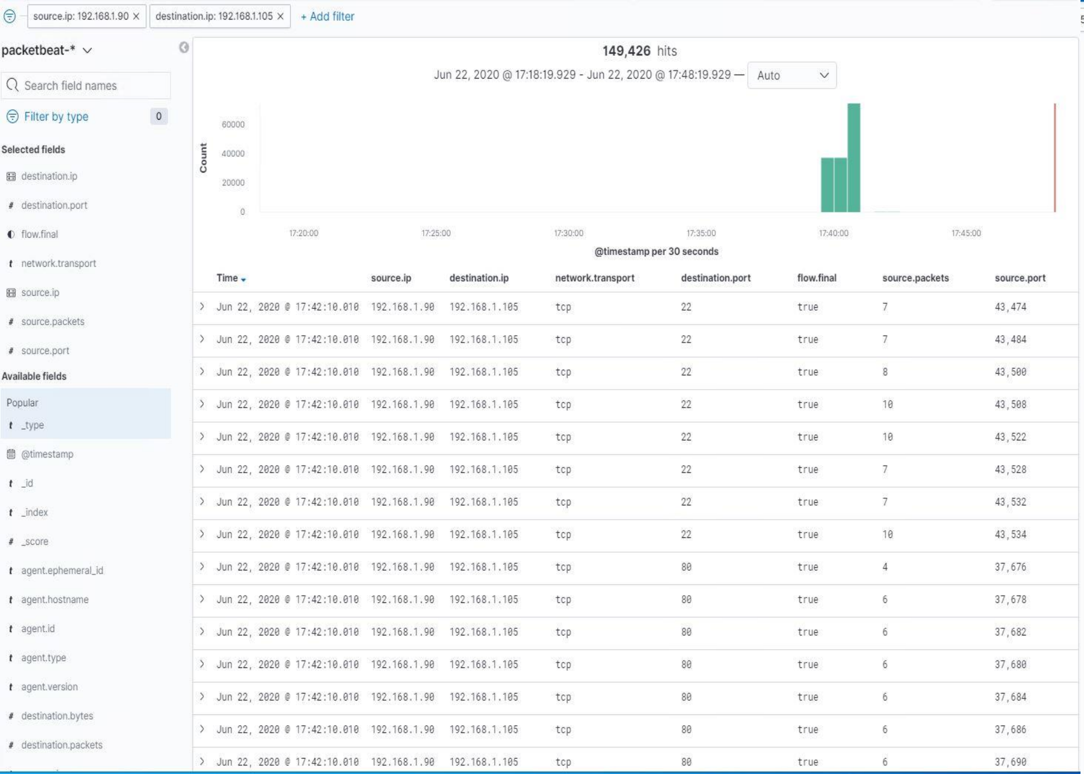
03

```
John –wordlist=
/usr/share/wordlists/rockyou
.txt hash.txt
```

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

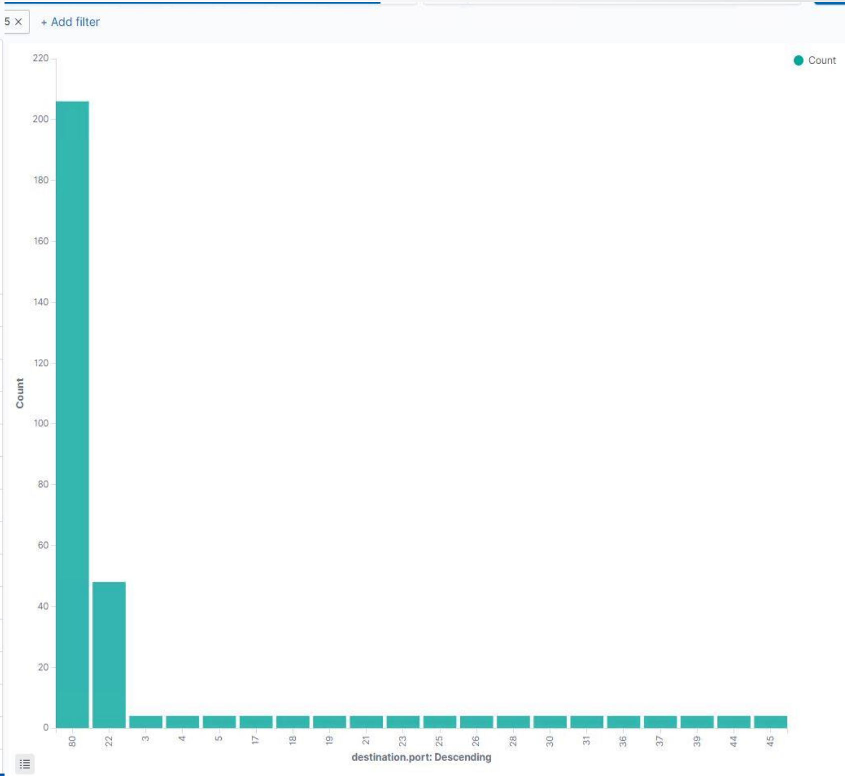
- Port scans took place from 17:39 to 17:41
- In this short period there were almost 150k packets exchanged
- The graph shows linear packet counts with exception to open ports / ports uncommonly used for web traffic were targeted indicating a scan



149,426 hits

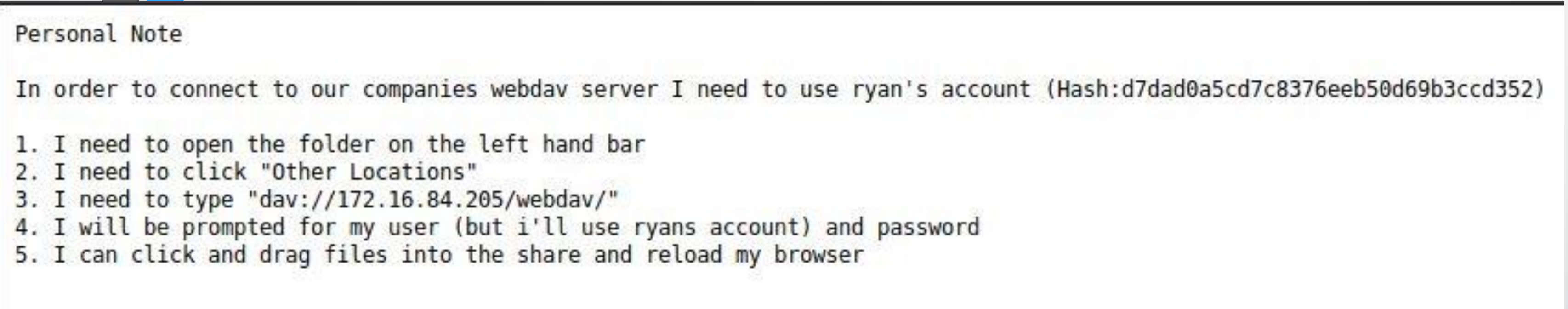
Jun 22, 2020 @ 17:18:19.929 - Jun 22, 2020 @ 17:48:19.929 —

Time	source.ip	destination.ip	network.transport	destination.port	flow.final	source.packets	source.port
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	7	43,474
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	7	43,484
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	8	43,500
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	10	43,508
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	10	43,522
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	7	43,528
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	7	43,532
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	22	true	10	43,534
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	4	37,676
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	6	37,678
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	6	37,682
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	6	37,680
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	6	37,684
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	6	37,686
Jun 22, 2020 @ 17:42:10.010	192.168.1.90	192.168.1.105	tcp	80	true	6	37,690



Analysis: Finding the Request for the Hidden Directory

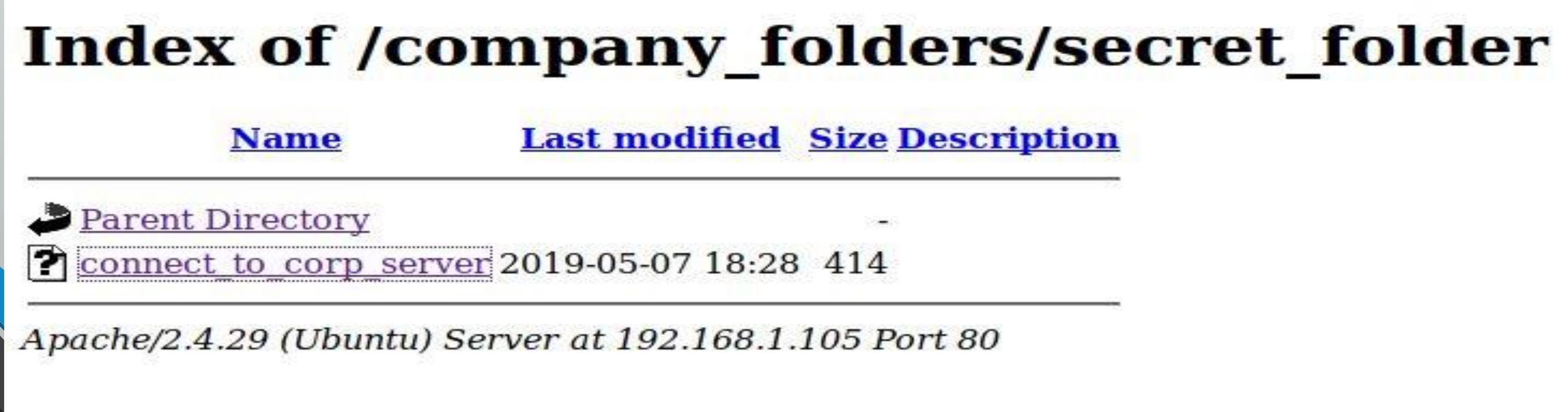
- June 18th @ 00:39 requests were made to access secret folder
- Full contents access was requested
- Only 1 file was contained in the folder, but it contained hash information



```
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
```



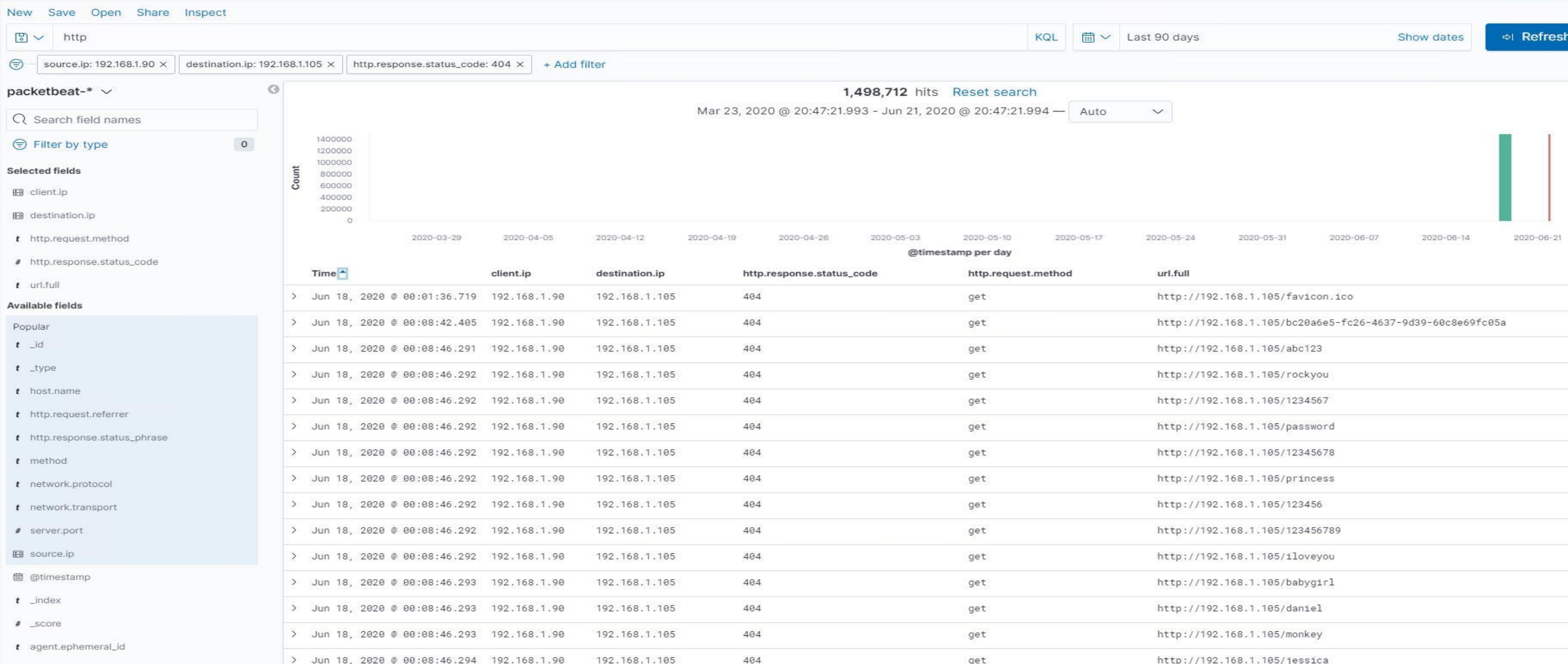
Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Analysis: Uncovering the Brute Force Attack

- 2 million attempts were made to brute force the secret folder
- The attacker took 1.5 attempts to gain the password indicative of weak password found in common wordlists



http

Last 90 days

source.ip: 192.168.1.90 × destination.ip: 192.168.1.105 × http.response.status_code: 404 ×

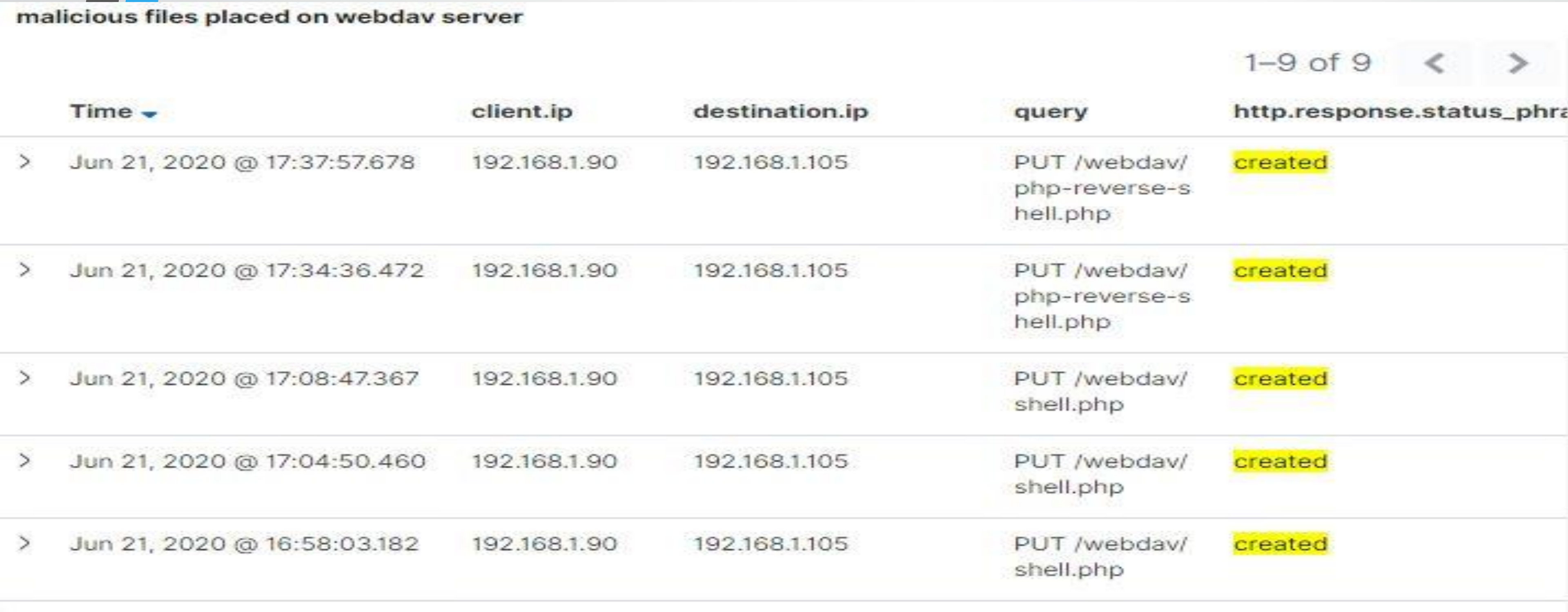
1,498,712 hits

Mar 23, 2020 @ 20:47:21.993 - Jun 21, 2020 @ 20:47:21.994 —

Time	client.ip	destination.ip	http.response.status_code	http.request.method	url.full
Jun 18, 2020 @ 00:01:36.719	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/favicon.ico
Jun 18, 2020 @ 00:08:42.405	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/bc20a6e5-fc26-4637-9d39-60c8e69fc05a
Jun 18, 2020 @ 00:08:46.291	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/abc123
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/rockyou
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/1234567
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/password
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/12345678
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/princess
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/123456
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/123456789
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/iloveyou
Jun 18, 2020 @ 00:08:46.293	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/babygirl
Jun 18, 2020 @ 00:08:46.293	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/daniel
Jun 18, 2020 @ 00:08:46.293	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/monkey
Jun 18, 2020 @ 00:08:46.294	192.168.1.90	192.168.1.105	404	get	http://192.168.1.105/jessica

Analysis: Finding the WebDAV Connection

- 6 requests were made to the webdav server as only 1 file existed it was accessed 1 time – also contained a hash
- The attacker exfiltrated this file and in turn uploaded a single file entitled shell.php which contained code creating a reverse tcp connection to attacker

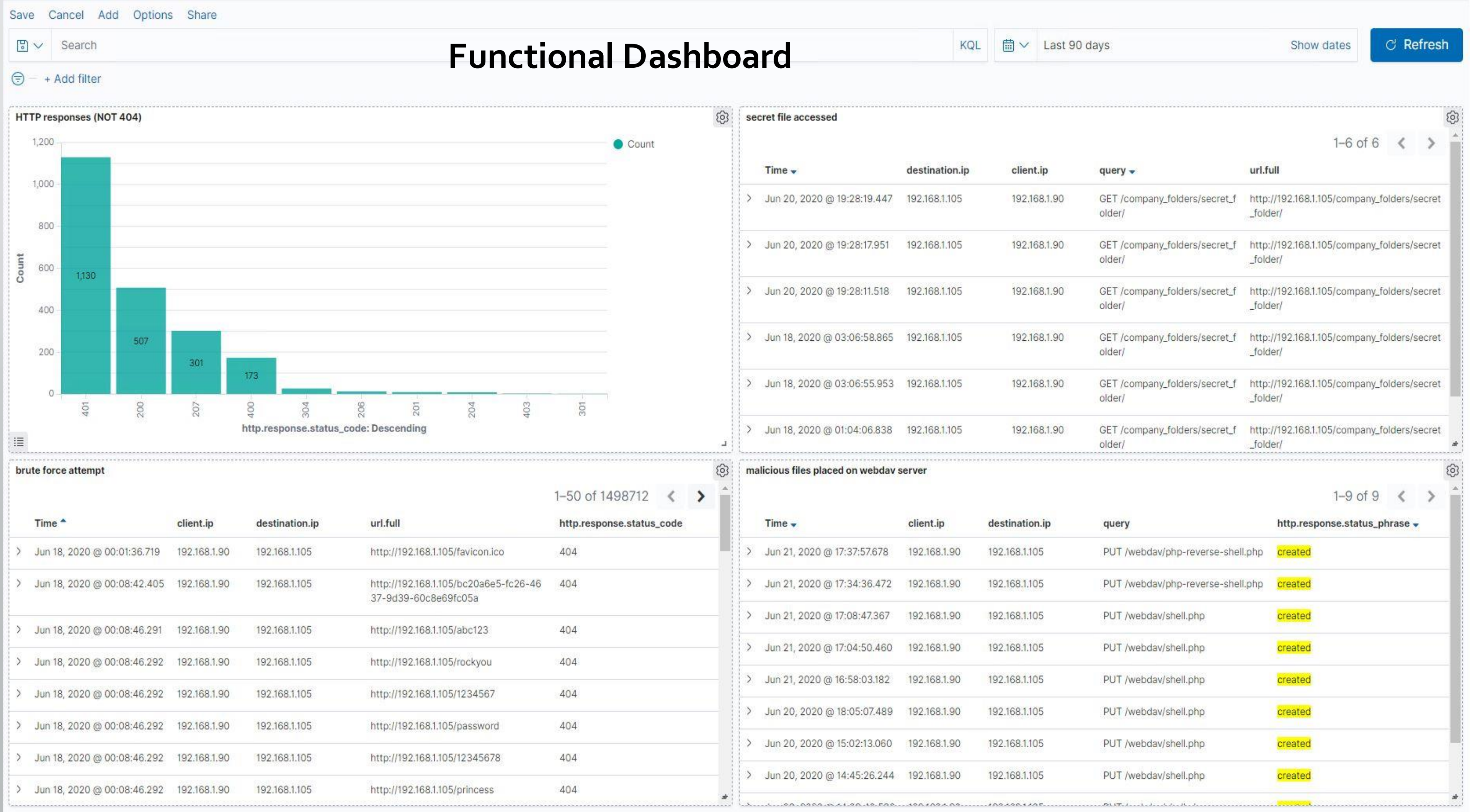


malicious files placed on webdav server

1–9 of 9 < >

	Time	client.ip	destination.ip	query	http.response.status_phra
>	Jun 21, 2020 @ 17:37:57.678	192.168.1.90	192.168.1.105	PUT /webdav/php-reverse-shell.php	created
>	Jun 21, 2020 @ 17:34:36.472	192.168.1.90	192.168.1.105	PUT /webdav/php-reverse-shell.php	created
>	Jun 21, 2020 @ 17:08:47.367	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
>	Jun 21, 2020 @ 17:04:50.460	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
>	Jun 21, 2020 @ 16:58:03.182	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created

Functional Dashboard



HTTP responses (NOT 404)

secret file accessed

1–6 of 6

Time	destination.ip	client.ip	query	url.full
Jun 20, 2020 @ 19:28:19.447	192.168.1.105	192.168.1.90	GET /company_folders/secret_folder/	http://192.168.1.105/company_folders/secret_folder/
Jun 20, 2020 @ 19:28:17.951	192.168.1.105	192.168.1.90	GET /company_folders/secret_folder/	http://192.168.1.105/company_folders/secret_folder/
Jun 20, 2020 @ 19:28:11.518	192.168.1.105	192.168.1.90	GET /company_folders/secret_folder/	http://192.168.1.105/company_folders/secret_folder/
Jun 18, 2020 @ 03:06:58.865	192.168.1.105	192.168.1.90	GET /company_folders/secret_folder/	http://192.168.1.105/company_folders/secret_folder/
Jun 18, 2020 @ 03:06:55.953	192.168.1.105	192.168.1.90	GET /company_folders/secret_folder/	http://192.168.1.105/company_folders/secret_folder/
Jun 18, 2020 @ 01:04:06.838	192.168.1.105	192.168.1.90	GET /company_folders/secret_folder/	http://192.168.1.105/company_folders/secret_folder/

brute force attempt

1–50 of 1498712

Time	client.ip	destination.ip	url.full	http.response.status_code
Jun 18, 2020 @ 00:01:36.719	192.168.1.90	192.168.1.105	http://192.168.1.105/favicon.ico	404
Jun 18, 2020 @ 00:08:42.405	192.168.1.90	192.168.1.105	http://192.168.1.105/bc20a6e5-fc26-4637-9d39-60c8e69fc05a	404
Jun 18, 2020 @ 00:08:46.291	192.168.1.90	192.168.1.105	http://192.168.1.105/abc123	404
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	http://192.168.1.105/rockyou	404
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	http://192.168.1.105/1234567	404
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	http://192.168.1.105/password	404
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	http://192.168.1.105/12345678	404
Jun 18, 2020 @ 00:08:46.292	192.168.1.90	192.168.1.105	http://192.168.1.105/princess	404

malicious files placed on webdav server

1–9 of 9

Time	client.ip	destination.ip	query	http.response.status_phrase
Jun 21, 2020 @ 17:37:57.678	192.168.1.90	192.168.1.105	PUT /webdav/php-reverse-shell.php	created
Jun 21, 2020 @ 17:34:36.472	192.168.1.90	192.168.1.105	PUT /webdav/php-reverse-shell.php	created
Jun 21, 2020 @ 17:08:47.367	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
Jun 21, 2020 @ 17:04:50.460	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
Jun 21, 2020 @ 16:58:03.182	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
Jun 20, 2020 @ 18:05:07.489	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
Jun 20, 2020 @ 15:02:13.060	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created
Jun 20, 2020 @ 14:45:26.244	192.168.1.90	192.168.1.105	PUT /webdav/shell.php	created

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

What kind of alarm can be set to detect future port scans?

-- An alert triggered for any request traffic targeting a port other than 80

What threshold would you set to activate this alarm?

--As the ports are closed the threshold would need to be single digit with at least 5 additional ports included as novice attacker likely would check for all ports

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

--Limit server response to requests to be limited to 80 only with drop on any other port

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

--Solution would only require configuration of ICMP request blocking on all ports except 80 as required for functionality

Mitigation: Finding the Request for the Hidden Directory

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

--Block all remote traffic to specific directories altogether as they do not reduce functionality

What threshold would you set to activate this alarm?

--Upon successful ability to locate directory an alert should be triggered to SOC team for evaluation

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

--Again basically blocking remote access to folders and locations not required for functionality

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

--Solution requires configuration to remove access remotely and should only be available though specific credential with geolocation validation

Mitigation: Preventing Brute Force Attacks

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

--Alert to email SOC team when possible brute force activity is identified

What threshold would you set to activate this alarm?

----Limitation on invalid login attempts set to 5 within 1 minute to trigger alert

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

--Login requirements can be increased to require multifactor authentication which would eliminate brute force ability

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

--Set mobile device authentication token with 6-digit numerical code set to expire every 60 seconds

Mitigation: Detecting the WebDAV Connection

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

--Email to SOC manager directly when any activity is detected on webdav server as it should only be used by 1 individual

What threshold would you set to activate this alarm?

--Guilty on first offense as the ramifications of unauthorized access with read/write ability is devastating

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

--This issue is one that bypasses the SOC team and would fall directly on management to isolate and identify

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

--Set alert and require authorization to write into webdav directory; consider multifactor authentication as well

Mitigation: Identifying Reverse Shell Uploads

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

--Simple alert to SOC team anytime directory and folder are modified in any manner

What threshold would you set to activate this alarm?

--Another serious vulnerability concern; therefore, upon detection, alert should be triggered

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

--Remote access to uploads should be strictly disabled as vpn to internal network is possible to satisfy authorized access

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

--Set strict internal network access to file uploads of any kind with zero exceptions

The End!