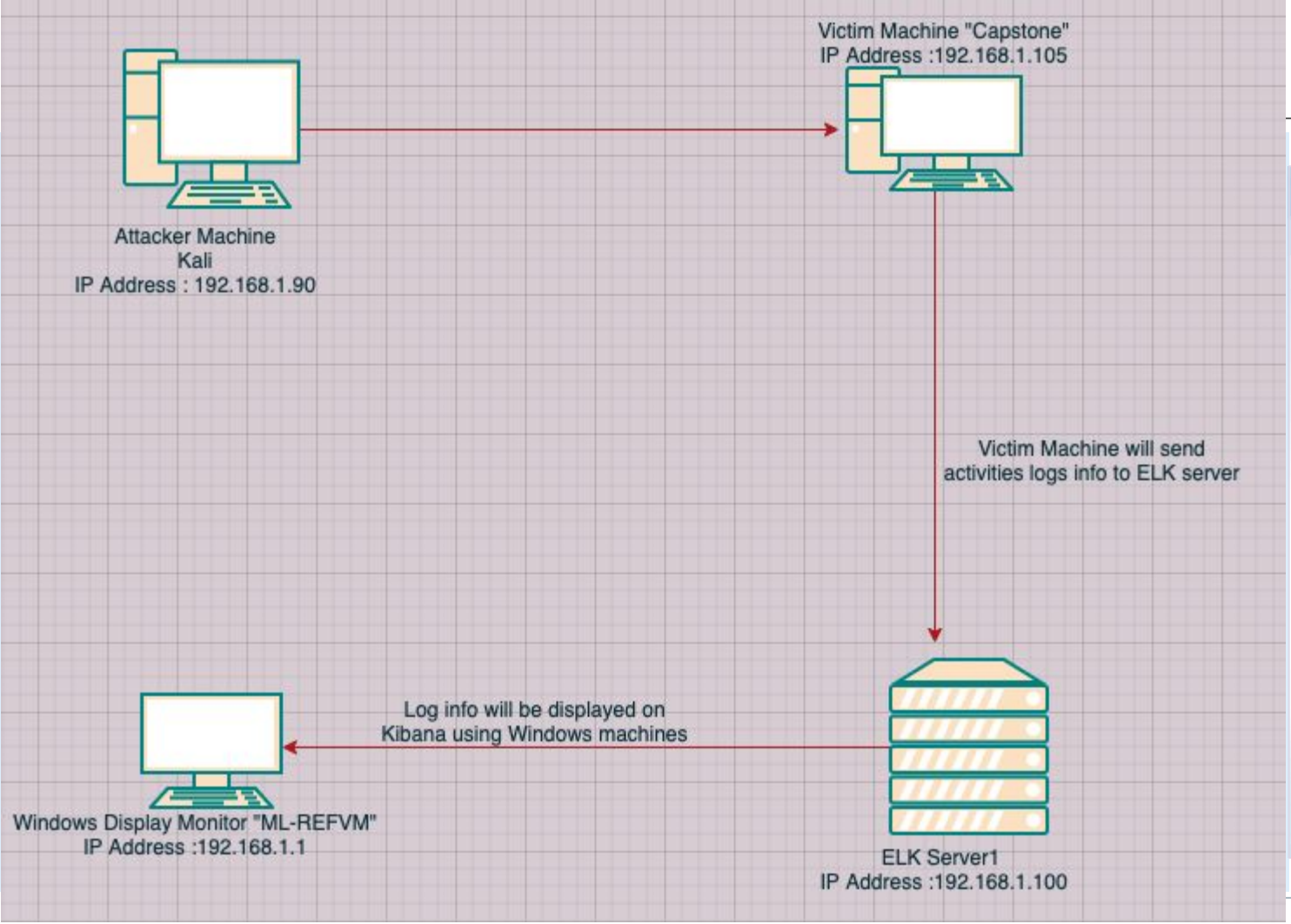
Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology



Network
Address
Range:192.186.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4:192.168.1.90
OS: Linux 2.6.32
Hostname:Kali

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: Linux
Hostname:Elk

IPv4:192.168.1.1
OS: Windows
Hostname: ML-REFVM

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-Refvm-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attacker Machine
Server1 (Capstone)	192.168.1.105	Vulnerable/Victim Machine
ELK	192.168.1.100	Monitoring Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Wordpress vulnerability	*Enumeration of users with wp scan*	*The attacker can have a list of users*
Weak Password.	Brute force	*Gained* access to passwords and the account.
Webdav Software	Allowed accessing the share folder from any machine.	Lead to uploading shell.php file.
Php file upload	Allow the Red Team to execute arbitrary code	Lead to viewing, creating and downloading files and denial of service

Exploitation: Open Port 80

01

Tools & Processes

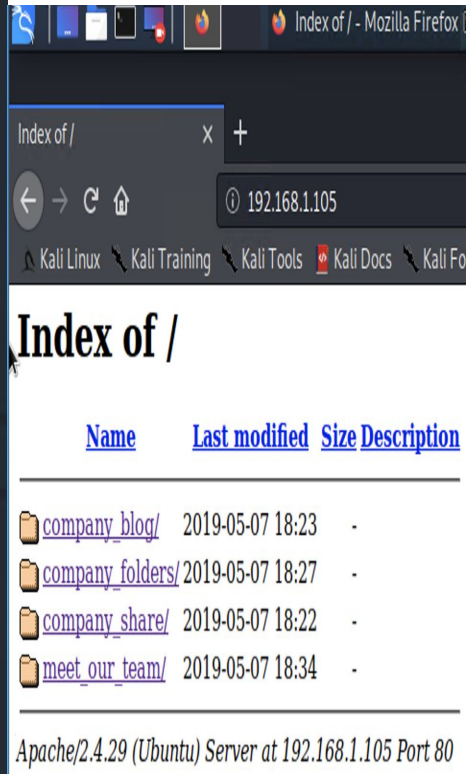
Red team used nmap to scanned for any open ports and service network in Capstone (Victim Machine)

02

Achievements

Nmap scanned gave red team intel about port 80 was open. I opened a web browser to see if there vital information to view on the victim's machine.

```
File  Actions  Edit  View  Help

root@Kali:~/Desktop# cd ~
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-31 19:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00049s 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 (0.00098s 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 (0.00080s 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 (0.000010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.59 seconds
root@Kali:~#
```



Exploitation: [ssh exploit]

01

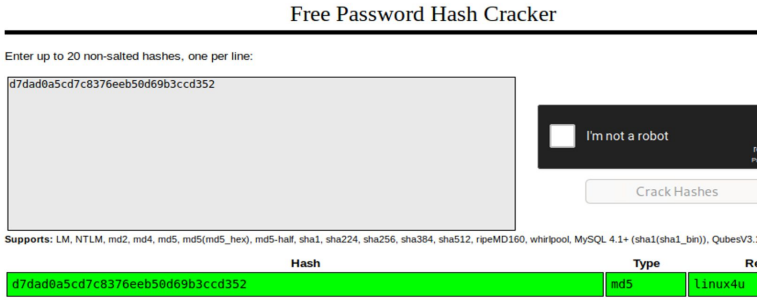
Tools & Processes

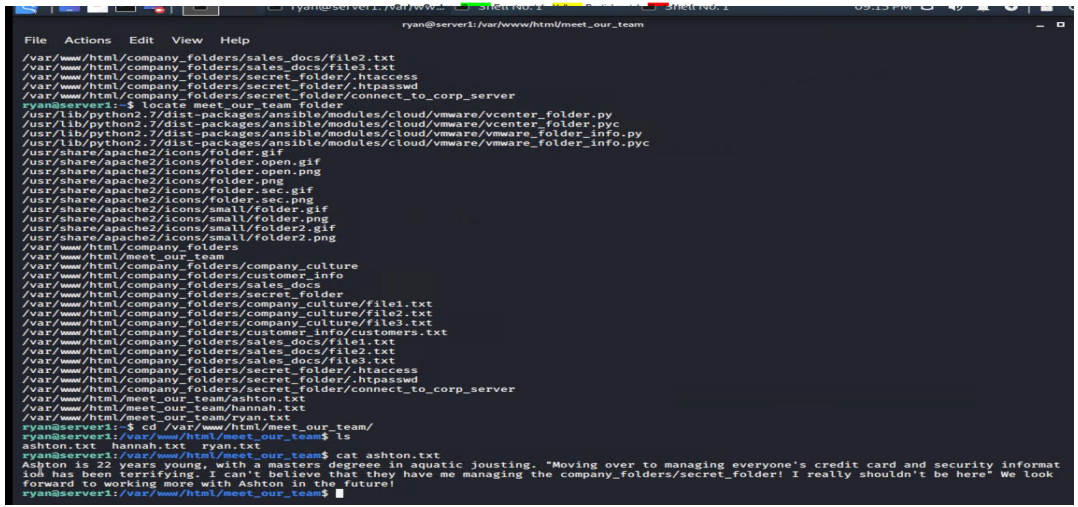
Port 22/tcp was open, Red Team ssh into ryan account using the password from the hash that was cracked by crackstation.net

Achievements

Red Team was able to gain access into ryan's account and was able to locate most of the company's important folders and files.

02





Exploitation: Brute Force Attack

01

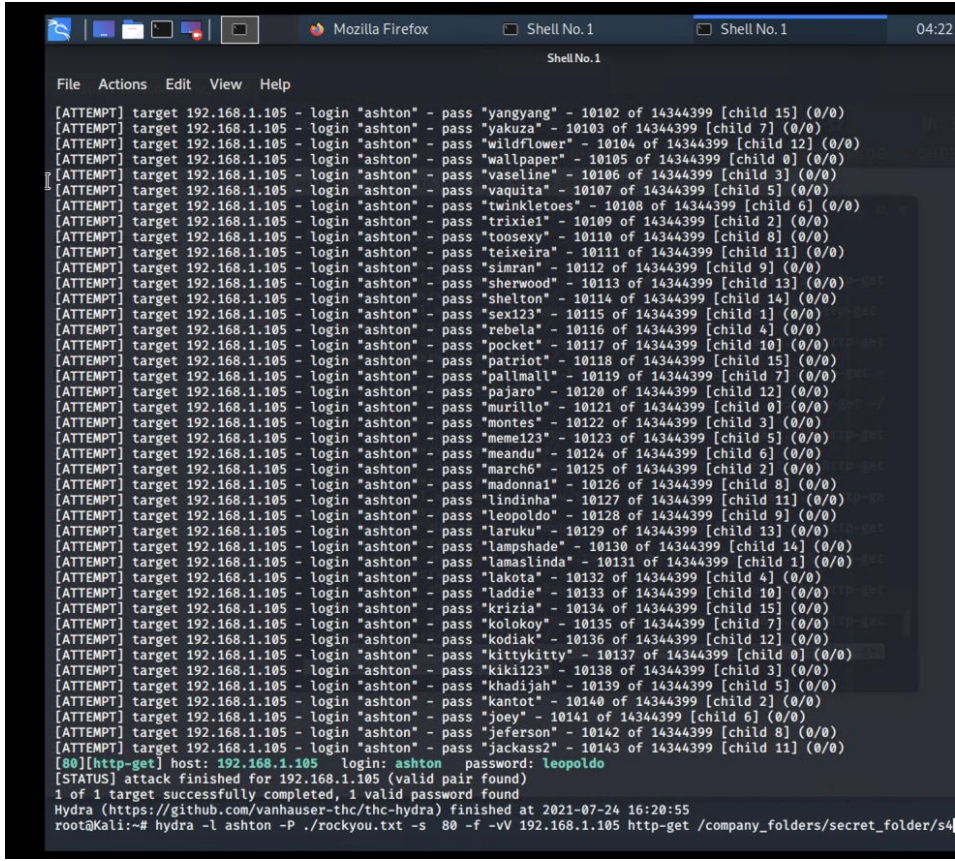
Tools & Processes

Hydra was to Brute force ashton's login credentials: Login:ashton- Password:leopoldo

02

Achievements

The exploit granted red team access to important intel to navigate to secret files.

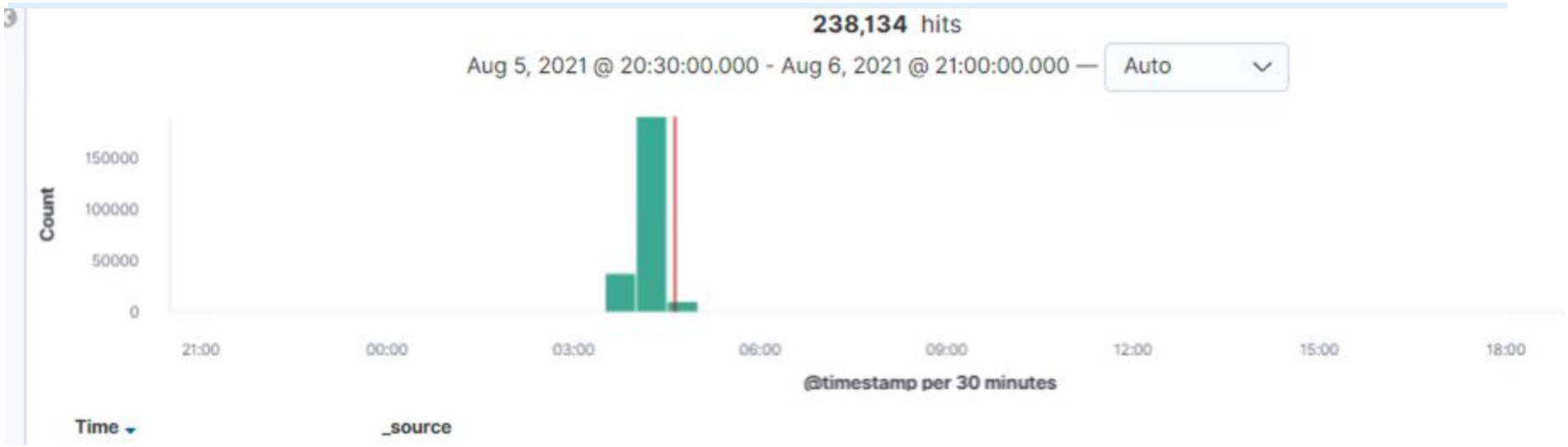


Blue Team

Log Analysis and Attack Characterization

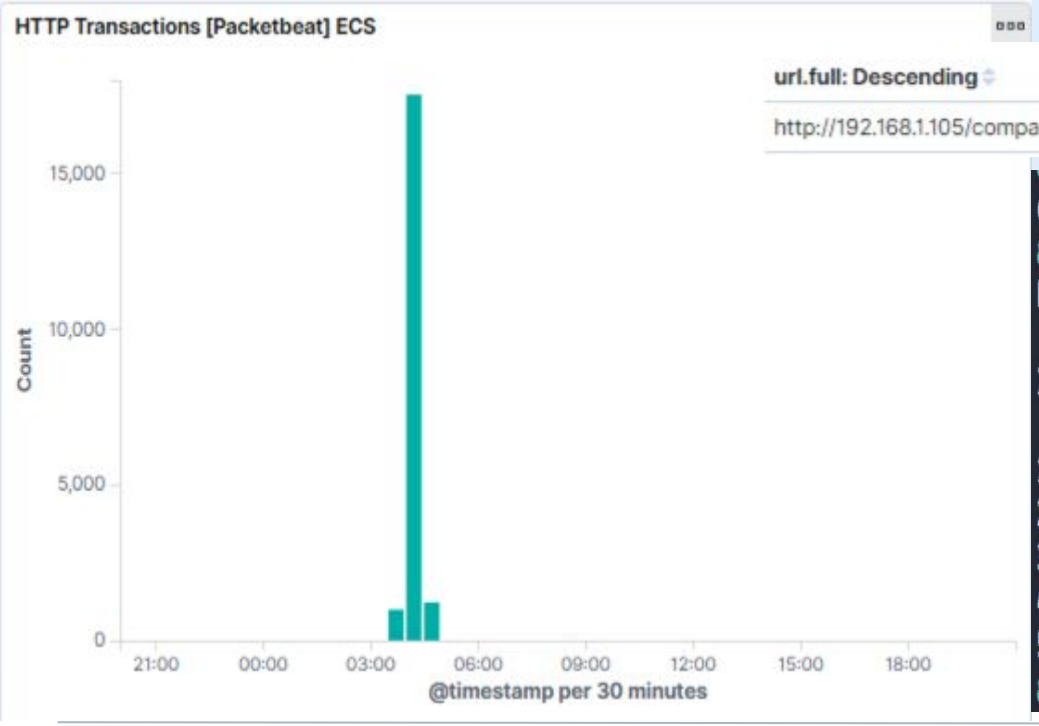
Analysis: Identifying the Port Scan

- The port scan began around 03:00 am
- 238,134 hits were sent from 192.168.1.90
- The nmap ping scan sends request to 443 port.



Analysis: Finding the Request for the Hidden Directory

- 16,362 request were made for the hidden directory at 04:00 am
- Secret_folder were requested which contained instructions on how to access webdav server using ryan's account and hashed password.

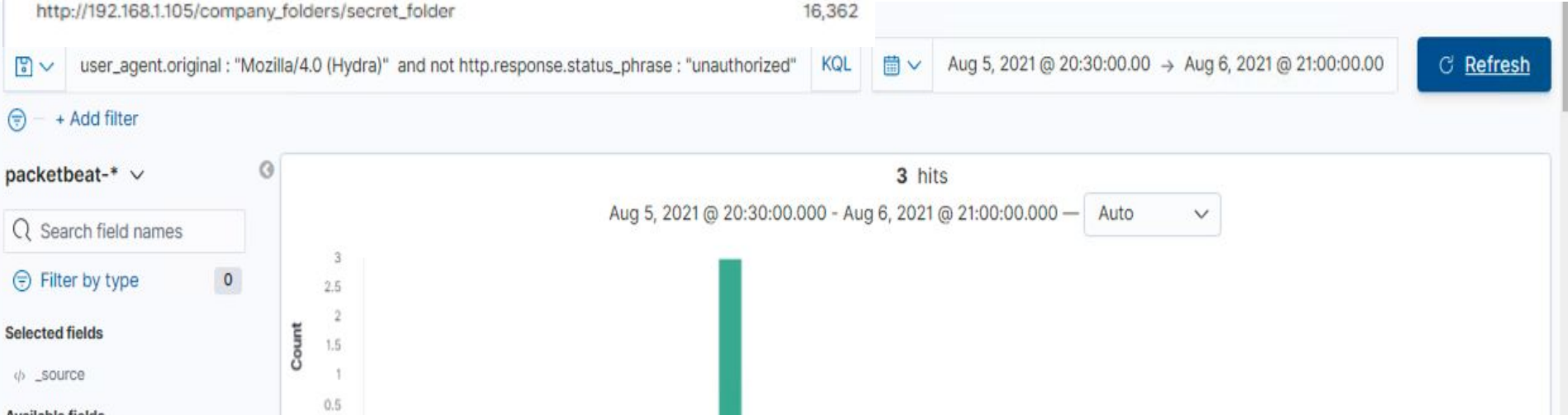


url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,362

```
connect_to_corp_server
ashton@server1:/var/www/html/company_folders/secret_folder$ cat connect_to_corp_server
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd

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
ashton@server1:/var/www/html/company_folders/secret_folder$
```

Analysis: Uncovering the Brute Force Attack

- 16,362 request was made in the brute force attack.
- Out of the 16,362 request , 3 were successful in discovering the password.



Analysis: Finding the WebDAV Connection

- 108 request were made to the Webdav directory.
- The shell.php was requested.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	264
http://192.168.1.105/webdav	108
http://192.168.1.105/webdav/passwd.dav	10

Export: Raw Formatted

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm when there are too many port scan on the target.

Blue Team can set a threshold to activate when there are more than 20 ports scan within 10 minutes.

System Hardening

Close the ports that we don't use and delay port scan, port scan can wait before another scan.

iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP

Mitigation: Finding the Request for the Hidden Directory

Alarm

Strong passwords and put file in encrypted folder.

The threshold can be set to zero for any authorized user who to try to access this folder.

System Hardening

nano /etc/httpd/conf/httpd.conf
* Locate directory section (/var/www/)
and set it as follows:

```
<Directory
/var/www/company_folders/secret_folder
Order allow,deny
Allow from 192.168.1.1
Allow from 192.168.1.105
Allow from 127
Deny from 192.168.1.90
</Directory>
```

Mitigation: Preventing Brute Force Attacks

Alarm

When there's more than 5 wrong/failed password.

Threshold be set at more than 5 failed logins

System Hardening

If the password is not correct for a certain number of time.block the IP address and send a reset link to the authorized user.

We can also display lockout message and locked the page from logins for a temporary for a period of time.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert anytime this directory is accessed by unauthorized user

The threshold should be set to zero attempt.

System Hardening

Connections to shared folders should be restricted and are not accessible on the web interface.

Block connections to the shared folder.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Blue Team can set an alarm for any incoming traffic to port 4444 and set an alert for any .php files that is uploaded to the server

The threshold should be set to more than 1 attempt

System Hardening

Block any file uploads into the server from the web interface.

the End