Capstone Engagement

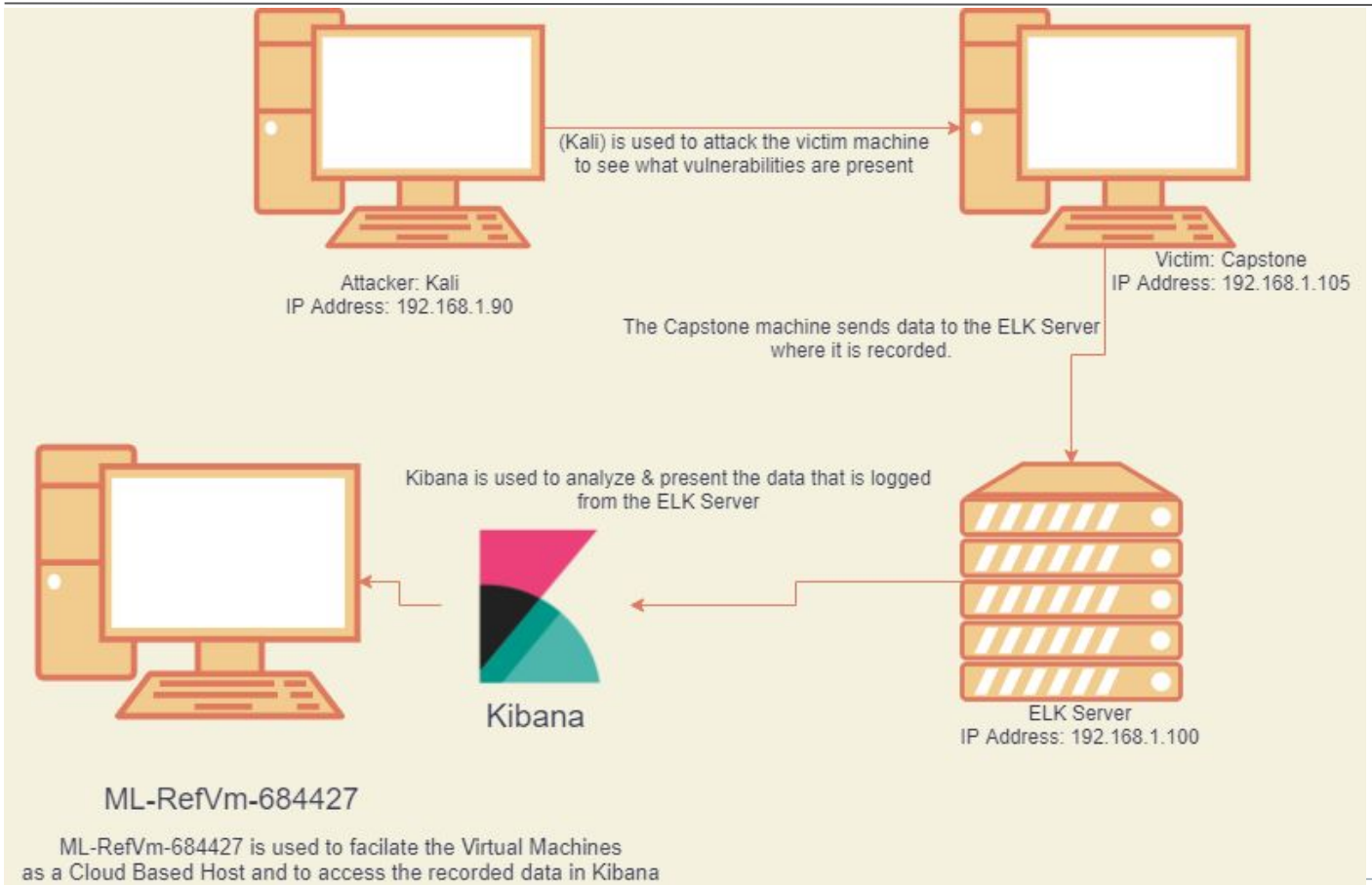
Assessment, Analysis, and Hardening of a Vulnerable System

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: 10.0.0.1

Machines
IPv4:192.168.1.105
OS: Ubuntu 18.04.1
Hostname: Capstone

IPv4:192.168.1.100
OS: 4.15,0,99-generic
Hostname: ELK

IPv4:192.168.1.1
OS: Windows 10
Hostname: ML-RefVm-684427

IPv4:192.168.1.90
OS: 5.4.0-kali3-amd64
Hostname: Kali

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	The Kali machine was used as the attacking machine
Capstone	192.168.1.105	Capstone was used as the victim machine representing a vulnerable server.
ML-RefVm-684427	192.168.1.1	This was used as a Cloud based Host Machine
ELK	192.168.1.100	This was used a monitoring machine for Capstone running Kibana.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 Open on the Network. CVE-2019-6579	Port 80 being open and accessible by anyone attempting to connect to the network.	This allows an attacker to gain access to the machine through the unsecured port 80.
Able to do Brute Force Attacks without lockout	The Machine is able to be attacked through a brute force attack without repercussion by the system.	This allows an attacker to Brute Force their way into a system by being able to input numerous usernames & password.
Had other user's credentials when logging into another user's account credentials stored.	Stores user credentials in plain text.	This allows attackers to easily find out user credentials.
Weak Passwords	A Weak Password is one that is easily detected by humans and computers such as a system default or short password.	The weak password was found in rockyou.txt relatively

Exploitation: Port 80 Open for Public Access

01

Tools & Processes

Nmap was used to scan the network which then lead to discovery of the Capstone machine which then lead to using Nmap to find which ports were open.

02

Achievements

Nmap found out Port 80 was open on the Capstone Machine.

03

Screenshot Belows shows the Open Port 80 from Nmap

```
Nmap scan report for 192.168.1.105
Host is up (0.00069s 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
```

Exploitation: Brute Force Attack Password

01

I used Hydra to Brute Force Ashton's account after finding out Ashton has the Admin account on the Capstone Machine.

02

With Hydra with using the Rockyou.txt wordlist I was able to find out Ashton's password for the ashton account is "leopoldo" which is a weak password.

03

Screenshot Belows shows the result of the Hydra Brute Force Attack on Ashton's account

Exploitation: : LFI Vulnerability

01

Cadaver was used to implant a reverse php shell onto the Capstone Machine.

02

Achievements
Was able to gain root access to the Capstone Machine with the php shell.

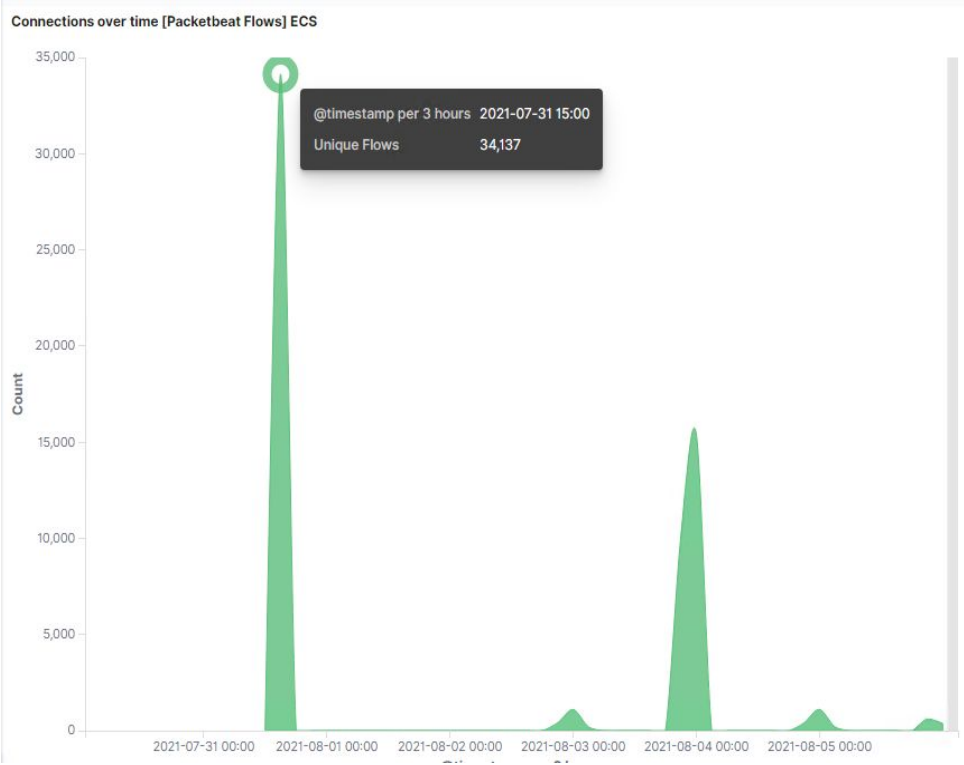
03

Screenshot belows shows the shell.php being uploaded to the Webdav on the Capstone Machine.

```
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> put shell.php
Uploading shell.php to `/webdav/shell.php':
Progress: [=============================>] 100.0% of 1114 bytes succeeded.
dav:/webdav/>
```

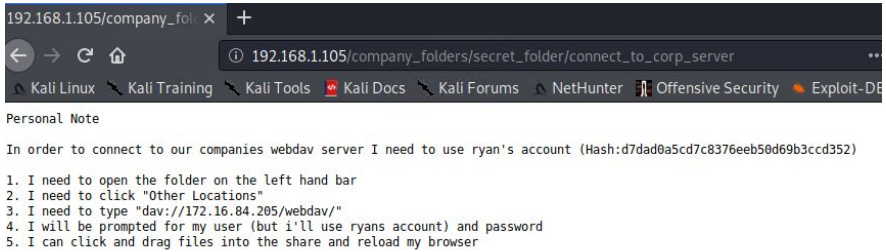
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The Port Scan occurred at approximately on July 31, 2021 at 3PM Local Time
- How many packets were sent, and from which IP? 34,137 were sent and from the IP address at 192.168.1.90
- What indicates that this was a port scan? This indicated as a port scan due to the high volume of traffic attempting connections in a small time window.

Analysis: Finding the Request for the Hidden Directory



- What time did the request occur?The request occurred at 16:16:35 on July 31, 2021.
- How many requests were made? There were 16,176 request made
- Which files were requested? the company_folders/secret_folder/connect_to_corp_server files were requested
- What did they contain? Ryan's account hash which contained his password.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,176
http://127.0.0.1/server-status?auto=	6,718
http://snnmnkxdhflwgthqismb.com/post.php	224
http://www.gstatic.com/generate_204	112
http://ocsp.godaddy.com	51

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 16,176
- How many requests had been made before the attacker discovered the password? 16,175

Top 10 HTTP requests [Packetbeat] ECS

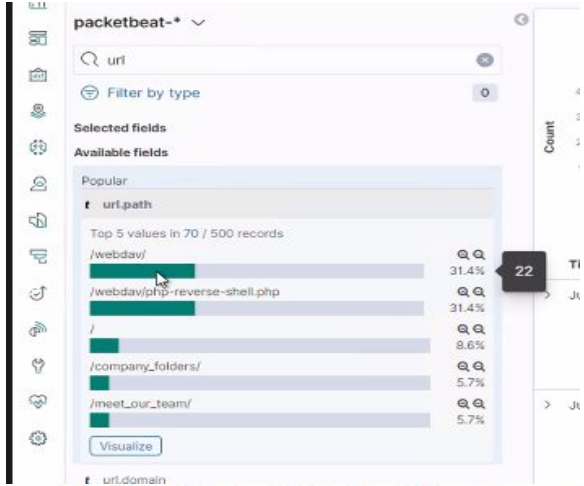
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,176
http://127.0.0.1/server-status?auto=	6,718
http://snnmnkxdhflwgthqismb.com/post.php	224
http://www.gstatic.com/generate_204	112
http://ocsp.godaddy.com	51

> Jul 31, 2021 @ 16:16:34.361 http.request.method: get status: OK url.path: /company_folders/secret_folder @timestamp: Jul 31, 2021 @ 16:16:34.361 client.ip: 192.168.1.90 client.port: 34886 client.bytes: 385B http.request.bytes: 385B http.request.headers.content-length: 0 http.response.status_code: 301 http.response.bytes: 626B http.response.body.bytes: 338B http.response.headers.content-length: 338 http.response.headers.content-type: text/html;

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? 22
- Which files were requested? php.reverse.shell.php



> Jul 31, 2021 @ 17:04:20.911 url.path: /webdav/shell.php http.request.method: put @timestamp: Jul 31, 2021 @ 17:04:20.911 ecs.version: 1.5.0 error.message: Unmatched request server.ip: 192.168.1.105 server.port: 80 client.bytes: 1.3KB client.ip: 192.168.1.90 client.port: 35248 method: put event.kind: event event.category: network_traffic event.dataset: http event.start: Jul 31, 2021 @ 17:04:20.911 network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

The following is An alarm that could be implemented to stop a Port Scan. when the destination.ip is 192.168.1.105 and 1000 TCP connections are made in an hour

System Hardening

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

1. Run a port scan ever so often to be able to see and close down any unwanted open ports.
2. Make sure to keep the firewall up to date and install any patches.
3. Install an Intrusion Detection System such as Splunk or Kibana to get alerted when a port scan is most likely occurring.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm that would help in alerting hidden directory requests would be an alarm is triggered when 5 requests to the hidden directory are made in an hour.

System Hardening

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

1. Edit configuration files to only allow trusted IP Addresses being able to access the hidden directory.
2. Enable encryption on sensitive data such as the Hidden Directory
3. Disable the Directory from being listed.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
An alarm that could be used to alert of a Brute Force Attack is to send out an alert any time a 401 Event Code comes back.

System Hardening

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

1. Implement a 30 minute scaling lockout after 5 unsuccessful login attempts.
2. Implement a strong password policy for all accounts.
3. Use a Captcha to determine the attempts are from a Machine or Human.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Create a whitelist of trusted IP Addresses & then proceed to make an alarm that alerts when there is an HTTP GET or HTTP PUT request from an IP Address not on said trusted whitelist.

System Hardening

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

1. Create a whitelist of trusted IP Addresses in the httpd.conf file in WebDAV section.
2. Make a strong password policy for the trusted IP Addresses with access.
3. Deny all connections to the WebDAV not from the trusted IP list.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
An alarm that can be used is an alert that is sent out whenever there is a *PUT* request in the WebDAV folder from a non-whitelisted IP Address.

System Hardening

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

1. Set a Deny All to all connections unless from a trusted IP Address.
2. Make WebDAV read only to discourage uploading a payload to the WebDAV.


The End