Red vs Blue Project

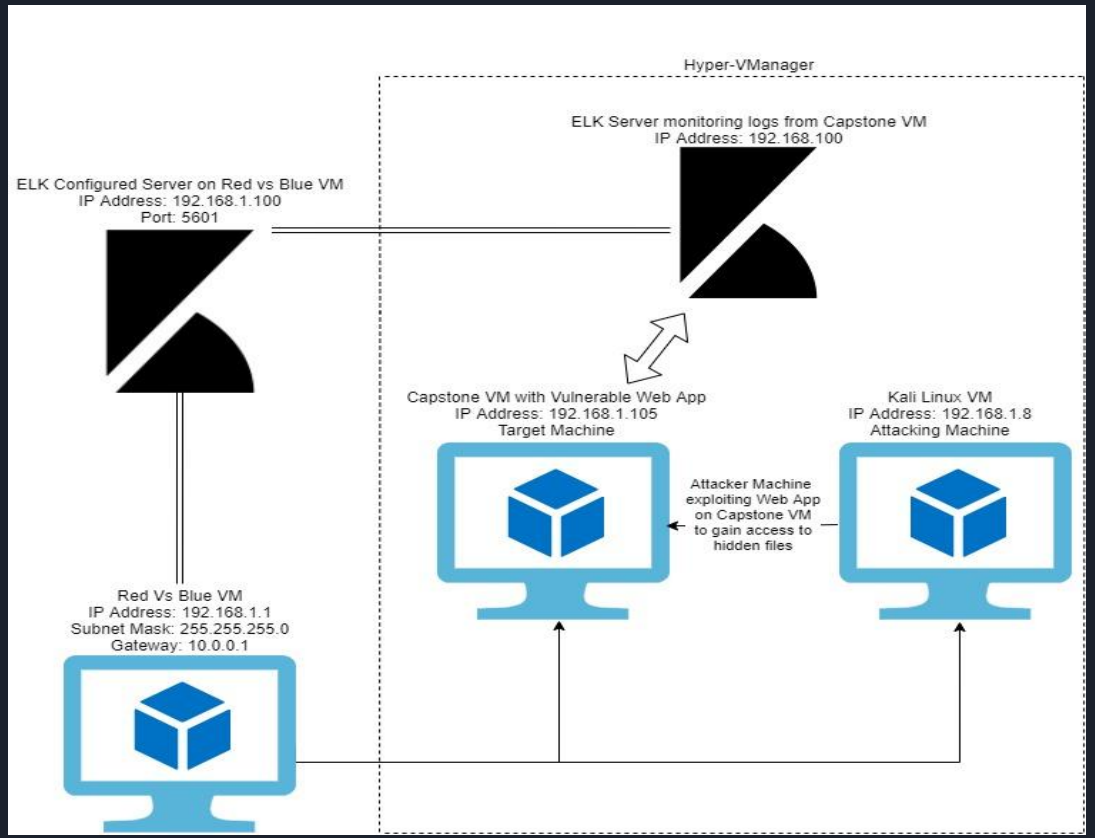
By: Taimur Khan

Purpose of Project

This project is designed to showcase both sides of a cyber security incident/ breach. The strategies of the offensive team, the hackers trying to gain access to hidden files, and the defensive team, cybersecurity professionals tasked to monitor logs for a potential attack, will be explored. This project is being done in a test environment so the network will also be explained and how the machines communicate with one another.

Network Topology

This is configured on a Azure Cloud Virtual Network. The Red vs Blue Virtual Machine (192.186.1.1) houses the ELK configured server on the designated Port 5601 to access the Kibana interface. Hyper-V Manager houses all the VMs to create a closed environment for testing. Capstone VM (192.168.1.105) has the vulnerable Web application that will be exploited by the Attacking Kali machine (192.168.1.8).



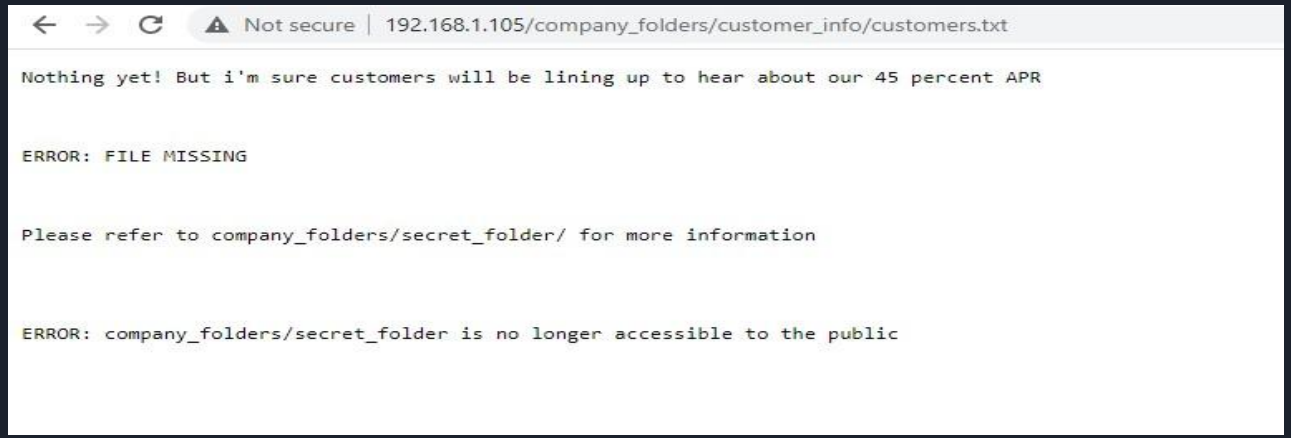
Red Team Attacking

The vulnerabilities discovered are some of the critical ways a hacker can exploit this system

1. Access Restriction for Users
2. Responding to Unknown Requests
3. Brute Force Attacks

Access Restriction for Users

This directory should not be accessible by customers. This gives the hacker enough information in the recon phase of the kill chain to figure out ways to exploit the system. This is a critical vulnerability because now the hacker has a target to focus on.



Responding to Unknown Requests

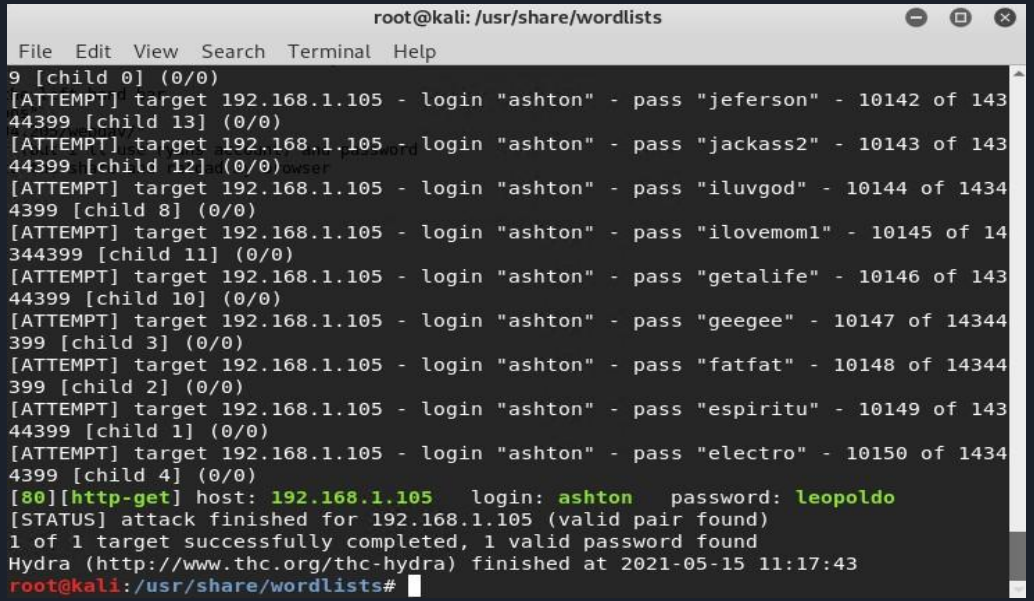
The CapStone machine must not respond to unknown network requests. This is a critical vulnerability because the attacker now has identified how to send a payload tailored specific to the service and version of the server.

```
root@kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-23 15:49 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00089s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.62 seconds
```

Brute Force Attacks

With the information gained from the recon phase, a company user has now been targeted to leverage the system further. Brute Force attacks are a critical vulnerability because it shows that password policies are not being followed so easy passwords can be used by hackers.



Blue Team Defending

The Blue Team must monitor logs and investigate any suspicious behaviour relating to:

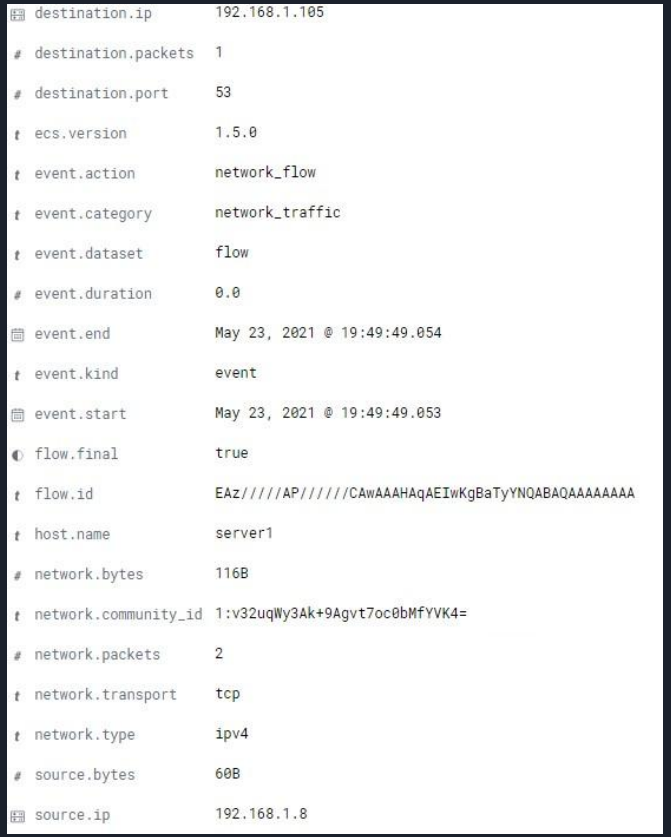
1. Access Restriction for Users
2. Responding to Unknown Requests
3. Brute Force Attacks

Access Restriction to Users

The CapStone VM is running a Web Application for the company and it has a directory with sensitive information in it. Below is evidence of a hacker gaining information through the web application. This directory containing customer information should not be on the same server as the Web Application. Customer data must always be protected and monitored to preserve privacy.

Responding to Unknown Requests

Here is a response and request from the Attacking Kali Machine to the CapStone VM. Unknown IP addresses should not get any response from the server. IP Addresses can be restricted to trusted sources only. TCP traffic should be monitored for this data.



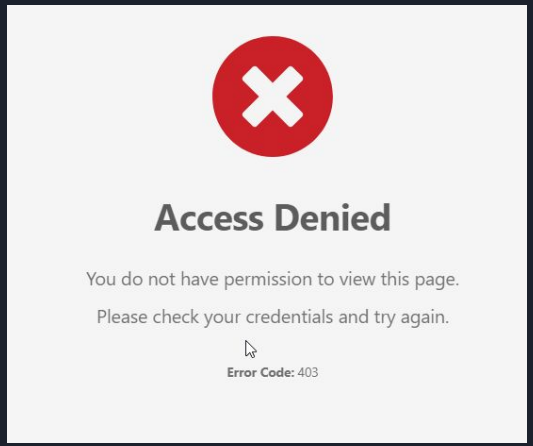
destination.ip	192.168.1.105
destination.packets	1
destination.port	53
ecs.version	1.5.0
event.action	network_flow
event.category	network_traffic
event.dataset	flow
event.duration	0.0
event.end	May 23, 2021 @ 19:49:49.054
event.kind	event
event.start	May 23, 2021 @ 19:49:49.053
flow.final	true
flow.id	EAz/////AP//////CAwAAAHAqAEIwKgBaTyYNQABAQAAAAAAAA
host.name	server1
network.bytes	116B
network.community_id	1:v32uqWy3Ak+9Agvt7oc0bMfYVK4=
network.packets	2
network.transport	tcp
network.type	ipv4
source.bytes	60B
source.ip	192.168.1.8

Brute Force Attacks

This search query shows 10,042 attempts to get into the secret folder. Brute Force Attacks send numerous requests to try and hack the system. HTTP traffic would need to be monitored to make sure numerous requests are not being made in short amount of time.

Mitigation : User Restriction

Users' roles must be configured with appropriate permissions and access to minimize the chance of the system being compromised. Customers on a website should not be able to view sensitive information relating to the internal structure and policies of a company. Additionally, company employees also should not have a lot of freedom within the system, since internal attacks are possible too. It is the job of the system administrator to configure permissions properly so that customers only see information relating to their role and employees are only allowed limited access throughout the network. An alert can be used to notify system admins that someone is trying to access confidential directories.



Mitigation: Unknown Requests

A company server should be on a private network that only responds to trusted sources which allows for less chance of being noticed by external users. Any requests being made to the server should be timed out as this would mean that they are not allowing requests from unknown IPs. Furthermore, an Intrusion Detection System and Intrusion Prevention System can be configured to monitor packets of network traffic to add another layer of security if any malicious packets get through. These can alert system admins that there is someone trying to get a response from the private server.

Mitigation: Brute Force Attacks

To minimize instances of brute force attacks, the system can be configured to not allow multiple logins within a short amount of time. Account lockout can also be used so when a threshold is met, the account is locked for a specified amount of time. Designing strong password policies is also key this includes complexity and length of the password so simple passwords cannot be cracked. An alert should be set up so if a hacker is trying to gain access to the system via Brute Force, the system admin is notified of a potential attack according to the number of logins in a short time span.

Conclusion

It is vital to understand how a system can be exploited from a defending and attacking perspective because a cybersecurity professional should always be adding new skills to ensure the standard of security practices is being met.