Capstone Engagement

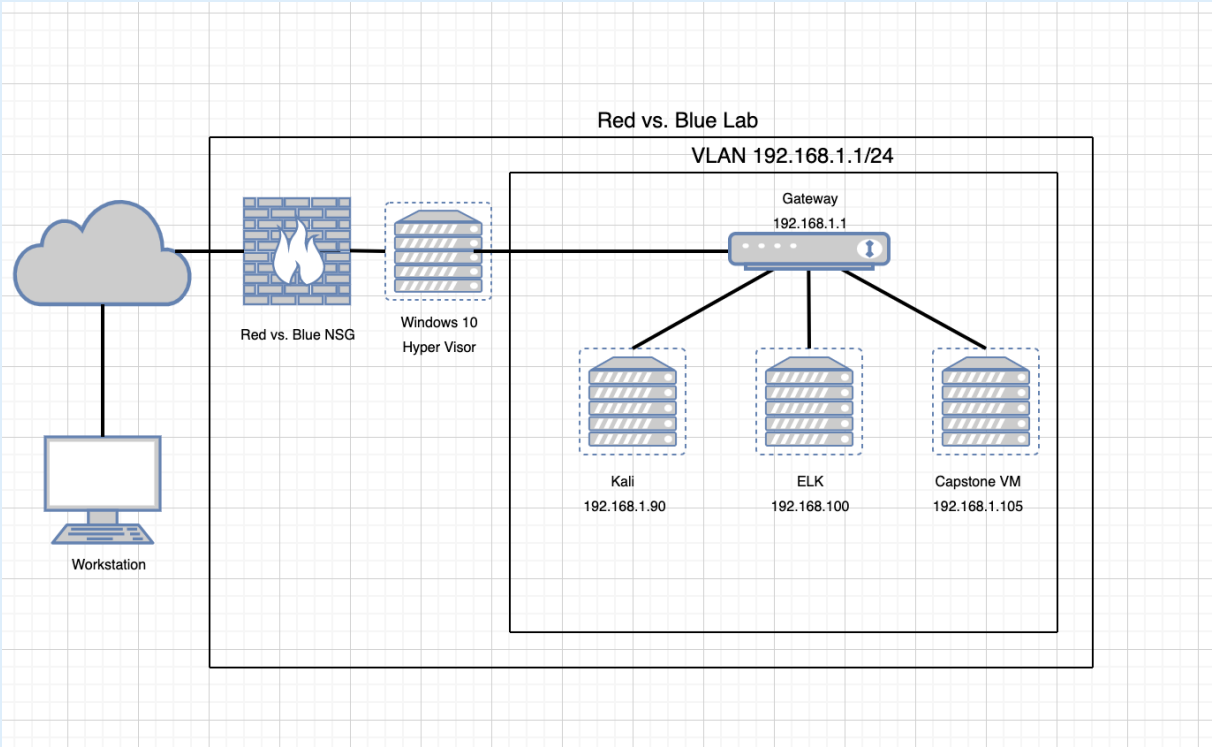
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



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

Machines
IPv4:192.168.1.90
OS:Kali-Linux-2020.1
Hostname:Kali

IPv4:192.168.1.100
OS:Kali-Linux-2020.1
Hostname:ELK

IPv4:192.168.1.105
OS:Kali-Linux-2020.1
Hostname:Capstone

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	Attacker
Capstone	192.168.1.105	Victim
ELK	192.168.1.100	Network Monitor
Gateway	192.168.1.1	Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Exposure of Information Through Directory Listing	A directory listing provides an attacker with the complete index of all the resources located inside of the directory.	Exposing the contents of a directory can provide useful intel for the attacker to find an entry point to the server via exposed credentials, as well as provide information that would allow the verification or creation of exploits.
Unrestricted Upload of File with Dangerous Type	The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.	Arbitrary code execution is possible if an uploaded file is interpreted and executed as code by the recipient. This is especially true for .asp and .php extensions uploaded to web servers because these file types are often treated as automatically executable.
Improper Restriction of Excessive Authentication Attempts	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.

Exploitation: Exposure of Information Through Directory Listing

01

Tools & Processes:

Nmap - Used to initially map the network.

FireFox - Used to explore directory listings on misconfigured Apache web server.

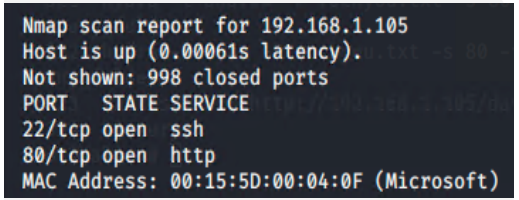
02

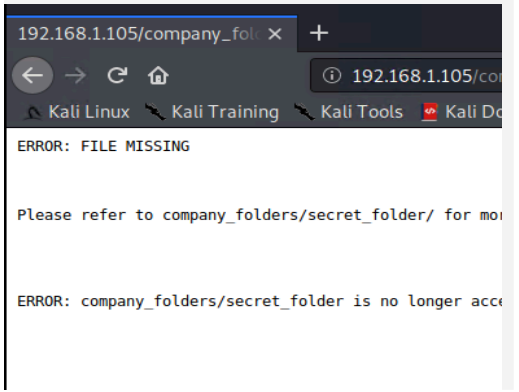
Achievement:

Discovered open port on victim machine that allowed exfiltration of sensitive data:

- location of secret folder
- user credential exposure

03





Exploitation: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes:

Hydra – Used to brute force http authentication of secret folder on web server.

Using the information (username) disclosed by previous vulnerability, in combination with a list of common passwords allowed trivial bypass of http authentication.

02

Achievements:

Discovered sensitive information:

- service disclosure (WebDAV)
- credential exposure

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
```

Exploitation: Vulnerable web service

01

Tools & Processes:

DAVTest - tests WebDAV enabled servers by uploading test executable files, used to quickly and easily determine if enabled DAV services are exploitable.

CaDAVer - used to transfer reverse-php-shell.php

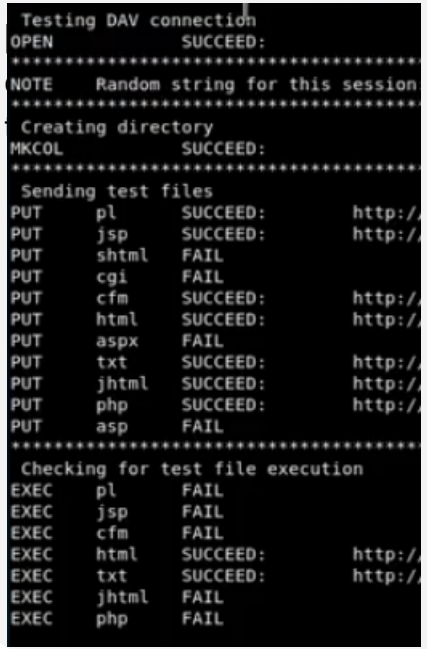
Firefox – Used to initiate reverse shell connection.

02

Achievements:

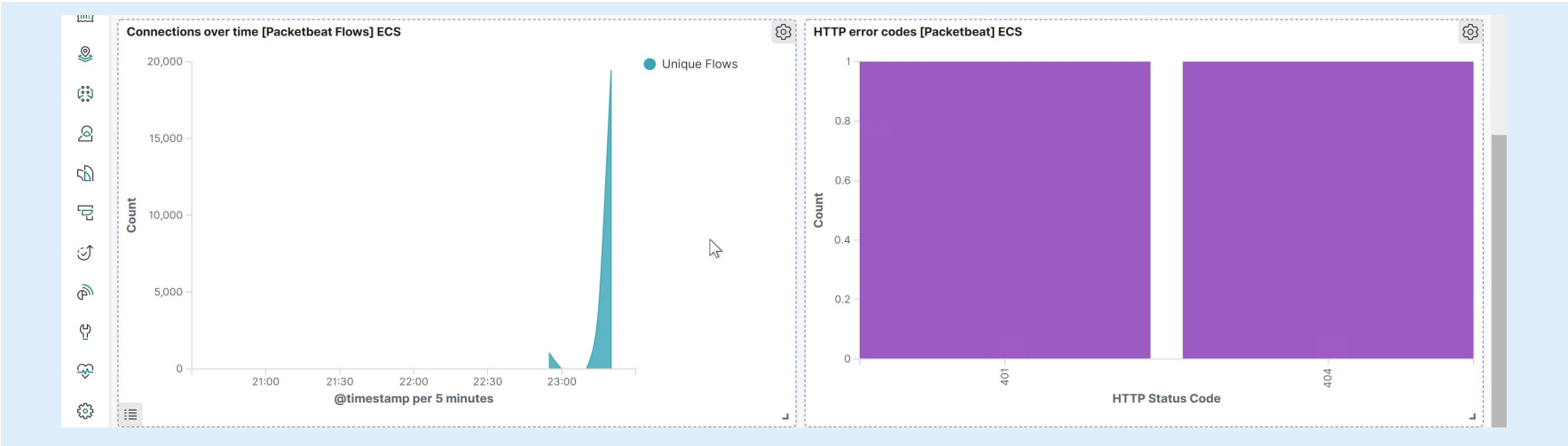
Shell was achieved on target machine via reverse connection, target data retrieved successfully.

03



Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Port scan initiated @ 2020-11-06T22:58:48.780
- 1245
- 50 connections in a 30 second timeframe, each using a different port against another host.

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/	16,361
http://192.168.1.105/favicon.ico	83
http://192.168.1.105/company_folders/	82
http://192.168.1.105/	34
http://192.168.1.105/webdav/	28

Export: Raw Formatted

- Initial requests were made @ 23:10:11.200 on November 6th, 2020
- File1.txt was requested. It contained WebDAV credentials used to further exploit the server.

Analysis: Uncovering the Brute Force Attack

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	1.9GB	38.3MB
192.168.1.90	192.168.1.105	50.4MB	90.8MB

Export: Raw Formatted

Top Hosts Creating Traffic [Packetbeat Flows] ECS

- 16,361 total requests were made during the attack.
- 16,353 requests were made before a successful login was found.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,361
http://192.168.1.105/favicon.ico	83
http://192.168.1.105/company_folders/	82
http://192.168.1.105/	34
http://192.168.1.105/webdav/	28

Export: Raw Formatted

- 28 total requests were made.
- Attacker requested a file name reverse-php-shell.php

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

A threshold alert can be configured to detect port scans on the network and monitors resource usage for anomalies.

Define the threshold of a likely port scan as more than 50 connections in a 30 second timeframe, each using a different port against another host.

System Hardening

Condition to trigger alert for port scanning:

```
"condition": { "script": { "inline":
"for (int i = 0; i <
ctx.payload.aggregations.by_src_ip.b
uckets.size(); i++) {for (int j = 0;
j <
ctx.payload.aggregations.by_src_ip.b
uckets[i].by_target_ip.buckets.size(
); j++) {if
(ctx.payload.aggregations.by_src_ip.
buckets[i].by_target_ip.buckets[j].u
nique_port_count.value > threshold)
return true;};};return false;",
"params": { "threshold": 50 } } }
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

A log threshold alert can be used to detect future malicious requests for confidential files and directories.

System Hardening

Dissallow directory listing browsing via .htaccess rule

<Options -MultiViews –Indexes>

Mitigation: Preventing Brute Force Attacks

Alarm

Set to trigger when repeated attempts to login fail.

Threshold set at 10 failed login attempts.

System Hardening

Temporarily block users after failed login attempts, permanently block repeat offenders.

Implement an intrusion prevention system, fail2ban or similar.

Mitigation: Detecting the WebDAV Connection

Alarm

Alert on high resource usage, concurrent logins, and failed login attempts.

System Hardening

- Instruct users to never share credentials.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set to detect interactive terminal spawned via php process.

System Hardening

.htaccess can be configured to block execution of uploaded reverse shells.

<Files *.php> Deny from All </Files>