Capstone Engagement

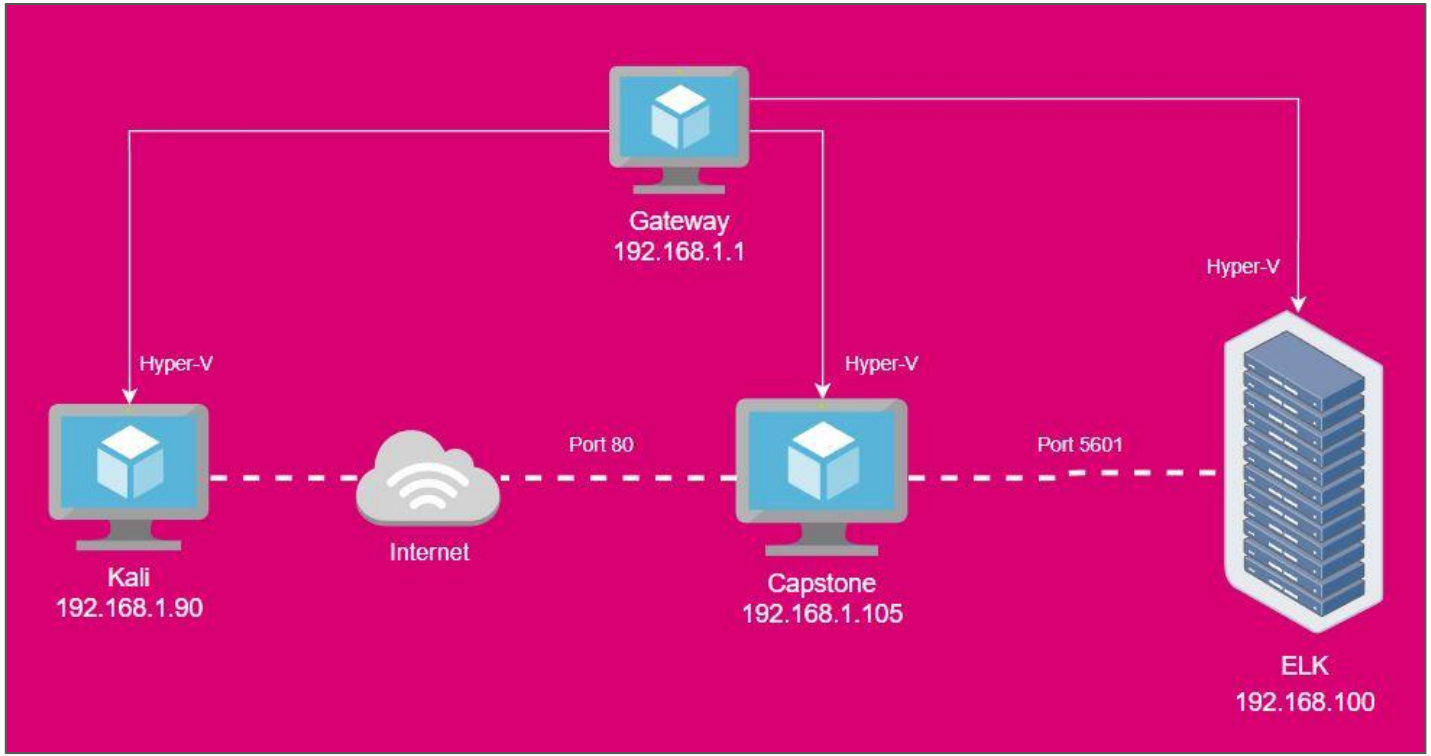
Assessment, Analysis, and Hardening of a Vulnerable System

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:192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Gateway

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Gateway	192.168.1.1	Gateway to 3 VM machines
ELK	192.168.1.100	ELK Log Server
CAPSTONE	192.168.1.105	Target Machine
Kali	192.168.1.90	Attacking Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Public-Facing Sensitive data	Files alluding to existence of a secret folder within the web server.	Gives attackers incentive to probe for more sensitive data.
Brute Force Attack and Hash Cracking	Attackers can use programs to guess login credentials or decrypt password hashes to gain credentials.	Discovered credentials can be used to potentially access sensitive data on the web server.
Web Misconfiguration	Security controls are not in place to restrict who can upload files to the web server.	Attackers can upload and plant malware to later be used on the server.
Local File Inclusion (LFI)	Allows local files to be read and/or executed on the target machine itself.	Attacker can execute the planted malware file to potentially gain a reverse shell on the web server.

Exploitation: Public-Facing Sensitive Data

01

Tools & Processes

-Nmap was used to scan the network for the target server

-dirb was used for site mapping to find URLs on the target site

-Web Browser was used to navigate through the web server's site.

02

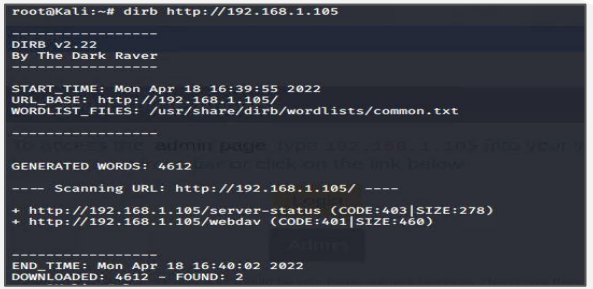
Achievements

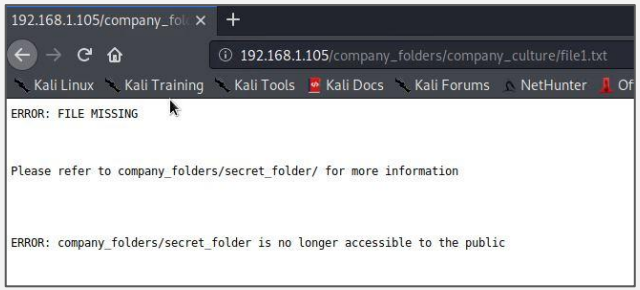
Nmap exposed the IP Address of the target machine which was input into a web browser to browse the server.

Dirb revealed an important URL on the server: "/webdav"

Using the web browser, searching through the web site revealed the existence of a secret folder only accessible by employees.

03





Exploitation: Brute Force and Hash Cracking

01

Tools & Processes

-Hydra was used to successfully brute force the credentials of an employee.

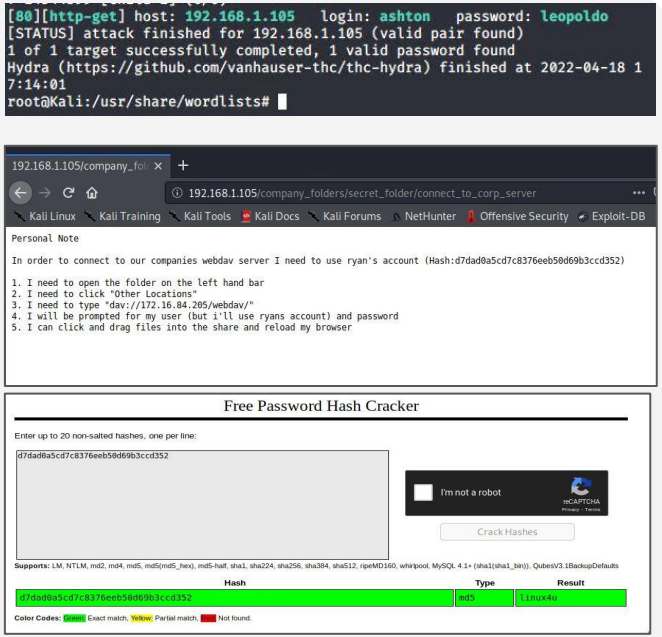
-Crack Station was used to successfully crack the hash that was given in the file “connect_to_corp_server”.

02

Achievements

With the credentials, the secret folder was access and this revealed a file with instructions on how to access the corporate server.
The instructions included a username:ryan and a password hash. Crack Station was used to successfully crack the password for ryan.

03



Exploitation: Web Misconfiguration

01

Tools & Processes

After logging in as Ryan, privileges were escalated and it was possible to upload a php shell script to execute a reverse shell

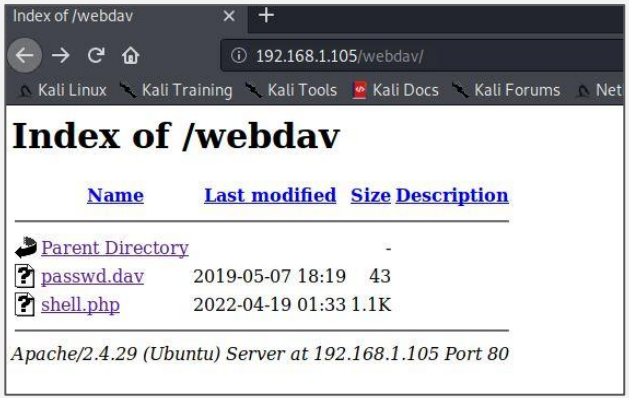
***Note: Even though privileges were escalated to gain ability to enable uploading, it can be considered a misconfiguration because it can be argued that the CEO does not need to have this kind of access.

02

Achievements

This exploit allowed the user to drag and drop a php shell script onto the server.

03



Exploitation: Local File Inclusion

01

Tools & Processes

-Metasploit was used in conjunction with the php shell script that was uploaded in the previous exploit.

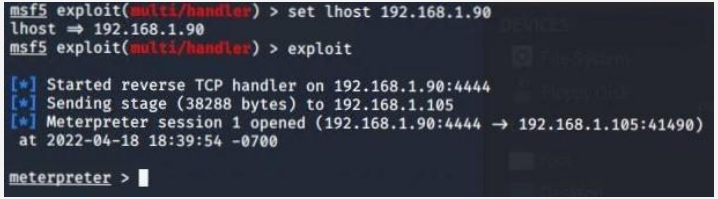
02

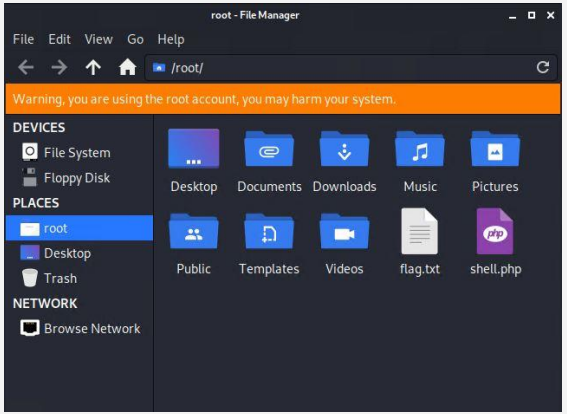
Achievements

This exploit allowed us to start a meterpreter session, which was then used to establish a shell in the target machine.

A file named “flag.txt” was then captured and downloaded to the Kali machine.

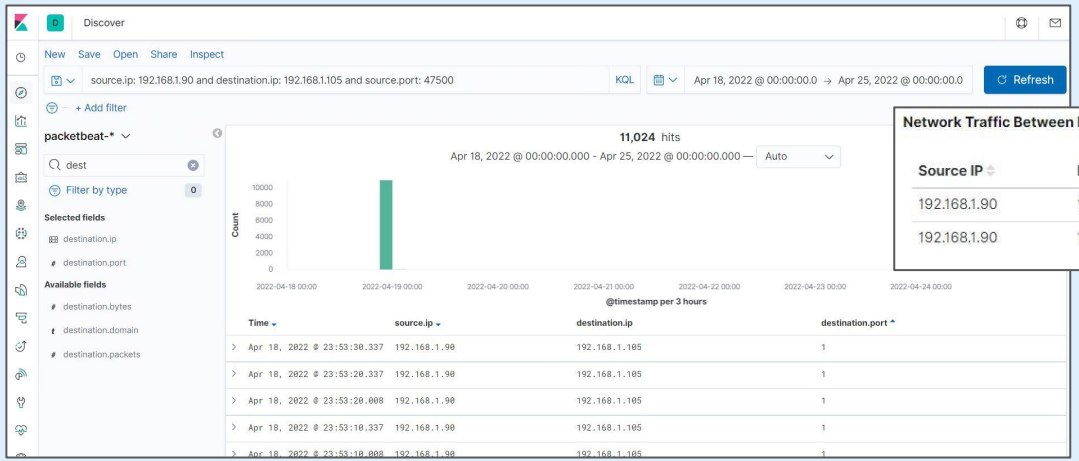
03





Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

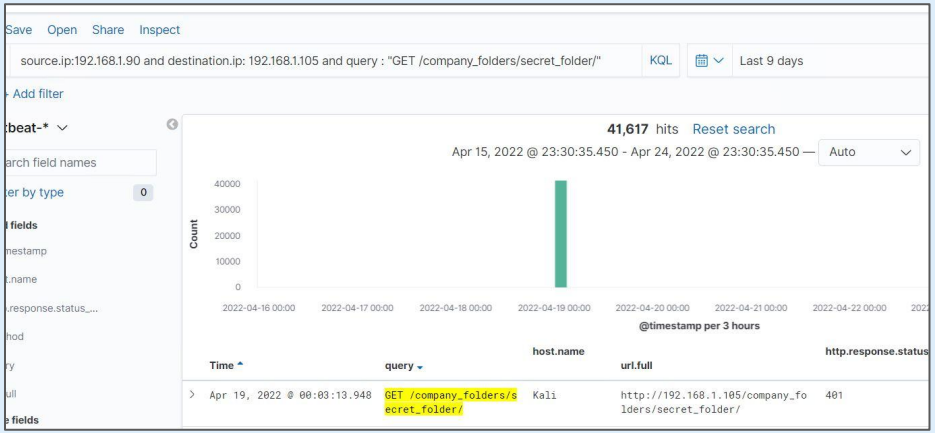


Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.105	657KB	622.1KB
192.168.1.90	104.26.7.139	16.3KB	249.3KB

- The port scan occurred at 11:53 pm
- 11,024 packets were sent from 192.168.1.90
- The top network traffic and top host creating traffic was from IP: 192.168.1.90. Filtering by destination port it can be seen that this machine is sending packets to most ports starting with port 1 and working its way up.

Analysis: Finding the Request for the Hidden Directory

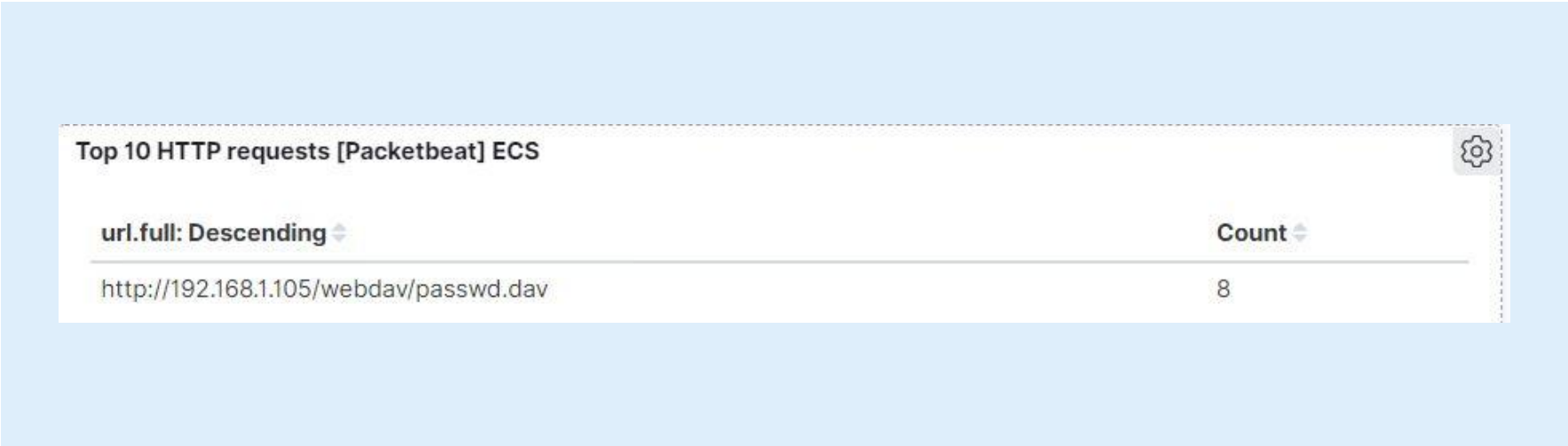


- The request occurred at 12:03am
- 41,617 requests were made
- The file “connect_to_corp_server” was requested. This file contained instructions on how to access the “webdav” server.

Analysis: Uncovering the Brute Force Attack

- 41,610 requests were made in the attack
- 41,609 requests were made before the attacker discovered the password.
- ***Note the other 7 requests were subsequent logins after gaining access.

Analysis: Finding the WebDAV Connection



- 8 requests were made to this directory
- The files that were requested were “shell.php” and “passwd.dav”

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Alarms can be set to trigger once a certain number of ports receive an arbitrary number of tcp packets within a set amount of time from the same IP Address.

The threshold to activate this alarm should be more than 100 ports receiving traffic from the same IP within 1 minute.

System Hardening

A firewall can be configured to recognize scans and block them. To harden against ICMP host discovery scans, simply filter inbound ICMP traffic.

For TCP scans, use rate limits to impede the scanning process. Once detected, the IP of the violators can be black-listed. Even if they try from another IP it will continue to blacklist before the scan is complete.

Setup Anti-spoofing rules to reject packets with a private spoofed IP.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm can be set to detect any unsuccessful http status codes for the query “GET /company_folders/secret_folder/” or any login from unauthorized IP Addresses.

The threshold should be when this resource is unsuccessfully requested more than 100 times within 5 minutes from unauthorized.

System Hardening

The most effective solution would be to first reconfigure the web server to remove any public-facing mention of the existence of a hidden directory.

Next, the hidden directory can have a list of white-listed IP Addresses that are allowed to connect to in addition to login credentials.

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm can be set to detect an arbitrary number of failed login attempts for access to any part of the web server.

Given the confidentiality implied with having “secrets” on the webserver the threshold for the alarm should be a strict 3 failed login attempts.

System Hardening

A solution to harden against a brute force attack is to lock out accounts when the threshold of 3 failed login attempts is met.

Mitigation: Detecting the WebDAV Connection

Alarm

Set an alarm to alert when the WebDAV directory is being accessed outside of normal working hours like between 9pm and 5am.

The threshold for this alarm should be every instance of this criteria being met.

System Hardening

A solution to harden against this vulnerability is to segment access to this directory to only certain white-listed IPs.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alarm can be set to alert when an attempt to upload a .php file occurs.

The threshold should be any instance that meets the criteria.

***If the server language changes, be sure to adjust this alarm to detect whatever language the server is built upon.

System Hardening

A solution to hardening the system against Reverse Shell Uploads is to restrict uploads to only whitelisted IPs and requiring multi-factor authentication in the form of a soft token in addition to password. Since files should not frequently be uploaded, this should be a viable option.


The End