Penetration Testing Report

Assessment, Analysis, and Hardening of a Vulnerable System

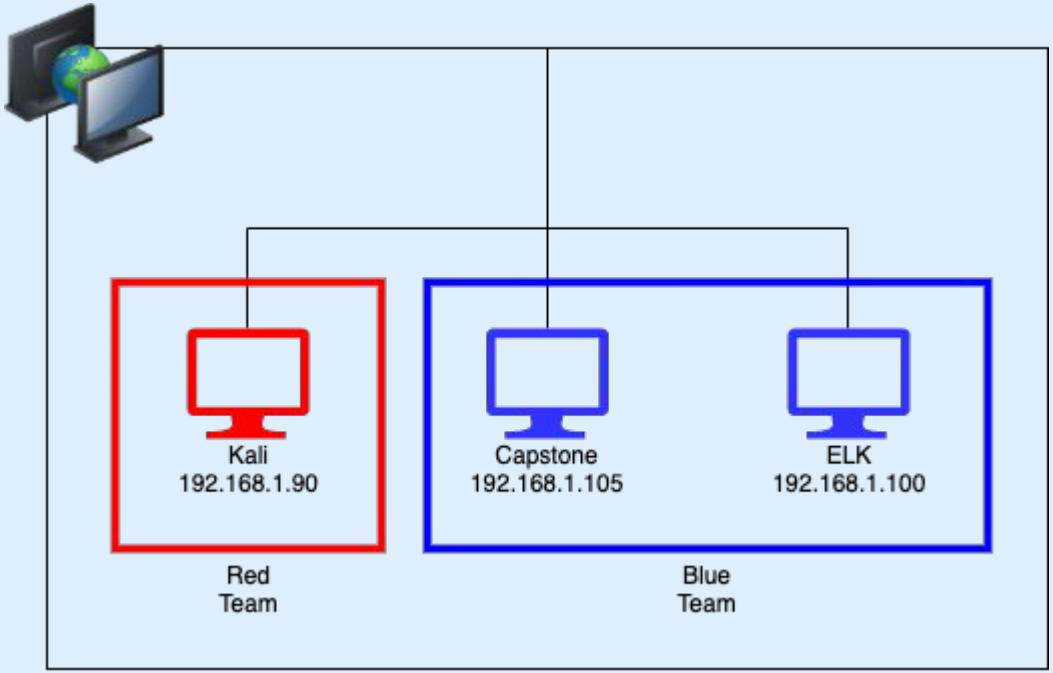
Ben Paris

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

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

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	Provide public browser access to the corporate repository
ELK	192.168.1.100	Provide browser accessible interface for log analysis and aggregation

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration	The ‘secret_folder’ is publicly available despite not being listed in the ‘company_folders’ directory.	Any user can navigate to the hidden directory, see the critical hint, and initiate a brute force attack.
Brute Force Vulnerability	Authentication for the ‘secret_folder’ directory does not limit failed login attempts.	A brute force attack will succeed in gaining unauthorized access to the ‘secret_folder’.
Sensitive Data Exposure	The content within the the easily broken ‘secret_folder’ gives the credentials for the webdav directory.	With access to the ‘secret_folder’ attackers also gain full access to the webdav directory.
Unauthorized File Upload	After breaking into the ‘secret_folder’ directory attackers will have the ability to upload and manage the webdav directory	Attackers could use this access to initiate a number of attacks by uploading malicious payloads.

Exploitation: Security Misconfiguration

01

Tools & Processes

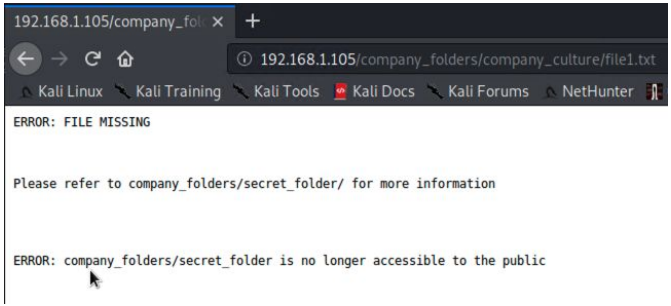
Using any internet browser to look at the different files on the site informs the user of the ‘secret_folder’.

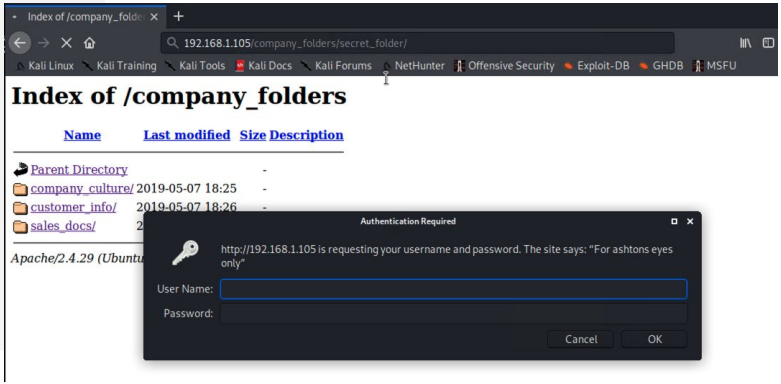
02

Achievements

This vulnerability not only gives attackers the path to the ‘secret_folder’ directory, but also gives them the username as shown in the authentication hint.

03





Exploitation: Brute Force Vulnerability

01

Tools & Processes

Using hydra, a common brute force tool, paired with the username given by the hint shown previously, one can quickly crack authentication for the secret directory.

02

Achievements

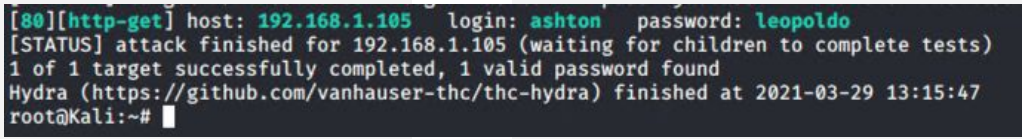
By identifying the password that goes with the username, the attacker now has access to the ‘secret_folder’ directory and the content within.

03

Hydra Command:

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -vV 192.168.1.105 http-get /company_folders/secret_folder

Hydra Output:



Exploitation: Sensitive Data Exposure

01

Tools & Processes

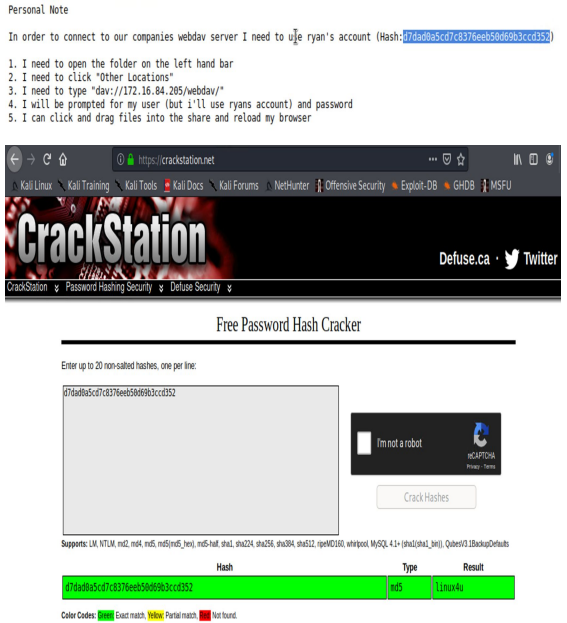
After gaining access to the ‘secret_folder’ the attackers can decode the hash for account name ryan using a hash decoder such as crackstations.net.

02

Achievements

By decoding the md5 hash, the attacker now has the credentials for the webdav directory.

03



Exploitation: Unauthorized Upload

01

Tools & Processes

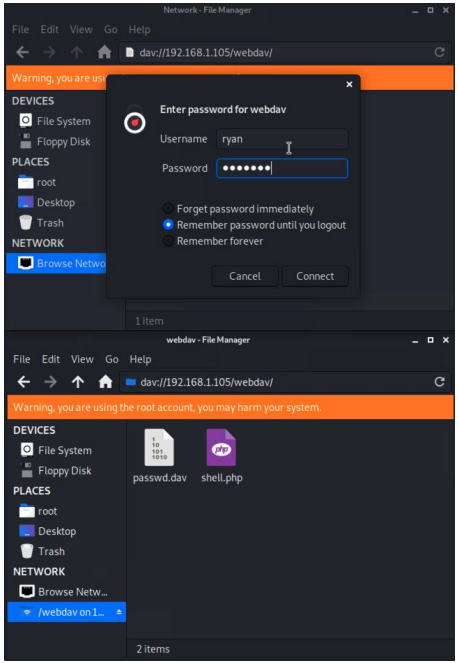
By using the credentials decoded in the Sensitive Data Exposure, the attacks can upload files to the webdav directory using their file manager.

02

Achievements

Uploading a reverse PHP shell created in msfvenom to this directory will alter the web contents and allow for a reverse shell to be established.

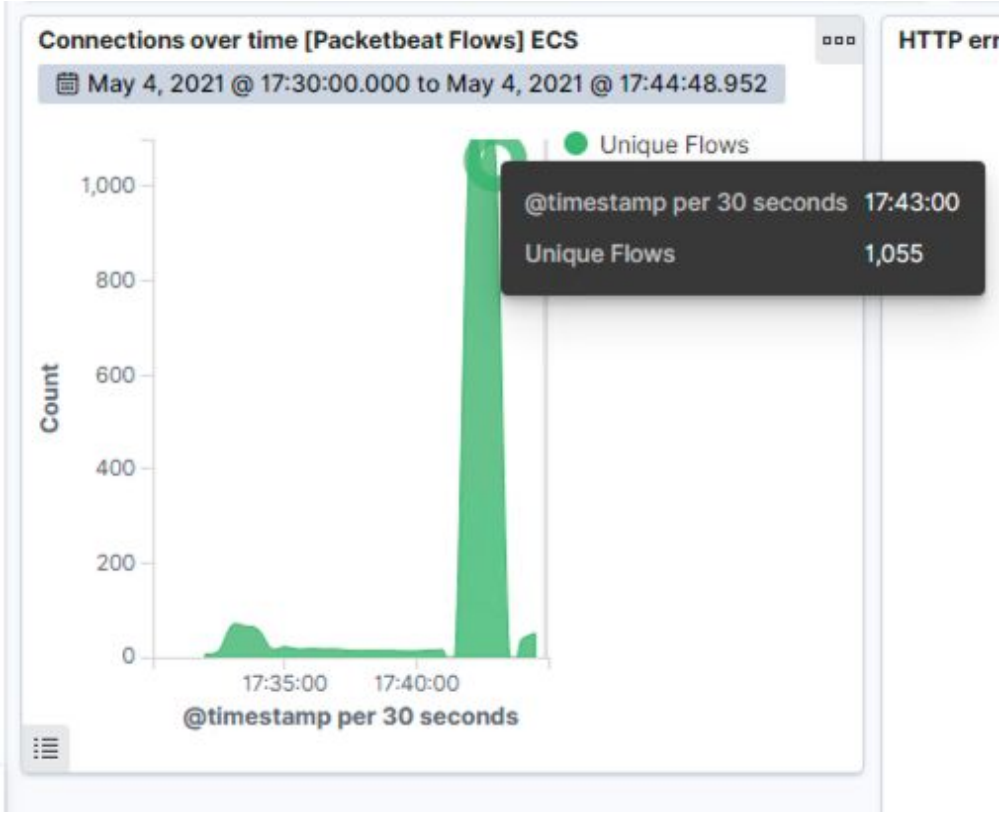
03



Blue Team
Log Analysis and Attack Characterization

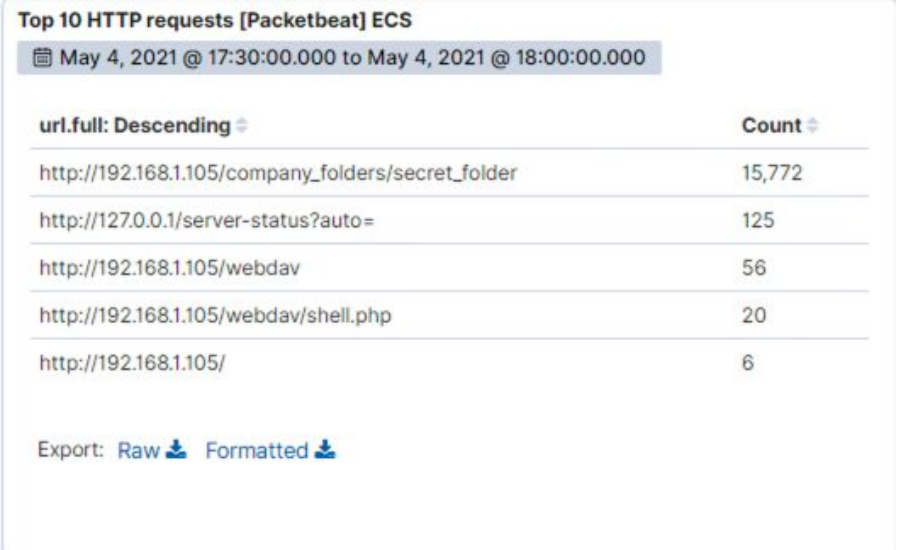
Analysis: Identifying the Port Scan

- The port scan occurred at 17:43
- Connections over time shows that the port scan is scanning the most likely 1000+ ports.



Analysis: Finding the Request for the Hidden Directory

- Under top HTTP requests we can see that there was 15,722 requests made to the “secret_folder” directory.
- This indicates a brute force attack, specifically on content which is known to be sensitive.



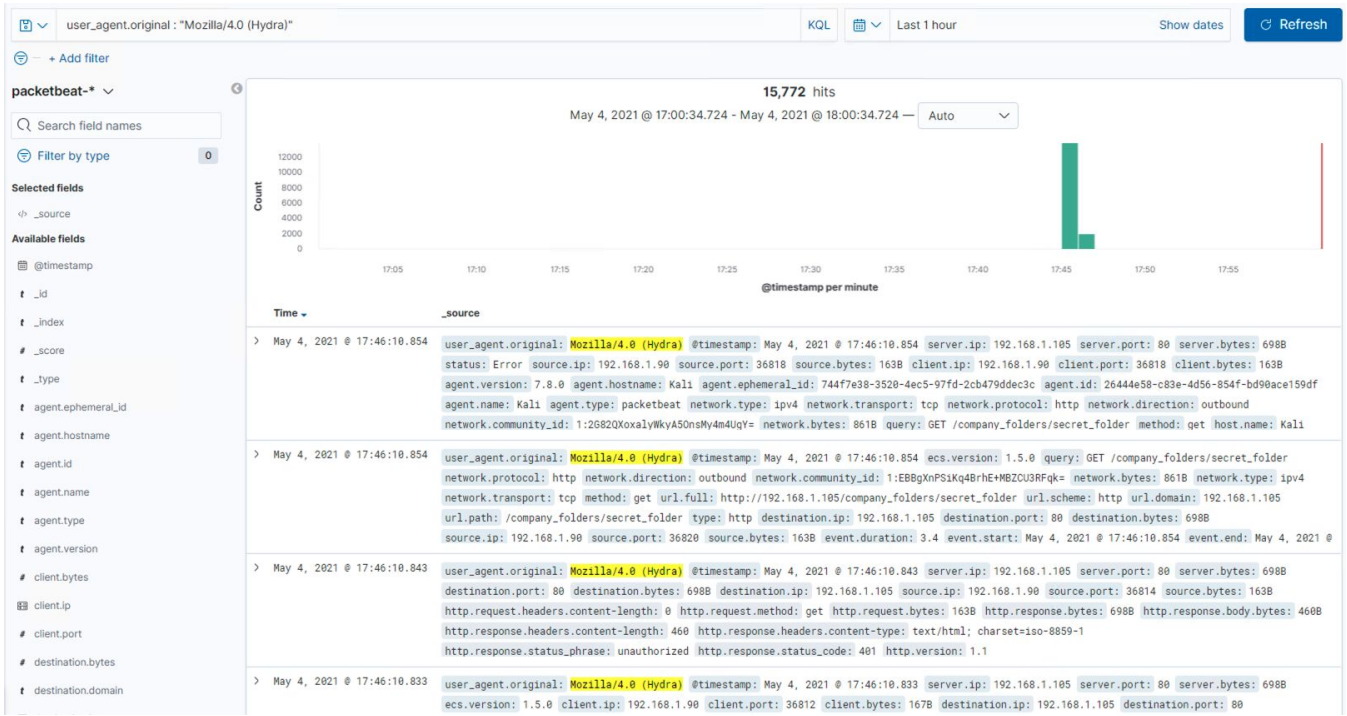
Top 10 HTTP requests [Packetbeat] ECS

May 4, 2021 @ 17:30:00.000 to May 4, 2021 @ 18:00:00.000

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,772
http://127.0.0.1/server-status?auto=	125
http://192.168.1.105/webdav	56
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/	6

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack



- In this kibana search we see that the requests for the secret folder were in fact part of a brute force attack
- Once again there are 15,722 hits, with the original user agent being “Mozilla/4.0 (Hydra)”

Analysis: Finding the WebDAV Connection

- Under top HTTP requests we also see 56 requests to the webdav directory
- We can also see 20 requests to a suspicious webdav/shell.php path
- This file is most likely a malicious upload achieved by attackers gaining access to the secret folder through brute force.

Top 10 HTTP requests [Packetbeat] ECS

May 4, 2021 @ 17:30:00.000 to May 4, 2021 @ 18:00:00.000

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,772
http://127.0.0.1/server-status?auto=	161
http://192.168.1.105/webdav	56
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/	6

Export: Raw Formatted

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

By setting an alarm that is triggered when a certain number of requests occur in an hour.

A threshold of 1000 connections would be a good threshold as this is plenty for the server and approximately what one port scan would amount to.

System Hardening

Doing local port scans in order to find and close open ports.

Update all software and firewalls, keep everything up to date in order to avoid vulnerabilities.

Set firewall to block port scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm that is triggered by excessive requests to the “secret_folder” would help in this scenario.

A threshold of 10 would be plenty to prevent any unauthorized personnel from getting through.

A notification could also be created that would alert the SOC of any brute force attempts.

System Hardening

Implementing lockout procedure and/or stronger password policy would help achieve a stronger wall of defense.

All together removing this directory from the internet would be the most secure course of action and would have completely prevented attacks.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Setting an alarm for any upload to the servers could help security and dev teams stay up to date with the whole site as well as provide alarm for any suspicious uploads.

System Hardening

If no uploads are wanted the system host could be configured to be read only so that no uploads can be completed.

The End