Ryan Cameron

Project 2

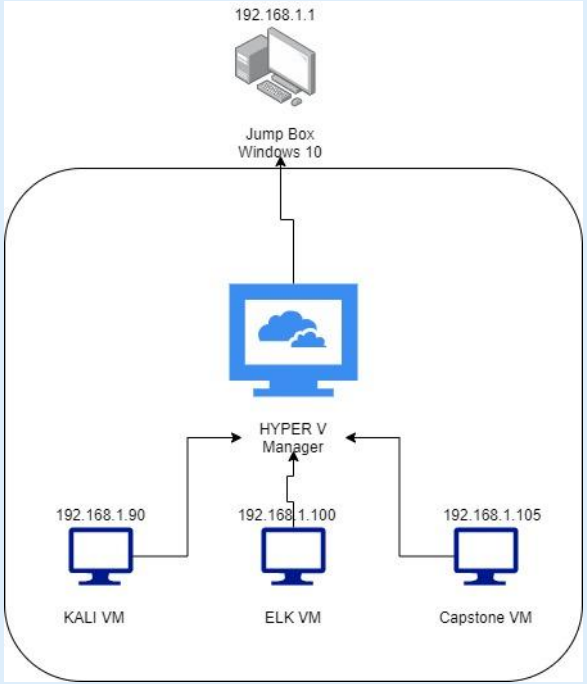
Assessment & Analysis

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.1/254
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Kali linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu
Hostname:ELK

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 10.0.0.46
OS: Windows 10
Hostname: ML-RefVm-684427

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali Linux	192.168.1.90	Attacker Machine
Capstone VM	192.168.1.105	Victim Machine
ELK VM	192.168.1.100	Elk Log & Monitoring
JumpBox VM	192.168.1.1	VM Host

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Password Protocol *Brute Force Attack*	*Used Hydra to Brute Force the URL. Information found allowed us to guess the username & password had been Brute Forced using a wordlist.*	*The brute force attack allowed access to the non-public files on the web-server.*
Insecure Hashing Technique MD5 Function Hash John the Ripper	Used john.exe to crack the hash found after brute forcing the URL.	The cracked hash allowed access to the remote Webdav file sharing server.
Weak Authentication & Information Integrity Payload Injection	Created a msfvenom payload to execute on the webdav server to enable access via meterpreter shell.	Meterpreter shell access allowed escalation of privileges to exploit the entire machine.

Exploitation: [Name of First Vulnerability]

01

Tools & Processes

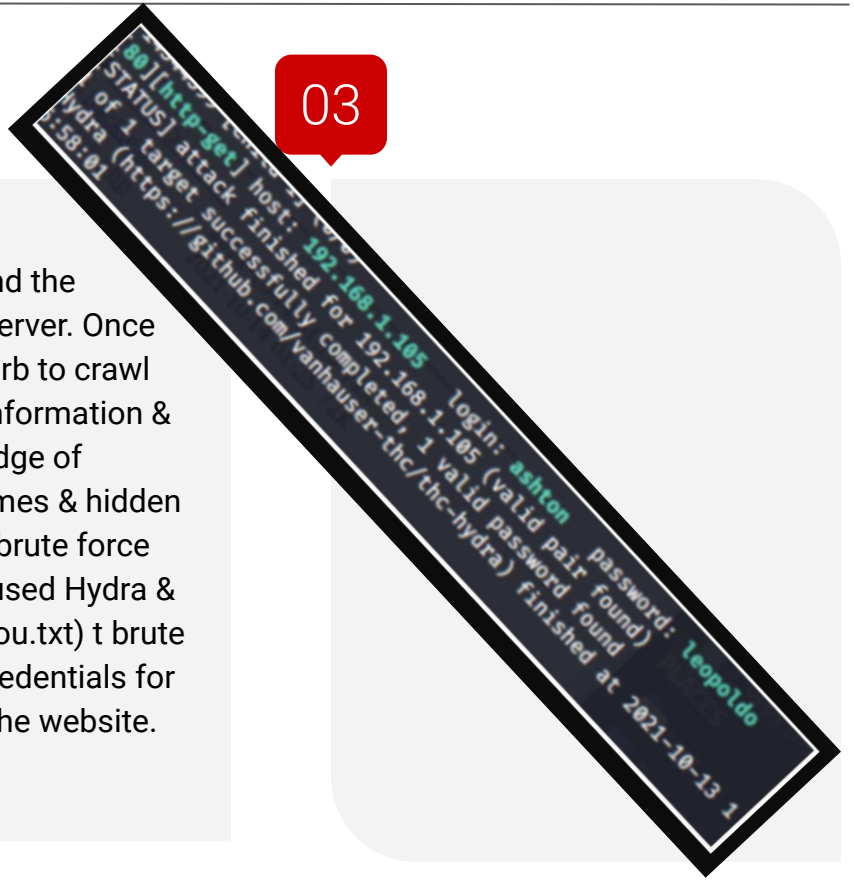
Nmap
Derb
Hydra

02

Achievements

Used Nmap to find the vulnerable web-server. Once found we used dirb to crawl the website for information & obtained knowledge of potential usernames & hidden URLs to use in a brute force attack. We then used Hydra & a wordlist (rockyou.txt) t brute force the login credentials for the back end of the website.

03



Exploitation: [Name of Second Vulnerability]

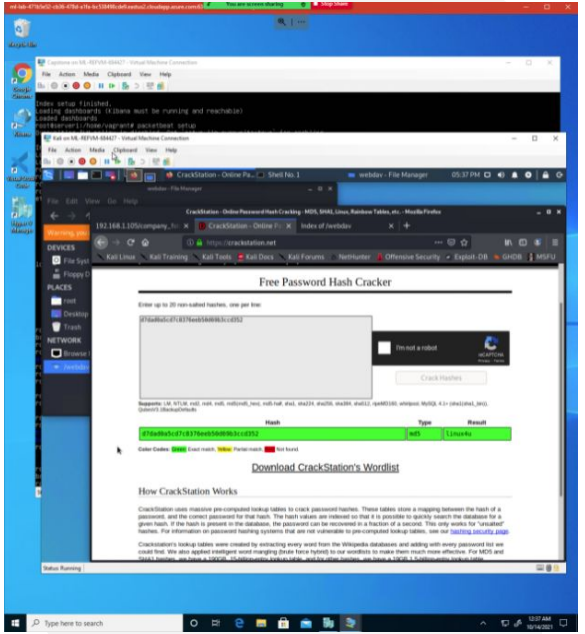
01

Tools & Processes
Crack station website

02

Achievements
After Brute Forcing the backend, we discovered a hash. We then used Crack Station website to crack the hash. The hash gave us the password to the webdav fie share server.

03



Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

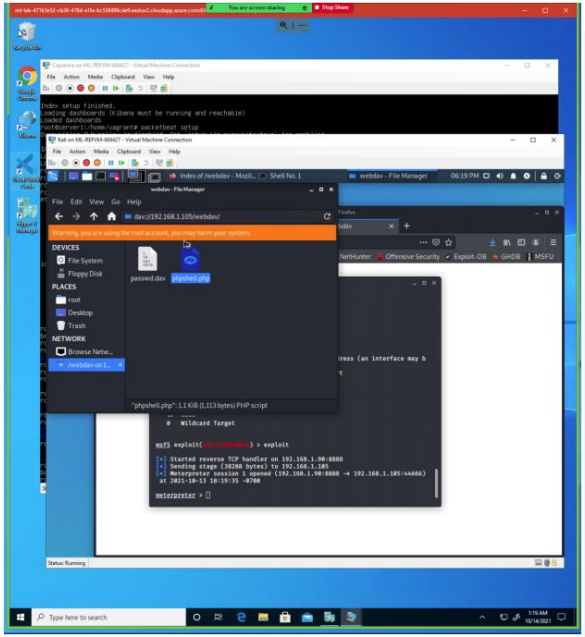
MsfVenom
Metasploit
Meterpreter

02

Achievements

Created a msfvenom payload to execute on the webdav server to enable access via meterpreter shell.

03

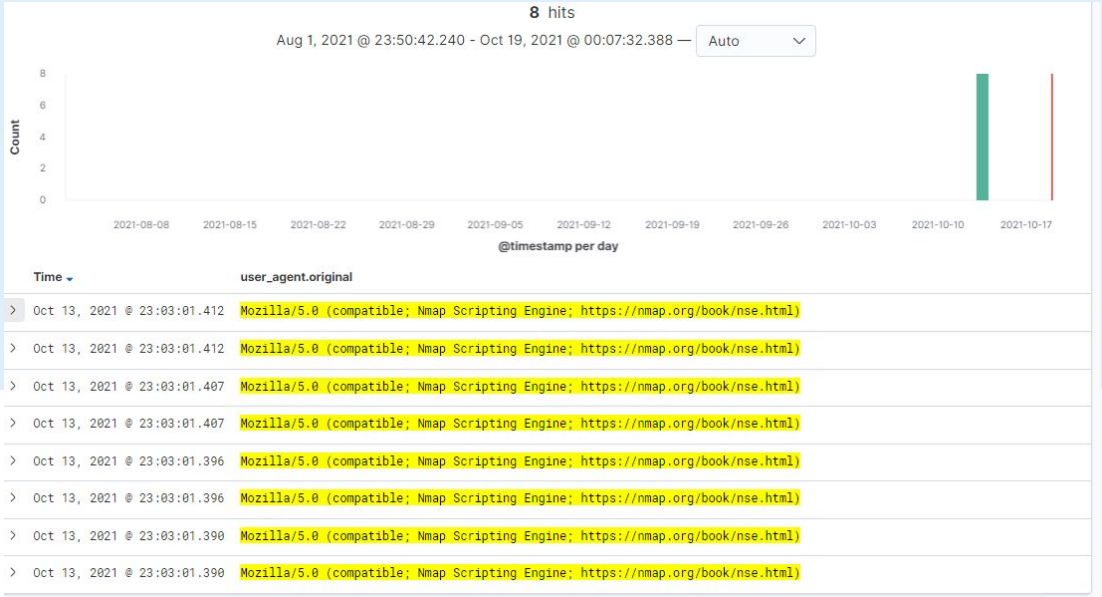


Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur? **10/13/21 at 20:55.**
- How many packets were sent, and from which IP? **7 packets**
- What indicates that this was a port scan? **Firefox - nMap was labeled in the User_Agent_orignal field**



Analysis: Finding the Request for the Hidden Directory

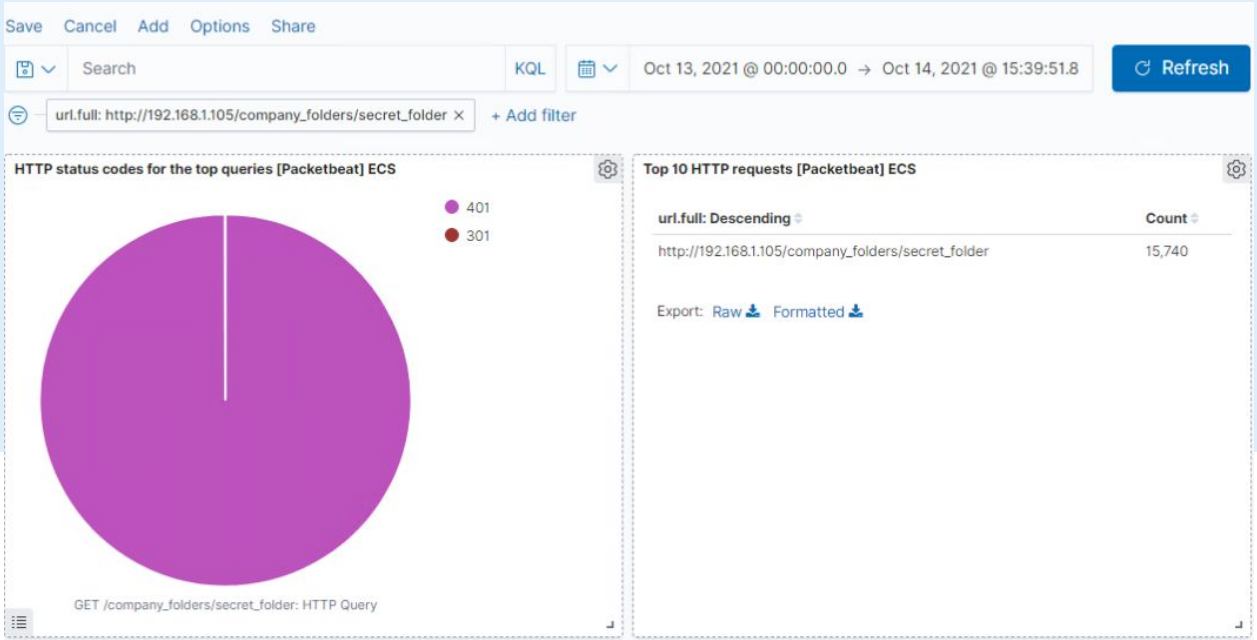
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?

  Between 8 - 11pm on October 13, 202. 15740 requests.

- Which files were requested? What did they contain?

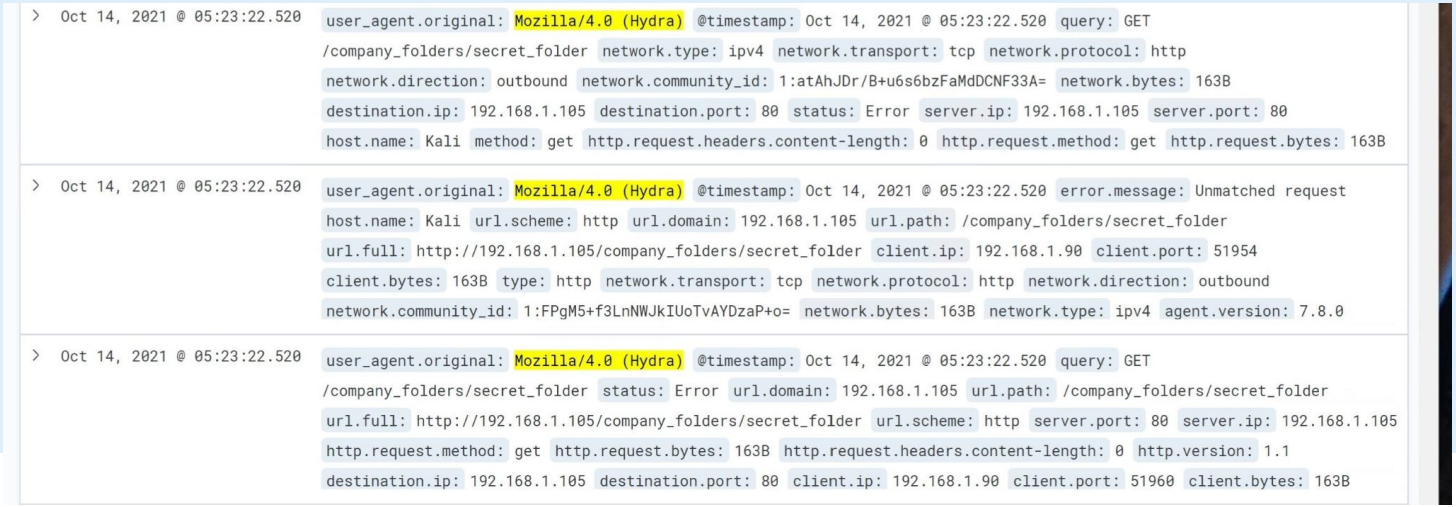
  Secret_folder has instructions on accessing the webdav server.



Analysis: Uncovering the Brute Force Attack

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 in the attack? 2**86,908 requests**
- How many requests had been made before the attacker discovered the password? **286,907**



> Oct 14, 2021 @ 05:23:22.520

user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Oct 14, 2021 @ 05:23:22.520 query: GET /company_folders/secret_folder network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:atAhJDr/B+u6s6bzFaMdDCNF33A= network.bytes: 163B destination.ip: 192.168.1.105 destination.port: 80 status: Error server.ip: 192.168.1.105 server.port: 80 host.name: Kali method: get http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 163B

> Oct 14, 2021 @ 05:23:22.520

user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Oct 14, 2021 @ 05:23:22.520 error.message: Unmatched request host.name: Kali url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder client.ip: 192.168.1.90 client.port: 51954 client.bytes: 163B type: http network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:FPgM5+f3LnNWJkIUoTvAYDzaP+o= network.bytes: 163B network.type: ipv4 agent.version: 7.8.0

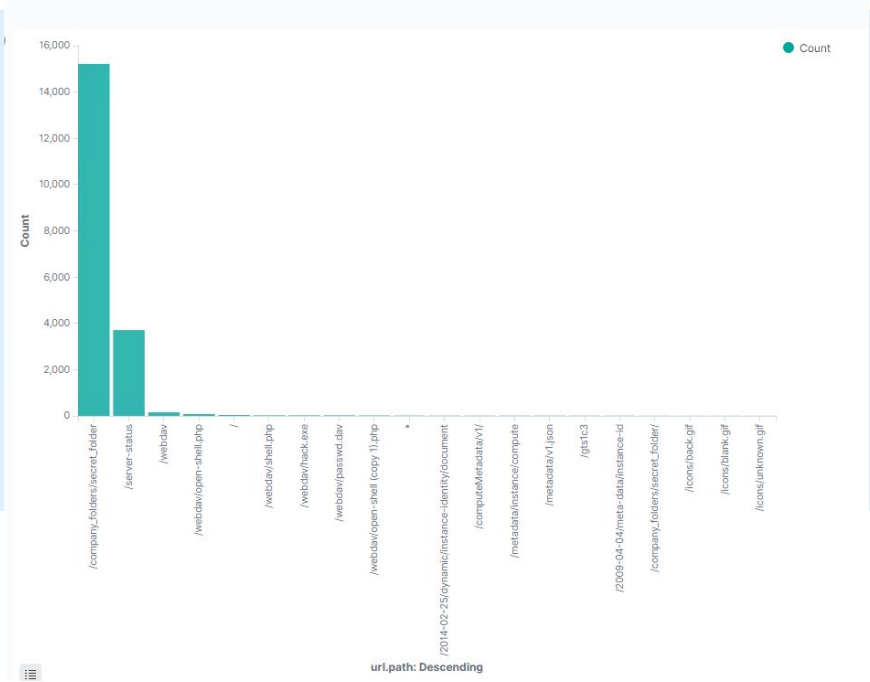
> Oct 14, 2021 @ 05:23:22.520

user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Oct 14, 2021 @ 05:23:22.520 query: GET /company_folders/secret_folder status: Error url.domain: 192.168.1.105 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http server.port: 80 server.ip: 192.168.1.105 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.version: 1.1 destination.ip: 192.168.1.105 destination.port: 80 client.ip: 192.168.1.90 client.port: 51960 client.bytes: 163B

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? **271,432**
- Which files were requested? **passwd.dav**



Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?
Setting threshold for number of requests that block IPs that send too many requests.

What threshold would you set to activate this alarm? **More than 100 requests in a minute**

System Hardening

What configurations can be set on the host to mitigate port scans?
Block incoming ports, except 80 & 443.
Block IP after certain amount of requests, (which can also double a s the solution).

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? **Set parameters to alert for influx of requests & status response phrases such as “unauthorized”.**

What threshold would you set to activate this alarm? **A number greater than the total amount of users who have access to this folder**

System Hardening

What configuration can be set on the host to block unwanted access?
Remove the folder & destination from public domain. Setup two factor authentication.

Describe the solution. If possible, provide required command lines.
Two Factor Authentication. You culd also deny certain IPs.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Large number of HTTP requests or error codes coming from one or more IPs

What threshold would you set to activate this alarm?
Any number of requests that is greater than average day of HTTP request traffic.

System Hardening

What configuration can be set on the host to block brute force attacks?
Password Complexity. Two factor authentication. Using CAPTCHA to block automated attempts to verify a human.

Describe the solution. If possible, provide the required command line(s).
Password Complexity. Two factor authentication. Using CAPTCHA to block automated attempts to verify a human.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
A large of HTTP requests to this directory.
A number greater than the amount of users who have access to the webdav directory.

What threshold would you set to activate this alarm?
A number greater than the amount of users who have access to the directory.

System Hardening

What configuration can be set on the host to control access?
Whitelist IPs & block everything else.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Set PUT requests alerts to web server folders that will then email necessary party. Setup rules for files to be read for malicious code such as php or exe.

What threshold would you set to activate this alarm?
Any files from unauthorized IPs or any new php or exe files.

System Hardening

What configuration can be set on the host to block file uploads?
Using IDS or anti-malware systems to detect and potentially block file uploads. Verify file type before upload.


The End