Capstone Engagement

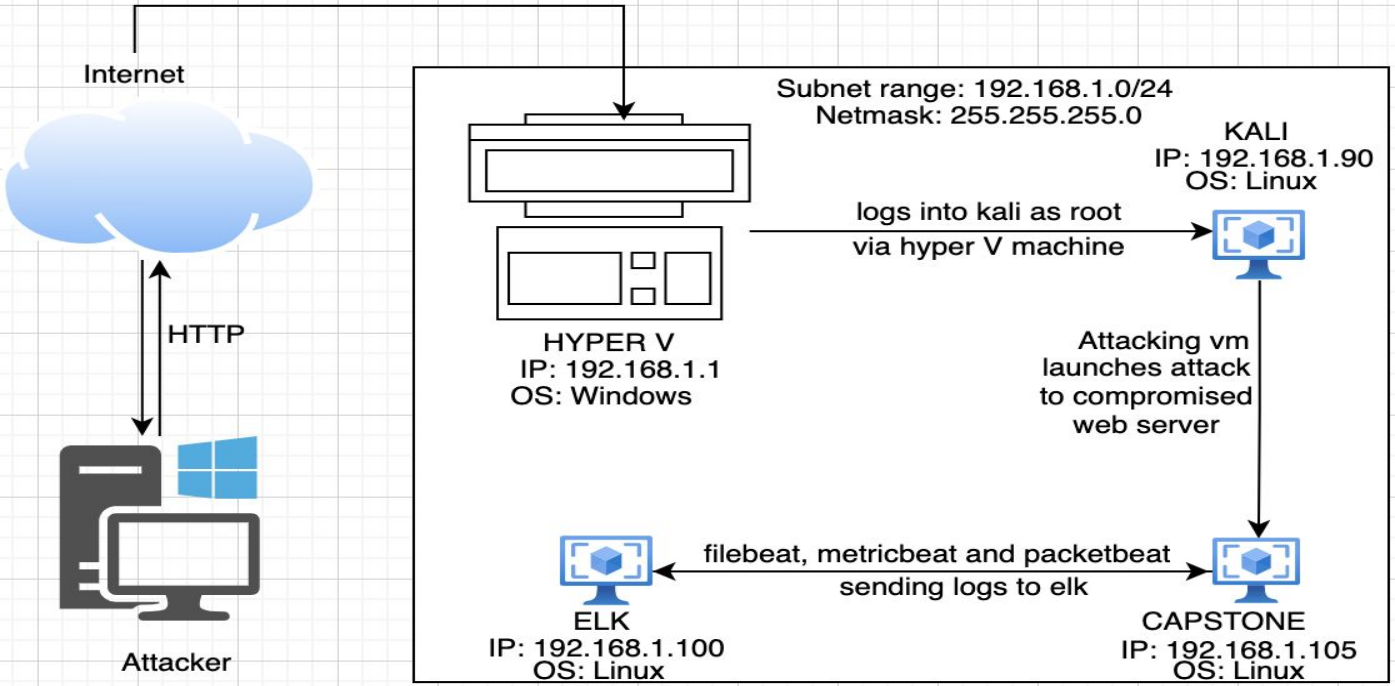
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.1-254
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper V M

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
Hyper V	192.168.1.1	Gateway Hosts all the 3 Vms
Kali	192.168.1.90	Attacker
Capstone	192.168.1.105	Vulnerable web server, Repository for company data, transmits logs to elk using the installed beats.
ELK	192.168.1.100	Our SIEM to receive and monitor logs from Capstone with Kibana. .

Vulnerability Assessment

Vulnerability	Description	Impact
Port scan vulnerability	Port scans were fully allowed. We were able to run version, os and service scans on the target. Found http running on target.	This aided in knowing which service and ip to launch the attack against. We used http to connect to the IP found to be running apache on http.
Brute-force Attack Vulnerability	Weak password for Ashton, weak hash function for ryan password. Md5sum hash is weak, use sha-256 instead.	Access to secret folder by attacker. Ashton's password was easy to brute-force with hydra, only took 1 minute. For Ryan, cracking his hash was literally done in seconds.
Webdav Connection & File Upload Vulnerability	Webdav folder allowing unusual php file upload from unauthorized source. Connection to Webdav server was super simple, 2-factor auth will help.	Access to webdav granted to attacker. Php file containing the reverse shell code can now be uploaded and executed by the attacker, gaining full access to corporate data.
Sensitive data exposure vulnerability	There is too much sensitive information on the website. Employee names, logins and secret folder information can easily be found on the site and used for malice.	Attacker will used this info to gain unauthorized access to hidden folders like webdav and continue to escalate privileges..

Exploitation: [Port Scanning]

01

Tools & Processes

-Used nmap to scan the subnetwork to find which vms were up and running, located the capstone vm running the web server.

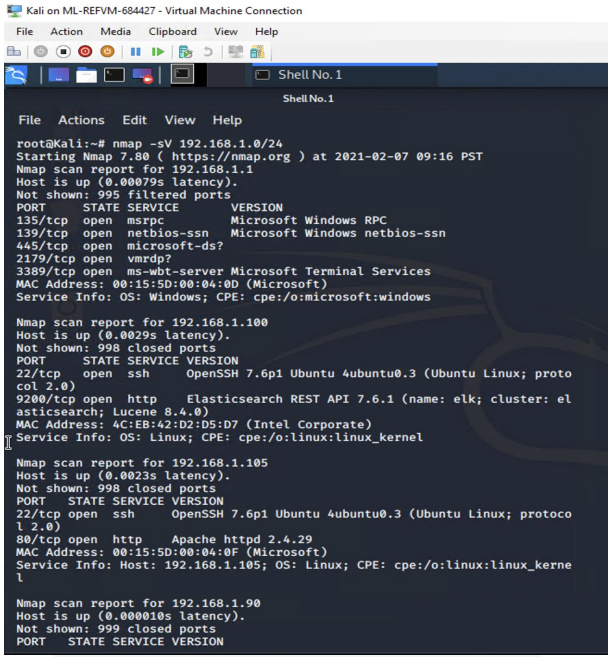
-run nmap -sV and -sn to reveal os, versions and services running on hosts to find any more vulnerabilities to attack.

02

Achievements

Found the web server's IP by locating which vm was running apache on http.

03



Since apache was running on http on 192.168.1.105, we concluded this was the web server's ip. We pinged it to make sure it was up and running.

Exploitation: [Brute-Force Vulnerability]

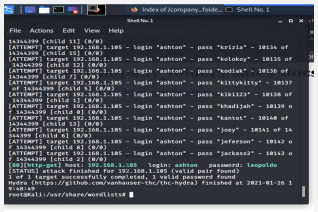
01

Tools & Processes

-Initially browsed the site to find useful info.

-Found some usernames and used hydra to brute-force ashton's password.

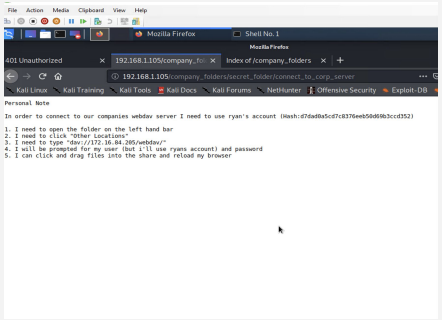
- Used crackstation to crack Ryan's pswd hash with md5sum



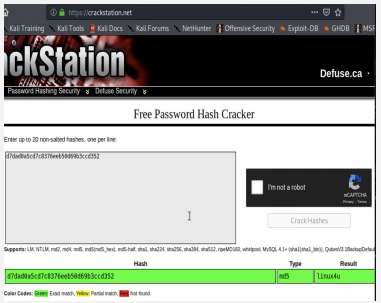
02

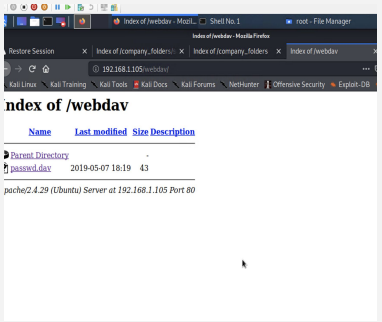
Achievements

-Granted access to secret folder logging in as Ashton, also webdav server by logging in as Ryan.



03





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

Exploitation: [Webdav Connection & File Upload Vulnerability]

01

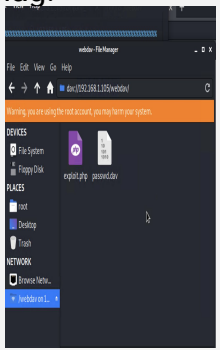
Tools & Processes

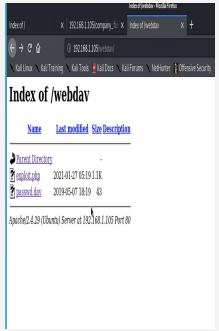
-Used msfvenom to create a php reverse shell on attacker machine and uploaded the exploit.php file onto webdav server after gaining access.
-Used Meterpreter to connect to the server after the shell was executed..

02

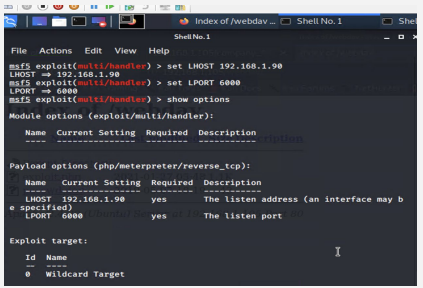
Achievements

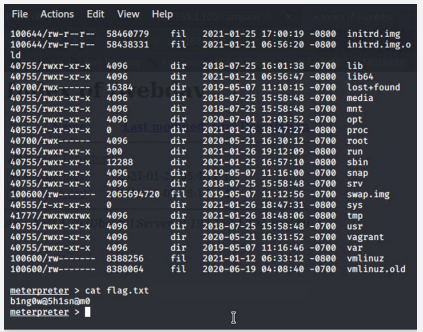
Successfully uploaded the reverse tcp shell, connected to web server using meterpreter and found the flag!





03





Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the scan occur? 03:29 AM
- How many packets were sent, and from which IP? 12,196 packets were sent and from 192.168.1.90

What indicates that this was a port scan? Port 52334 is usually used for port mapping. (TCP and UDP)

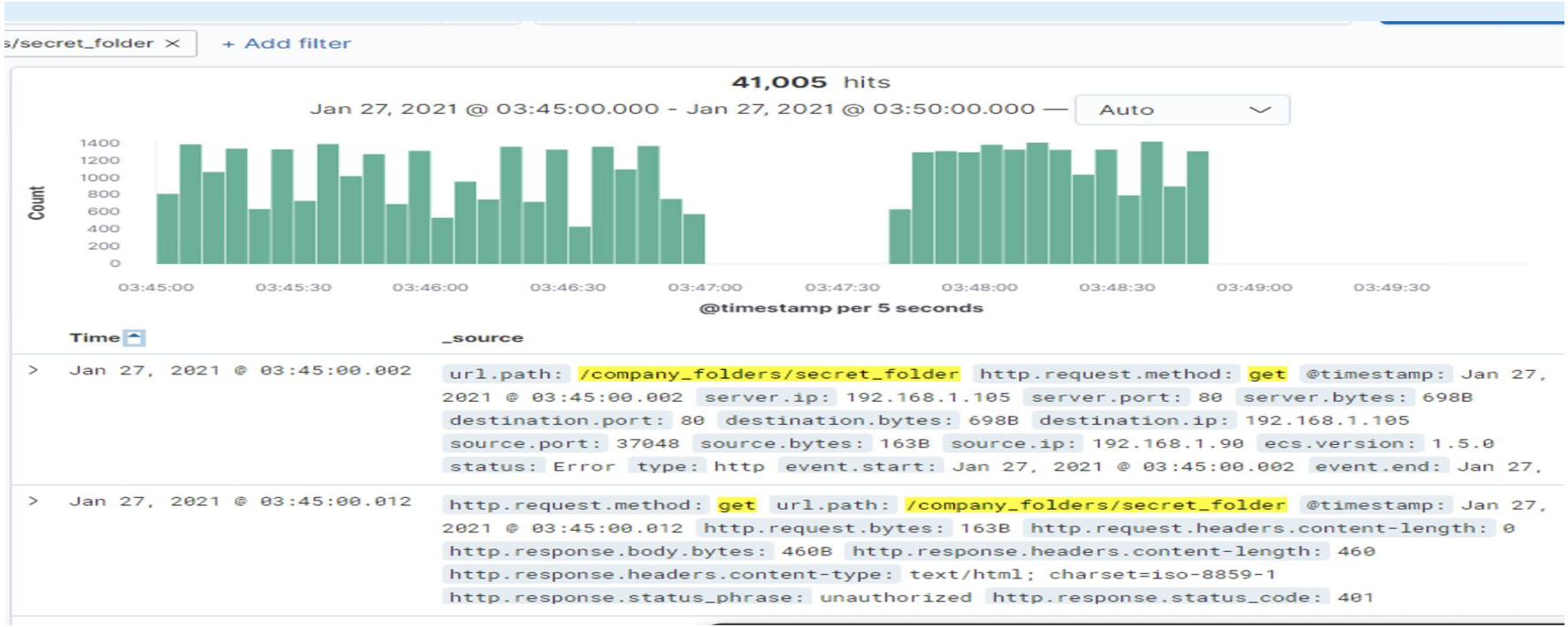
@timestamp per 3 seconds

Time	_source
> Jan 27, 2021 @ 03:29:50.338	event.category: network_traffic network.transport: tcp agent.name: Kali agent.hostname: Kali @timestamp: Jan 27, 2021 @ 03:29:50.338 event.action: network_flow event.start: Jan 27, 2021 @ 02:47:45.954 event.end: Jan 27, 2021 @ 03:29:49.943 event.duration: 2523989.3 event.dataset: flow event.kind: event type: flow source.ip: 192.168.1.90 source.port: 52334 source.packets: 12,916
> Jan 27, 2021 @ 03:29:40.338	agent.hostname: Kali agent.name: Kali event.category: network_traffic network.transport: tcp @timestamp: Jan 27, 2021 @ 03:29:40.338 type: flow ecs.version: 1.5.0 host.name: Kali agent.version: 7.8.0 agent.ephemeral_id: 40ad3f2d-c8e8-4504-a6fe-fcbc15dde160 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.type: packetbeat destination.packets: 7,562 destination.bytes: 2.2MB
> Jan 27, 2021 @ 03:29:30.338	event.category: network_traffic agent.name: Kali agent.hostname: Kali network.transport: tcp @timestamp: Jan 27, 2021 @ 03:29:30.338 destination.ip: 192.168.1.100 destination.port: 9200 destination.packets: 7,193 destination.bytes: 2.1MB event.kind: event event.action: network_flow event.start: Jan 27, 2021 @ 02:47:45.954 event.end: Jan 27, 2021 @ 03:29:30.208

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? Started at 03:45
- How many requests were made? 41,005

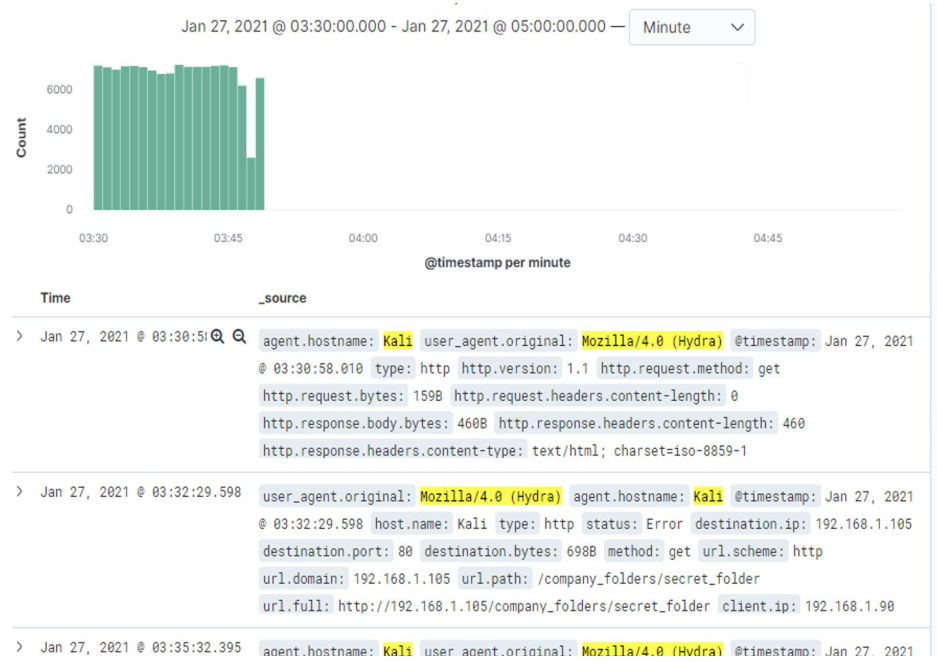
Which files were requested? What did they contain? Attacker requested for ‘connect_to_corp_server’ file which contained guidelines to access the corporate server.

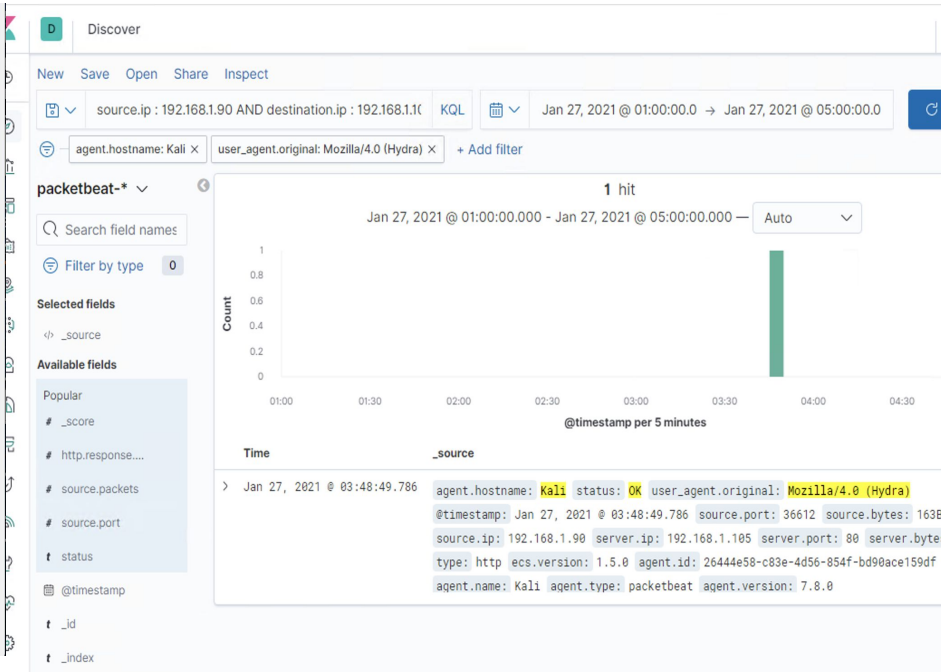


Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 22,079 requests

How many requests had been made b4 attacker discovered the password? 20,571 requests before the first success at 03:48





Brute force attacks started at 3:30 and continued till a first successful attempt at 3:48

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 48 (30+14)
- Which files were requested? Attacker requested for “exploit.php” 14 times

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	30
http://192.168.1.105/	20
http://192.168.1.105/webdav/	14
http://192.168.1.105/webdav/exploit.php	14
http://192.168.1.105/icons/blank.gif	8

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?
Set alarm to detect TCP requests, or specifically SYN requests since nmap uses SYN requests. If set at a good threshold, it should alert when nmap scans our network because a scan will usually generate several requests at a time.

What threshold would you set to activate this alarm? 15-20

System Hardening

What configurations can be set on the host to mitigate port scans?
-Configure host to block all scans from unrecognized sources.
-Block probes
-use tcp wrappers
-use scan detector apps like PortSentry and Scanlogd.

Describe the solution. If possible, provide required command lines.
Within firewall settings, “Deny All” and “Allow” only authorized IPs.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

-Allow only authorized access, block and notify from unauthorized.

What threshold would you set to activate this alarm?
1 attempt only

System Hardening

What configuration can be set on the host to block unwanted access?
-Change user permissions and access
-Create a whitelist of recognized ips and block all other traffic.
-Ensure a 2-step verification process to access the hidden directory.

Describe the solution. If possible, provide required command lines.
To change user access on server, “chmod +(0,0,0) /secret_folder”

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
-Create an alert to detect unusual volume of 401 responses from the server.

What threshold would you set to activate this alarm?
10

System Hardening

What configuration can be set on the host to block brute force attacks?
-set user account lockout configuration to lock user out after a certain number of failed attempts.
-2-step auth
-Change password and hash to something more complex

Describe the solution. If possible, provide the required command line(s).
Set to lockout user for 45 minutes after every 10 failed tries.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

-Alert when there is a login attempt to webdav not from the whitelisted ips.

What threshold would you set to activate this alarm?
1 attempt only

System Hardening

What configuration can be set on the host to control access?
-Remove directory from server so it cannot be accessed from unauthorized sources.
-If the company still wants to keep it on there, create a whitelist of ips that are authorized to access the folder. Ensure 2-step verification to webdav.

Describe the solution. If possible, provide the required command line(s).
In the /etc/httpd/conf/httpd.conf file, add the ips of the authorized vms.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

-Alert when there is an attempt to modify directory contents.
-Alert us when there is a post request with code/executable content.

What threshold would you set to activate this alarm?
Only one for the 2 alarms above.

System Hardening

What configuration can be set on the host to block file uploads?
-Block access to this folder so no user can read/write/execute
-Use filebeat to scan for modified/uploaded files regularly.

Describe the solution. If possible, provide the required command line.
Chmod + (0,0,0) “/webdav”


The End