Capstone Engagement

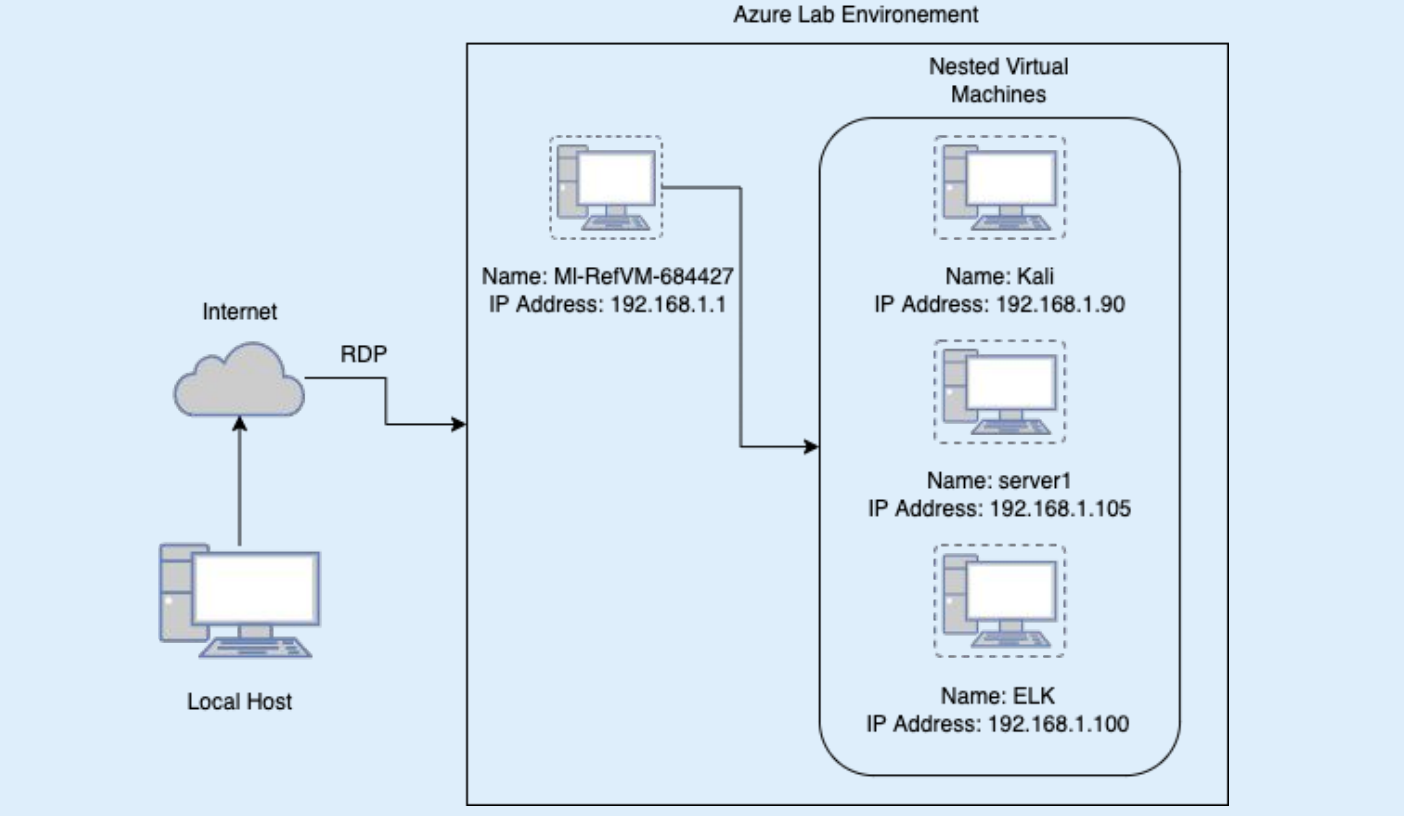
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefVM-684427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux Ubuntu
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux Ubuntu
Hostname: server1

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	Virtual Machine hosting the three other virtual machines below
server1	192.168.1.105	Victim machine, a vulnerable web server
ELK	192.168.1.100	ELK server to generate filebeat, metricbeat, and packetbeat logs during the attack
Kali	192.168.1.90	The attacking machine, used to brute force into the victim machine and locate the flag

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Occurs when a web application does not adequately protect sensitive information from being disclosed to attackers. Examples include login credentials, password hashes, etc..	*Allows the attacker to view confidential data that could assist in executing other attacks. An example could be the username linked to a password protected directory.*
Brute Force Vulnerability	Occurs when an attacker attempts a large number of combinations to gain access to a system. The most common are username and password combinations.	Once an attacker successfully gains access through brute force, they are able to continue with the attack. A brute force attack is a means to gain access to a system/directory
Local File Inclusion	Occurs when a web application allows a user to submit input into files or upload files to the server	A malicious file can be uploaded to the server allowing the attacker to gain full control of his/her system

Exploitation: Sensitive Data Exposure

01

Tools & Processes

Nmap was used to identify the target machine. Once I gained access to the webserver, I analyzed files and directories to search for a hidden folder.

02

Achievements

Through thorough analysis of the web-server I was able to identify the name and location of the hidden directory

03

```
ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder is no longer accessible to the public
```

Exploitation: Brute Force Vulnerability

01

Tools & Processes

The results from the first vulnerability led me to obtain the username for the hidden directory. Hydra was then used to brute force into the folder to gain access to sensitive data. CrackStation online hash cracker was also used to uncover the password of the second protected directory.

02

Achievements

Once inside the directory, I had access to confidential company documents which included the hashed password for the “/webdav/” directory. Login credentials gives me access to view, edit and upload files.

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [ch
/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [ch
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)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-21 11:18:52
root@Kali:/usr/share/wordlists#
```

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

Exploitation: Local File Inclusion

01

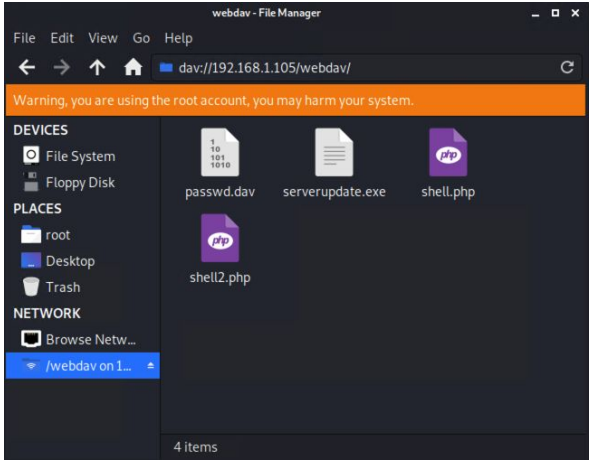
Tools & Processes
Crackstation Online Hashcracker was used to decrypt the hashed password found in the previous step. The username was already provided in the document located within the hidden directory

02

Achievements
Decrypting the hashed password allowed me to connect to the corporate web server as an authenticated user. Further allowing me to edit files or even upload files such as the malicious reverse shell file seen on the screenshot.

03

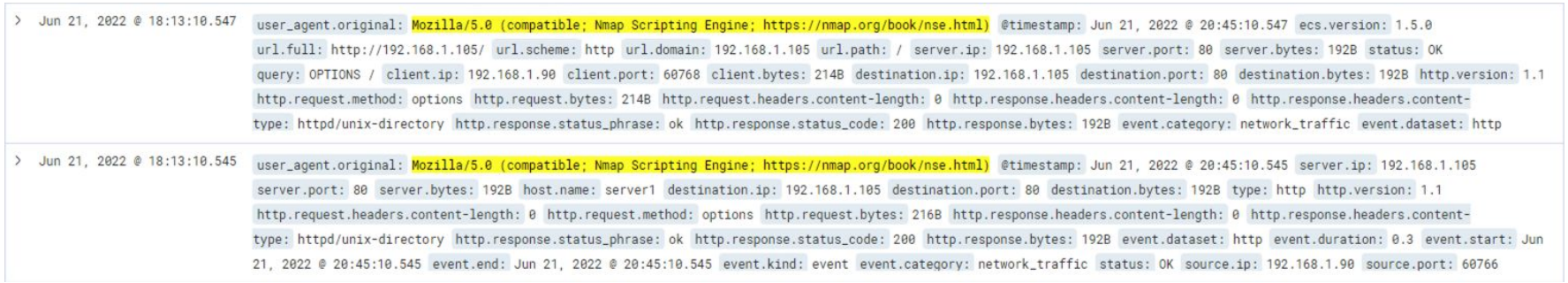
Password: linux4u



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.

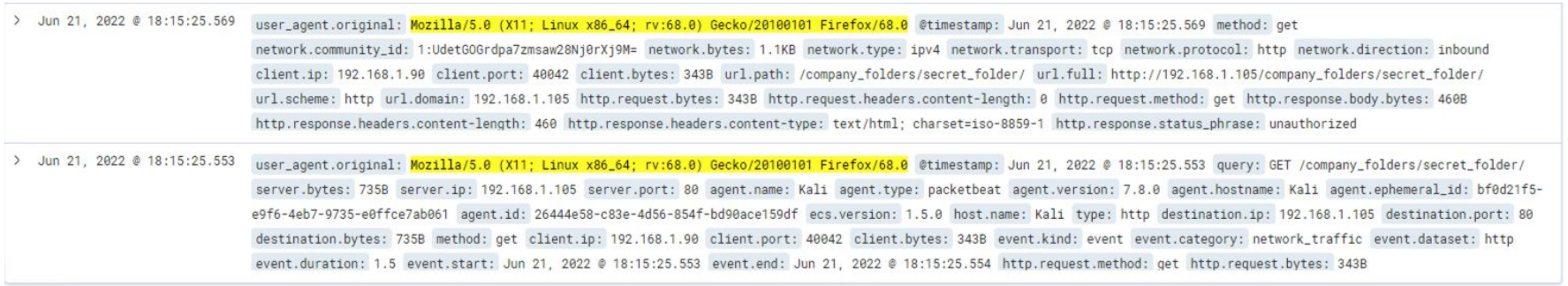


> Jun 21, 2022 @ 18:13:10.547 user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) @timestamp: Jun 21, 2022 @ 20:45:10.547 ecs.version: 1.5.0 url.full: http://192.168.1.105/ url.scheme: http url.domain: 192.168.1.105 url.path: / server.ip: 192.168.1.105 server.port: 80 server.bytes: 192B status: OK query: OPTIONS / client.ip: 192.168.1.90 client.port: 60768 client.bytes: 214B destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 192B http.version: 1.1 http.request.method: options http.request.bytes: 214B http.request.headers.content-length: 0 http.response.headers.content-length: 0 http.response.headers.content-type: httpd/unix-directory http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 192B event.category: network_traffic event.dataset: http

> Jun 21, 2022 @ 18:13:10.545 user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) @timestamp: Jun 21, 2022 @ 20:45:10.545 server.ip: 192.168.1.105 server.port: 80 server.bytes: 192B host.name: server1 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 192B type: http http.version: 1.1 http.request.headers.content-length: 0 http.request.method: options http.request.bytes: 216B http.response.headers.content-length: 0 http.response.headers.content-type: httpd/unix-directory http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 192B event.dataset: http event.duration: 0.3 event.start: Jun 21, 2022 @ 20:45:10.545 event.end: Jun 21, 2022 @ 20:45:10.545 event.kind: event event.category: network_traffic status: OK source.ip: 192.168.1.90 source.port: 60766

- Port scan occurred at 6:13 PM on June 21, 2022
- 58 Packets were sent from 192.168.1.90
- These logs relate to a port scan ran using NMAP

Analysis: Finding the Request for the Hidden Directory



> Jun 21, 2022 @ 18:15:25.569

user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 @timestamp: Jun 21, 2022 @ 18:15:25.569 method: get
network.community_id: 1:UdetGOGrdpa7zmsaw28Nj0rXj9M= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
client.ip: 192.168.1.90 client.port: 40042 client.bytes: 343B url.path: /company_folders/secret_folder/ url.full: http://192.168.1.105/company_folders/secret_folder/
url.scheme: http url.domain: 192.168.1.105 http.request.bytes: 343B http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes: 460B
http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized

> Jun 21, 2022 @ 18:15:25.553

user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 @timestamp: Jun 21, 2022 @ 18:15:25.553 query: GET /company_folders/secret_folder/
server.bytes: 735B server.ip: 192.168.1.105 server.port: 80 agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: bf0d21f5-
e9f6-4eb7-9735-e0ffce7ab061 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df ecs.version: 1.5.0 host.name: Kali type: http destination.ip: 192.168.1.105 destination.port: 80
destination.bytes: 735B method: get client.ip: 192.168.1.90 client.port: 40042 client.bytes: 343B event.kind: event event.category: network_traffic event.dataset: http
event.duration: 1.5 event.start: Jun 21, 2022 @ 18:15:25.553 event.end: Jun 21, 2022 @ 18:15:25.554 http.request.method: get http.request.bytes: 343B

- Request to view hidden directory made at 6:15 PM. 6 Requests were sent.
- Hidden directory access was requested with a path of “http://192.168.1.105/company_folders/secret_folder/”

Analysis: Uncovering the Brute Force Attack

> Jun 21, 2022 @ 18:18:43.297

user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jun 21, 2022 @ 18:18:43.297 method: get event.kind: event event.category: network_traffic event.dataset: http event.start: Jun 21, 2022 @ 18:18:43.297 destination.ip: 192.168.1.105 destination.port: 80 client.ip: 192.168.1.90 client.port: 57820 client.bytes: 164B url.path: /company_folders/secret_folder/ url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http url.domain: 192.168.1.105 query: GET /company_folders/secret_folder/ agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: bf0d21f5-e9f6-4eb7-9735-e0ffce7ab061 source.ip: 192.168.1.90 source.port: 57820 source.bytes: 164B status: Error http.request.method: get

> Jun 21, 2022 @ 18:18:42.838

user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jun 21, 2022 @ 18:18:42.838 network.direction: outbound network.community_id: 1:/tlEKEv/kOKOk+SrhWbddmPe9K4= network.bytes: 862B network.type: ipv4 network.transport: tcp network.protocol: http destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B source.ip: 192.168.1.90 source.port: 57682 source.bytes: 164B agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: bf0d21f5-e9f6-4eb7-9735-e0ffce7ab061 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat method: get http.version: 1.1 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 164B http.response.bytes: 698B http.response.body.bytes: 460B

- 12,366 requests were made during the attack
- 12,344 requests were generated before the attacker uncovered the password

Analysis: Finding the WebDAV Connection

> Jun 21, 2022 @ 18:20:08.842

url.path: /webdav @timestamp: Jun 21, 2022 @ 18:20:08.842 user_agent.original: gvfs/1.42.2 ecs.version: 1.5.0 url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav url.scheme: http query: OPTIONS /webdav method: options source.bytes: 203B source.ip: 192.168.1.90 source.port: 60640 agent.ephemeral_id: 117fc52f-2fee-455a-a90a-a1bb2ab39c13 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat status: OK destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 356B client.ip: 192.168.1.90 client.port: 60640 client.bytes: 203B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:f59mrud6M4k4KztOnVGuT0HSImM= network.bytes: 559B event.kind: event event.category: network_traffic event.dataset: http

> Jun 21, 2022 @ 18:20:08.821

url.path: /webdav @timestamp: Jun 21, 2022 @ 18:20:08.821 status: OK destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 356B host.name: Kali http.request.method: options http.request.bytes: 203B http.request.headers.content-length: 0 http.response.status_code: 200 http.response.bytes: 356B http.response.headers.content-length: 0 http.response.headers.content-type: httpd/unix-directory http.response.status_phrase: ok http.version: 1.1 client.ip: 192.168.1.90 client.port: 60640 client.bytes: 203B network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:f59mrud6M4k4KztOnVGuT0HSImM= network.bytes: 559B network.type: ipv4 type: http event.start: Jun 21, 2022 @ 18:20:08.821 event.end: Jun 21, 2022 @ 18:20:08.829 event.kind: event

- 42 requests were made to this directory
- Password file was requested that consisted of the password hash of an account by the name of ryan. File upload was detected.

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Generating an alarm can be very useful to detect any future port scans, an alarm can be set to go off when the same source IP address sends packets to different ports
- A threshold allows us to set a number in which the alarm will go off, in this case, a threshold of 10 ports is sufficient; If the number of ports, packets are being sent to exceed 10, then the alarm will be set off

System Hardening

- Implementing a firewall is a good technique to mitigate port scans, a firewall prevents unauthorised access, controls ports and their visibility as well as detecting when an incoming port scan is occurring
- TCP wrappers are also another technique used to mitigate port scans. TCP wrappers allow admins to have flexibility to permit or deny access to the server based on IP and domain names

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alarm can be set to detect multiple requests from the same source IP to the hidden directory that have a response code of 401
- A threshold of 5 or more bad requests would set off the alarm. This is because login credentials to the hidden directory should be known and should not take more than 5 attempts to gain access

System Hardening

- Firewalls can be used to blacklist IP addresses and ports on the network. If the firewall detects multiple requests from the same source IP you can blacklist that IP address from accessing any part of your network.
- Firewalld can be used to blacklist IP addresses using a single command
- firewall-cmd –permanent –add-rich-rule=”rule family=’ipv4’ source address=’<IP Address>’ reject”

Mitigation: Preventing Brute Force Attacks

Alarm

- A simple alarm can be set to detect a high volume of requests coming from the same source as well as detecting the user agent involved in the traffic. If the user agent is, Hydra, in this case then an alarm can be set to detect traffic involving Hydra or any other brute force tools
- A reasonable threshold for brute force attacks would be 5 or more bad requests

System Hardening

- Account lockouts can be implemented. Once a user has attempted 3 login requests the account should be locked out for a period of time
- In the case above, around 12,000 login requests were made using the same account. If that account is locked out after 3 failed logins, a brute force attack becomes much harder to pull off.

Mitigation: Detecting the WebDAV Connection

Alarm

- When reviewing logs, an alarm can be set when the url.path field is "http://192.168.1.105/webdav/" as well as the source IP being one that is not supposed to have access to the directory
- A threshold of 0 should be set on this alarm because the directory is for authorised access only

System Hardening

- Access controls can be set to allow authorised users or IP addresses to access the directory
- Host Based Access Controls (HBAC) can be set to specific users or a group of users

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Logs involving HTTP PUT requests along with data indicating that is a file upload coming from an unknown source
- A threshold for this alarm should be set to 0 as no unauthorised user should be uploading a file to the server

System Hardening

- Administrator can restrict file uploads to specific file types
- Verifying file types can also be done to mitigate attackers attempting to “mask” the file type. Ex. renaming a .exe to a .docx
- All file uploads need to be authenticated based on what user is uploading the file, however this does not indicate if the users machine has been infected


The End