Capstone Engagement

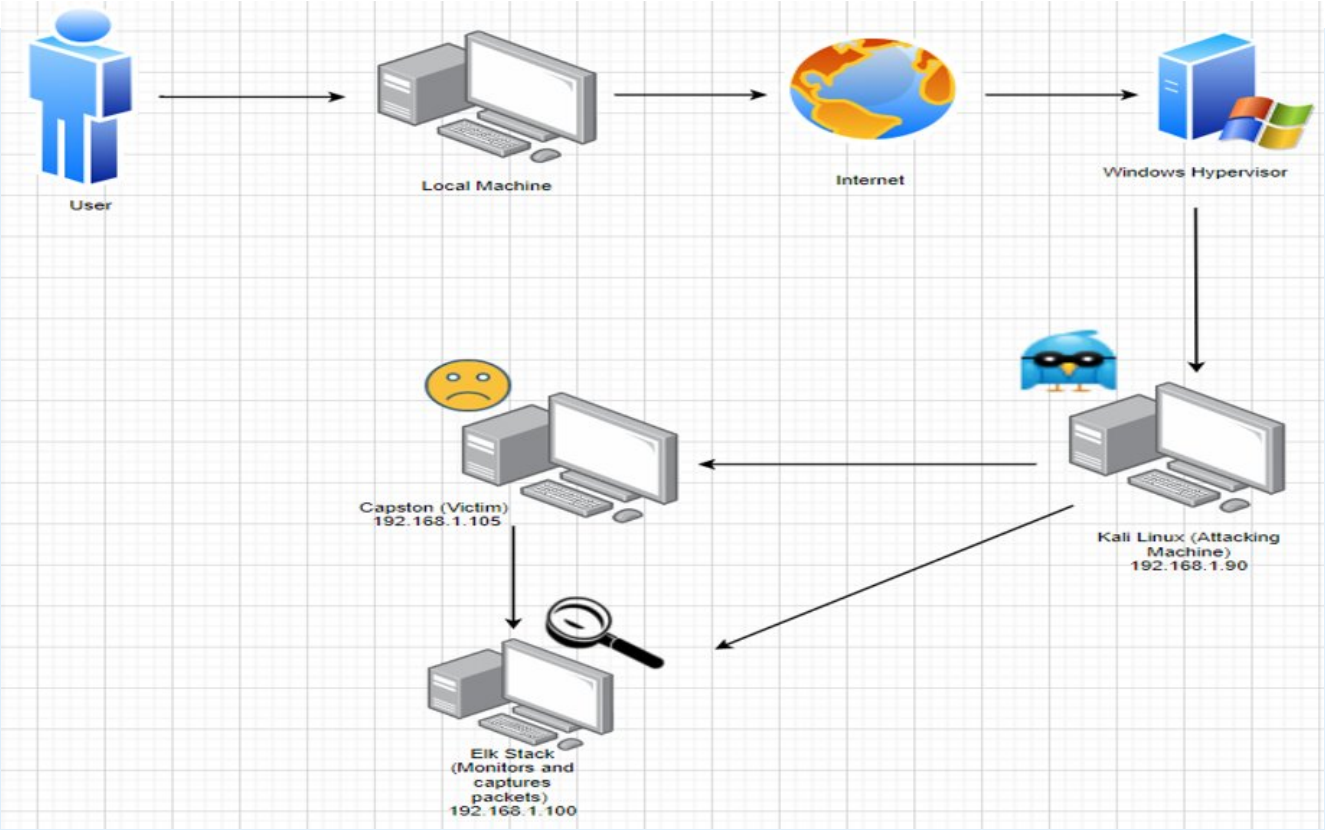
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.90
OS: Linux (Kali)
Hostname: Attacker

IPv4: 192.168.1.105
OS: Linux (Ubuntu 18.04)
Hostname: Defender

IPv4: 192.168.1.100
OS: Linux (Ubuntu 18.04)
Hostname: ELK Stack

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	Used to run scans, gather information and launched the attack
Server 1	192.168.1.105	Host the website and information (server being attacked)
ELK	192.168.1.100	SIEM; Monitors and captures packets and logs

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Sensitive Data Exposure	This is #3 in OWASP's Top 10 web application vulnerabilities	This allows unauthorized access to sensitive data
Brute-Force Vulnerability	If site allows multiple login attempts	This allows password to be cracked easily.
Local File Inclusion (LFI)	This allows access into confidential files.	An LFI vulnerability allows for remote code execution

Exploitation: Sensitive Data Exposure

01

Tools & Processes

- How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

We used Nmap and URL Manipulation

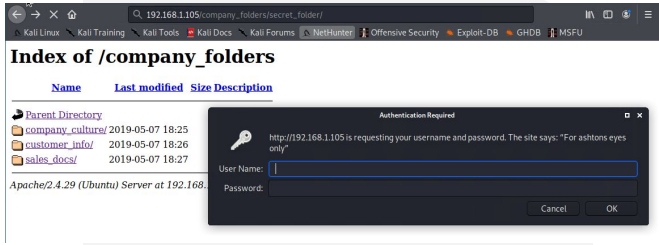
02

Achievements

- What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

We got access to /secret_folder directory, exposed Ashton's user data, and allowed potential further access into server1.

03



Exploitation: Brute-Force Vulnerability

01

Tools & Processes

- How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

We used Hydra to exploit this vulnerability

02

Achievements

- What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

Cracked Ashton's password using Hydra

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" -
 10144 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ilovemom1"
 - 10145 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "getalife"
- 10146 of 14344399 [child 12] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leo
poldo
[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 202
0-10-01 16:27:54
root@Kali:~#
```

Exploitation: LFI Vulnerability

01

Tools & Processes

- How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

We used File/Network Manager

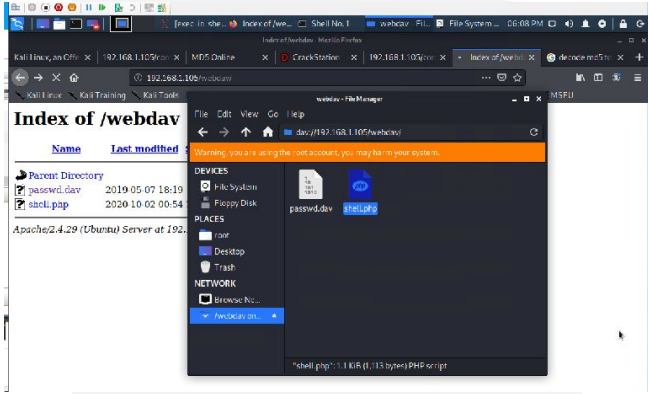
02

Achievements

- What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

- We uploaded custom msfvenom payload onto server. This allowed for reverse tcp shell code to be executed and granted meterpreter shell access

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.

Oct 1, 2020	event.dataset	Message
No additional entries found		
23:04:59.000	apache.access	[apache][access] 192.168.1.90 - "get / HTTP/1.0" 200 1580
23:04:59.000	apache.access	[apache][access] 192.168.1.90 - "options / HTTP/1.1" 200 192
23:04:59.000	apache.access	[apache][access] 192.168.1.90 - "get /nmaplowercheck1601593499 HTTP/1.1" 404 455
23:04:59.000	apache.access	[apache][access] 192.168.1.90 - "propfind / HTTP/1.1" 405 523
23:04:59.000	apache.access	[apache][access] 192.168.1.90 - "post / HTTP/1.1" 404 455
23:04:59.000	apache.access	[apache][access] 192.168.1.90 - "get /robots.txt HTTP/1.1" 404 455

- What time did the port scan occur? 11:04:59 GMT
- How many packets were sent, and from which IP? 192.168.1.90
- What indicates that this was a port scan? Nmap was labeled on it

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.

> Oct 1, 2020 @ 23:30:17.502

```
url.full: http://192.168.1.105/company_folders/secret_folder @timestamp: Oct 1, 2020 @ 23:30:17.502 method: get server.ip: 192.168.1.105 server.port: 80 server.bytes: 626B
event.duration: 0.6 event.start: Oct 1, 2020 @ 23:30:17.502 event.end: Oct 1, 2020 @ 23:30:17.503 event.kind: event event.category: network_traffic event.dataset: http
http.request.method: get http.request.bytes: 385B http.request.headers.content-length: 0 http.response.bytes: 626B http.response.body.bytes: 338B
http.response.headers.content-length: 338 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: moved permanently
http.response.status_code: 301 http.version: 1.1 host.name: server1 agent.type: packetbeat agent.ephemeral_id: 4e98adcd-5a6d-4edb-a76b-f35069935ff7 agent.hostname: server1
```

> Oct 1, 2020 @ 23:30:23.032

```
url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server @timestamp: Oct 1, 2020 @ 23:30:23.032 network.community_id: 1:OyDOZbD0aEuRO+LF0mRvs43ZYkk=
network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound type: http user_agent.original: Mozilla/5.0 (X11; Linux
x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 ecs.version: 1.5.0 destination.port: 80 destination.bytes: 674B destination.ip: 192.168.1.105 host.name: server1
server.ip: 192.168.1.105 server.port: 80 server.bytes: 674B http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ http.request.bytes: 470B
http.request.headers.content-length: 0 http.request.method: get http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 674B
```

> Oct 1, 2020 @ 23:30:22.961

```
url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server @timestamp: Oct 1, 2020 @ 23:30:22.961 http.response.body.bytes: 414B
http.response.headers.content-length: 414 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 674B http.version: 1.1 http.request.method: get
http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ http.request.bytes: 470B http.request.headers.content-length: 0 url.scheme: http
url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/connect_to_corp_server query: GET /company_folders/secret_folder/connect_to_corp_server source.bytes: 470B
source.ip: 192.168.1.90 source.port: 46144 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 method: get event.kind: event
```

- What time did the request occur? How many requests were made? It occurred at 23:30 GMT and 15,000 requests were made
- Which files were requested? What did they contain? The file connect_to_corp_server was requested. This file contained instructions for uploading files onto the server and Ryan's password hash

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.

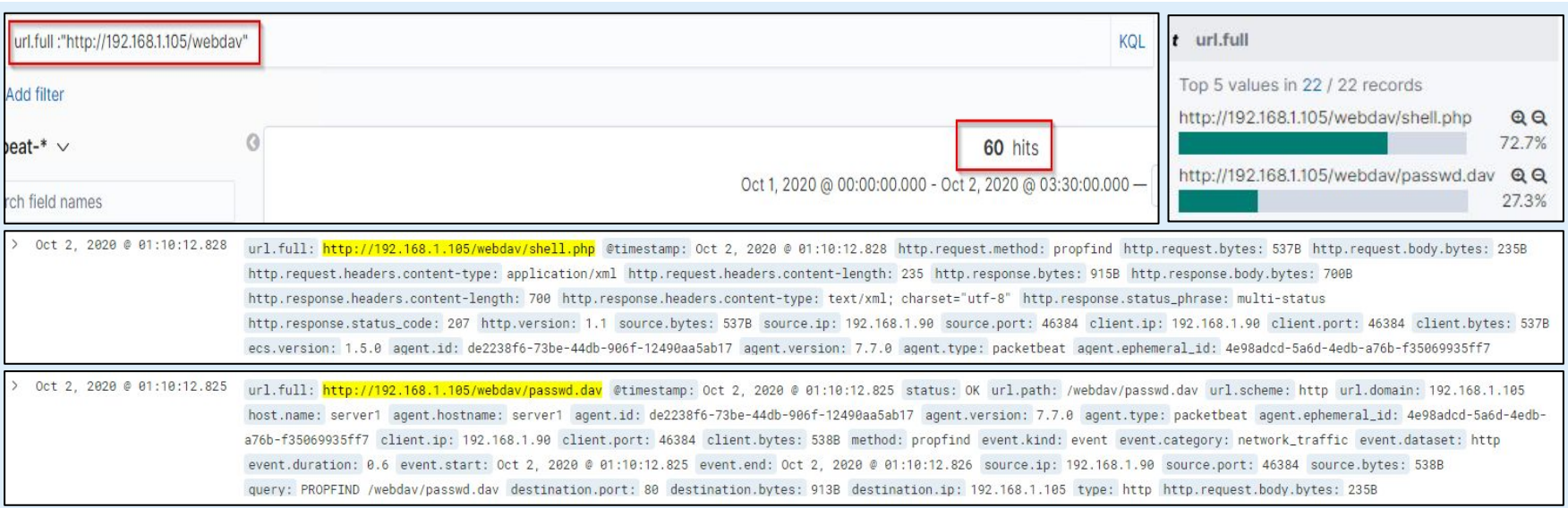

```
> Oct 1, 2020 @ 23:26:46.000  log.file.path: /var/log/apache2/access.log.2  user_agent.original: Mozilla/4.0 (Hydra)  agent.hostname: server1  agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a
agent.type: filebeat  agent.ephemeral_id: 2b77bd4d-dce6-4a0f-81c3-30300e4fd12b  agent.version: 7.7.0  log.offset: 68,985  source.address: 192.168.1.90  source.ip: 192.168.1.90
fileset.name: access  url.original: /company_folders/secret_folder  input.type: log  @timestamp: Oct 1, 2020 @ 23:26:46.000  ecs.version: 1.5.0  service.type: apache
host.name: server1  http.request.referrer: -  http.request.method: get  http.response.status_code: 401  http.response.body.bytes: 698B  http.version: 1.1  event.kind: event
event.created: Oct 5, 2020 @ 06:56:44.788  event.module: apache  event.category: web  event.dataset: apache.access  event.outcome: failure  user.name: ashton
```


```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" -
 10144 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ilovemom1"
 - 10145 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "getalife"
- 10146 of 14344399 [child 12] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leo
poldo
[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 202
0-10-01 16:27:54
root@Kali:~#
```

- How many requests were made in the attack? 10,000
- How many requests had been made before the attacker discovered the password? 10,146

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? 60
- Which files were requested? The files passwd.dav and the payload shell.php were requested

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 an alert in the SIEM to monitor the number of login attempts and time

What threshold would you set to activate this alarm?

- Have the alert trigger based on what user triggered it

System Hardening

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

- Turn off all unnecessary services on hosts
- Install firewall software on hosts

Describe the solution. If possible, provide required command lines.

- Setting up the firewall to block requests from network scanners
- Remove unnecessary services reducing possibility of exploitation

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- We can set an alarm to monitor the number of login attempts

What threshold would you set to activate this alarm?

- 3
- No baseline is needed as this is the standard number of attempts allowed

System Hardening

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

- Block the account if discover more than 3 attempts or if the attempts are done in a short period of time

Describe the solution. If possible, provide required command lines.

- Create an aleart that triggers after 3 attempts and automatically blocks the account

Mitigation: Preventing Brute Force Attacks

Alarm

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

- I would set an alarm in the SIEM that was set to detect multiple unsuccessful login attempts

What threshold would you set to activate this alarm?

- The alert would trigger after 3 unsuccessful attemps

System Hardening

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

- After 3 login attempts, the account will be locked

Describe the solution. If possible, provide the required command line(s).

- By setting the host, the vulnerability to brute force attacks is reduced because after three failed attemps the host stops responding to login requests

the End