INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

6COSC019C.2 Cyber Security

Coursework By

Shazan Fazal

20191172 | w1790385

Module Leader: Mr. Saman Hettiarachchi

May 2023

Contents

List of Figures

Scenario

A medium-sized medical clinic with 50 employees, including doctors, nurses, administrative staff, and IT personnel. The clinic offers a wide range of medical services, including general health check-ups, specialized treatments, and surgeries.

The clinic handles sensitive patient data, including medical histories, diagnoses, lab results, and financial information. Additionally, the clinic may also handle employee data, such as payroll and HR records. Due to the sensitive nature of the data, the clinic must comply with relevant healthcare regulations such as HIPAA.

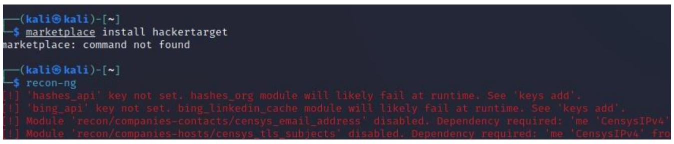
The clinic has three types of users: patients, employees, and third-party vendors. Patients access the clinic's system to book appointments, view their medical records, and make payments. Employees access the system to manage patient data, schedule appointments, and communicate with colleagues. Third-party vendors, such as labs and insurance companies, may access the system to exchange information with the clinic.

A- Information Gathering

A.1 OSINT Activities

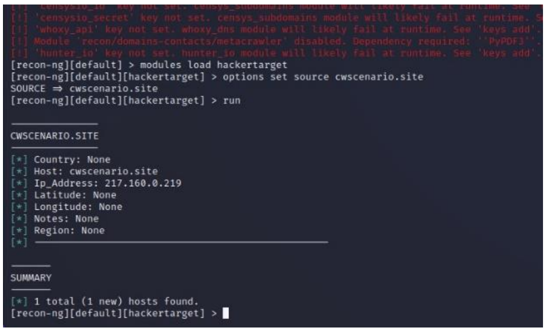
A.1.1 Examples

A.1.1.1 Recon-ng



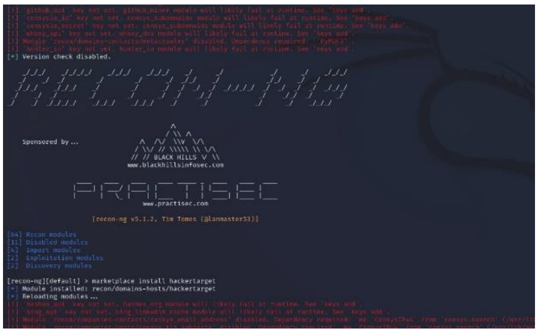
```
┌──(kali㉿kali)-[~]
└─$ marketplace install hackertarget
marketplace: command not found

┌──(kali㉿kali)-[~]
└─$ recon-ng
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: 'me 'CensysIPv4'
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'me 'CensysIPv4' fro
```

Figure 1 Recon-ng done with OSINT activity.



```
[!] 'censysio_id' key not set. censys_subdomains module will likely fail at runtime. See
[!] 'censysio_secret' key not set. censys_subdomains module will likely fail at runtime. S
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set source cwscenario.site
SOURCE ⇒ cwscenario.site
[recon-ng][default][hackertarget] > run

───────────────
CWSCENARIO.SITE
───────────────
[*] Country: None
[*] Host: cwscenario.site
[*] Ip_Address: 217.160.0.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > █
```

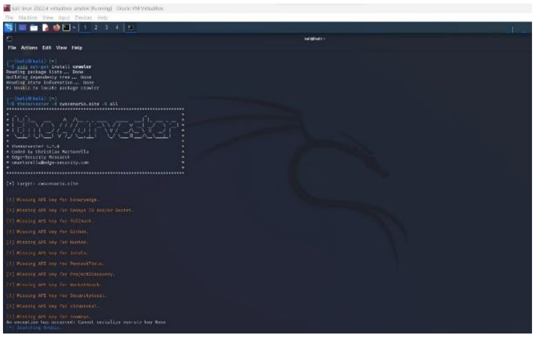
Figure 2 Recon-ng done with OSINT activity IMG-2.



```
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[*] Version check disabled.

    Sponsored by ...
                              BLACK HILLS
                       www.blackhillsinfosec.com

                            PRACTISEC
                         www.practisec.com

                 [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[84] Recon modules
[11] Disabled modules
[4]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: ''censysIPv4' from 'censys.search' (/usr/li
```

Figure 3 Recon-ng done with OSINT activity IMG-3.

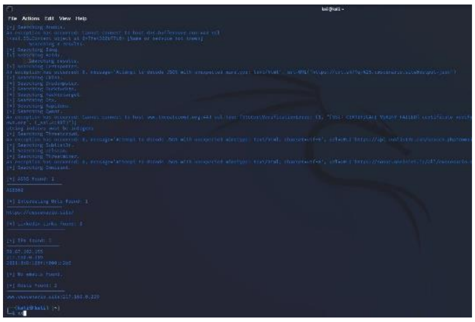
A.1.1.2 The Harvester



File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install crawler
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package crawler

┌──(kali㉿kali)-[~]
└─$ theHarvester -d cwscenario.site -b all
*******************************************************************
*                                                                 *
* theHarvester [illegible]                                        *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: cwscenario.site

[!] Missing API key for binaryedge.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for FullHunt.

[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for Intelx.

[!] Missing API key for PentestTools.

[!] Missing API key for ProjectDiscovery.

[!] Missing API key for RocketReach.

[!] Missing API key for Securitytrail.

[!] Missing API key for virustotal.

[!] Missing API key for Zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Anubis.
```

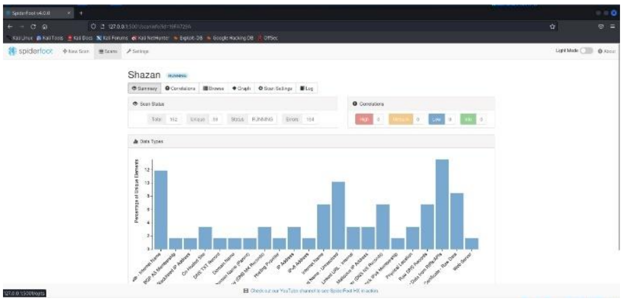
Figure 4 OSINT investigated by Harvester IMG-1.



```
[*] Searching Anubis.
An exception has occurred: Cannot connect to host [illegible]
[illegible] [Name or service not known]
        Searching 0 results.
[*] Searching Bing.
[*] Searching [illegible].
        Searching results.
[*] Searching [illegible].
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://[illegible]')
[*] Searching [illegible].
[*] Searching Dnsdumpster.
[*] Searching Duckduckgo.
[*] Searching Hackertarget.
[*] Searching Otx.
[*] Searching Rapiddns.
[*] Searching Qwant.
An exception has occurred: Cannot connect to host [illegible] [illegible]
[illegible]
string indices must be integers
[*] Searching Threatcrowd.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://[illegible]
[*] Searching Sublist3r.
[*] Searching urlscan.
[*] Searching Threatminer.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://[illegible]
[*] Searching Omnisint.

[*] ASNS found: 1
--------------------
AS5502

[*] Interesting Urls found: 1
--------------------
https://cwscenario.site/

[*] LinkedIn Links found: 0
--------------------

[*] IPs found: 3
--------------------
[illegible]
[illegible]
[illegible]

[*] No emails found.

[*] Hosts found: 2
--------------------
ww.cwscenario.site:217.160.0.220

┌──(kali㉿kali)-[~]
└─$
```

Figure 5 OSINT investigated by Harvester IMG-2.

A.1.1.3 Spider Foot



Total 152 Unique 59 Status RUNNING Errors 154

Figure 6 Spider foot was used to investigate OSINT.

A.1.2 Research and Evaluation

Open-Source Intelligence, or OSINT, is a vital weapon in penetration testers' toolbox. OSINT assists penetration testers in locating potential attack routes and vulnerabilities in a target organization's systems and infrastructure by acquiring publicly accessible information from a variety of sources, including social media, search engines, and governmental databases. Being non-invasive, or not requiring any direct contact with the target organization, is one of OSINT's main advantages. Because it can do so without letting the organization know about the testing, it serves as a useful first step in the penetration testing process.

Penetration testers can plan and carry out a more successful penetration testing strategy by using OSINT techniques to get a thorough grasp of the target organization's environment, including its technology stack, important individuals, and potential holes (sentinelone, 2023).

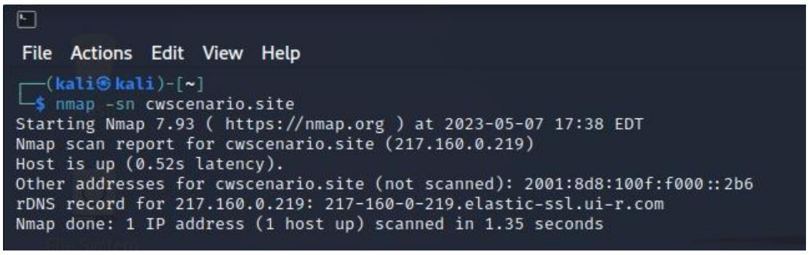
A.1.3 Scenario Assessment

The medical clinic's servers hold private information about patients and staff. These details comprise medical histories, diagnoses, test results, financial data, payroll information, and HR files. Due to its sensitivity, this material is a possible target for attackers, and serious consequences may result if they are successful in accessing it through data tampering.

Attackers may exploit this sensitive information to commit fraud, identity theft, or financial crimes if they are able to obtain it. Additionally, tampering with data might result in incorrect medical diagnosis and treatments, which lowers the standard of care patients receive. Compromises with employee data, such as those with payroll and HR records, can also result in problems including employee unhappiness, turnover, and legal concerns.

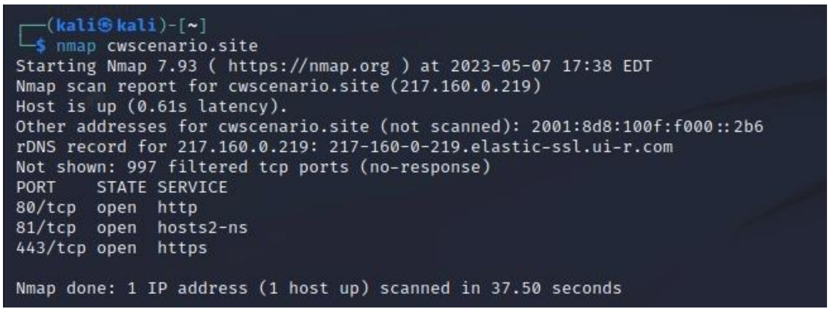
A.2 Reconnaissance

A.2.1 Testing Web Application



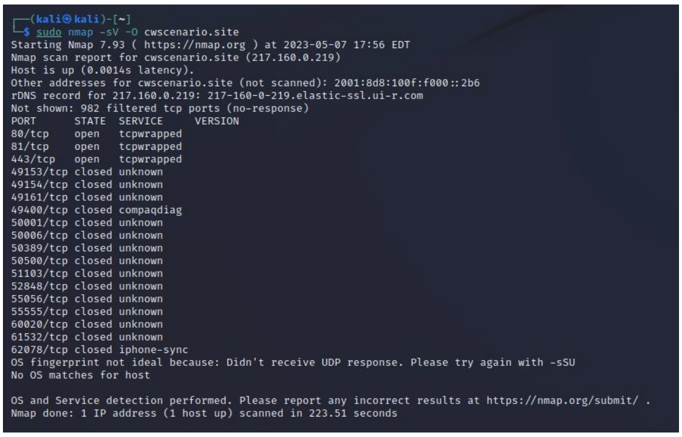
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn cwscenario.site
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 17:38 EDT
Nmap scan report for cwscenario.site (217.160.0.219)
Host is up (0.52s latency).
Other addresses for cwscenario.site (not scanned): 2001:8d8:100f:f000::2b6
rDNS record for 217.160.0.219: 217-160-0-219.elastic-ssl.ui-r.com
Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

Figure 7 Checking if the host is available.



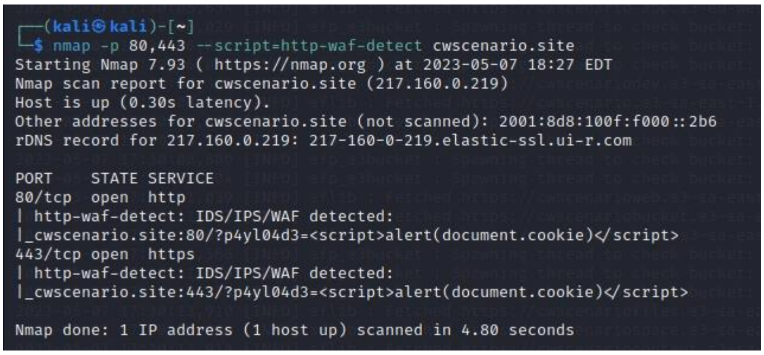
```
┌──(kali㉿kali)-[~]
└─$ nmap cwscenario.site
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 17:38 EDT
Nmap scan report for cwscenario.site (217.160.0.219)
Host is up (0.61s latency).
Other addresses for cwscenario.site (not scanned): 2001:8d8:100f:f000::2b6
rDNS record for 217.160.0.219: 217-160-0-219.elastic-ssl.ui-r.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
81/tcp  open  hosts2-ns
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 37.50 seconds
```

Figure 8 Checked the open TCP port of the relevant server.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O cwscenario.site
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 17:56 EDT
Nmap scan report for cwscenario.site (217.160.0.219)
Host is up (0.0014s latency).
Other addresses for cwscenario.site (not scanned): 2001:8d8:100f:f000::2b6
rDNS record for 217.160.0.219: 217-160-0-219.elastic-ssl.ui-r.com
Not shown: 982 filtered tcp ports (no-response)
PORT      STATE  SERVICE     VERSION
80/tcp    open   tcpwrapped
81/tcp    open   tcpwrapped
443/tcp   open   tcpwrapped
49153/tcp closed unknown
49154/tcp closed unknown
49161/tcp closed unknown
49400/tcp closed compaqdiag
50001/tcp closed unknown
50006/tcp closed unknown
50389/tcp closed unknown
50500/tcp closed unknown
51103/tcp closed unknown
52848/tcp closed unknown
55056/tcp closed unknown
55555/tcp closed unknown
60020/tcp closed unknown
61532/tcp closed unknown
62078/tcp closed iphone-sync
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 223.51 seconds
```

Figure 9 The Host Operating system was identified along with their versions of open ports.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,443 --script=http-waf-detect cwscenario.site
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 18:27 EDT
Nmap scan report for cwscenario.site (217.160.0.219)
Host is up (0.30s latency).
Other addresses for cwscenario.site (not scanned): 2001:8d8:100f:f000::2b6
rDNS record for 217.160.0.219: 217-160-0-219.elastic-ssl.ui-r.com

PORT    STATE SERVICE
80/tcp  open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_cwscenario.site:80/?p4yl04d3=<script>alert(document.cookie)</script>
443/tcp open  https
| http-waf-detect: IDS/IPS/WAF detected:
|_cwscenario.site:443/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds
```

Figure 10 Checking of the firewall is enabled.

A.2.2 Scenario Assessment

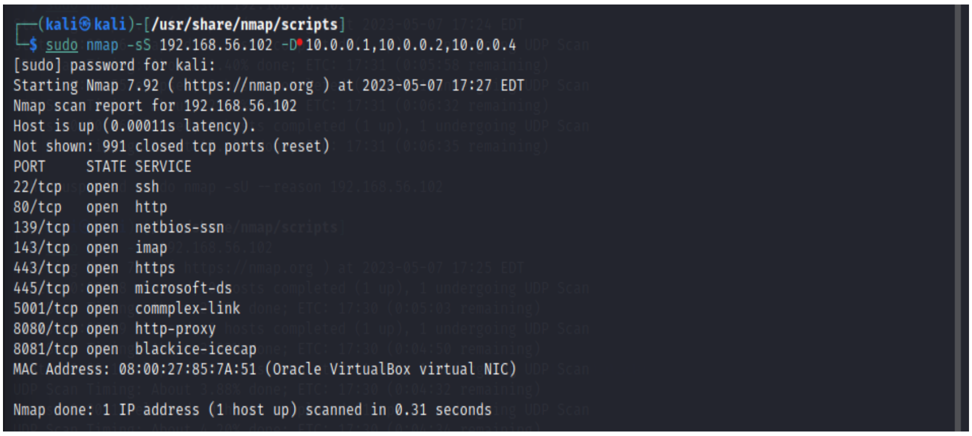
An essential step in the web application testing process is reconnaissance and data collecting. Gathering data on the target system, including its IP address, network topology, web applications, operating systems, and other pertinent data, is a step in this procedure. In the future, it will be possible to take advantage of a company's web services using the information gathered throughout this process.

The medium-sized medical clinic in the scenario handles sensitive patient data, necessitating adherence to HIPAA requirements. A hacker with access to the clinic's web services could take financial information, medical histories, diagnoses, and lab results in addition to other private data.

For example, if a hacker conducts reconnaissance on the clinic's online application, they can learn about the design, data flows, and data storage of the system. With the aid of this data, holes in the system's defenses that could be exploited to allow unauthorized access can be found. Once they gain access, they can steal confidential information, put ransomware or other malicious software on the system, or launch other assaults that might seriously harm the clinic's operations.

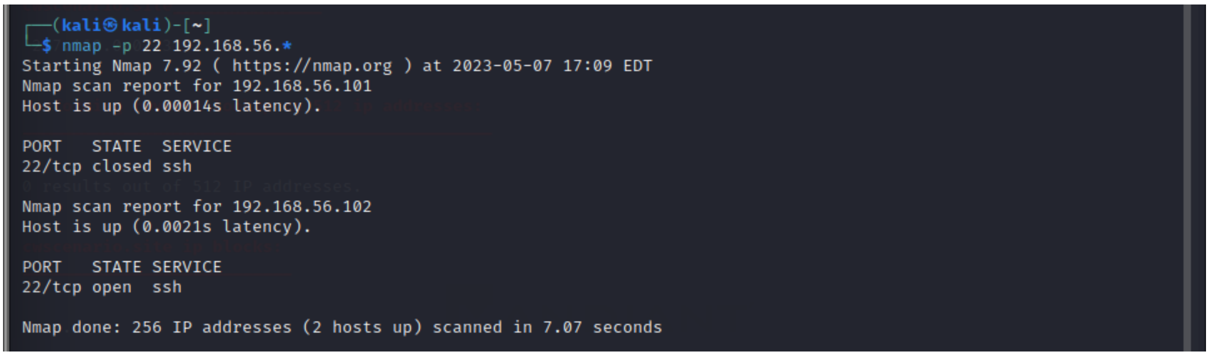
A.3 Port Scanning and Enumeration

A.3.1 Identified Ports



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS 192.168.56.102 -D 10.0.0.1,10.0.0.2,10.0.0.4
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-07 17:27 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00011s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:85:7A:51 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Figure 11 Scanning and enumerating the open ports using the nmap



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 192.168.56.*
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-07 17:09 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00014s latency).

PORT   STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 192.168.56.102
Host is up (0.0021s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 7.07 seconds
```

Figure 12 The remote access port is being scanned.

A.3.2 Research

An open port is an endpoint for network communication that enables data to flow to a product or service. For many network services, like email, web browsing, and file sharing, it is necessary. Threats like malware infestations, denial-of-service (DoS) assaults, and unwanted access could all result from an exposed port. Attackers can use open ports to their advantage by looking for weak points, exploiting vulnerabilities to obtain access, and installing malware or ransomware to encrypt or steal data.

A.3.3 Scenario Assessment

The medical clinic's network has several open ports. Since these open ports present possible entry points for attackers to exploit, they pose a serious threat to the clinic's sensitive patient and employee data.

Open ports may put the clinic's network and systems at risk by allowing attackers unrestricted access. To access the clinic's internal network, for instance, an attacker could utilize an open port to get past the firewalls. As a result, the attacker might be able to steal or manipulate private data on clients and staff, including financial and medical records, medical histories, and lab results. Further compromising the security and integrity of the data is the possibility that an attacker may utilize the clinic's network's open ports to introduce malware or other harmful software.

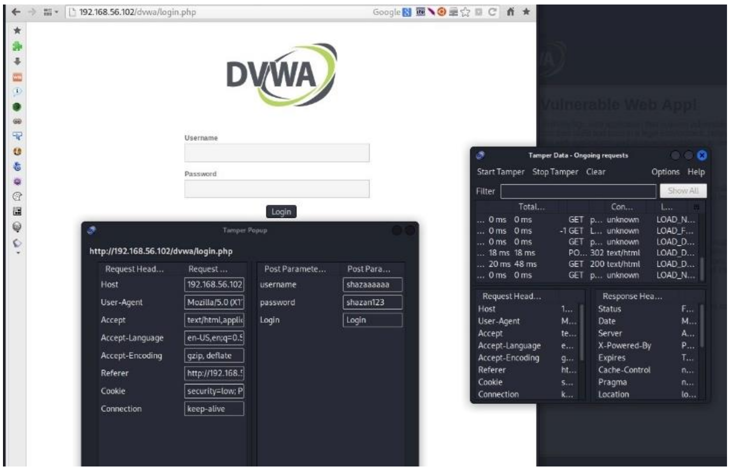
Open ports may also expose the clinic's network and systems to assault by enabling attackers to conduct analysis on them. An attacker can learn about the applications and services running on the clinic's network by looking for open ports, which could help them find security holes and weaknesses they can exploit. For instance, if a hacker discovers an open port using an out-of-date, unpatched version of software, they may exploit this flaw to access the clinic's network and steal or modify data.

These open ports provide possible points of entry for attackers to access the clinic's network and systems without authorization, steal or alter data, and perform reconnaissance to find flaws and vulnerabilities to exploit.

B- Server-Side Exploits

B.1 Data tampering

B.1.1 Vulnerability



192.168.56.102/dvwa/login.php

Tamper Popup

http://192.168.56.102/dvwa/login.php

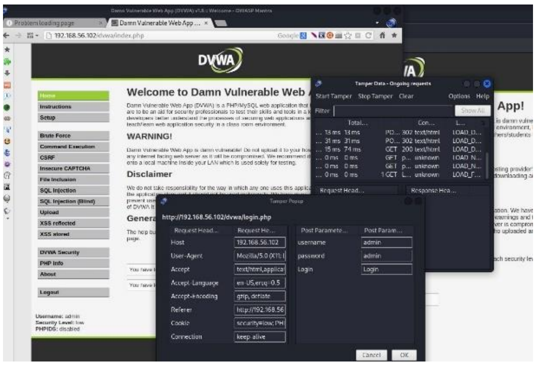
Request Head...	Request ...
Host	192.168.56.102
User-Agent	Mozilla/5.0 (X1
Accept	text/html,applic
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://192.168.5
Cookie	security=low; P
Connection	keep-alive

Post Paramete...	Post Para...
username	shazaaaaaa
password	shazan123
Login	Login

```
    Total...         Con...             L...
... 0 ms   0 ms      GET   p...  unknown      LOAD_N...
... 0 ms   0 ms    -1 GET  L...  unknown      LOAD_F...
... 0 ms   0 ms      GET   p...  unknown      LOAD_D...
... 18 ms  18 ms     PO... 302 text/html      LOAD_D...
... 20 ms  48 ms     GET   200 text/html      LOAD_D...
... 0 ms   0 ms      GET   p...  unknown      LOAD_N...
```

Request Head...		Response Hea...	
Host	1...	Status	F...
User-Agent	M...	Date	M...
Accept	te...	Server	A...
Accept-Language	e...	X-Powered-By	P...
Accept-Encoding	g...	Expires	T...
Referer	ht...	Cache-Control	n...
Cookie	s...	Pragma	n...
Connection	k...	Location	lo...

Figure 13 Credential Retrieval process



192.168.56.102/dvwa/index.php

Welcome to Damn Vulnerable Web

Username: admin
Security Level: low
PHPIDS: disabled

Tamper Popup

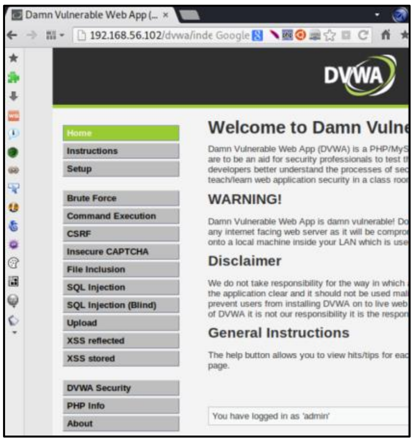
http://192.168.56.102/dvwa/login.php

Request Head...	Request He...
Host	192.168.56.102
User-Agent	Mozilla/5.0 (X11;
Accept	text/html,applica
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://192.168.56
Cookie	security=low; PH
Connection	keep-alive

Post Paramete...	Post Param...
username	admin
password	admin
Login	Login

```
    Total...         Con...             L...
... 13 ms  13 ms     PO... 302 text/html      LOAD_D...
... 31 ms  31 ms     PO... 302 text/html      LOAD_D...
... 15 ms  74 ms     GET   200 text/html      LOAD_D...
... 0 ms   0 ms      GET   p...  unknown      LOAD_N...
... 0 ms   0 ms      GET   p...  unknown      LOAD_N...
... 0 ms   0 ms     1 GET  L...  unknown      LOAD_F...
```

Figure 14 Data tampering made with known credentials.



192.168.56.102/dvwa/inde

Welcome to Damn Vulne

Damn Vulnerable Web App (DVWA) is a PHP/MyS are to be an aid for security professionals to test t developers better understand the processes of sec teach/learn web application security in a class roo

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do any internet facing web server as it will be compro onto a local machine inside your LAN which is use

Disclaimer

We do not take responsibility for the way in which the application clear and it should not be used mal prevent users from installing DVWA on to live web of DVWA it is not our responsibility it is the respon

General Instructions

The help button allows you to view hits/tips for eac page.

You have logged in as 'admin'

Figure 15 Success Authenticated with tempered data.

B.1.2 Research

Data tampering refers to modifying or deleting resources without user authorization. Data tampering in online applications is the process by which a hacker or other suspicious person enters a website and modifies, deletes, or gains access to unapproved files. A hacker or malicious user can potentially interfere inadvertently by employing a script vulnerability, which allows the script to run by disguising it as user input from a page or a web link. Data tempering started in the 1980's in way to sabotage data to delete data (Francis, 2014).

Data tampering is against the **integrity** principle of cyber security.

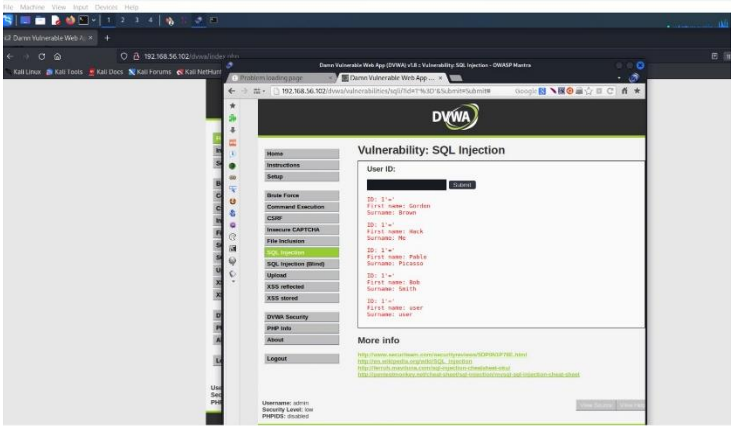
B.1.3 Scenario Assessment

Data tampering poses a severe risk to the servers at the medical clinic's security of the sensitive data kept there. Attackers could possibly access a massive amount of medical and staff data, which could have serious repercussions for people's security and privacy. Since correct medical information is essential for proper diagnosis, treatment, and overall healthcare outcomes, data integrity is crucial in the medical industry. Therefore, it is possible for sensitive data to be changed, removed, or added with serious consequences.

Data manipulation can have serious repercussions for the medical clinic, its clients, and its staff. Attackers can alter the data to their benefit, which can result in incorrect diagnosis and treatments, phony claims, and financial loss. Additionally, tampering with data can result in a breach of confidence between a clinic and its stakeholders, harming the clinic's reputation and influencing its commercial operations.

B.2 SQL injection

B.2.1 Vulnerability



Vulnerability: SQL Injection

User ID:

```
ID: 1'='
First name: Gordon
Surname: Brown

ID: 1'='
First name: Hack
Surname: Me

ID: 1'='
First name: Pablo
Surname: Picasso

ID: 1'='
First name: Bob
Surname: Smith

ID: 1'='
First name: user
Surname: user
```

More info

Username: admin
Security Level: low
PHPIDS: disabled

Figure 16 SQL injection returning multiple data.

B.2.2 Research

An attacker can enter malicious SQL statements into input fields and carry out unauthorized operations on a database using a vulnerability known as SQL injection in online applications.

Data theft, modification, or deletion as well as system compromise can arise through this(VanMSFT, 2023).

The **confidentiality**, **integrity**, and **availability** principles are broken by SQL injection.

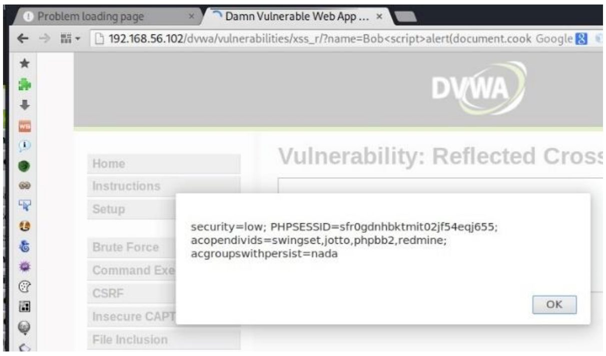
B.2.3 Scenario Assessment

An attacker who successfully conducts a SQL injection attack in the context of the medical clinic scenario may be able to get sensitive patient data, such as medical histories, diagnoses, lab results, and financial information. The attacker might also get access to employee data, including payroll and HR records.

It would be extremely risky for the medical clinic if such an assault succeeded since it might jeopardize critical data, which could result in patient distrust, legal action, and financial losses.

B.3 XSS Scripting

B.3.1 Vulnerability



```
192.168.56.102/dvwa/vulnerabilities/xss_r/?name=Bob<script>alert(document.cook
```

```
security=low; PHPSESSID=sfr0gdnhbktmit02jf54eqj655;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
```

Figure 17 PHPSESSID cookie as an alert showed

B.3.2 Research

The attacker uses web-applications to send malicious code which would deal with users' interaction with insecure application. During this threat the users will not be notification or cannot identify that it came from an untrusted source. In fact, the attacker will be able to access cookies, session tokens and any other sensitive information the browser collects (Rick-Anderson, 2023) .

Confidentiality and **Integrity** are the cyber security principles that were broken in this attack.

B.3.3 Scenario Assessment

In the case of medical clinics, an attacker could introduce malicious scripts that steal user data, including session cookies or login credentials, by taking advantage of an XSS vulnerability in the clinic's servers.

Once an attacker has access to a user's session, they may be able to read or change any sensitive data that the clinic holds, including patient information, financial data, and other details. If the clinic doesn't follow healthcare rules like HIPAA, this could result in a breach of patient confidence, a loss of confidentiality, and even legal consequences.

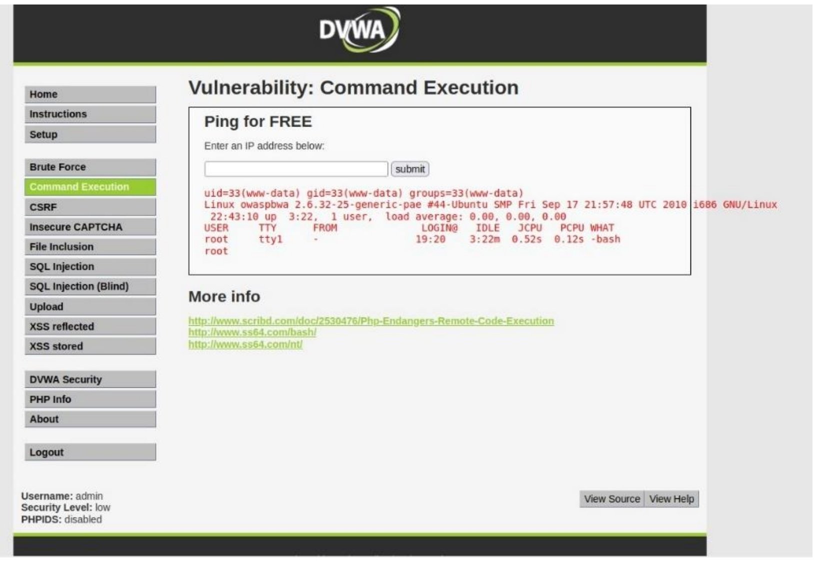
Additionally, a hacker might utilize the clinic's server as a distribution point for malware or phishing scams to target unwary individuals, such as staff members or outside suppliers who access the server. This could result in future data and system compromises for the clinic, harm to the clinic's reputation, and financial losses.

B.4 OWASP

B.4.1 Other Vulnerabilities

B.4.1.1 Command Execution

Web applications frequently have security flaws called "command execution vulnerabilities" that let attackers run arbitrary server-side code. By validating input data, cleaning up user input, implementing secure coding techniques, segregating privileges, and keeping an eye out for unusual activities, these attacks can be avoided.



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
 22:43:10 up  3:22,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                19:20    3:22m  0.52s  0.12s -bash
root
```

More info

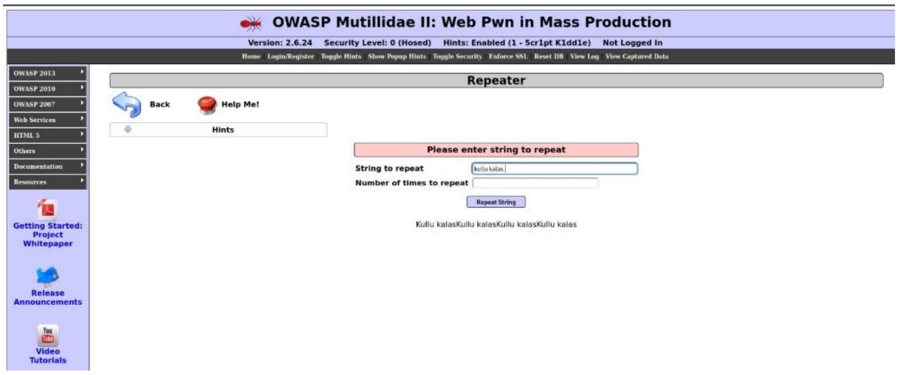
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: low
PHPIDS: disabled

Figure 18 To obtain information with command execution

B.4.1.2 Buffer overflow vulnerability

When a computer attempts to write more data to a buffer in memory than the buffer can contain, a vulnerability called a buffer overflow takes place. Adjacent memory locations may be overwritten as a result, which an attacker may use to inject and run malicious code. Poor input validation or utilizing unsafe programming languages are two common causes of buffer overflow vulnerabilities.



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

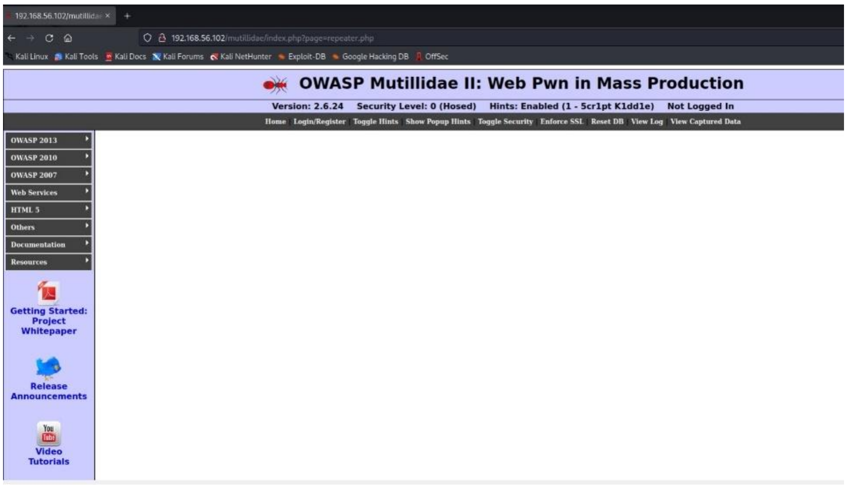
Repeater

Please enter string to repeat

String to repeat: kullu kalas

Number of times to repeat:

Kullu kalasKullu kalasKullu kalasKullu kalas



192.168.56.102/mutillidae/index.php?page=repeater.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

B.4.2 Scenario Assessment

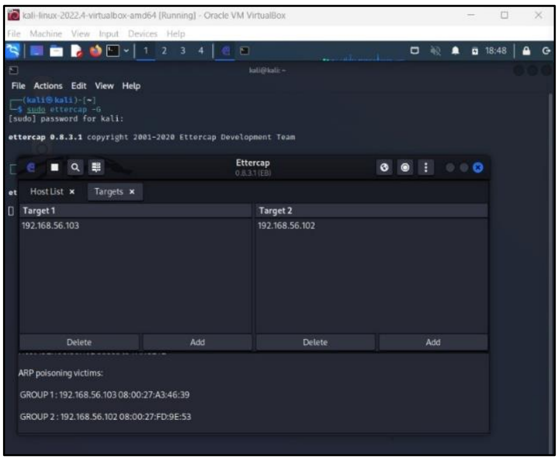
By executing arbitrary instructions on the server that hosts the web application, command execution vulnerabilities could provide an attacker access to sensitive information or total control of the system. An attacker may, for instance, upload a file containing malicious code for the server to execute with elevated privileges or insert malicious code into a form's input field. The attacker could then make use of this access to steal sensitive information such as patient data, financial information, or other data.

Attackers may also use buffer overflow flaws to gain control of the server or run malicious code. An attacker could provide an input that causes a server with a buffer overflow vulnerability to overflow and overwrite nearby memory, allowing them to run whatever code they want. The attacker might then have complete control over the server, which they could use to steal confidential information or carry out assaults on other targets.

C- Client-side exploits

C.1 Man in the Middle Attack (MiTM)

C.1.1 Traffic Capture

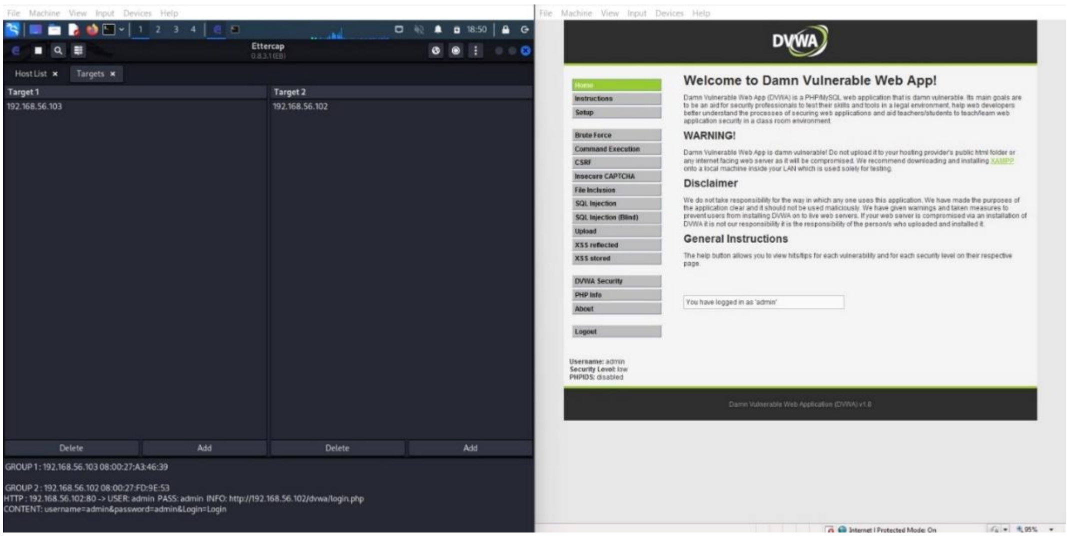

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:48
kali@kali: ~
File Actions Edit View Help
Ettercap
0.8.3.1 (EB)
Host List
Targets
Delete
Add
Delete
Add

```
┌──(kali㉿kali)-[~]
└─$ sudo ettercap -G
[sudo] password for kali:

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

Target 1	Target 2
192.168.56.103	192.168.56.102

```
ARP poisoning victims:

GROUP 1 : 192.168.56.103 08:00:27:A3:46:39

GROUP 2 : 192.168.56.102 08:00:27:FD:9E:53
```

Figure 19 execution of Ettercap to listen.



Target 1	Target 2
192.168.56.103	192.168.56.102

```
GROUP 1 : 192.168.56.103 08:00:27:A3:46:39

GROUP 2 : 192.168.56.102 08:00:27:FD:9E:53
HTTP : 192.168.56.102:80 -> USER: admin  PASS: admin  INFO: http://192.168.56.102/dvwa/login.php
CONTENT: username=admin&password=admin&Login=Login
```

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Figure 20 Data captured once the user logged with Ettercap.

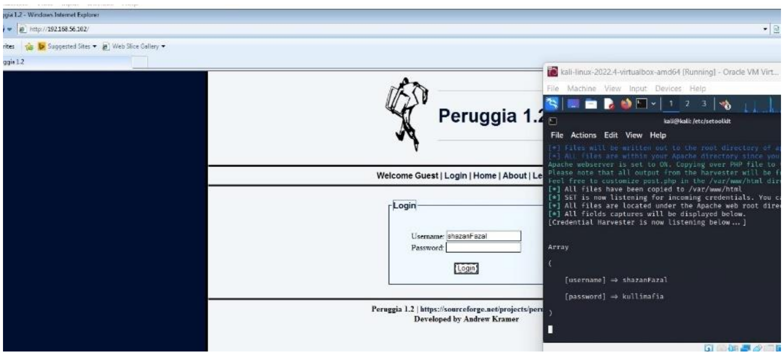
C.1.2 Scenario Assessment

A man in the middle attack (MiTM) involves the attacker listening in on, changing, or injecting messages into a conversation between two parties. Sensitive information, including patient data, employee data, and financial information, may be compromised if a MiTM attack is conducted on the clinic's client-side system. Attackers could get session cookies, login information, and other sensitive information that could be exploited to log into the system without authorization.

For instance, a hacker could obtain a worker's or a third-party vendor's login information, granting them access to private medical and financial information. Additionally, they might introduce malware or harmful code into the communication stream, which might be used to corrupt or alter data or even take over the system.

C.2 Social Engineering Attack

C.2.1 Attack Capture


Peruggia 1.2 - Windows Internet Explorer
http://192.168.56.102/
Suggested Sites
Web Slice Gallery
Peruggia 1.2
Peruggia 1.2
Welcome Guest | Login | Home | About | Le
Login
Login
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM Virt...
File Machine View Input Devices Help
kali@kali: /etc/setoolkit
File Actions Edit View Help

Username: shazanFazal
Password:

Peruggia 1.2 | https://sourceforge.net/projects/peru
Developed by Andrew Kramer

```
[*] Files will be written out to the root directory of a
[*] All files are within your Apache directory since you
Apache webserver is set to ON. Copying over PHP file to
Please note that all output from the harvester will be f
Feel free to customize post.php in the /var/www/html dir
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You ca
[*] All files are located under the Apache web root dire
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]


Array
(
    [username] => shazanFazal
    [password] => kullimafia
)
```

Figure 21 Capturing credential of the users

C.2.2 Scenario Assessment

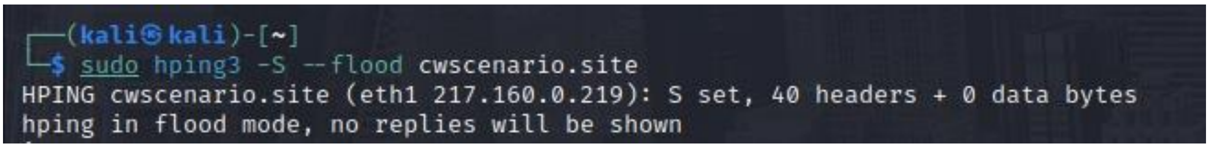
Attacks of this kind, known as social engineering, aim to manipulate people into disclosing private information or carrying out security-compromising behaviours. Attackers can use social engineering techniques to gather sensitive patient and personnel data in the context of the medical clinic scenario. Attackers may assume the identity of an IT administrator or a third-party vendor, for instance, and coerce staff members into revealing critical information like login passwords. Alternately, attackers can utilize social engineering strategies to get victims to divulge their financial or personal information.

Due to the potential for data breaches and the exposure of private patient and employee information, these assaults constitute a serious risk to the medical clinic. A data breach might cost the clinic money, but it can also harm the clinic's reputation.

D - Denial of Service attacks

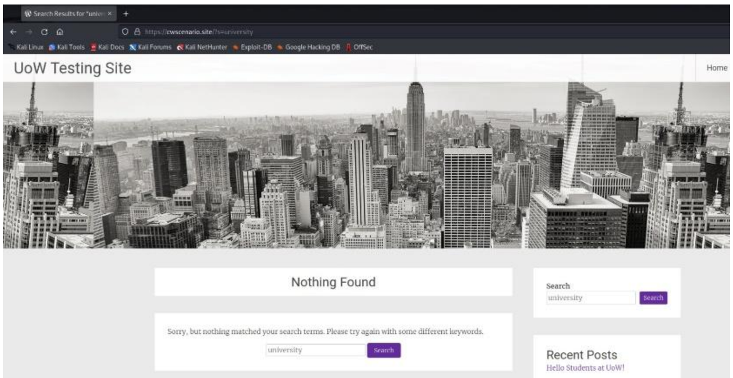
D.1 DoS the web server

D.1.1 Attacker



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S --flood cwscenario.site
HPING cwscenario.site (eth1 217.160.0.219): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 22 Command to flood

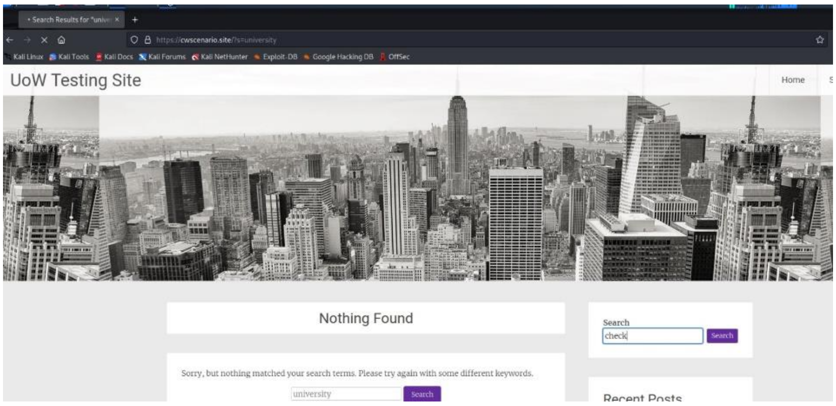


UoW Testing Site

Nothing Found

Sorry, but nothing matched your search terms. Please try again with some different keywords.

Figure 23 Before search query



UoW Testing Site

Nothing Found

Sorry, but nothing matched your search terms. Please try again with some different keywords.

Figure 24 After search query

D.1.2 Cyber Security Tenet Violation

The Availability tenet of cyber security is broken by the web server's vulnerability to a Denial of Service (DoS) attack. Assuring timely, uninterrupted access to information and services for authorized users is referred to as availability. The goal of a DoS attack is to make the web server unavailable to legitimate users by flooding it with traffic. By interfering with business processes and resulting in losses, this kind of attack can seriously harm a corporation.

D.1.3 Scenario Assessment

Since the clinic's website and patient portal are utilized for patient communication, appointment scheduling, and access to medical records, the web server is a crucial part of how the clinic runs. These services could become unavailable because of a DoS attack on the web server, seriously disrupting clinic operations and having an adverse effect on patient care. Patients who are unable to access the clinic's services may seek care elsewhere, which could cause the clinic to lose money and harm its reputation. The clinic may also have to pay costs related to mitigating the assault, such as paying security consultants, buying more technology, or putting money into stronger defences to thwart future attacks.

E- Recommendations to protect the scenario company server.

E.1 Reconnaissance phase

When testing a web application, there are a few things that can be done to reduce the risks to the results from the reconnaissance phase. First off, it is advised to restrict the information an attacker can gather during the reconnaissance phase. This can be achieved by clearing out extraneous data from sources that are accessible to the public, like websites and social media profiles. Adding firewalls, intrusion detection systems, and other security measures can also aid in spotting and blocking attacks. To stop vulnerabilities from being exploited, software and systems need to be updated and patched often. Finally, carrying out routine security audits and penetration tests can assist in locating and addressing any vulnerabilities in the web application (Lyon, 2009).

E.2 Port Knocking

Port knocking is a method for enhancing network security by permitting access to some ports that are typically locked down. Sending connection requests to a set of predetermined ports on a server causes it to open those ports to incoming traffic. The ports will be shut down after the process is finished. This makes it more difficult for attackers to access a system because they would need to be aware of the precise sequence to do so. By reducing the number of open ports available to attackers and making it more challenging to find and exploit vulnerabilities, port knocking can help defend against threats discovered during the reconnaissance phase(Jithin, 2017).

E.3 SQL Injection exploits

Implementing effective input validation and parameterized queries is crucial for safeguarding a database against SQL injection attacks. Input validation involves verifying that user inputs, such as form data, are in the desired format and fall within allowable bounds. Instead of having user input directly in the query, parameterized queries employ placeholders for user input that are later substituted with filtered values at runtime.

Access controls should also be put in place to limit access to sensitive information and processes. This entails setting up role-based access restrictions, setting user role-based permission boundaries, and making sure that only authenticated and permitted users can access the database. Regular security testing and audits can assist in finding weaknesses and guarantee the security of the database. Keeping software and systems up to date with the most recent security patches and defenses can also help stop known vulnerabilities from being exploited (VanMSFT, 2023).

E.4 Cross site scripting

Implementing input validation and output encoding techniques is crucial for defending a web application from Cross-Site Scripting (XSS) attacks. While output encoding makes sure that any user-supplied data is properly encoded to prevent it from being executed as script, input validation entails filtering user input to remove any dangerous scripts or characters. To prevent XSS attacks, web developers should also employ frameworks that include built-in security mechanisms, like Content Security Policy (CSP) and HTTP-only cookies. Regular security audits and penetration tests can also aid in locating and addressing any potential web application vulnerabilities (Wickramasinghe, 2023).

E.5 Security Analyst

To prevent or lessen the effects of Man in the Middle (MitM) attacks, security analysts can put in place several safeguards, including end-to-end encryption, digital certificates, and secure protocols like HTTPS, intrusion detection and prevention tools, network segmentation, vulnerability analyses, and user education and awareness training. These steps can lessen the harm caused by MitM attacks and aid in their detection or prevention.

E.6 Social Engineering Attack

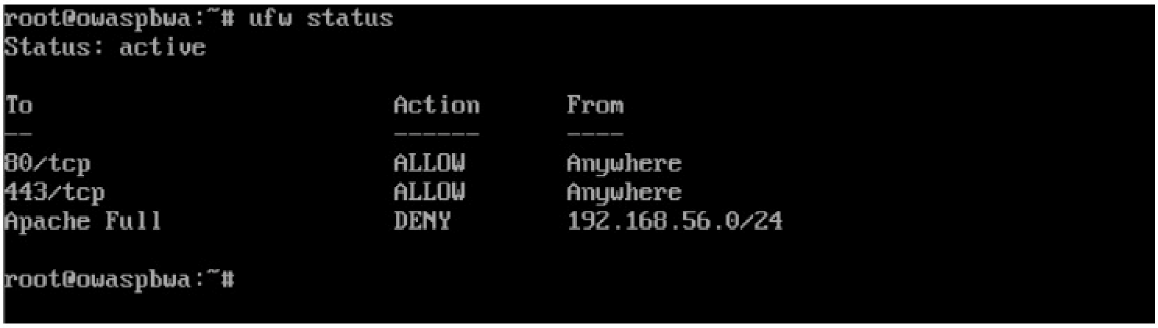
Companies can take several actions to protect people from social engineering assaults. Employee education and awareness campaigns can be regularly held to inform staff members of the risks posed by social engineering attacks and how to protect themselves. Access controls, two-factor authentication, and strong password policies are some measures that businesses can take to restrict an attacker's access to information. Phishing emails and other dangerous content can also be stopped using email filters and anti-malware software. Security monitoring tools can also be used by businesses to track suspicious user activity and spot potential security lapses. Finally, organizations should have an incident response strategy in place to react swiftly and successfully to any potential security incidents (Fruhlinger, 2022).

E.7 DoS Attack

Companies can use a range of defences against DoS assaults, including load balancing, rate limiting, and traffic filtering. To recognize and stop suspicious traffic, they can also employ intrusion detection and prevention systems. Assessments of vulnerabilities and testing on a regular basis can help to spot any gaps in their defences (James, 2022).

E.8 Intrusion Detection and Prevention System

E.8.1 Examples of firewall and iptables



```
root@owaspbwa:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
Apache Full                DENY        192.168.56.0/24

root@owaspbwa:~#
```

E.8.2 Tools Evaluation

E.8.2.1 Firewall (UFW) and iptables

To prevent unwanted access, a firewall must be installed because of the clinic's sensitive data. For the circumstances of the clinic, ufw and iptables are both viable firewall choices. Administrators may quickly configure and administer firewall rules using the user-friendly interface for iptables known as ufw. The command-line tool iptables, on the other hand, offers more customization and control choices.

Both ufw and iptables are quite successful at defending against network assaults like DDoS, port scanning, and unwanted access attempts. They can also be set up to block traffic coming from IP addresses or ports.

Due to its user-friendly interface, which makes firewall configuration and management easier in the present case, ufw is the better choice. Because it's a medical clinic, the employees might not have a lot of technological expertise, and ufw makes management simpler without sacrificing security. The clinic's advanced technical IT staff, on the other hand, might like using iptables for finer-grained control over the firewall. The clinic's unique needs and available resources will ultimately determine which of ufw and iptables to use.

E.8.3 Difference between Intrusion Detection System and Intrusion Prevention System

A network's potential dangers can be found and dealt with using intrusion detection systems (IDS) and intrusion prevention systems (IPS). The main distinction between the two is that while IPS actively blocks or removes communication that is considered risky, IDS passively scans network traffic for suspicious activities and notifies administrators.

IDSs can be either host-based or network-based systems. Network-based IDS (NIDS) tracks network traffic and evaluates it in comparison to a set of rules to find potential risks. Individual hosts have host-based IDS (HIDS) installed, which keeps track of activity on the host.

The goal of IPS, on the other hand, is to actively prevent attacks by throttling or discarding suspicious traffic. A network-based system (NIPS) or a host-based system (HIPS) can both be used as IPS. While HIPS is placed on individual hosts and can stop assaults on the host itself, NIPS monitors network traffic and stops harmful traffic before it reaches its intended target.

While both IDS and IPS are used to identify and stop network attacks, IDS monitors and notifies in a passive manner while IPS aggressively drops traffic. The organization's specific needs and available resources will determine which option is best.

E.8.4 Scenario Assessment

A firewall like ufw is recommended over iptables for a medium-sized medical clinic managing sensitive patient data, such as medical histories, diagnoses, lab results, and financial information. UFW offers a higher level of security against unauthorized access and malware threats and is simpler to set up and configure. Additionally, it enables the clinic to regulate incoming and outgoing network traffic by restricting access to IP addresses and ports. Overall, ufw provides a more straightforward and efficient solution for safeguarding patient and staff data while continuing to permit critical interaction with third-party providers.

References

Fortinet. (2023). What is Cross-Site Scripting (XSS)? How to Prevent it? *Fortinet*. Available from https://www.fortinet.com/resources/cyberglossary/cross-site-scripting?utm_source=blog&utm_medium=blog&utm_campaign=cross-site-scripting [Accessed 7 May 2023].

Francis, A. (2014). Data Tampering - Meaning, Types and Countermeasures. *MBA Knowledge Base*. Available from https://www.mbaknol.com/information-systems-management/data-tampering-meaning-types-and-countermeasures/ [Accessed 7 May 2023].

Fruhlinger, J. (2022). Social engineering: Definition, examples, and techniques. *CSO Online*. Available from https://www.csoonline.com/article/3648654/social-engineering-definition-examples-and-techniques.html [Accessed 8 May 2023].

James, R. (2022). Denial-of-service attacks (DoS) - Types And Preventions A Complete Guide. *BeEncrypted*. Available from https://beencrypted.com/cybersec/network/denial-of-service-attacks-dos/ [Accessed 8 May 2023].

Jithin, P.M. (2017). What is Port Knocking? *Interserver Tips*. Available from https://www.interserver.net/tips/kb/what-is-port-knocking/ [Accessed 7 May 2023].

Kurt Baker. (2023). What is OSINT Open Source Intelligence? - CrowdStrike. *crowdstrike.com*. Available from https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/ [Accessed 8 May 2023].

Lyon, G.F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA, USA: Insecure.

PortSwigger. (2023). What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy. Available from https://portswigger.net/web-security/cross-site-scripting [Accessed 7 May 2023].

Rick-Anderson. (2023). Prevent Cross-Site Scripting (XSS) in ASP.NET Core. Available from https://learn.microsoft.com/en-us/aspnet/core/security/cross-site-scripting [Accessed 7 May 2023].

Sandipan Roy. (2022). Cross-site scripting: Explanation and prevention with Go. *Red Hat Developer*. Available from https://developers.redhat.com/articles/2022/06/28/cross-site-scripting-explanation-and-prevention-go [Accessed 7 May 2023].

sentinelone. (2023). What is Open Source Intelligence (OSINT)? *SentinelOne*. Available from https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/ [Accessed 8 May 2023].

Shanika Wickramasinghe. (2023). Cross-Site Scripting (XSS) Attacks & How To Prevent Them. *Splunk-Blogs*. Available from https://www.splunk.com/en_us/blog/learn/cross-site-scripting-xss-attacks.html [Accessed 7 May 2023].

VanMSFT. (2023). SQL Injection - SQL Server. Available from https://learn.microsoft.com/en-us/sql/relational-databases/security/sql-injection [Accessed 7 May 2023].