



Cybersecurity Internship Task Report

Name: Apurba Bera

Report-Date: 06/06/2024

Task Level: Beginner



E-Learning Providers

Table of contents

Task Level (Beginner)

1. Task 1...

Command

Findings

Mitigations

2. Task 2...

Commen

Findings

Mitigations

3. Task 3...

Filter used

Credentials

Mitigations

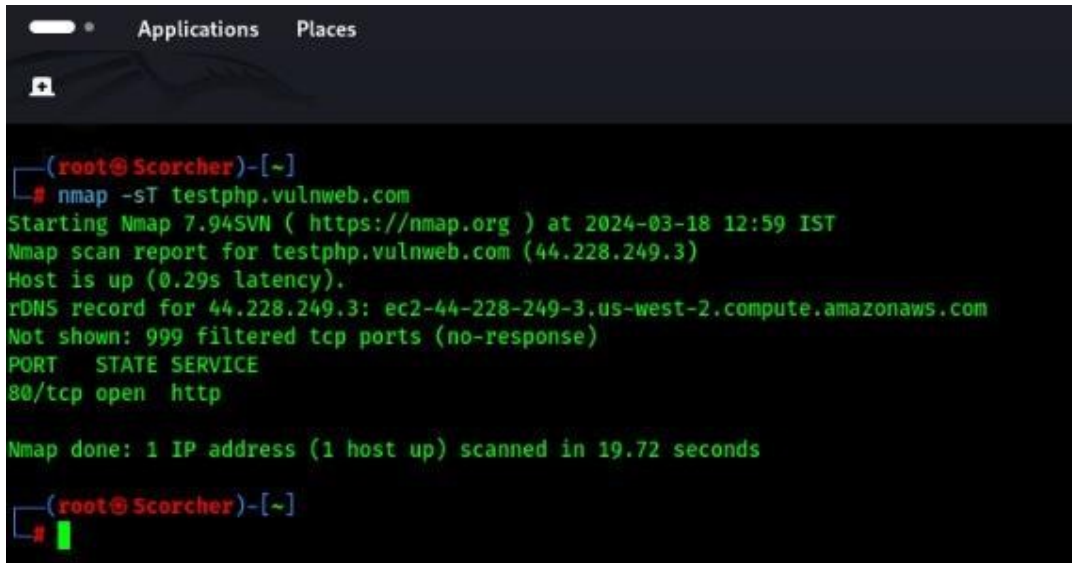
Task Level (Beginner):

Task 1

Find all the ports that are open on the website <http://testphp.vulnweb.com/>

Command: `nmap -sT testphp.vulnweb.com`

Findings: Port 80 (http) is open



```
(root@ Scorch)~]
# nmap -sT testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 12:59 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.29s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 19.72 seconds

(root@ Scorch)~]
#
```



Mitigations

When an attacker using Nmap send multiple request to the IP to find the open ports and other details. There are some mitigation needed to be taken from the Victim side.

Use a strong firewall to separate incoming and outgoing traffic to limit the nonessential ports and services, and allow only essential services to communicate. Uses an intrusion detection prevention system to monitor network traffic and detect suspicious or

Malicious activity, including Nmap scans. • Update all systems and software with the latest security patches to prevent vulnerabilities that can be exploited by Nmap.

Apply a rate limit to the network to control the number of connection requests from a single source to prevent malicious attacks and slow down detection efforts.

Task 2

Brute force the website <http://testphp.vulnweb.com/> and find the directories that are present on the website

Command: `dirb http://testphp.vulnweb.com`

Findings:

- ❖ <http://testphp.vulnweb.com/>
- ❖ <http://testphp.vulnweb.com/admin/>
- ❖ <http://testphp.vulnweb.com/CVS/>
- ❖ <http://testphp.vulnweb.com/inages/>
- ❖ <http://testphp.vulnweb.com/pictures/>
- ❖ <http://testphp.vulnweb.com/secured/>
- ❖ <http://testphp.vulnweb.com/vendor/>
- ❖ <http://testphp.vulnweb.com/CVS/Entries>

```
(root@Scorcher)-[~]
# dirb http://testphp.vulnweb.com

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Mon Mar 18 13:07:07 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----
---- Entering directory: http://testphp.vulnweb.com/CVS/ ----
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)

(!) FATAL: Too many errors connecting to host
(Possible cause: COULDN'T CONNECT)

-----
END_TIME: Mon Mar 18 14:02:07 2024
DOWNLOADED: 16753 - FOUND: 9
```

Mitigations

A brute force attack is a type of cyber attack in which an attacker attempts to gain unauthorized access to a system or account by systematically trying all possible combinations of usernames and passwords until the correct one is found. These attacks are often automated and can be a significant threat to systems with weak or easily guessable credentials.

To mitigate these attacks:

- **Enforce strong password policies that require complex passwords with a combination of uppercase and lowercase letters, numbers, and special characters.**
- **Implement rate limiting on login attempts to restrict the number of login requests from a single IP address or user within a specified time frame. This makes it more difficult for attackers to conduct large-scale brute force attacks.**
- **Implement IP whitelisting to restrict access to certain systems or services based on predefined IP addresses. This can help prevent unauthorized access from unknown or suspicious locations.**

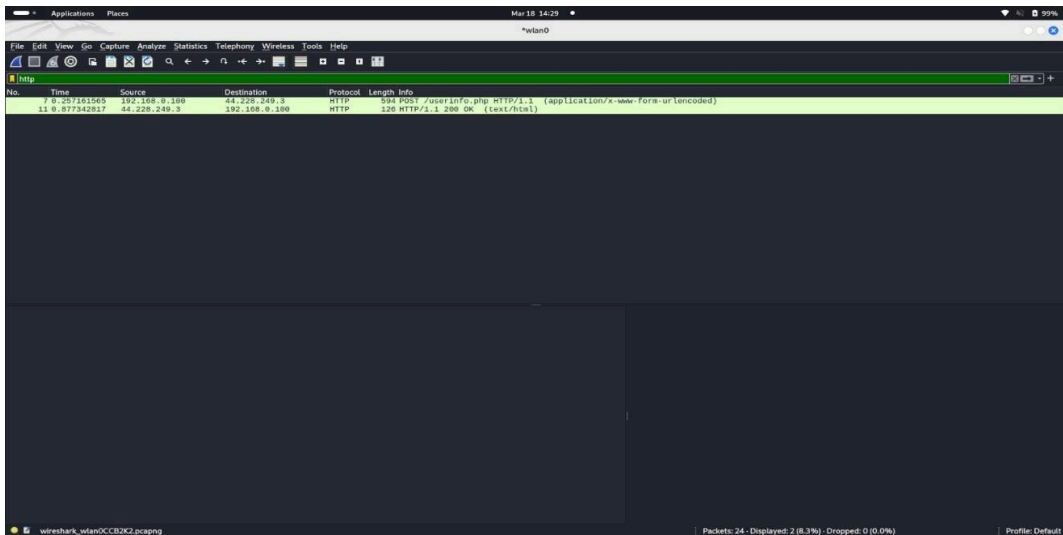
Keep all software, including operating systems and authentication mechanisms, up-to-date with the latest security patches. Vulnerabilities in outdated systems can be exploited by attackers to facilitate brute force attacks.

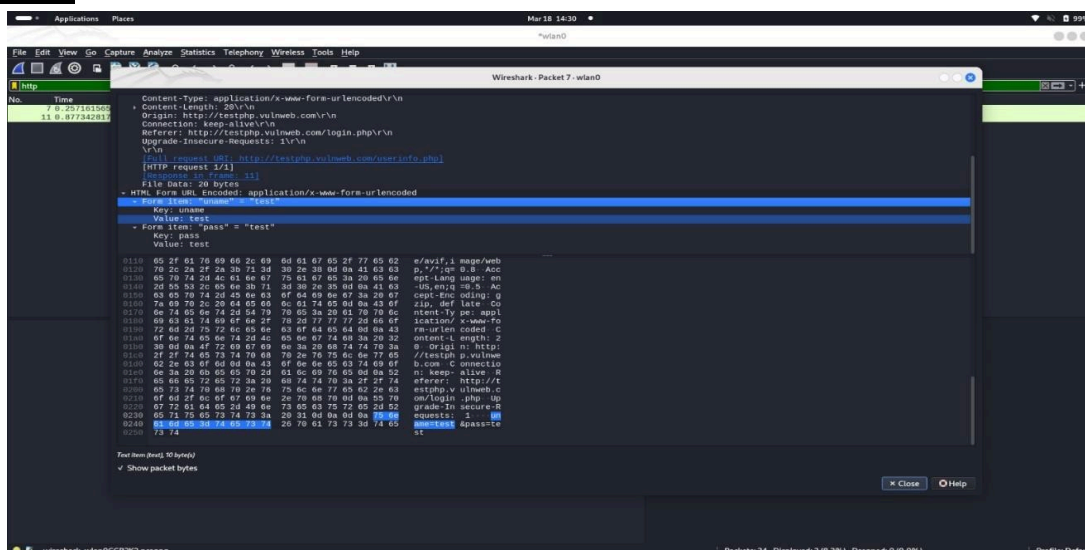
Conduct regular security audits and penetration testing to identify and address vulnerabilities in your systems. This proactive approach helps discover and fix potential weaknesses before they can be exploited.

Task 3

Make a login in the website <http://testphp.vulnweb.com/> and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.

- Filter used :HTTP
- Credentials: Username: test
Password: test





Mitigations

Credential sniffing is a type of cyber attack where an attacker intercepts and captures usernames and passwords as they are transmitted over a network. This can occur in various ways, such as through the use of packet sniffers or malicious software.

To mitigate these attacks

- Use secure communication protocols such as HTTPS for web traffic and SSH for remote access. Encryption helps protect sensitive information from being intercepted during transmission,
- Use VPNs to create a secure and encrypted tunnel for communication over untrusted networks. This helps in securing data transmitted between remote users and the internal network.
- Implement strong encryption (WPA3) and use complex passwords for Wi-Fi networks. Avoid using insecure protocols like WEP, which are susceptible to credential sniffing attacks.
- Implement endpoint security solutions, including antivirus and anti-malware software, to detect and prevent the installation of malicious sniffing tools on devices.
- Secure web applications by using secure coding practices, validating input, and implementing secure session management to prevent credential exposure.