VULNERABILITIES

TEAM NO.:7.4

TEAMMATES:N.HARIKA

P.MONISH

D.SRAVANI

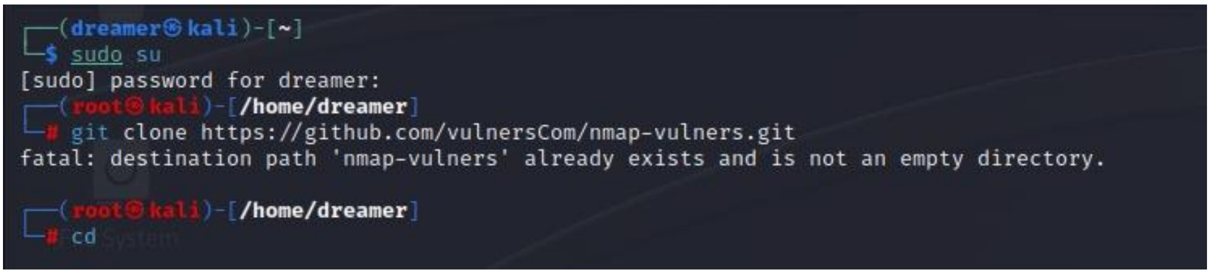
M.LIKHITHA

TOTAL VULNERABILITIES SCANNED : 17

Practice website: https://hackthissite.org

Open ports that we have find using nmap

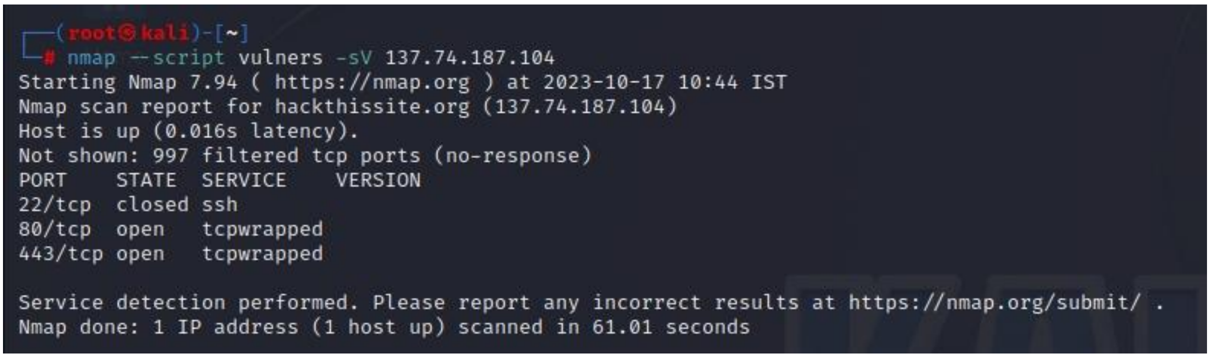
Step-1:



```
┌──(dreamer㉿kali)-[~]
└─$ sudo su
[sudo] password for dreamer:
┌──(root㉿kali)-[/home/dreamer]
└─# git clone https://github.com/vulnersCom/nmap-vulners.git
fatal: destination path 'nmap-vulners' already exists and is not an empty directory.

┌──(root㉿kali)-[/home/dreamer]
└─# cd
```

Step-2:



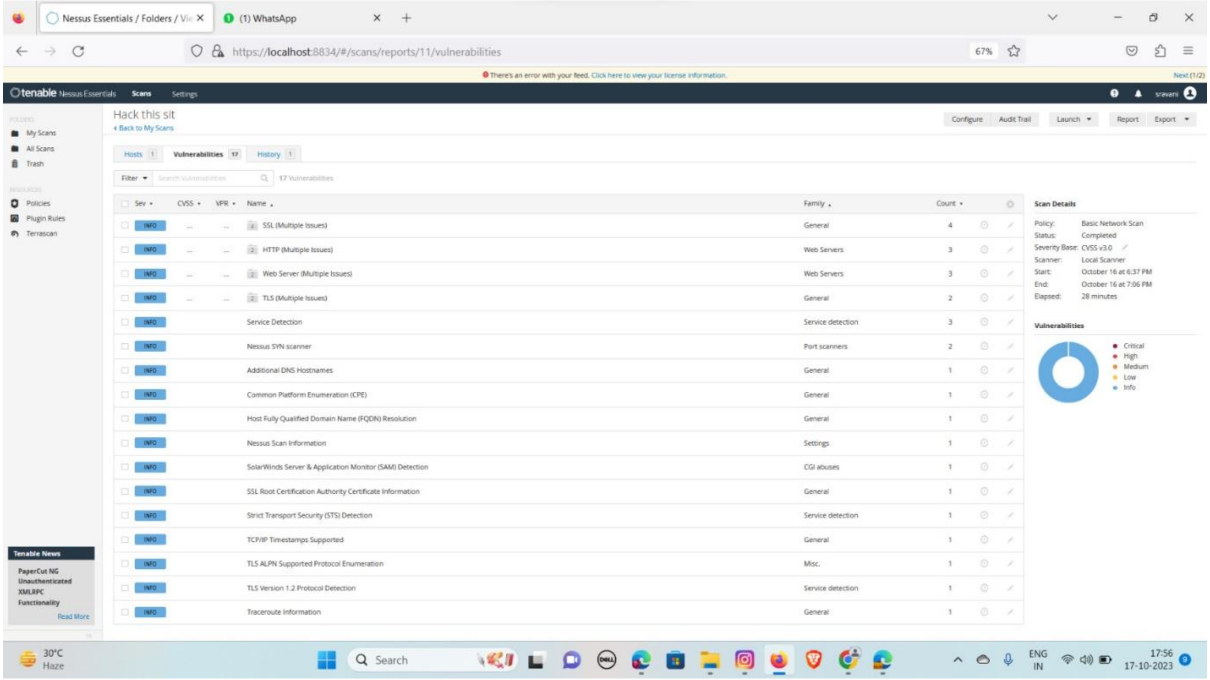
```
┌──(root㉿kali)-[~]
└─# nmap --script vulners -sV 137.74.187.104
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 10:44 IST
Nmap scan report for hackthissite.org (137.74.187.104)
Host is up (0.016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE    VERSION
22/tcp  closed ssh
80/tcp  open   tcpwrapped
443/tcp open   tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.01 seconds
```

we can see that port no. 80 and 443 are open so, they can be vulnerable.

Now by using Nessus tool we can find the vulnerabilities

As mentioned above we have find 17 vulnerabilities using Nessus



https://localhost:8834/#/scans/reports/11/vulnerabilities

There's an error with your feed. Click here to view your license information.

Hack this sit

Hosts 1 | Vulnerabilities 17 | History 1

17 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO	...	...	4 SSL (Multiple Issues)	General	4
INFO	...	...	2 HTTP (Multiple Issues)	Web Servers	3
INFO	...	...	2 Web Server (Multiple Issues)	Web Servers	3
INFO	...	...	2 TLS (Multiple Issues)	General	2
INFO			Service Detection	Service detection	3
INFO			Nessus SYN scanner	Port scanners	2
INFO			Additional DNS Hostnames	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO			Nessus Scan Information	Settings	1
INFO			SolarWinds Server & Application Monitor (SAM) Detection	CGI abuses	1
INFO			SSL Root Certification Authority Certificate Information	General	1
INFO			Strict Transport Security (STS) Detection	Service detection	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			TLS ALPN Supported Protocol Enumeration	Misc.	1
INFO			TLS Version 1.2 Protocol Detection	Service detection	1
INFO			Traceroute Information	General	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: October 16 at 6:37 PM
End: October 16 at 7:06 PM
Elapsed: 28 minutes

Vulnerabilities

1.ADDITIONAL DNS HOSTNAMES:

Description:

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

FIXING THE VULNERABILITY:

Check the DNS host before doing any action .

DNS host names. Allowed characters: DNS names can contain only alphabetic characters (A-Z), numeric characters (0-9), the minus sign (-), and the period (.).

2. Common Platform Enumeration:

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

FIXING THE VULNERABILITY:

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

3. SolarWinds Server & Application Monitor (SAM) Detection:

DESCRIPTION:

SolarWinds Server & Application Monitor (SAM), a server and application performance monitoring solution, is running on the rem.

See Also

https://www.solarwinds.com/server-application-monitor

Output

```
  URL     : https://hackthissite.org/
  Version : unknown
```

To see debug logs, please visit individual host

Hosts

443 / tcp / www

137.74.187.100

FIXING THE VULNERABILITY:

Delete any System Restore points and Shadow volumes that existed prior to restricting access to %windir%\system32\config.

· Restrict SAM files

4. Strict Transport Security (STS) Detection

Description:

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

FIXING THE VULNERABILITY:

Enable HSTS

1. Log in to the Cloudflare dashboard Open external link and select your account.
2. Select your website.
3. Go to SSL/TLS > Edge Certificates.
4. For HTTP Strict Transport Security (HSTS), select Enable HSTS.
5. Read the dialog and select I understand.
6. Select Next.
7. Configure the HSTS settings.
8. Select Save.

5. TCP/IP Timestamps Supported

Description:

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

FIXING THE VULNERABILITY:

TCP timestamps are enabled by default. If you disable TCP timestamps, the timestamps are not displayed in the traffic capture file. You can run the show tcp_timestamps command to determine whether the TCP timestamps are enabled or disabled before running set tcp_timestamps

6. TLS ALPN Supported Protocol Enumeration:

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

HOW TO FIX IT:

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

7.TLS Version 1.2 Protocol Detection

Description:

The remote service accepts connections encrypted using TLS 1.2

HOW TO FIX IT:

Step to enable TLS 1.2 in Google Chrome

1. Open Google Chrome.
2. Press Alt + F and select Settings.
3. Select the Advanced tab.
4. Select the System category.
5. Select Open your computer's proxy settings.
6. Select Advanced tab.
7. Scroll down to Security category and tick the box for Use TLS 1.2.
8. Click OK.

9.SSL / TLS Versions Supported

Description:

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

HOW TO FIX IT:

you'll need to specify the right protocol in your server's configuration file. For example, if your site runs on a Nginx server, you'll have to edit the nginx. conf file and specify the TLS version you've installed. Add the upgraded protocol and disable all deprecated versions.

10.SSL/TLS Recommended Cipher Suites

Description:

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

Solution:

Only enable support for recommened cipher suites.

11.Web Server No 404 Error Code Check

Description:

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

HOW TO FIX IT:

1. Retry the web page by pressing F5, clicking/tapping the refresh/reload button, or repeatedly trying the URL from the address bar. ...
2. Check for errors in the URL. ...
3. Move up one directory level at a time in the URL until you find something. ...
4. Search for the page from a popular search engine.

12.Web Server robots.txt Information Disclosure

Description:

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

Solution:

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

13.HyperText Transfer Protocol (HTTP) Information

Description:

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

14 .HTTP Server Type and Version

Description

This plugin attempts to determine the type and the version of the remote web server.

Output

The remote web server type is :

HackThisSite

To see debug logs, please visit individual host

Hosts

443 / tcp / www

137.74.187.100

15.SSL Cipher Block Chaining Cipher Suites Supported

Description:

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

Hosts:

443 / tcp / www

137.74.187.100

16.SL Cipher Suites Supported:

Description:

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Hosts:

443 / tcp / www

137.74.187.100

17.SSL Perfect Forward Secrecy Cipher Suites Supported:

Description:

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

Hosts

443 / tcp / www

137.74.187.100