Brainfuck

Used **Nmap** tool to scan the open ports and services on the machine.

Text

Description automatically generated

With port 443 open, Used web browser to access the same.

Graphical user interface

Description automatically generated with medium confidence

For enumerating on the sub directories of the website, used **Gobuster** tool but did not get any information.

A screenshot of a computer

Description automatically generated

Next as the Certificate has been self-signed, it threw lot of errors on that. As checked on the certificate details, it exposed the owner’s email address and two DNS addresses of the server.

Text

Description automatically generated

Graphical user interface, text, website

Description automatically generated

With these above been exposed, added them to the host file as below -

Text

Description automatically generated

Once added to the hosts file, tried accessing the same on the web browser resulted in a new Wordpress website

Graphical user interface, application

Description automatically generated

According to the Wappalyzer plugin on the webpage, it has Wordpress version 4.7.3.

With the above version, used **Wpscan** to scan the Wordpress website to check possible vulnerabilities and plugins.

Text

Description automatically generated

The scan results show a vulnerable plugin as the older version is out of date.

Text

Description automatically generated

When checked online for possible exploits for the above found plugin, there is a privilege escalation exploit - <https://www.exploit-db.com/exploits/41006>

Graphical user interface, application, Word

Description automatically generated

Followed the exploit POC and changed the code according to our environment. Since the Wordpress default credentials are **Admin**, tried the same while inputting it to the target machine.

Text

Description automatically generated

Once the html file is created, open up on a web browser and click Login with the Admin username. It will be redirected to the wordpress page and then traverse to /wp-admin page for admin page.

Then traversed to Settings page under the Wordpress website which has the SMTP integration credentials.

A screenshot of a computer

Description automatically generated

As clicked on the password filed and inspected the element, it exposes the SMTP credentials of the user Oretis.

Text

Description automatically generated

With the above found credentials, used the same to access port 110(POP3) via telnet.

Text

Description automatically generated

Then listed out all the available mails on the mail server.

Text

Description automatically generated

One of the emails exposed user credentials for the other Secret forum which we found in the DNS details.

Visited the Secret website and logged in with the above found credentials.

A screenshot of a computer

Description automatically generated with medium confidence

As checked the conversion between the Admin and Orestis, they seem to discuss about the SSH key which is then directed to an encrypted conversation.

The encrypted conversation did not make any sense even when tried decrypting with Cyber Chef(<https://gchq.github.io/CyberChef/>) a famous tool for cracking any type of encrypted values.

As enumerated more, we could see that we have the plain text and cipher text for a part of the encrypted conversation as Orestis always uses a phrase at the end of his reply – “**Orestis - Hacking for fun and profit”**

Lets consider the above as the Key and decrypt the cipher text.

Graphical user interface, text

Description automatically generated

And the Cipher text be – **“Pieagnm - Jkoijeg nbw zwx mle grwsnn”**

Graphical user interface, text, application, chat or text message

Description automatically generated

As used online Vignere Cipher decoder, we could see that the plain text here is Brainfuckmybrainfuckmybrainfu – which seems to be the key for next conversation as usually the Vignere Cipher key’s are a set of repetitive words.

Graphical user interface, text, application

Description automatically generated

**Cipher Text – Xua zxcbje iai c leer nzgpg ii uy**

**Plain Text – Say please and I just might do so**

**Cipher Text - Ybgbq wpl gw lto udgnju fcpp, C jybc zfu zrryolqp zfuz xjs rkeqxfrl ojwceec J uovg**

**Plain Text - There you go you stupid fuck, I hope you remember your key password because I don’t.**

**Cipher Text – mnvze://10.10.10.17/8zb5ra10m915218697q1h658wfoq0zc8/frmfycu/sp\_ptr**

**Plain Text - https://10.10.10.17/8ba5aa10e915218697d1c658\*\*\*\*\*\*/orestis/id\_rsa**

Visited the above-mentioned webpage by changing our server IP address and downloaded the file to the local machine.

Text

Description automatically generated

Then used **John** tool to convert the Public key to John’s extension.

Text

Description automatically generated

Used the **John** tool to brute force the RSA Public key and found the password.

Text

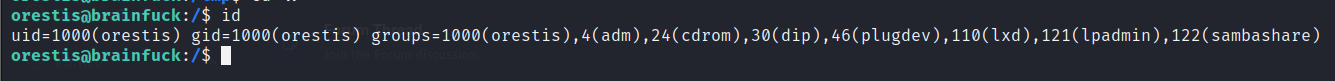
Description automatically generated with medium confidence

Logged in to SSH session with the above found credentials.

A screenshot of a computer

Description automatically generated with medium confidence

Checked the user privileges with **Id** command and we could see the current user has **lxc** privileges.



As goggled for ways to exploit **lxc** privileged user and found the article -<https://www.hackingarticles.in/lxd-privilege-escalation/>

Followed the steps in the article and got the root access on the machine.

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

Finally found the root flag on the machine by accessing the root.txt file.