登录

Pentest Wiki Part 7 渗透报告&逆向IDA入门&快速搭建系统服务

wing / 2018-01-02 09:34:00 / 浏览数 2310 新手 入门资料 顶(0) 踩(0)

渗透报告

前言

本文档旨在定义渗透测试报告的基本标准。
虽然高度鼓励使用自己的定制和品牌格式，但以下内容应提供对报告中所需项目的高层次理解以及报告结构，以便为读者(客户)提供价值。

报告是渗透测试中最重要的一环。
您将使用报告来传达您所做的事情，说明您是如何做到的，最重要的是，让你所测试机构知道应如何修复渗透测试期间发现的漏洞。

报告结构

报告分为两个主要部分，以向不同的受众介绍测试的目标，方法和结果。

执行摘要

本部分将向读者(客户)传达渗透测试的具体目标和渗透测试的高级结果。目标受众是那些负责安全方案的监督的人员以及可能受到威胁的组织中的任何成员。执行摘要应包含

- 背景：
  背景部分应向读者(客户)解释渗透测试的总体目的。
  测试部分确定的风险，对策和渗透测试有关的术语的详细信息应该提供给读者(客户)，以使读者(客户)了解整体的渗透测试和相关结果。

整体来说这个领域将是展现测试的整体效果和渗透测试师实现先前会议中提出的目标的能力的叙述。
对测试过程确定的系统性问题（例如系统性问题--缺少有效的补丁=找到的MS08-067）进行简要描述，以及实现对目标信息的访问和识别 对业务的潜在影响。

风险排名/资料

整体风险排名/概况/分数将在这个区域被识别和解释。 在预备阶段，Pentester将确定评分机制和追踪/分级风险的个体机制。
FAIR，DREAD和其他自定义排名中的各种方法将被合并到环境分数中并进行定义。

（客户）的■■■■■■目前是七（7）。 这个评级意味着安全控制的风险会随着潜在的重大财务损失而受到损害。
顾问根据一个高风险和几个中等风险漏洞确定了这个风险评分，并且定向攻击的成功。
识别出的最严重的漏洞是在面向企业公开的网站上存在默认密码，该密码允许访问许多敏感文档并能够控制设备上的内容。
此漏洞可能导致用户帐户被盗，敏感信息泄露或完全系统泄露。 几个较小的严重漏洞可能导致盗窃有效的帐户凭证和泄露信息。
总体发现：
一般调查结果将提供基本和统计格式的渗透测试中发现的问题的概要。
测试目标用图形表示，测试结果，过程，攻击情景，成功率以及在测试前会议中定义的其他可测量指标应该存在。 此外，问题的原因应该以易于阅读的格式呈现。
（例如，显示被利用问题的根本原因的图表）

这一领域还应包括描述环境内对策有效性的指标。（例如，我们运行了x次攻击和IPS拦截了y，其他对策也应该具有相似的设计和效果指标。）

推荐摘要：
报告的建议部分应使读者(客户)高度了解和解决所确定的风险所需的任务，以及实施解决方案建议所需的一般工作量。
本节还将确定用于优先考虑后续路线图顺序的权重机制。

战略路线图

路线图应该包括一个优先计划，用于修复发现的不安全物品，并且应该根据商业目标/潜在影响水平来衡量。
本节应直接映射到已确定的目标以及PTES-Threat建模部分中创建的威胁矩阵。
通过分解为预定义的时间/目标为基础的目标，本节将创建一个行动的路径，以不同的增量。 例：

技术报告

本部分将向读者(客户)传达测试的技术细节以及商定前的所有方面/内容，作为参与前活动的关键成功指标。
技术报告部分将详细描述测试的范围，信息，攻击路径，影响和修复建议。

介绍：

技术报告的引言部分旨在作为初步清单：

渗透测试团队的测试
联系信息
涉及测试的资产
测试的目的

测试范围
测试的强度
途径
威胁/分级结构

本部分应作为测试涉及的具体资源和测试的总体技术范围的参考。

信息收集：

情报收集和信息评估是良好渗透测试的基础。测试人员对环境的了解越多，测试的结果就越好。在本节中，应编写若干项目，向客户展示通过执行PTES情报收集阶段可获得

被动情报：

从间接分析收集到的情报，如DNS，谷歌IP /基础设施相关信息。本节将重点介绍用于在CLIENT环境中剖析技术的技术，而不直接向资产发送任何流量。

主动收集：

本节将介绍基础架构映射，端口扫描，体系结构评估等脚步打印活动的方法和结果。本节将重点介绍通过直接向资源发送流量来在CLIENT环境中分析的技术。

企业情报：

有关组织结构，业务单位，市场份额，垂直和其他企业职能的信息应该映射到业务流程和先前确定的被测试的实物资产。

人员情报：

在情报收集阶段发现的将用户映射到CLIENT组织的任何和所有信息。本部分应显示用于收集情报的技术，例如公共/私人员工仓库，邮件储存库，组织结构图和其他导致员工

漏洞评估：

漏洞评估是识别TEST中存在的潜在漏洞和每个威胁的威胁分类的行为。在本节中，应该提供用于识别漏洞的方法的定义以及漏洞的证据/分类。另外这个部分应该包括：

- 漏洞分类级别
  - 技术漏洞
- OSI层漏洞
- 扫描器的发现
- 手动识别
- 整体公开
- 逻辑漏洞
- 非OSI漏洞
- 漏洞的类型
- 如何/在哪里找到
- 公开的
- 结果摘要
- 开发/漏洞确认：

利用漏洞或漏洞确认是触发前面部分中确定的漏洞以获得对目标资产的特定访问级别的行为。本节应详细回顾为确认定义的漏洞所采取的所有步骤以及以下内容：

- 渗透时间表
- 选定的渗透目标
- 渗透活动
- 定向攻击
- 目标主机无法被利用
- 目标主机能够被利用
- 个人主机信息
- 进行攻击
- 攻击成功
- 访问级别授予+升级路径
- 整理
- 漏洞部分参考
- 额外的缓解技术
- 补偿控制建议
- 间接攻击
- 网络钓鱼
- 时间表/攻击细节
- 确定目标
- 成功/失败比率

- 授予访问级别
- 客户端
  - 时间表/攻击细节
  - 确定目标
  - 成功/失败比率
  - 授予访问级别
- 浏览器端
  - 时间表/攻击细节
  - 确定目标
  - 成功/失败比率
  - 授予访问级别

后渗透

所有测试中最关键的项目之一是与正在测试的客户端的实际影响的联系。虽然上面的章节中介绍了漏洞的技术性质和成功利用漏洞的能力，但是后渗透部分应该将开发能力与

- 权限升级路径
- 使用的技术
- 获取由客户定义的关键信息
- 信息的价值
- 访问核心业务系统
- 访问合规性保护的数据集
- 附加信息/系统访问
- 持久的能力
- 能力渗透
- 对策有效性

本节应涵盖范围内系统的对策措施的有效性。其中应包括有效（主动）和被动（被动）对策部分，以及在测试阶段触发的任何事件响应活动的详细信息。有效抵制评估活动的

- 检测能力
  - FW/WAF/IDS/IPS
  - 人
  - DLP
  - 日志
  - 响应和有效性
    风险：

一旦通过后渗透确认存在的漏洞对业务的直接影响进行评估，就可以进行风险量化。在本节中，上述结果与预先接触部分的风险值，信息危急程度，企业评估以及派生的业务

- 评估事件频率
- 可能的事件频率
- 估计威胁能力（从3 - 威胁建模）
- 估算控制强度（6）
- 复合漏洞（5）
- 所需技能水平
- 需要访问级别
- 估算每个事件的损失量
- 主要损失
- 二次损失
- 识别风险根源分析
- 根本原因永远不是一个补丁
- 识别失败的进程
- 导出风险
- 威胁
- 漏洞
- 交叠
- 结论：

最后的测试概述。建议本部分回显整个测试的部分内容，并支持CLIENT安全状态的增长。应该以积极的方面结束，提供支持和指导，使安全方案能够取得进展，未来的检测

参考链接

http://www.pentest-standard.org/index.php/Reporting
https://github.com/juliocesarfort/public-pentesting-reports
https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

逆向工程

IDA

插件选项

-O 命令行参数允许用户将设置传递给插件。
一个使用设置的插件会调用get_plugin_options()函数来获得参数。

由于可能有独立编程人员编写的插件，每个插件的设置都需要单独加上-O前缀

例如，一个名为"decomp"的插件规定它的参数具有以下格式：

```
-Odecomp:option1:option2:option3
```

在这种情况下，get_plugin_options("decomp")将返回选项字符串的"option1：option2：option3"部分。

如果在命令行中存在多个-O参数，那么它们会被之间的"："连接起来。

■■■窗口

"Name"窗口提供二进制文件中所有全局名称的摘要列表。
函数名就是对程序虚拟地址的符号描述。
（译者注：指的是View-Open Subviews-Names窗口，也可通过快捷键Shift+F12打开）

IDA最初在文件的初始加载过程中从符号表和签名分析中导出名称列表。
名称可以按字母顺序排列，也可以按虚拟地址顺序（升序或降序）排序。

"名称"窗口对于快速导航到程序列表中的已知位置非常有用。
双击任何名称窗口条目将立即跳转反汇编视图显示选定的名称。

显示的名称会被调整为不同的颜色和字母。
方案概述如下：

F 常规功能。这些是IDA不能识别为库函数的功能。

L 库函数 IDA通过使用签名匹配算法识别库函数。
如果给定的库函数不存在签名，则该函数将被标记为常规函数。

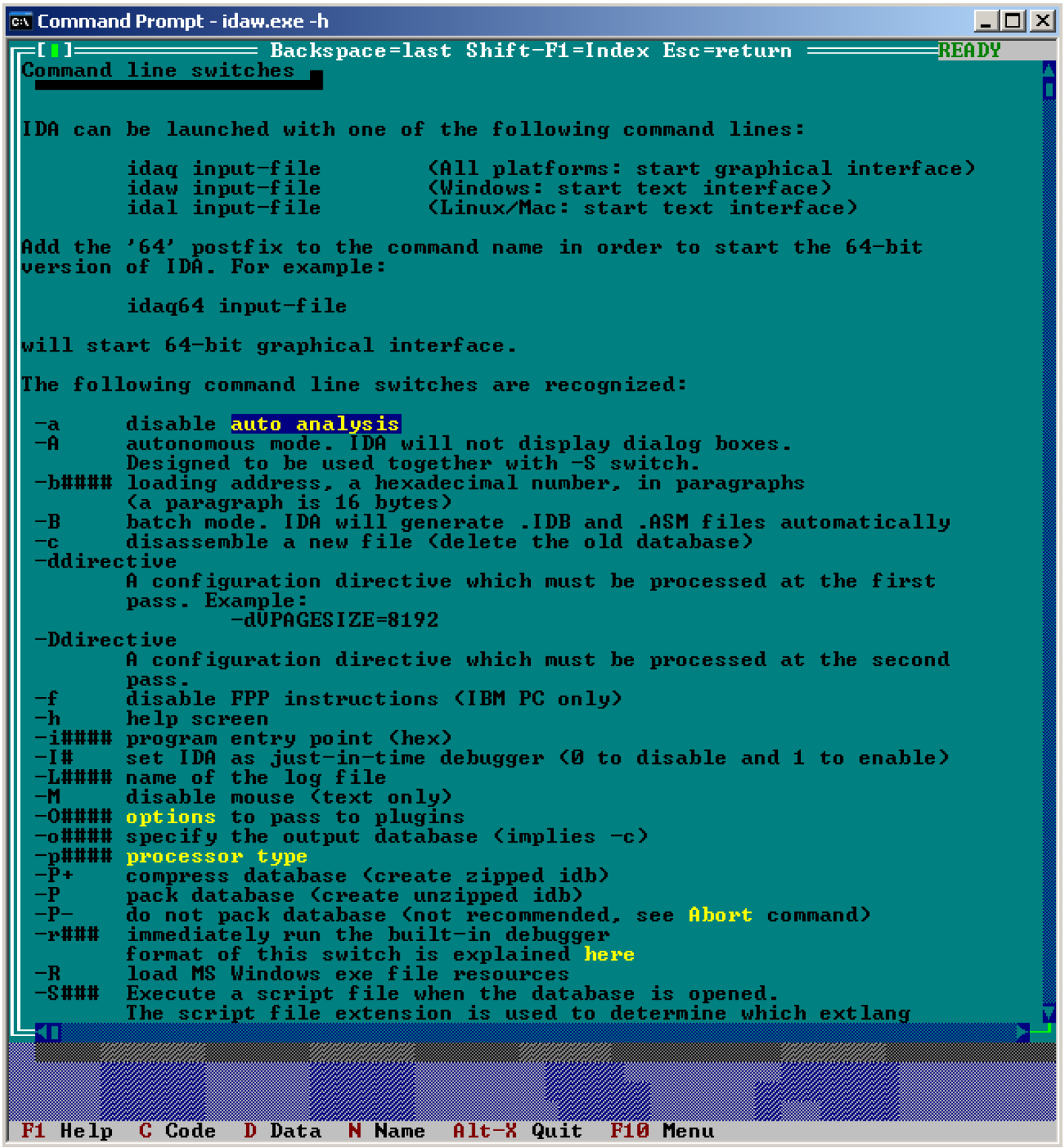
I 导入的名称，通常是从共享库导入的函数名称。
这和库函数的不同之处在于，导入的名称不存在任何代码，而库函数的主体将出现在反汇编中。

C 无名代码（Named code）。IDA不认为这些代码是某个函数的一部分。
当IDA在程序的符号表中找到了一个函数名，但是却没有发现对该函数的调用时，就会把他们判定为无名代码。

D 数据。命名的数据位置通常代表全局变量。

A 字符串数据。这是一个引用的数据位置，包含一系列符合IDA已知字符串数据类型的字符序列，例如以空字符结尾的ASCII C字符串。

命令行模式



可以使用以下命令之一启动IDA：

```
idaq input-file■■■■■■■■■■■■■■■
idaw input-file■Windows■■■■■■■■■
idal input-file■Linux / Mac■■■■■■■■■
```

将“64”后缀添加到命令名称中，以启动64位版本的IDA。例如：

```
idaq64 input-file
```

将启动64位图形界面。

命令行的参数包括以下几种：

```
-a ■■■■■■■
-A ■■■■■■ IDA■■■■■■■■■
  ■■■-S■■■■■■■■
-b + #### ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

```
-B ■■■■■■■ IDA■■■■■■.IDB■.ASM■■
-c ■■■■■■■■■■■■■■■■
-d + directive
  ■■■■■■■■■■■
  ■■:
      -dVPAGESIZE=8192
-D + directive
 ■■■■■■■■■■■■
-f ■■FPP■■ (■■IBM PC■■■■)
-h ■■■■■
-i + #### ■■■■■■■■■■■■■
-I + #■IDA■■■■■■■■■■■0■■■■1■■■■
-L + #### ■■log■■■■■
-M ■■■■■■■■■■■
-O + #### ■■■■■■■■■
-o + #### ■■■■■■■■■■■-c■
-p + #### ■■■■■■■■
-P+ ■■■■■■■■■■■■■IDB■
-P ■■■■■■■■■■■■■IDB■
-P-■■■■■■■■■■■■■■■■■Abort■■■■
-r + ###  ■■■■■■■■■■■■■■■###■■■■■
-R ■■MS Windows exe■■■■■
-S###  ■■■■■■■■■■■■■■■
  ■■■■■■■■■■■■■■■extlang■■■■■■■
  ■■■■■■■■■■■■■■■■■■■
  ■■■■
       -S"myscript.idc argument1 \"argument 2\" argument3"
      ■■■■■■■■■“ARGV”■■IDC■■■■■
      ■■“ARGV.count”■■■■■■■■■■
      ■■■■■■“ARGV [0]”■■■■■■■
-T###  ■■■■■■■■■■■■■■■■■■
  ■“■■■■■”■■■■■■■
-t     ■■■■■■■■■■■■
-W###  ■■MS Windows■■
-x ■■■■■■■
   ■■Dump■■■■■■■■■■■
    ■■■■■■■EXE■COM■■■■■■
-z debug:
              00000001 drefs
              00000002 offsets
              00000004 first
              00000008 idp module
              00000010 idr module
              00000020 plugin module
              00000040 ids files
              00000080 config file
              00000100 check heap
              00000200 checkarg
              00000400 demangler
              00000800 queue
              00001000 rollback
              00002000 already data or code
              00004000 type system
              00008000 show all notifications
              00010000 debugger
              00200000 Appcall
              00400000 source-level debugger
-? ■■■■■■■■■
?  ■■■■■■■■■
```

对于批处理模式，必须使用以下命令行调用IDA：

```
idaq -B input-file
```

相当于

```
idaq -c -A -Sanalysis.idc input-file
```

文本界面（idaw.exe / idal）更适合批处理模式，因为它使用较少的系统资源。
但是，请注意，常用插件不会自动加载到批处理模式，因为analysis.idc文件会退出，内核没有机会加载它们。

有关更多信息，请参阅IDC子目录中的analysis.idc文件。

主要功能

IDA是一个交互式反汇编程序。用户可以主动参与反汇编过程。
它不能自动分析程序，而是向你提示可疑的地方，未解决的问题等。
而你的工作就是指挥IDA进行分析。

如果你第一次使用IDA，下面是一些你会发现非常有用的命令：

转换为指令（Code）：热键是“C”
转换为数据（Data）：热键是“D”

所做的所有更改都保存到磁盘
（译者注：即.idb数据库文件。IDA不会对原程序做任何改动。除非使用Patch Program插件）。
当您再次运行时，IDA会从磁盘读取被分析文件的所有信息，以便可以继续您的工作。
（译者注：同样指的是.idb数据库文件，无论原程序被改动甚至是删除都不影响）

```
CODE:00401000 6A 00 push0
CODE:00401002 E8 64 02 00 00callGetModuleHandleA ; Call Procedure
```

按下D，你会看到：

```
CODE:00401000 6A 00 push0
CODE:00401000   ;
-------------------------------------------------------------------------
CODE:00401002 E8db 0E8h
CODE:00401003 64db  64h ; d
CODE:00401004 02db2
CODE:00401005 00db0
CODE:00401006 00db0
CODE:00401007   ;
-------------------------------------------------------------------------
```

逆向的不是很友好，只有ida的介绍使用，建议大家去ctf-wiki里面看看re这块的。

快速搭建系统服务

如何快速设置FTP服务器

请用pip或easy_install安装pyftpdlib。

```
sudo easy_install pysendfile
sudo easy_install pyftpdlib
```

或者

```
sudo pip2 install pysendfile
sudo pip2 install pyftpdlib
```

如果您已经成功安装了pyftpdlib，请按以下步骤启动：

```
root@lab:/tmp/pyftpdlib# python -m pyftpdlib -w -p 21
pyftpdlib/authorizers.py:240: RuntimeWarning: write permissions assigned to anonymous user.
 RuntimeWarning)
 [I 2016-03-06 10:00:11] >>> starting FTP server on 0.0.0.0:21, pid=2090 <<<
 [I 2016-03-06 10:00:11] concurrency model: async
 [I 2016-03-06 10:00:11] masquerade (NAT) address: None
 [I 2016-03-06 10:00:11] passive ports: None
 [I 2016-03-06 10:00:40] 192.168.1.103:52874-[] FTP session opened (connect)
 [I 2016-03-06 10:00:40] 192.168.1.103:52874-[anonymous] USER 'anonymous' logged in.
 [I 2016-03-06 10:00:45] 192.168.1.103:52874-[anonymous] FTP session closed (disconnect).
 [I 2016-03-06 10:01:42] 192.168.1.101:49312-[] FTP session opened (connect)
 [I 2016-03-06 10:02:12] 192.168.1.101:49312-[] FTP session closed (disconnect).
 [I 2016-03-06 10:02:24] 192.168.1.101:49313-[] FTP session opened (connect)
 [I 2016-03-06 10:02:31] 192.168.1.101:49313-[anonymous] USER 'anonymous' logged in.
 [I 2016-03-06 10:06:28] 192.168.1.101:49313-[anonymous] RETR /tmp/pyftpdlib/setup.py completed=1 bytes=5183 seconds=0.004
 [I 2016-03-06 10:07:29] 192.168.1.101:49313-[anonymous] FTP session closed (disconnect).
 [I 2016-03-06 10:08:11] 192.168.1.104:1033-[] FTP session opened (connect)
 [I 2016-03-06 10:08:17] 192.168.1.104:1033-[anonymous] USER 'anonymous' logged in.
 [I 2016-03-06 10:10:43] 192.168.1.104:1033-[anonymous] FTP session closed (disconnect).
```

Windows FTP控制台客户端：

```
C:\Documents and Settings\test\Desktop>ver

Microsoft Windows XP [Version 5.1.2600]

C:\Documents and Settings\test\Desktop>ftp 192.168.1.103
Connected to 192.168.1.103.
220 pyftpdlib 1.5.0 ready.
User (192.168.1.103:(none)): anonymous
331 Username ok, send password.
Password:
230 Login successful.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
.ci
.coveragerc
.git
...
```

您也可以使用其他客户端，例如：ncftp。

Twistd

如何用Twisted启动一个ftp服务器。

```
root@lab:/tmp# twistd -n ftp --help
Usage: twistd [options] ftp [options].
   WARNING: This FTP server is probably INSECURE do not use it.
Options:
 -p, --port=            set the port number [default: 2121]
 -r, --root=            define the root of the ftp-site. [default:
                        /usr/local/ftp]
     --userAnonymous=   Name of the anonymous user. [default: anonymous]
     --help             Display this help and exit.
     --help-auth-type=  Show help for a particular authentication type.
     --auth=            Specify an authentication method for the server.
     --password-file=   Specify a file containing username:password login info
                        for         authenticated connections. (DEPRECATED; see
                        --help-auth instead)
     --version          Display Twisted version and exit.
     --help-auth        Show all authentication methods available.

sroot@lab:/tmp# tudo easy_install twisted
root@lab:/tmp# twistd -n ftp -p 2121 --userAnonymous=anonymous
2016-03-06 11:24:24-0500 [-] Log opened.
2016-03-06 11:24:24-0500 [-] twistd 15.5.0 (/usr/bin/python 2.7.11) starting up.
2016-03-06 11:24:24-0500 [-] reactor class: twisted.internet.epollreactor.EPollReactor.
2016-03-06 11:24:24-0500 [-] FTPFactory starting on 2121
2016-03-06 11:24:24-0500 [-] Starting factory <twisted.protocols.ftp.FTPFactory instance at 0xb6c2474c>
```

点击收藏 | 0 关注 | 0

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

1. 3 条回复


小哲 2018-01-02 10:14:38

你飘了..怎么感觉像是翻译过来的、、、

0 回复Ta


hades 2018-01-02 10:25:48

@小哲 就是翻译

0 回复Ta


wing 2018-01-02 10:55:52

@小哲 渗透测试报告这个我不是很了解，翻译的可能会生涩，但是除了报告其他的可能还有问题，欢迎指出，把改过来。蟹蟹啊。

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