登录

Pentest Wiki Part3 渗透工具

wing / 2017-12-29 12:28:00 / 浏览数 4696 新手 入门资料 顶(0) 踩(0)

渗透测试工具

■■■■■■
攻击可能是渗透测试中最迷人的部分之一了，但它通常是用暴力破解而不是精确制导来完成的。只有当你知道针对目标的一个特定漏洞很可能会成功的时候，你才应该发起一

渗透测试操作系统

- Kali - 为数字取证和渗透测试而设计的Linux发行版
- ArchStrike - 安全专业人员和相关爱好者使用操作系统，基于Arch Linux
- BlackArch - 为渗透测试工程师和安全研究员设计的操作系统，基于Arch Linux的发行版
- NST - 网络安全套件发行版
- Pentoo - 以安全研究为重点的操作系统，LiveCD启动，基于Gentoo
- BackBox - 为渗透测试工程师和安全评估设计的操作系统，基于Ubuntu发行版
- Parrot - 类似Kali的操作系统，支持多种架构

基本的渗透测试工具

- Metasploit Framework - 世界范围内最广为使用的渗透测试软件
- Burp Suite - 用于Web应用程序安全测试的集成平台
- ExploitPack - 包含大量利用工具(Exploit)的图形化渗透测试工具
- BeeF - 针对于浏览器攻击的框架项目
- faraday - 协同渗透测试与漏洞管理平台
- evilgrade - 较新的攻击工具框架
- commix - 全自动操作系统命令注入和利用工具
- routersploit - 针对路由器的全自动渗透测试工具
- exploit-database - Offensive 安全团队的漏洞利用信息数据库集合

Docker for Penetration Testing

- `docker pull kalilinux/kali-linux-docker` Kali Linux的Docker版
- `docker pull owasp/zap2docker-stable` - OWASP ZAP扫描器
- `docker pull wpscanteam/wpscan` - WPScan，WordPress安全检测工具
- `docker pull pandrew/metasploit` - metasploit的Docker
- `docker pull citizenstig/dvwa` - DVWA漏洞演示平台Docker
- `docker pull wpscanteam/vulnerablewordpress` - 已知存在漏洞的WordPress版本
- `docker pull hmlio/vaas-cve-2014-6271` - bash破壳漏洞Docker
- `docker pull hmlio/vaas-cve-2014-0160` - 心脏滴血漏洞Docker
- `docker pull opendns/security-ninjas` - 安全忍者Docker
- `docker pull diogomonica/docker-bench-security` - bench安全测试Docker
- `docker pull ismisepaul/securityshepherd` - OWASP 安全指导
- `docker pull danmx/docker-owasp-webgoat` - OWASP Web靶场Docker
- `docker-compose build && docker-compose up` - OWASP Node.js渗透靶场
- `docker pull citizenstig/nowasp` - OWASP 多种Web渗透靶场程序
- `docker pull bkimminich/juice-shop` - OWASP Juice Shop渗透靶场

安全漏洞扫描器

- Nexpose - 漏洞和风险管理软件
- Nessus - 漏洞，配置和合规性评估
- Nikto - Web应用程序安全扫描器
- OpenVAS - 开源漏洞扫描器和管理软件
- OWASP Zed Attack Proxy - 为Web应用程序设计的渗透测试工具
- Secapps - 集成Web应用程序安全测试环境
- w3af - Web应用程序攻击和评估框架
- Wapiti - Web应用程序漏洞扫描器

- WebReaver - 为 Mac OS X设计的Web应用程序漏洞扫描器
- DVCS Ripper - Rip网络可访问（分布式）版本控制系统：SVN / GIT / HG / BZR
- arachni - Web应用程序安全扫描框架

网络工具

- nmap - 安全审计和网络嗅探的免费扫描器
- pig - Linux平台的网络数据包构造工具
- tcpdump/libpcap - 一个运行在命令行下的通用数据包分析工具
- Wireshark - 一个同时支持Unix和Windows平台的网络协议分析工具
- Network Tools - 各种网络工具: ping, lookup, whois, 等等
- netsniff-ng - 网络嗅探中的瑞士军刀
- Intercepter-NG - 多功能的网络嗅探套件
- SPARTA - 针对网络基础设施的渗透测试工具
- dnschef - 为渗透测试员设计，可高度定制化的DNS代理
- DNSDumpster - 在线DNS侦察和搜索服务
- dnsenum - 用于枚举域名DNS信息，尝试区域传输并进行子域名爆破和DNS反向查询的Perl脚本
- dnsmap - 被动DNS网络映射工具
- dnsrecon - DNS枚举脚本
- dnstracer - 追踪DNS服务器获取信息的来源并获取完整的DNS链路
- passivedns-client - 提供一个用于查询多个被动DNS提供商的库和查询工具
- passivedns - 一个用于记录所有DNS服务器返回信息从而用于被动DNS设置的网络嗅探器
- Mass Scan - TCP端口扫描器，通过异步传输SYN数据包实现，可在5分钟内扫描整个互联网
- Zarp - Zarp是一个以内网为主的网络攻击工具
- mitmproxy - 为渗透测试员和软件开发者设计的支持SSL的HTTP代理
- mallory - 通过SSH代理HTTP和HTTPS
- Netzob - 针对通信协议的流量构造和模糊测试的逆向工程
- DET - DET是同时使用单个或多个隧道进行数据渗漏的POC(概念证明实例)
- pwnat - 攻击防火墙和NAT的漏洞
- dsniff - 一套用于网络审计和渗透测试的工具
- tgcd - 一个简易实用的Unix网络程序，可以将基于TCP/IP的网络服务入口扩展到防火墙之外
- smbmap - 一个方便的SMB枚举工具
- scapy - 一个基于Python的交互式书包操作程序和调用库
- Dshell - 网络取证分析框架
- Debookee (MAC OS X) - 拦截你网络上任何设备的流量
- Dripcap - dripcap 数据包分析工具

无线网络工具

- Aircrack-ng - 一个用于无线网络审计的工具集合
- Kismet - 无线网络的检测工具，嗅探工具和IDS(入侵检测系统)
- Reaver - 针对WiFi防护设置的暴力攻击
- Wifite - 自动化无线网络攻击工具
- wifiphisher - 针对WiFi的自动化钓鱼攻击

SSL 分析工具

- SSLyze - SSL配置扫描器
- sslstrip - 一个HTTPS分割攻击的演示
- sslstrip2 - 攻击基于HSTS的网络交互
- tls_prober - 获取服务器的SSL/TLS指纹

Web 安全

- WPScan - WordPress的黑盒漏洞扫描器
- SQLmap - 自动化SQL注入检测和数据库接管工具
- weevely3 - Webshell管理工具
- Wappalyzer - Wappalyzer分析当前网站所使用的技术
- cms-explorer - CMS Explorer 用于分析各种cms开发的网站所运行的各种特定模块，插件和主题
- joomscan - Joomla网站的漏洞扫描器

- WhatWeb - 网站指纹识别
- BlindElephant - Web应用指纹识别
- fimap - 用于扫描，构造，审计，利用远程文件包含或本地文件包含漏洞甚至谷歌搜索查找存在该漏洞的网站
- Kadabra - 自动化本地文件包含漏洞扫描和利用工具
- Kadimus - 本地文件包含漏洞扫描和利用工具
- liffy - 本地文件包含漏洞利用工具

十六进制编辑器

- HexEdit.js - 在线十六进制编辑器
- Hexinator (商业) - 世上最好的十六进制编辑器

密文破解

- John the Ripper - 快速密文爆破工具
- Online MD5 cracker - 在线MD5哈希破解
- Hashcat - 更快的哈希破解工具

Windows实用工具

- Sysinternals Suite - 故障排除实用程序
- Windows Credentials Editor - 用于列出已登录会话并添加，修改，列出和删除关联的凭据
- mimikatz - 针对Windows系统的权限凭据提取工具
- PowerSploit - 基于powershell的后渗透攻击框架
- Windows Exploit Suggester - 根据目标系统的安全补丁扫描已知的安全漏洞
- Responder - 有毒的 LLMNR, NBT-NS and MDNS，多用于建立各种钓鱼认证服务器
- Empire - Empire 是一个纯PowerShell实现的后渗透攻击套件
- Fibratus - 用于攻击和调试Windows内核的工具

Linux实用工具

- Linux Exploit Suggester - Linux Exploit Suggester基于操作系统发行版本号发现已知的安全漏洞

DDoS(分布式拒绝服务) 工具

- LOIC - 一个为Windows设计的网络压力测试工具(现已支持Mac OS——译者注)
- JS LOIC - LOIC的浏览器版本，JavaScript实现
- T50 - 更快的网络压力测试工具

社会工程学工具

- SET - 来自TrustedSec设计的社会工程学工具套件

公开资源情报分析工具或平台

- Maltego - 来自Paterva设计的开源智能取证专用软件
- theHarvester - 电子邮件地址，子域名和人名的收割机
- creepy - 一个地理位置相关的开源情报工具
- metagoofil - 原始数据收割机
- Google Hacking Database - Google dorks的数据库，可用于侦察
- Censys - 通过每天用ZMap和ZGrab扫描收集主机和网站上的数据
- Shodan - Shodan是世界上第一个物联网设备搜索引擎
- recon-ng - 一个Python开发的全功能侦察工具
- github-dorks - 一个用于扫描GitHub的repos/organizations来发现潜在敏感信息泄露的命令行工具
- vcsmap - 一个基于插件的工具，用于从公共版本控制系统扫描敏感信息
- ZoomEye - ZoomEye是一个网络空间搜索引擎，让用户找到特定的网络组件(IP，服务等等)

匿名工具

- Tor - 一个洋葱路由免费匿名工具
- I2P - 隐形互联网工程
- Nipe - 一个使所有流量通过Tor网络发出的脚本

逆向工程工具

- IDA Pro - 一个支持Windows，Mac OS和Linux平台的反汇编工具和调试器，支持多种架构
- IDA Free - IDA v5.0的免费版本
- WDK/WinDbg - Windows 驱动套件和WinDbg调试器
- OllyDbg - 一个强调二进制代码分析的x86调试器
- Radare2 - 开源跨平台逆向工程框架
- x64_dbg - 为Windows设计的x64/x32开源调试器
- Immunity Debugger - 编写漏洞利用和分析恶意软件的强大工具
- Evan's Debugger - Linux平台类似ollydbg的调试器
- Medusa disassembler - 一个开源的交互式反汇编程序
- plasma - 针对x86/ARM/MIPS的开源交互式反汇编工具. 生成伪代码并自动代码高亮和缩进
- peda - python编写的GDB调试辅助工具

CTF Tools

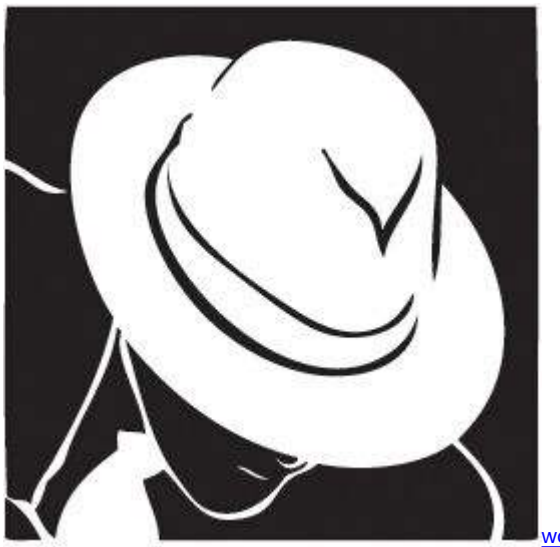
- Pwntools - CTF夺旗赛的破解工具

常用网址

1. https://github.com/
2. https://sectools.org/
3. https://packetstormsecurity.com/
4. https://tools.kali.org/
5. https://blackarch.org/tools.html
6. https://tools.pentestbox.org/
7. http://www.toolswatch.org/
8. http://www.kitploit.com/
9. http://www.darknet.org.uk/
10. http://seclist.us/
11. http://sourceforge.net/

上一篇：【探讨】一次不算太成功的渗透 下一篇：利用BHO实现IE浏览器劫持

1. 2 条回复



wooyun 2017-12-29 13:08:54

动动手指，沙发就是你的了！

0 回复Ta

旋风洗衣机 2018-01-03 18:14:56

第二个，只好坐腿上了

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