**互联网工具**

BurpSuite 拦截和修改和暴力破解HTTP/HTTPS发送的request、response来得到正确账号信息 P121

DirBuster 检测隐藏网址URL（管理网页、备份网页、多余网页）P72

HHTrack 网页复制 P69

MSBSA（Microsoft Baseline Security Analyzer) 弱点扫描工具（内部网络）对目标整体性安全评估 P95

nslookup cmd->nslookup 网址（查询及测试dns服务器的所有IP）P62

NMAP 探测网络状况、端口、防火墙、IPS防御开放情况 P80

OWASP ZAP 弱点扫描 P84拦截和修改HTTP/HTTPS发送的request、response，扫描URL，检测隐藏网址URL（管理网页、备份网页、多余网页）测试及攻击漏洞 P116

SysinternalsSuite 微软系统工具包

SiteDigger 扫描web语句错误 P66

SQLmap 针对SQL Injection 测试数据库所有账号的自动化工具 P135

theHarvester.py cmd->python 路径 -d 网址 -b all（查找指定网站电子邮箱信息及其他相关信息）P67

thc-hydra 拦截和修改和暴力破解FTP发送的request、response来得到正确账号信息

whois 查询网域注册等相关信息（可能有系统管理员信息，进而猜测账号、密码、使用系统信息等）P64

w3af 框架（插件扩展：1.Discovery/crawl:搜索网站资源，寻找URL、forms等可能注入的地方

2.Audit:对Discovery发现的注入点尝试注入资料，判断是否可用

3.Attack:利用Audit阶段发现的弱点进行爆破，若成功会留下后门Shell或下载数据内容 P89

(其他扩展：1.Infrastructure:判断待测目标的系统信息，例，有无安装WAF（Web ApplicationFirewalls）、操作系统及网站服务器类型等）

2.Grep:分析其他Plugin取得的请求与回答（requests/response)内容来判断是否有漏洞存在

3.Output:指定w3af运行时存储（或输出）形式（Console、text、html等）

4.Mangle:用户利用正则表达式（Regular Expressions)将比对相符的request/response内容进行取代

5.Bruteforce:如果需要登陆时，w3af将采用暴力破解账号以及密码的方式尝试登陆

6.Evasion:尝试修改其他Plugin产生的HTTP数据内容，用来规避简易型的入侵检测机制）P89

Wfetch 测试网站启用的方法（HEAD、GET、POST、PUT、DELETE、TRACE、OPTIONS、CONNECT）P97

WebScarb 【只能用于IE（XP）】拦截和修改HTTP/HTTPS发送的request、response P107

**开源的暴力破解工具**

CIntruder 是一款暴力破解验证码的工具，python写的，支持代理和OCR的http form crack

HTTPBrute HTTP认证系统暴力破解软件

Md5CrackGui 是老外开发的一款MD5密码暴力破解软件，使用JAVA编写，编写遵循GPL V3的开源程序。更多信息http://md5crack.adintr.com/

**渗透演练系统**

BodgeIt 包含了XSS、SQL注入、调试代码、CSRF、不安全的对象应用以及程序逻辑上面的一些问题

DVWA (Dam Vulnerable Web Application) 用于常规WEB漏洞教学和检测的WEB脆弱性测试程序。包含了SQL注入、XSS、盲注等常见的一些安全漏洞

Exploit KB / exploit.co.il 包含了各种存在漏洞的WEB应用，可以测试各种SQL注入漏洞。此应用程序还包含在BT5里

Hackxor online黑客游戏,亦可以下载安装完整版进行部署,包括常见的WEB漏洞演练。包含常见的漏洞XSS、CSRF、SQL注入、RCE等

John the Ripper 密码字典、暴力猜解破解 P152

mutillidae 供专门被允许的安全测试和入侵的Web应用程序，其中包含了丰富的渗透测试项目，如SQL注入、跨站脚本、clickjacking、本地文件包含、远程代码执行等

RainbowCrack 建表排列组合破解密码 P146

WackoPicko 用于测试Web应用程序漏洞扫描工具。它包含了命令行注射、sessionid问题、文件包含、参数篡改、sql注入、xss、flash form反射性xss、弱口令扫描等

**测试环境**

WebGoat 逼真的教学环境

OWASP Hackademic 是由OWASP开发的一个项目，你可以用它来测试各种攻击手法，目前包含了10个有问题的WEB应用程序

OWASPbwa虚拟机 PHP+MYSQL+APACHE P30

XSSeducation 是由AJ00200开发的一套专门测试跨站的程序。里面包含了各种场景的测试

**HACKER软件**

regshot 分析注册表的改动

process Hacker 内存查看等

HeidSQL Portable ？

CFF Explorer 了解应用程序如何构建，分析软件架构

Burpsuite 拦截HTTP流量

EchoMirage 拦截TCP流量

wireshark 查看更详细的连接信息，抓包工具

Sysinternals{AccessChk 为了确保创建安全的环境，Windows 管理员通常需要了解特定用户或用户组对文件、目录、注册表项和 Windows 服务等资源具有哪种访问权限。

AccessChk 能够通过直观的界面和输出快速回答这些问题。

AccessEnum 这一简单但强大的安全工具可以向您显示，谁可以用何种访问权限访问您系统中的目录、文件和注册表项。使用此工具可查找权限漏洞。

AdExplorer Active Directory Explorer 是一个高级的 Active Directory (AD) 查看器和编辑器。

AdInsight 一种 LDAP（轻型目录访问协议）实时监视工具，旨在对 Active Directory 客户端应用程序进行故障排除。

AdRestore 恢复已删除的 Server 2003 Active Directory 对象。

Autologon 登录过程中跳过密码屏幕。

Autoruns 查看哪些程序被配置为在系统启动和您登录时自动启动。Autoruns 还能够完整列出应用程序可以配置自动启动设置的注册表和文件位置。

BgInfo 此完全可配置程序会自动生成桌面背景，其中包含有关系统的 IP 地址、计算机名称、网络适配器及更多内容的重要信息。

BlueScreen 此屏幕保护程序不仅精确模拟“蓝屏”，而且也模拟重新启动（完成 CHKDSK），并可在 Windows NT 4、Windows 2000、Windows XP、Server 2003 和 Windows 9x 上工作。

CacheSet 是一个允许您利用 NT 提供的功能来控制缓存管理器的工作集大小的程序。它与 NT 的所有版本都兼容。

ClockRes 查看系统时钟的分辨率，亦即计时器最大分辨率。

Contig 您是否希望迅速对您频繁使用的文件进行碎片整理？使用 Contig 优化单个的文件，或者创建连续的新文件。

Coreinfo 是一个新的命令行实用工具，可向您显示逻辑处理器与物理处理器之间的映射、NUMA 节点和它们所处的插槽，以及分配给每个逻辑处理器的缓存。

Ctrl2cap 这是一个内核模式的驱动程序，可在键盘类驱动程序上演示键盘输入过滤，以便将 Caps-Lock 转变为控制键。在此级别过滤允许在 NT 刚好要“看到”键之前变换和隐藏键。Ctrl2cap 还显示如何使用 NtDisplayString() 打印初始化蓝屏的消息。

DebugView Sysinternals 的另一个优先程序：此程序截取设备驱动程序对 DbgPrint 的调用和 Win32 程序生成的 OutputDebugString。它允许在不使用活动的调试器的情况下，在本地计算机上或通过 Internet 查看和记录调试会话输出。

Desktops 使用这一新的实用工具可以创建最多四个虚拟桌面，使用任务栏界面或热键预览每个桌面上的内容并在这些桌面之间轻松地进行切换。

Disk2vhd 可简化从物理系统到虚拟机 (p2v) 的迁移。

DiskExt 显示卷磁盘映射。

Diskmon 此实用工具会捕捉所有硬盘活动，或者在您的系统任务栏中象软件磁盘活动灯一样工作。

DiskView 图形磁盘扇区实用工具。

Disk Usage (DU) 按目录查看磁盘使用情况。

EFSDump 查看加密文件的信息。

Handle 此易用命令行实用工具将显示哪些进程打开了哪些文件，以及更多其他信息。

Hex2dec 将十六进制数字转换为十进制及反向转换。

接合点 创建 Win2K NTFS 符号链接。

LDMDump 转储逻辑磁盘管理器在磁盘上的数据库内容，其中说明了 Windows 2000 动态磁盘的分区情况。

ListDLLs 列出所有当前加载的 DLL，包括加载位置及其版本号。2.0 版将打印已加载模块的完整路径名。

LiveKd 使用 Microsoft 内核调试程序检查真实系统。

LoadOrder 查看设备加载到 WinNT/2K 系统中的顺序。

LogonSessions 列出系统中的活动登录会话。

MoveFile 使您可以安排在系统下一次重新启动时执行移动和删除命令。

NTFSInfo 用 NTFSInfo 可以查看有关 NTFS 卷的详细信息，包括主文件表 (MFT) 和 MFT 区的大小和位置，以及 NTFS 元数据文件的大小

PageDefrag 对您的分页文件和注册表配置单元进行碎片整理。

PendMoves 枚举在系统下一次启动时所要执行的文件重命名和删除命令的列表。

PipeList 显示系统上的命名管道，包括每个管道的最大实例数和活动实例数。

PortMon 通过高级监视工具监视串行端口和并行端口的活动。它能识别所有的标准串行和并行 IOCTL，甚至可以显示部分正在发送和接收的数据。3.x 版具有强大的新 UI 增强功能和高级筛选功能。

ProcDump 这一新的命令行实用工具旨在捕获其他方式难以隔离和重现 CPU 峰值的进程转储。该工具还可用作用于创建进程转储的一般实用工具，并可以在进程具有挂起的窗口或未处理的异常时监视和生成进程转储。

Process Explorer 找出进程打开了哪些文件、注册表项和其他对象以及已加载哪些 DLL 等信息。这个功能异常强大的实用工具甚至可以显示每个进程的所有者。

Process Monitor 实时监视文件系统、注册表、进程、线程和 DLL 活动。

ProcFeatures 会报告处理器和 Windows 对“物理地址扩展”和“无执行”缓冲区溢出保护的支持情况。

PsExec 在远程系统上执行进程。

PsFile 查看远程打开的文件。

PsGetSid 显示计算机或用户的 SID。

PsInfo 获取有关系统的信息。

PsKill v1.13（2009 年 12 月 1 日）终止本地或远程进程。

PsList 显示有关进程和线程的信息。

PsLoggedOn 显示登录到某个系统的用户。

PsLogList 转储事件日志记录。

PsPasswd 更改帐户密码。

PsService 查看和控制服务。

PsShutdown 关闭并重新启动（可选）计算机。

PsSuspend 挂起和继续进程。

PsTools 套件包括一些命令行程序，可列出本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志，以及执行其他任务。

RegDelNull 扫描并删除包含嵌入空字符的注册表项，标准注册表编辑工具不能删除这种注册表项。

RegJump 跳至 Regedit 中指定的注册表路径。

RootkitRevealer 扫描系统以找出基于 Rootkit 的恶意软件。

SDelete 安全地覆盖敏感文件，并使用此符合 DoD 的安全删除程序清理先前删除文件所在的可用空间。

ShareEnum 扫描网络上的文件共享并查看其安全设置，以关闭安全漏洞。

ShellRunas 通过方便的 shell 上下文菜单项，作为另一个用户启动程序。

Sigcheck 转储文件版本信息并检查系统中的映像是否已进行数字签名。

Streams 显示 NTFS 备用数据流。

Strings 在二进制映像中搜索 ANSI 和 UNICODE 字符串。

Sync 将缓存数据刷新到磁盘。

TCPView 活动套接字命令行查看器，查看本地与远程主机连接等。

VMMap 是进程虚拟和物理内存分析实用工具。

VolumeId 设置 FAT 或 NTFS 驱动器的卷 ID。

Whois 查看 Internet 地址的所有者。

WinObj 基本对象管理器命名空间查看器。

ZoomIt 在屏幕上进行缩放和绘图的演示实用工具。}