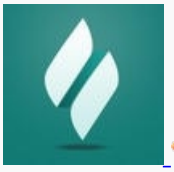
19个安全专家一定要关注的开源 GitHub 项目 3 回复406 查看

实验楼管理员 L64
2016-05-04 14:45 技术分享 技术分享

虽然大多数管理员完全有能力以手动方式执行任务或者编写脚本以实现流程自动化，但借力于现成工具显然更具成本效率。与此同时，拥有超过800个安全类项目的GitHub则是一座IT管理员不容错过的宝库，其中大量工具与框架足以应对恶意软件分析、渗透测试、计算机与网络取证、事件响应以及网络监控等等现实问题。

在今天的文章中，我们将共同了解那些值得关注的系统与网络保护方案。

全部回复



实验楼管理员 L64

1.渗透测试

首先来看渗透测试，这里要提的是Rapid7公司的**Metasploit Framework**。凭借其丰富的资源库，安全专家能够利用这套方案对应用程序进行漏洞检测与安全评估。

此平台立足于模块化结构以实现广泛的通用性，包括可接入面向计算机、手机、路由器、交换机、工业控制系统以及嵌入式设备的功能模块与测试机制。另外，Metasploit还支持Windows、Linux、Android以及iOS等平台。

Metasploit的功能非常全面，但在渗透测试方面，我们还可以选择其他工具，首先是**Browser Exploitation Framework**(简称BeEF)，这款工具专门面向浏览器，可利用客户端攻击向量评估企业环境下Web层面的安全水平。

Mimikatz则是另一款渗透工具，允许测试人员在Windows设备或者网络当中获得立足点。Mimikatz非常强大，允许测试人员提取纯文本密码、哈希值、PIN码以及Kerberos ticket等来自内存的令牌，同时可将受感染系统中的证书与对应私钥导出。Mimikatz可单独使用，同时亦被包含在Metasploit中作为Meterpreter脚本。

2.纵深防御工具

CloudFlare打造的**CFSSL**堪称“瑞士军刀”，其能够签署、验证及绑定TLS证书。CFSSL由命令行工具与HTTP API服务器共同构成，允许管理员建立定制化TLS/PKI工具并利用多套签署密钥进行证书验证。CFSSL还具备一套完整的TLS端点扫描工具，旨在测试服务器配置以识别其中的最新安全漏洞，同时可传输软件包以实现证书配置与撤销。

在软件开发流程当中，密钥与密码等敏感数据的泄露可谓屡见不鲜。**Gitrob** 能够帮助专家扫描自己的GitHub库以找到敏感文件。尽管GitHub内置有信息搜索功能，但Gitrob能够将全部公共库与成员库汇总成单一列表以简化相关流程。这款工具可通过列表根据不同模式匹配文件名称，找到包含敏感信息的文件。Gitrob还能将全部信息保存在PostgreSQL数据库中，并通过简单的Web应用显示

搜索结果。

Lynis是一款面向Linux、Mac OS X、BSD以及Solaris等Unix类系统的安全审计与强化工具。它能够深入扫描并检测系统中的问题、存在漏洞的软件包以及配置设置，并提出相关解决建议。作为蓝绿检测中蓝色团队中的常用工具，Lynis能够轻松实现安全评估、合规性测试、漏洞检测、配置管理以及补丁管理。

国家安全局的**系统完整性管理平台**(简称SIMP)允许安全团队针对网络系统定义并应用安全策略及标准。各组织可利用这套框架满足安全合规要求并自动完成日常任务。SIMP能够立足于网络行为显示操作轨迹以及安全团队的工作偏差，用户需要购买红帽企业Linux授权，方可使用。

2016-05-04 14:46

实验楼管理员 L64

3.网络安全监控

Bro Network Security Monitor面向网络中的全部设备实现可视化，同时能够介入网络流量并检查网络数据包，其分析器则可以检测应用层。安全专家可利用Bro的特定域名脚本语言创建有针对性的站点监控策略。根据该项目的官方网站所介绍，Bro适用于各类科学环境，例如高校、研究实验室以及超级计算中心等。

OSSEC将基于主机的入侵检测系统与日志监控及SIEM(即安全信息与事件管理)功能相结合，同时适用于Linux、Mac OS、Solaris、AIX以及Windows等系统平台。安全团队可利用它实现日志分析、文件完整性检查、策略监控、rootkit检测、实时报警与主动响应等功能。企业还可通过配置发送与未授权文件系统修改及软件日志内恶意行为相关的警报，从而满足合规性要求。

Moloch是一套大型全数据包捕捉式索引与数据库系统，负责实现事件处理、网络安全监控及数字化取证。Moloch允许管理员浏览、搜索并导出其捕捉到的全部网络流量，其中还包含一款用于数据捕捉的单线程C应用、一款用于处理用户界面的Node.js应用外加一套Elasticsearch数据库。

4.事件响应与取证

Mozilla Defense Platform(简称MozDef)能够自动实现事件处理，包括为安全专家提供统一平台对安全事件进行实时监控、响应及协作。MozDef利用Elasticsearch、Meteor以及MongoDB以扩展传统SIEM功能，且属于Mozilla公司自身所使用的成熟平台。

OS X Auditor能够对内核扩展、系统代理与守护程序、第三方代理、已下载文件以及当前运行系统中的已安装应用(或者副本)进行解析与散列处理。这款取证工具可提取多种用户信息，包括隔离文件、浏览器历史记录与cookie、文件下载、LastSession、HTML5数据库与localstore、登录数据、社交与邮件账户乃至已保存无线连接等。OS X Auditor还会验证每个文件的实际来源以实现取证调查。

作为微软与Unix系统上的利器，**Sleuth Kit**允许调查员识别并恢复数字化证据，同时可创建镜像以实现事件响应。调查人员能够分析文件内容、自动完成具体进程并执行MD5镜像完整性检查。该套件还包含一套库与命令行工具，并通过其Autopsy图形界面进行工具访问。

GRR快速响应框架专注于面向Linux、OS X以及Windows客户端的远程实时取证。调查人员可在目标系统中安装Python代理以实现实时远程内存分析、数字化证据收集，并对CPU、内存及I/O使用情况等系统细节进行监控。GRR还利用SleuthKit帮助用户进行原始文件系统访问。

2016-05-04 14:46

实验楼管理员 L64

5.研究工具与漏洞扫描工具

Radare项目是一款面向Android、Linux、BSD、iOS、OS X、Solaris、Haiku、FirefoxOS以及QNX等系统的逆向工程框架与命令行工具，同时支持32位与64位Windows。该项目最初为取证工具兼脚本化命令行十六进制编辑器，但在发展中逐渐引入了库与工具，能够分析二进制文件、拆卸代码、调试程序并接入远程gdb服务器。Radare支持多种架构类型，包括英特尔、ARM、Sparc以及PowerPC等等。

Brakeman是一款面向Ruby on Rails应用的漏洞扫描工具，允许大家对应用进行分部数据流分析。Brakeman能够帮助管理员发现Web应用中的SQL注入、SSL验证回避以及信息泄露等漏洞。Brakeman可作为网站安全扫描工具使用。

Quick Android Review Kit(简称Qark)负责搜索Android应用中的漏洞，包括源代码与打包APK。该工具能够识别出不当导出组件、无效x.509证书、数据泄露、私钥嵌入源代码、密码强度过低或使用不当以及点击劫持等多种问题。Qark还能够提供与所发现漏洞相关的信息，并创建概念验证APK以证明其发现结果。

在恶意软件分析方面，我们可以选择**Cuckoo Sandbox**。这是一套自动化动态恶意软件分析系统，源自2010年谷歌组织的Summer of Code项目。Cuckoo能够建立隔离的虚拟环境，并在其中运行可疑文件并监控其行为。Cuckoo还能够彻查内存并分析数据——例如追踪API调用并记录文件的创建与删除行为——以检测可疑文件在系统中的动向。

Jupyter并非安全类项目，但其可共享的notebooks则是一款不可或缺的安全工具。安全专家能够借此共享实时代码、可视化结果与解释性文本，另外notebooks还支持嵌入shell。其它值得关注的项目组件还包括多用户服务器Jupyterhub、diff工具、Docker stack以及一套OAuth软件包。

编译自：http://www.infoworld.com/article/3051771/security/19-open-source-github-projects-for-security-pros.html ——作者： Fahmida Y. Rashid

转载自： http://os.51cto.com/art/201604/510184.htm——译者： 核子可乐

2016-05-04 14:47

公司
关于我们
联系我们
加入我们
技术博客
合作
我要投稿
教师合作
高校合作
友情链接
服务
实战训练营
会员服务
实验报告
常见问题
隐私条款
学习路径
Python学习路径
Linux学习路径
大数据学习路径
Java学习路径
PHP学习路径
全部

×Close

注意

取消 确定

×

发帖

标题

至少输入5个字

描述

- 编辑
- 预览

Markdown 语法

推荐使用 Markdown 语法，至少输入 5 个字

板块
标签

取消 提交

×

发帖

标题

19个安全专家一定要关注的

描述

- 编辑
- 预览

Markdown 语法

虽然大多数管理员完全有能力以手动方式执行

板块
标签

取消 提交

确定删除

删除后不可恢复

取消 确定