流沙的记忆

Linux漏洞扫描工具【lynis】

Lynis是一款Unix系统的安全审计以及加固工具，能够进行深层次的安全扫描，其目的是检测潜在的时间并对未来的系统加固提供建议。这款软件会扫描一般系统信息，脆弱软件包以及潜在的错误配置.

特征：

1. 漏洞扫描
2. 系统加固
3. 入侵检测
4. 中心管理
5. 自定义行为规划
6. 报告
7. 安全面板
8. 持续监测
9. 技术支持

目标：

1. 自动安全审计
2. 符合性测试
3. 漏洞侦测

有助于：

1. 配置管理
2. 软件补丁管理
3. 系统加固
4. 渗透测试
5. 恶意软件扫描
6. 入侵检测

1、安装软件包

```
# yum --enablerepo=epel -y install lynis
```

也可以使用下面方式安装

```
方式一：root@kali:~# wget https://cisofy.com/files/lynis-2.2.0.tar.gz
方式二：root@kali:~# curl https://cisofy.com/files/lynis-2.2.0.tar.gz -o lynis.tar.gz
方式三：直接使用浏览器打开页面：https://cisofy.com/download/lynis/  ，然后选择下载，下载完后，解压，编译安装
```

2、扫描系统

```
# lynis audit system
```

或者

```
lynis --check-all
```

如果执行上面命令总需要输入回车才能往下执行，你可以使用-c和-Q选项跳过用户输入：

```
$ sudo ./lynis -c -Q
```

```
2017-12-14 17:21:58 Skipped test PHP-2320 (Check PHP disabled functions)
2017-12-14 17:21:58 Reason to skip: Prerequisities not met (ie missing tool, other type of Linux distribution)
2017-12-14 17:21:58 ===-------------------------------------------------------------===
2017-12-14 17:21:58 Skipped test PHP-2368 (Check PHP register_globals option)
2017-12-14 17:21:58 Reason to skip: Prerequisities not met (ie missing tool, other type of Linux distribution)
2017-12-14 17:21:58 ===-------------------------------------------------------------===
2017-12-14 17:21:58 Skipped test PHP-2372 (Check PHP expose_php option)
2017-12-14 17:21:58 Reason to skip: Prerequisities not met (ie missing tool, other type of Linux distribution)
2017-12-14 17:21:58 ===-------------------------------------------------------------===
2017-12-14 17:21:58 Skipped test PHP-2374 (Check PHP enable_dl option)
2017-12-14 17:21:58 Reason to skip: Prerequisities not met (ie missing tool, other type of Linux distribution)
2017-12-14 17:21:58 ===-------------------------------------------------------------===
2017-12-14 17:21:58 Skipped test PHP-2376 (Check PHP allow_url_fopen option)
2017-12-14 17:21:58 Reason to skip: Prerequisities not met (ie missing tool, other type of Linux distribution)
2017-12-14 17:21:58 ===-------------------------------------------------------------===
2017-12-14 17:21:58 Skipped test PHP-2378 (Check PHP allow_url_include option)
2017-12-14 17:21:58 Reason to skip: Prerequisities not met (ie missing tool, other type of Linux distribution)
2017-12-14 17:21:58 ===-------------------------------------------------------------===
```

3、查看日志

日志保存在 /var/log/lynis-report.dat

搜索 “warning” “suggestion”找到建议内容

```
#  grep -E "^warning|^suggestion" /var/log/lynis-report.dat
```

```
suggestion[]=SSH-7408|Consider hardening SSH configuration|X11Forwarding (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowAgentForwarding (YES --> NO)|-|
suggestion[]=BANN-7126|Add a legal banner to /etc/issue, to warn unauthorized users|-|-|
suggestion[]=BANN-7130|Add legal banner to /etc/issue.net, to warn unauthorized users|-|-|
suggestion[]=ACCT-9622|Enable process accounting|-|-|
suggestion[]=ACCT-9630|Audit daemon is enabled with an empty ruleset. Disable the daemon or define rules|-|-|
suggestion[]=FINT-4350|Install a file integrity tool to monitor changes to critical and sensitive files|-|-|
suggestion[]=TOOL-5002|Determine if automation tools are present for system management|-|-|
suggestion[]=KRNL-6000|One or more sysctl values differ from the scan profile and could be tweaked|-|-|
suggestion[]=HRDN-7222|Harden compilers like restricting access to root user only|-|-|
suggestion[]=HRDN-7230|Harden the system by installing at least one malware scanner, to perform periodic file sys
s|-|Install a tool like rkhunter, chkrootkit, OSSEC|
```

4.创建Lynis计划任务

如果你想为你的系统创建一个日扫描报告，你可以设置cron：

```
$ crontab -e
添加cron任务：

30 22 * * * /usr/bin/lynis -c --auditor "automated" --cronjob > /var/log/lynis/report.txt
上面任务每天晚上10:30会执行扫描，并把输出的信息保存到/var/log/lynis.log日志文件中。
```

一个人走的快，但是走不远；一群人才能走的远；挑战自己，GO! GO! GO!

流沙的记忆
关注 - 4
粉丝 - 2
+加关注

0 0

« 上一篇：Redis 单机安装【一】
» 下一篇：Centos 6.8下安装oracle10g数据库、

posted @ 2018-01-04 15:36 流沙的记忆 阅读(2377) 评论(0) 编辑 收藏

· 月活3.31亿，年营收11亿美元，Reddit的用户最个值钱？
· 比尔·盖茨发布2019新年信：意料之外
· 三星的新手表取消了旋转表圈，新真无线耳机电池缩水
» 更多新闻...