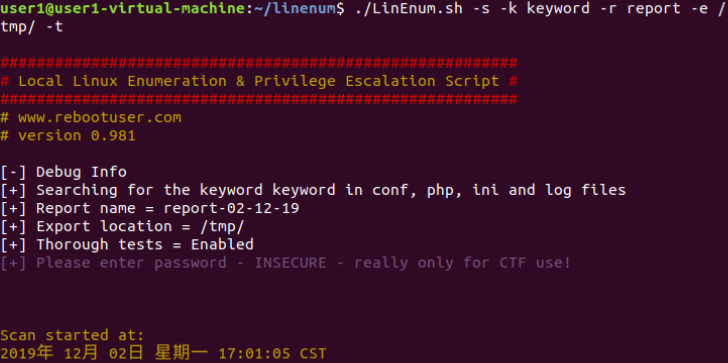
**LinEnum工具:底层系统的所有信息:**

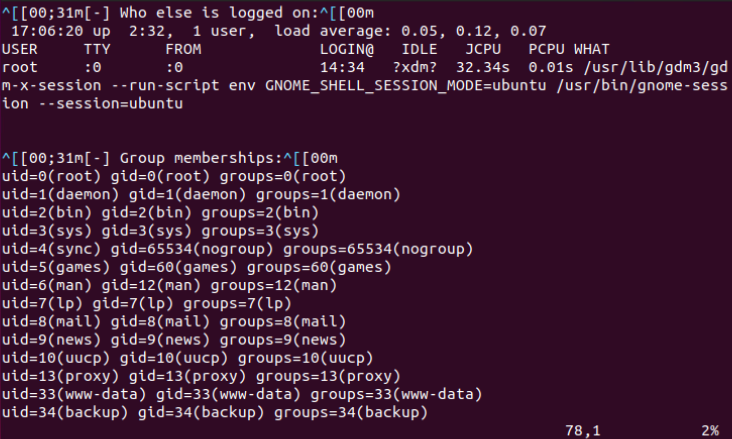
在进行任何类型的权限提升攻击之前，首先要在 Linux 主机上进行一个良好的信息收集工作，并识别所有关于系统的信息。包括用户、服务、定时任务、软件版本、弱信任对象、错误配置的文件权限，甚至是 Docker 信息。

工具:LinEnum 底层系统的所有信息

https://github.com/rebootuser/linenum







1.找任何可用的漏洞或服务、计划任务中的错误配置(总是有一个潜在的可能性可以直接使系统挂掉)

2.直接在系统或应用程序上进行攻击

**linux-exploit-suggester工具:分析主机系统识别缺失的补丁和漏洞:**

使用 linux-exploit-suggester 工具分析主机系统并识别缺失的补丁和漏洞，一旦识别出漏

洞，该工具还将提供可用 PoC 漏洞的链接。

https://github.com/mzet-/linux-exploit-suggester

LES tool is designed to assist in detecting security deficiencies for given Linux kernel/Linux-based machine.

