六、进程管理

Linux黑客基础–45–进程管理（1）–概述

进程是一个正在运行和使用资源的程序

查看

查找

发现占用系统资源比较多的进程

管理后台的进程

进程优先级的调整

结束进程

进程的调度（周期）执行

Linux黑客基础–45–进程管理（1）–如何查看进程

Viewing Processes 进程的查看

ps

ps – report a snapshot of the current processes.

ps aux　查看所有进程的详细信息

1、init进程是系统调用的第一个进程，编号为1，也是所有进程的父进程

2、pstree　查看进程数

3、ps –elf　查看所有进程的详细信息（优先级、父进程）

4、ps –U hy –u hy　查看指定用户的进程

5、ps –p "2 6"　查看指定的进程

USER The user who invoked the process

PID The process ID

%CPU The percent of CPU this process is using

%MEM The percent of memory this process is using

COMMAND The name of the command that started the process

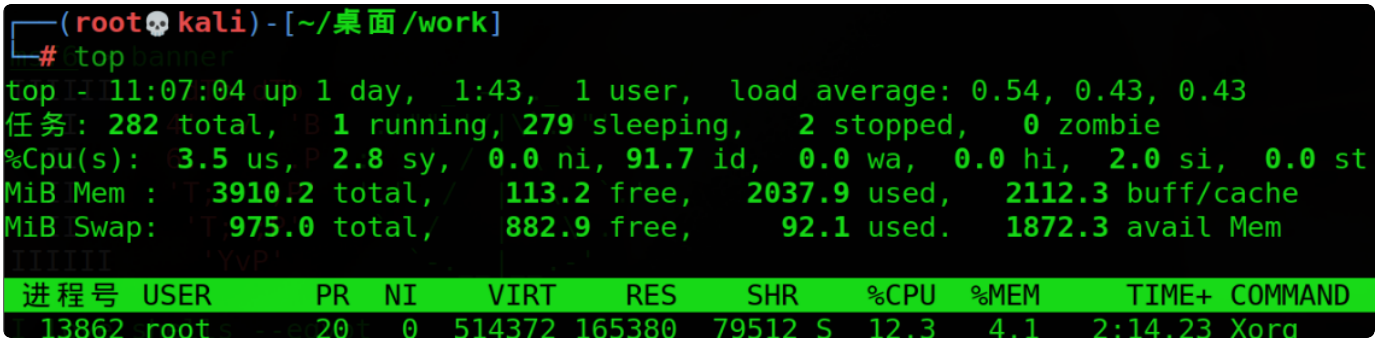
Linux黑客基础–46–进程管理（2）–进程查看和结束进程

Filtering by Process Name　根据进程的名字进行过滤

ps aux | grep msfconsole　查看指定软件的进程

Finding the Greediest Processes with top　通过 top 命令查找资源占用率过高的进程

动态查看　list dynamically—by default, every 10 seconds.　默认每10秒刷新一次



1、交互

H or ?

–k：杀死一个进程

–r: 调整进程的优先级

–l：查看系统得分平衡负载

–t：按照cpu占用排序

–M：按照内存占用排序

2、选项

–d：设定更新间隔

3、程序的管理

程序之间是可以相互控制的!

通过给予该程序一个信号（signal）去告知该程序你想要让他作什么

查看常用的信号值

kill –l （小写）或者是 man 7 signal

15/signal 正常结束一个进程

9/sigkill 强制结束一个进程，副作用会有一些半成品（如交换文件.swp文件）

1/sighup 常用于重启一个服务进程，重新读取服务的配置文件

2/sigint 相当于ctrl–c 中断一个程序的运行

19/sigstop　相当于ctrl-z　把程序放在后台并停止运行

结束一个进程

kill 【信号】进程id（pid）

查看后台任务

jobs

把后台任务调用前台运行

fg　任务编号

把后台停止任务启动

bg　任务编号

Linux黑客基础-47-进程管理（3）-SIGHUP信号的理解

案例：kali中配置启用ssh服务，并允许root用户可以使用口令认证进行远程登录

（1）ssh服务（22/tcp）

更安全的远程登录方式

进程名：sshd　ps aux | grep sshd　查看进程

netstat -tunlp | grep "22"　查看端口

（2）使用终端工具远程连接kali

（3）编辑ssh服务配置文件

/etc/ssh/sshd_config

cp -r /etc/ssh/sshd_config.d /etc/ssh/sshd_config.bak

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PermitEmptyPasswords yes
```

systemctl restart ssh

Linux黑客基础–48–进程管理（4）–如何踢掉一个在线用户

1、进程的常见状态

R（Running）：该程序正在运行中

S（Sleep）：该程序目前正在睡眠状态（idle），但可以被唤醒（signal）

D：不可被唤醒的睡眠状态，通常这支程序可能在等待I/O的情况

T：停止状态（stop），可能是在工作控制（背景暂停）或出错状态

Z（Zombie）：僵尸状态，程序已经终止但却无法从内存移除

2、结束进程

kill –信号 进程号

killall –信号 程序名

结束进程树

pkill

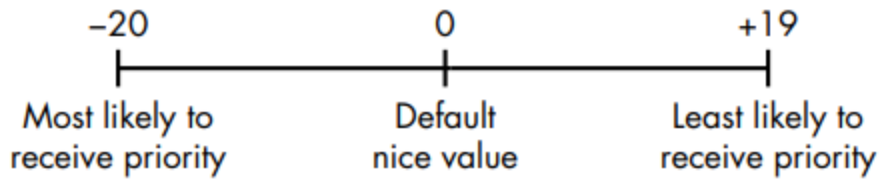
pkill –u 用户名 踢掉一个在线用户

pgrep –u hy 根据指定用户过滤进程

Linux黑客基础–49–进程管理（5）–进程优先级的调整

优先执行程序（priority，PRI），这个PRI值越低代表优先级越优

优先级的范围



PRI（new）=PRI（old）+nice

nice值可以调整的范围为-20~19

root可随意调整自己或他人程序的nice值，且范围为-20~19

一般用户仅可调整自己程序的nice值，且范围仅为0~19（避免一般用户抢占系统资源）

一般使用者仅可将nice值越调越高，例如本来nice为5，则未来仅能调整到大于5

Setting the Priority When Starting a Process　在运行进程时设置优先级

nice

nice -n 10 ping www.baidu.com

ps -lef | grep ping

使用 renice 命令改变正在运行的进程优先级

renice

renice -5 3341

ps -lef | grep ping

top -u 用户名　查看指定用户的进程动态进程表

```
┌──(hy㉿kali)-[/root]
└─$ top -u root
top - 10:21:11 up 30 min,  1 user,  load average: 0.20, 0.27, 0.27
任务: 227 total,   1 running, 224 sleeping,   2 stopped,   0 zombie
%Cpu(s):  3.0 us,  2.1 sy,  0.0 ni, 93.7 id,  0.0 wa,  0.0 hi,  1.2 si,  0.0 st
MiB Mem :   3898.0 total,   2133.2 free,    951.8 used,    813.0 buff/cache
MiB Swap:    975.0 total,    975.0 free,      0.0 used.   2649.8 avail Mem
```

Linux黑客基础-50-进程管理（6）-后台进程管理及at调度工具

把程序放在后台执行

程序 &

vi hhh.txt &

jobs 查看进程

fg 程序名 调入前台

bg 程序名 把后台停止的任务启动

任务的调度（安任务在什么时间执行）

Scheduling Processes

一次性调度 服务 atd

周期性调度 服务 crond