

Assignment 2

Testing out kali linux tools

1 Information Gathering

Information gathering involves collecting data about a target, such as domain names, IP addresses, and organizational details, to understand its security posture and potential weaknesses. Tools like Nmap and Shodan are used for this purpose.

```

PING geeksforgeeks.org (34.218.62.116) 56(84) bytes of data.
^Z
zsh: suspended ping geeksforgeeks.org

(grim@kali)-[~]
$ nmap -sV 34.218.62.116
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 23:13 IST
Nmap scan report for ec2-34-218-62-116.us-west-2.compute.amazonaws.com (34.218.62.116)
Host is up (0.28s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp?
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
554/tcp   open  rtsp?
1723/tcp  open  pptp?
Service Info: OS: Linux; CPE: cpe:o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.31 seconds

```

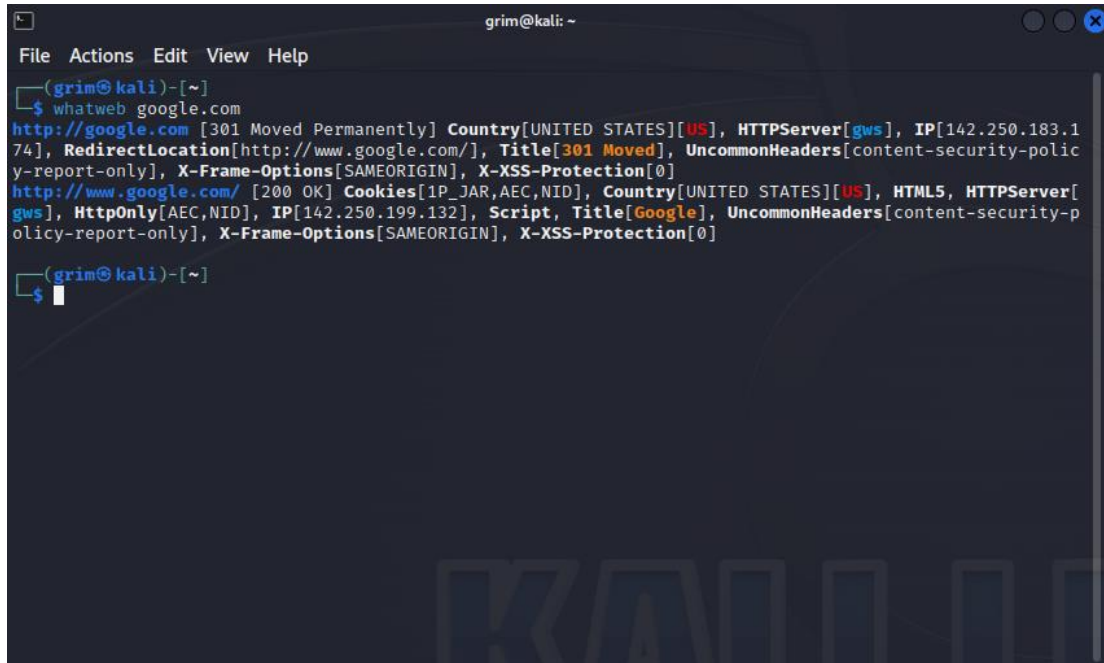
2 Vulnerability Analysis

Vulnerability analysis assesses systems for security weaknesses and potential entry points for attackers. Tools like Nessus and OpenVAS scan for vulnerabilities and provide reports for remediation.

```
grim@kali: ~  
File Actions Edit View Help  
74], RedirectLocation[http://www.google.com/], Title[301 Moved], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]  
http://www.google.com/ [200 OK] Cookies[1P_JAR,AEC,NID], Country[UNITED STATES][US], HTML5, HTTPServer[gws], HttpOnly[AEC,NID], IP[142.250.199.132], Script, Title[Google], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]  
  
(grim@kali)-[~]  
$ sq  
sq: command not found  
  
(grim@kali)-[~]  
$ sqlmap  
  
[H]  
[C]  
[V ...] {1.7.8#stable}  
https://sqlmap.org  
  
Usage: python3 sqlmap [options]  
  
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help  
  
(grim@kali)-[~]  
$
```

3 Web penetration Analysis

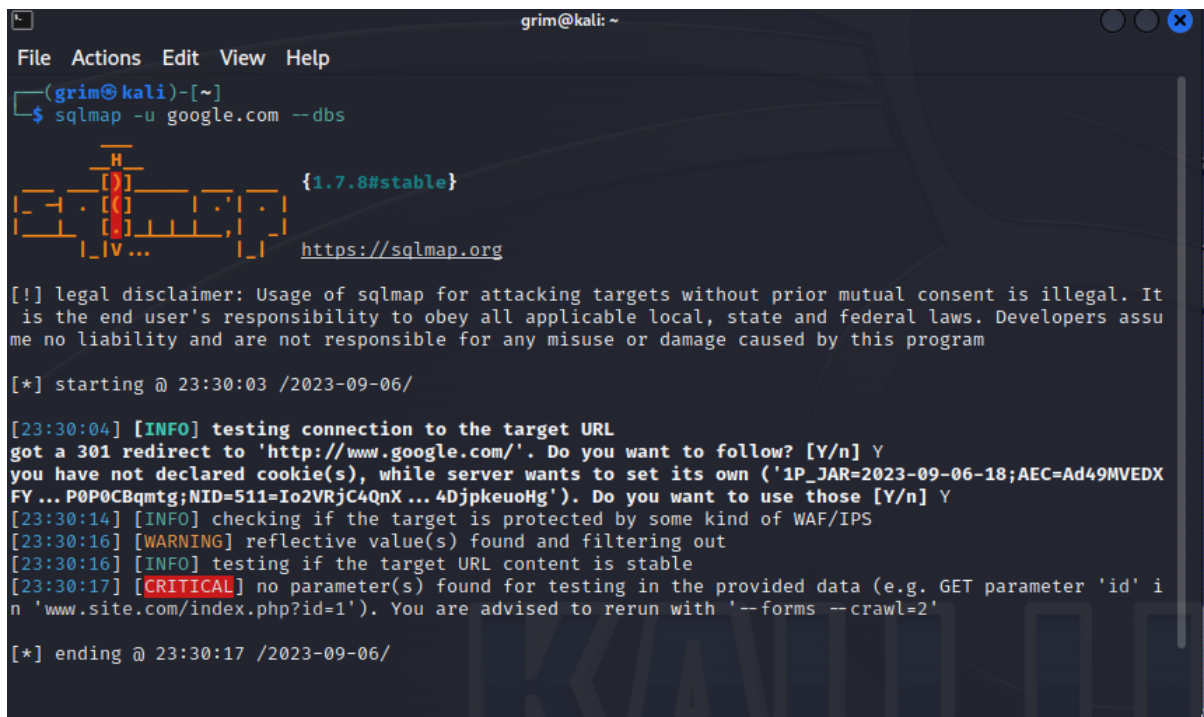
Web application analysis focuses on assessing the security of web applications. Tools like OWASP ZAP and Burp Suite help identify issues like SQL injection and cross-site scripting (XSS).




```
grim@kali: ~  
File Actions Edit View Help  
(grim@kali)-[~]  
$ whatweb google.com  
http://google.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[gws], IP[142.250.183.174], RedirectLocation[http://www.google.com/], Title[301 Moved], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]  
http://www.google.com/ [200 OK] Cookies[1P_JAR,AEC,NID], Country[UNITED STATES][US], HTML5, HTTPServer[gws], HttpOnly[AEC,NID], IP[142.250.199.132], Script, Title[Google], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]  
(grim@kali)-[~]  
$
```

4 Database Assessment

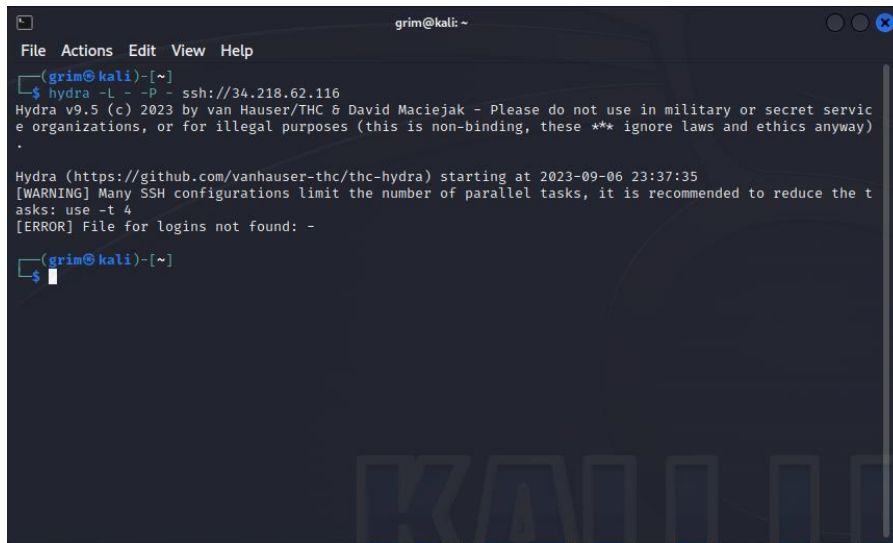
Database assessment evaluates the security of databases, including access controls and data integrity. Tools like SQLMap can identify and exploit vulnerabilities in database systems.



```
grim@kali: ~  
File Actions Edit View Help  
(grim@kali)-[~]  
$ sqlmap -u google.com --dbs  
 {1.7.8#stable}  
https://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 23:30:03 /2023-09-06/  
[23:30:04] [INFO] testing connection to the target URL  
got a 301 redirect to 'http://www.google.com/'. Do you want to follow? [Y/n] Y  
you have not declared cookie(s), while server wants to set its own ('1P_JAR=2023-09-06-18;AEC=Ad49MVEDXFY...P0P0CBqmtg;NID=511=Io2VRjC4QnX...4DjpkeuoHg'). Do you want to use those [Y/n] Y  
[23:30:14] [INFO] checking if the target is protected by some kind of WAF/IPS  
[23:30:16] [WARNING] reflective value(s) found and filtering out  
[23:30:16] [INFO] testing if the target URL content is stable  
[23:30:17] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'  
[*] ending @ 23:30:17 /2023-09-06/
```

5 Password Attacks

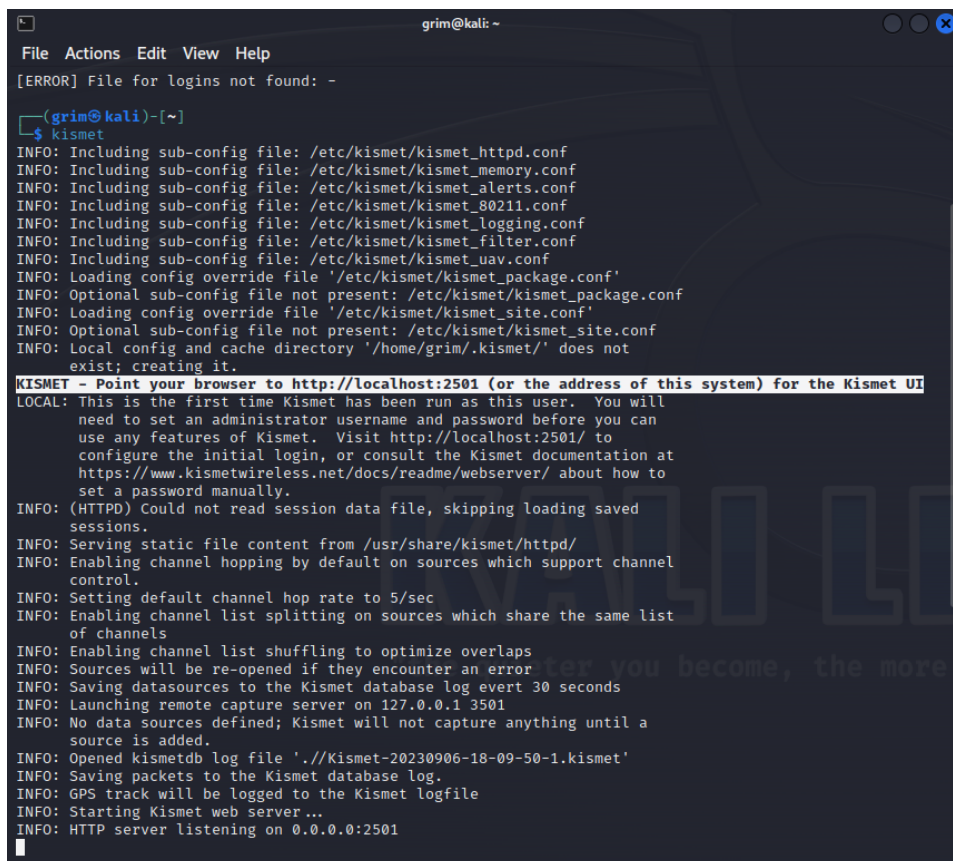
Password attacks involve attempting to crack or guess user passwords. Tools like John the Ripper and Hydra are used to perform brute-force attacks or dictionary-based password cracking.

A terminal window titled 'grim@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The user enters the command '\$ hydra -L - -P - ssh://34.218.62.116'. The output shows Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak, a warning about SSH configurations, and an error message '[ERROR] File for logins not found: -'. The prompt returns to '(grim@kali)-[~]' with a cursor on the next line.

```
grim@kali: ~  
File Actions Edit View Help  
(grim@kali)-[~]  
$ hydra -L - -P - ssh://34.218.62.116  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service  
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)  
.  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-06 23:37:35  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the t  
asks: use -t 4  
[ERROR] File for logins not found: -  
(grim@kali)-[~]  
$
```

6 Wireless Attacks

Wireless attacks target Wi-Fi networks. Tools like Aircrack-ng and Reaver can be used to exploit weak encryption and gain unauthorized access to wireless networks.

A terminal window titled 'grim@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The user enters the command '\$ kismet'. The output shows various INFO messages about including sub-config files, loading config overrides, and setting up the Kismet web server. A highlighted line says 'KISMET - Point your browser to http://localhost:2501 (or the address of this system) for the Kismet UI'. The terminal ends with 'INFO: HTTP server listening on 0.0.0.0:2501'.

```
grim@kali: ~  
File Actions Edit View Help  
[ERROR] File for logins not found: -  
(grim@kali)-[~]  
$ kismet  
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf  
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf  
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf  
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf  
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf  
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf  
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf  
INFO: Loading config override file '/etc/kismet/kismet_package.conf'  
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf  
INFO: Loading config override file '/etc/kismet/kismet_site.conf'  
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf  
INFO: Local config and cache directory '/home/grim/.kismet/' does not  
exist; creating it.  
KISMET - Point your browser to http://localhost:2501 (or the address of this system) for the Kismet UI  
LOCAL: This is the first time Kismet has been run as this user. You will  
need to set an administrator username and password before you can  
use any features of Kismet. Visit http://localhost:2501/ to  
configure the initial login, or consult the Kismet documentation at  
https://www.kismetwireless.net/docs/readme/webserver/ about how to  
set a password manually.  
INFO: (HTTPD) Could not read session data file, skipping loading saved  
sessions.  
INFO: Serving static file content from /usr/share/kismet/httpd/  
INFO: Enabling channel hopping by default on sources which support channel  
control.  
INFO: Setting default channel hop rate to 5/sec  
INFO: Enabling channel list splitting on sources which share the same list  
of channels  
INFO: Enabling channel list shuffling to optimize overlaps  
INFO: Sources will be re-opened if they encounter an error  
INFO: Saving datasources to the Kismet database log every 30 seconds  
INFO: Launching remote capture server on 127.0.0.1 3501  
INFO: No data sources defined; Kismet will not capture anything until a  
source is added.  
INFO: Opened kismetdb log file './Kismet-20230906-18-09-50-1.kismet'  
INFO: Saving packets to the Kismet database log.  
INFO: GPS track will be logged to the Kismet logfile  
INFO: Starting Kismet web server...  
INFO: HTTP server listening on 0.0.0.0:2501
```

7 Reverse Engineering

Reverse engineering is the process of dissecting and analyzing software or hardware to understand its inner workings. Tools like IDA Pro and Ghidra assist in reverse engineering tasks.

```
(grim@kali)-[~]
└─$ nasm -f elf source.asm -o source.o
nasm: fatal: unable to open input file `source.asm' No such file or directory

(grim@kali)-[~]
└─$ clang source.c -o output
clang: error: no such file or directory: 'source.c'
clang: error: no input files

(grim@kali)-[~]
└─$
```

8 Exploitation tools

Exploitation tools are used to leverage vulnerabilities and gain unauthorized access to systems. Metasploit is a well-known framework for developing and executing exploits.

```
(grim@kali)-[~]
└─$ msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%                               %
%%  %%  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  https://metasploit.com %%%%%%%%%
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%  %  %%%%%%%%%%%%%%%%%%%%%%%%%%  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
"the quieter you become, the more

= [ metasploit v6.3.27-dev ]
+ -- -- [ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- -- [ 1383 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

9 Sniffing and spoofing

Sniffing tools like Wireshark intercept and analyze network traffic, while spoofing tools like Ettercap allow attackers to manipulate network packets, often for malicious purposes.

```
msf6 > sudo tcpdump -i etho0 -n
[*] exec: sudo tcpdump -i etho0 -n

[sudo] password for grim:
tcpdump: etho0: No such device exists
(No such device exists)
msf6 >
```

10 Post Exploitation

Post-exploitation tools and techniques are used by attackers after gaining access to a system to maintain control, escalate privileges, and exfiltrate data. These may include backdoors and privilege escalation exploits.

```
msf6 > uname -a
[*] exec: uname -a

Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux
msf6 > cat /etc/*-release
[*] exec: cat /etc/*-release

PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
msf6 > sudo -l
[*] exec: sudo -l

Matching Defaults entries for grim on kali:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User grim may run the following commands on kali:
    (ALL : ALL) ALL
msf6 >
```

11 Forensics

Digital forensics involves the collection and analysis of digital evidence for legal purposes. Tools like Autopsy and The Sleuth Kit help investigators uncover information and build a case in cybercrime investigations.

```
msf6 > sudo -l
[*] exec: sudo -l

Matching Defaults entries for grim on kali:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User grim may run the following commands on kali:
    (ALL : ALL) ALL
msf6 >
Zsh: suspended msfconsole

(grim@kali)-[~]
└─$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda           8:0    0 25.4G  0 disk
└─sda1       8:1    0 24.4G  0 part /
└─sda2       8:2    0    1K  0 part
└─sda5       8:5    0  975M  0 part [SWAP]
sr0          11:0    1 1024M  0 rom

(grim@kali)-[~]
└─$ fdisk -l
fdisk: cannot open /dev/sda: Permission denied

(grim@kali)-[~]
└─$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 20836  9308 ?        Ss   22:48   0:01 /sbin/init splash
root         2  0.0  0.0      0   0 ?        S    22:48   0:00 [kthreadd]
root         3  0.0  0.0      0   0 ?        I<   22:48   0:00 [rcu_gp]
root         4  0.0  0.0      0   0 ?        I<   22:48   0:00 [rcu_par_gp]
root         5  0.0  0.0      0   0 ?        I<   22:48   0:00 [slub_flushwq]
root         6  0.0  0.0      0   0 ?        I<   22:48   0:00 [netns]
root         7  0.0  0.0      0   0 ?        I    22:48   0:00 [kworker/0:0-events]
root         8  0.0  0.0      0   0 ?        I<   22:48   0:00 [kworker/0:0H-events_highpri]
root        10  0.0  0.0      0   0 ?        I<   22:48   0:00 [mm_percpu_wq]
root        11  0.0  0.0      0   0 ?        I    22:48   0:00 [rcu_tasks_kthread]
root        12  0.0  0.0      0   0 ?        I    22:48   0:00 [rcu_tasks_rude_kthread]
root        13  0.0  0.0      0   0 ?        I    22:48   0:00 [rcu_tasks_trace_kthread]
root        14  0.0  0.0      0   0 ?        S    22:48   0:00 [ksoftirqd/0]
root        15  0.0  0.0      0   0 ?        I    22:48   0:03 [rcu_preempt]
root        16  0.0  0.0      0   0 ?        S    22:48   0:00 [migration/0]
root        17  0.0  0.0      0   0 ?        S    22:48   0:00 [idle_inject/0]
root        19  0.0  0.0      0   0 ?        S    22:48   0:00 [cpuhp/0]
root        20  0.0  0.0      0   0 ?        S    22:48   0:00 [cpuhp/1]
root        21  0.0  0.0      0   0 ?        S    22:48   0:00 [idle_inject/1]
root        22  0.0  0.0      0   0 ?        S    22:48   0:00 [migration/1]
```