**Part 1:**

2.

sudo vim /etc/logrotate.conf

A screenshot of a computer

Description automatically generated with medium confidence

3.

┌──(kali㉿kali)-[~]

└─$ service rsyslog stop

Warning: Stopping rsyslog.service, but it can still be activated by:

syslog.socket

┌──(kali㉿kali)-[~]

└─$ tail -n 15 /var/log/syslog

Nov 16 14:55:04 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2208.0" x-pid="407" x-info="https://www.rsyslog.com"] exiting on signal 15.

Nov 16 14:55:04 kali systemd[1]: rsyslog.service: Deactivated successfully.

Nov 16 14:55:04 kali systemd[1]: Stopped System Logging Service.

Nov 16 14:55:04 kali systemd[1]: Starting System Logging Service...

Nov 16 14:55:04 kali rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2208.0]

Nov 16 14:55:04 kali systemd[1]: Started System Logging Service.

Nov 16 14:55:04 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2208.0" x-pid="8782" x-info="https://www.rsyslog.com"] start

Nov 16 15:00:25 kali systemd[1]: Stopping System Logging Service...

Nov 16 15:00:25 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2208.0" x-pid="8782" x-info="https://www.rsyslog.com"] exiting on signal 15.

Nov 16 15:00:25 kali systemd[1]: rsyslog.service: Deactivated successfully.

Nov 16 15:00:25 kali systemd[1]: Stopped System Logging Service.

Nov 16 15:00:25 kali systemd[1]: Starting System Logging Service...

Nov 16 15:00:25 kali rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2208.0]

Nov 16 15:00:25 kali systemd[1]: Started System Logging Service.

Nov 16 15:00:25 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2208.0" x-pid="10107" x-info="https://www.rsyslog.com"] start

┌──(kali㉿kali)-[~]

└─$

4.

┌──(kali㉿kali)-[~]

└─$ ls /var/log/kern.log\*

/var/log/kern.log /var/log/kern.log.2.gz /var/log/kern.log.4.gz

/var/log/kern.log.1 /var/log/kern.log.3.gz

┌──(kali㉿kali)-[~]

└─$ sudo shred -f -n 10 /var/log/kern.log.\*

┌──(kali㉿kali)-[~]

└─$

**Part 2:**

1.

┌──(kali㉿kali)-[~]

└─$ service apache2 start

┌──(kali㉿kali)-[~]

└─$

2.

┌──(kali㉿kali)-[~]

└─$ sudo vim /var/www/html/index.html

Graphical user interface, text

Description automatically generated

5.

┌──(kali㉿kali)-[~]

└─$ service postgresql start

┌──(kali㉿kali)-[~]

└─$ sudo msfconsole

\_ \_

/ \ /\ \_\_ \_ \_\_ /\_/ \_\_

| |\ / | \_\_\_\_\_ \ \ \_\_\_ \_\_\_\_\_ | | / \ \_ \ \

| | \/| | | \_\_\_\ |- -| /\ / \_\_\ | -\_\_/ | || | || | |- -|

|\_| | | | \_|\_\_ | |\_ / -\ \_\_\ \ | | | | \\_\_/| | | |\_

|/ |\_\_\_\_/ \\_\_\_\/ /\ \\\_\_\_/ \/ \\_\_| |\_\ \\_\_\_\

=[ metasploit v6.2.20-dev ]

+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post ]

+ -- --=[ 951 payloads - 45 encoders - 11 nops ]

+ -- --=[ 9 evasion ]

Metasploit tip: Use the edit command to open the

currently active module in your editor

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db\_connect msf\_user:root@127.0.0.1/hackers\_arise\_db

[\*] Connected to Postgres data service: 127.0.0.1/hackers\_arise\_db