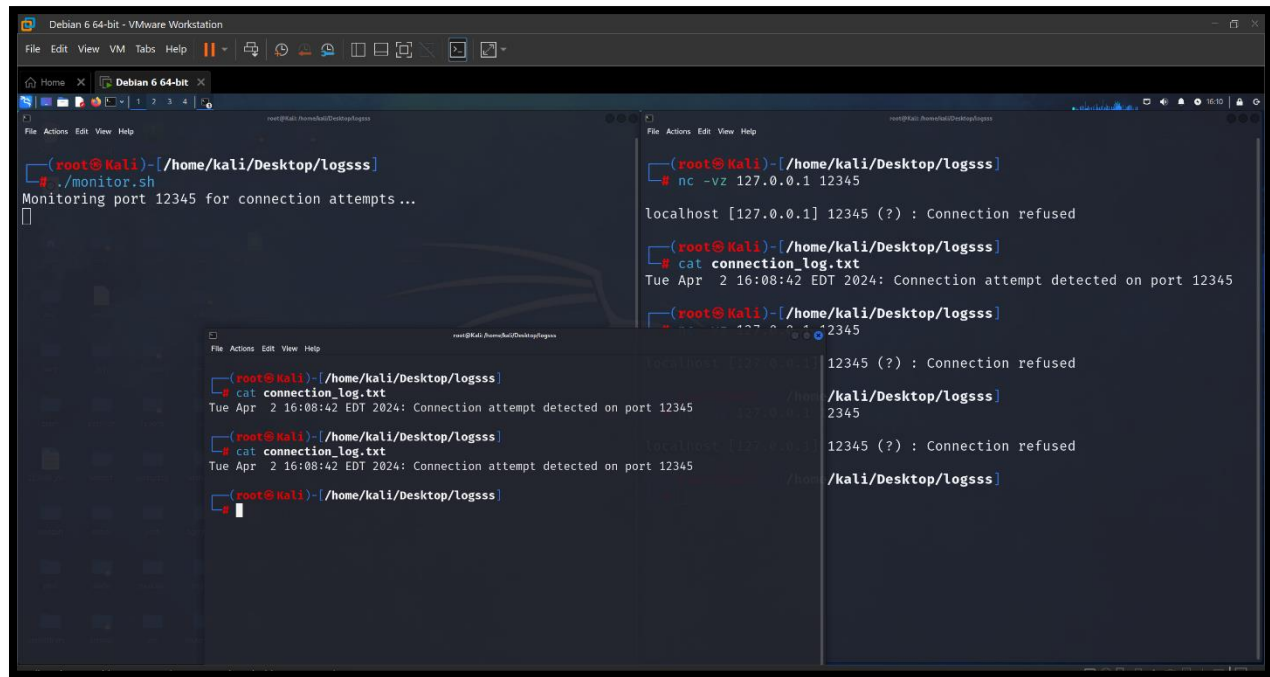


## Sample Logs Creation and Detection in Linux

The **monitor.sh** script monitors port **12345** for connection attempts, logging any detected attempts to the **connection\_log.txt** file. Malicious port access through **netcat** and **telnet** can be detected and logged using this script.

Linkedin: <https://www.linkedin.com/in/ehtishamcyber/>



### monitor.sh

```
#!/bin/bash
```

```
# Port number to monitor
```

```
port=12345
```

```
# Log file path
```

```
log_file="connection_log.txt"
```

```
# Function to log connection attempts
```

```
log_connection() {
```

```
    echo "$(date): Connection attempt detected on port $port" >> "$log_file"
```

```
}
```

# Start monitoring network traffic on the specified port and log any connection attempts

```
sudo tcpdump -i lo -n -l port $port >> /dev/null &
```

# Trap to log connection attempts

```
trap log_connection EXIT
```

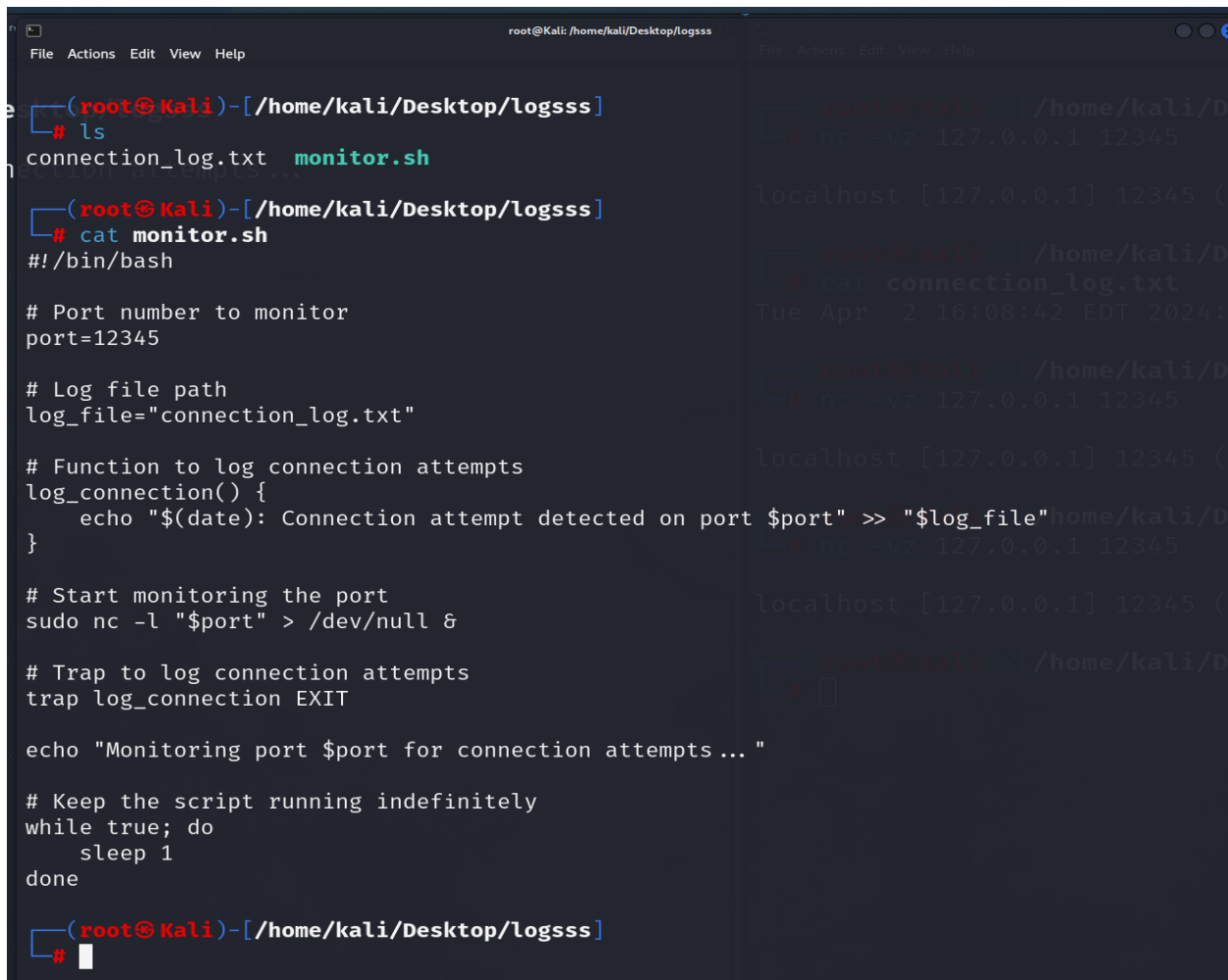
```
echo "Monitoring port $port for connection attempts..."
```

# Keep the script running indefinitely

```
while true; do
```

```
    sleep 1
```

```
done
```



```
root@Kali: /home/kali/Desktop/logsss
File Actions Edit View Help
(root@Kali)-[/home/kali/Desktop/logsss]
# ls
connection_log.txt  monitor.sh

(root@Kali)-[/home/kali/Desktop/logsss]
# cat monitor.sh
#!/bin/bash

# Port number to monitor
port=12345

# Log file path
log_file="connection_log.txt"

# Function to log connection attempts
log_connection() {
    echo "$(date): Connection attempt detected on port $port" >> "$log_file"
}

# Start monitoring the port
sudo nc -l "$port" > /dev/null &

# Trap to log connection attempts
trap log_connection EXIT

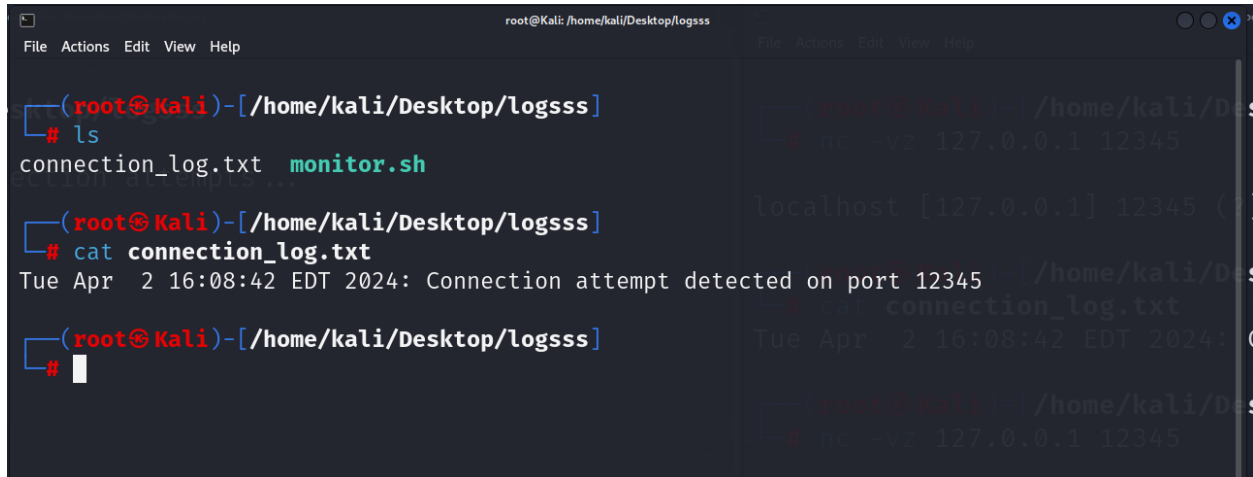
echo "Monitoring port $port for connection attempts..."

# Keep the script running indefinitely
while true; do
    sleep 1
done

(root@Kali)-[/home/kali/Desktop/logsss]
#
```

## connection\_log.txt

To store and collect Logs.



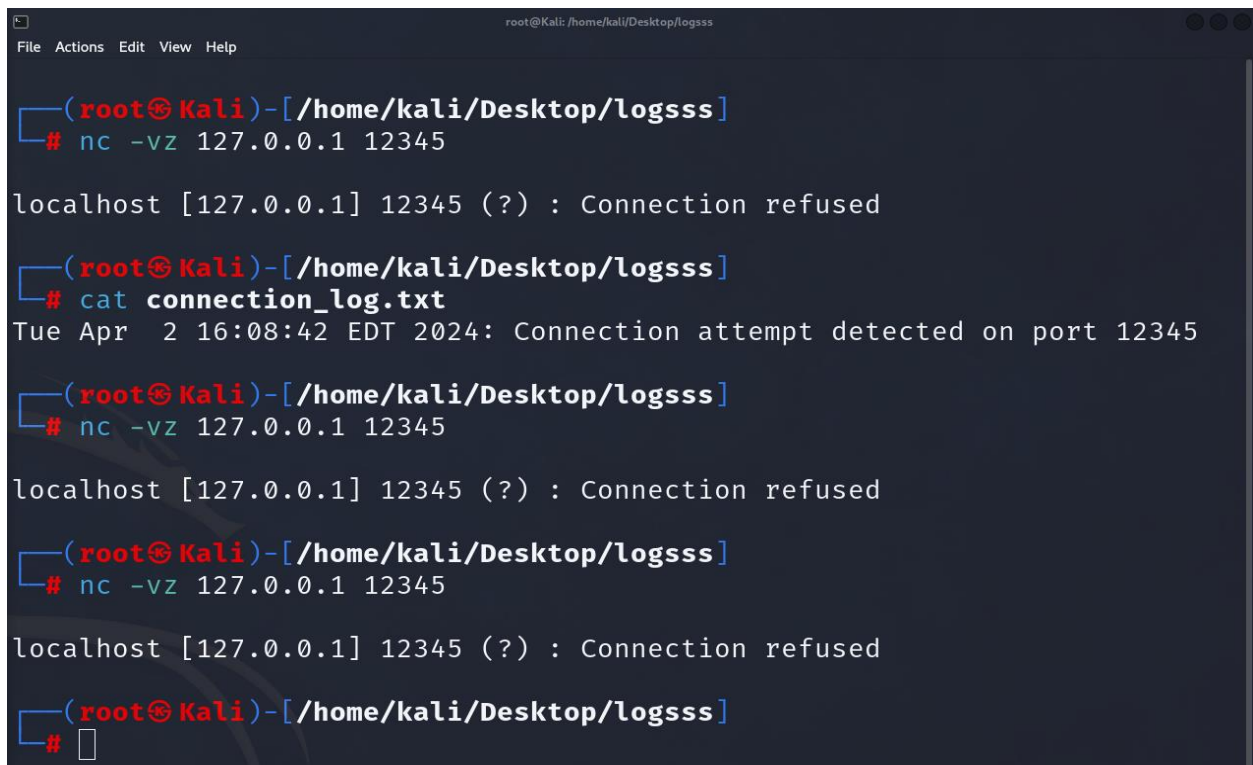
```
root@Kali: /home/kali/Desktop/logsss
File Actions Edit View Help

(root@Kali)-[/home/kali/Desktop/logsss]
# ls
connection_log.txt  monitor.sh

(root@Kali)-[/home/kali/Desktop/logsss]
# cat connection_log.txt
Tue Apr 2 16:08:42 EDT 2024: Connection attempt detected on port 12345

(root@Kali)-[/home/kali/Desktop/logsss]
#
```

## Malicious port accessing through netcat and telnet



```
root@Kali: /home/kali/Desktop/logsss
File Actions Edit View Help

(root@Kali)-[/home/kali/Desktop/logsss]
# nc -vz 127.0.0.1 12345

localhost [127.0.0.1] 12345 (?) : Connection refused

(root@Kali)-[/home/kali/Desktop/logsss]
# cat connection_log.txt
Tue Apr 2 16:08:42 EDT 2024: Connection attempt detected on port 12345

(root@Kali)-[/home/kali/Desktop/logsss]
# nc -vz 127.0.0.1 12345

localhost [127.0.0.1] 12345 (?) : Connection refused

(root@Kali)-[/home/kali/Desktop/logsss]
# nc -vz 127.0.0.1 12345

localhost [127.0.0.1] 12345 (?) : Connection refused

(root@Kali)-[/home/kali/Desktop/logsss]
#
```

## References:

This hands-on exercise Utilizing ChatGPT to guide the implementation of logging connection attempts on a specified port in Linux, facilitating a practical understanding of the concept.