Top Networking Commands for Cybersecurity Analysts

```
$ nmap -sS 192.168.1.1
```

-> Performs a stealth TCP SYN scan on the target to identify open ports.

```
$ netstat -tulnp
```

-> Displays all listening TCP/UDP ports with their associated processes.

```
$ tcpdump -i eth0
```

-> Captures packets on the eth0 interface and shows real-time traffic.

```
$ wireshark &
```

-> Launches the Wireshark GUI for advanced packet capture and analysis.

```
$ iptables -L
```

-> Lists current iptables firewall rules for input, output, and forward chains.

```
$ ufw allow 22/tcp
```

-> Adds a UFW rule to allow incoming SSH connections on port 22.

```
$ lsof -i
```

-> Lists open files and their associated network connections.

```
$ nc -lvp 4444
```

-> Opens a TCP listener on port 4444 in verbose mode, used for testing and reverse shells.

```
$ curl http://example.com
```

-> Sends an HTTP GET request to the specified URL and prints the response.

```
$ wget http://example.com/file.txt
```

-> Downloads the specified file and saves it locally, showing progress.