🔥 IP Blocker Script (UFW)

Author: Daniel Chisasura

Version: 1.0

License: MIT

Platform: Linux (Debian/Ubuntu-based systems)

📄 Overview

This Bash script automates the process of blocking multiple malicious IP addresses using **UFW (Uncomplicated Firewall)**. It reads IPs from a file and applies deny rules to prevent incoming traffic from those sources. Ideal for system administrators and security professionals looking to quickly mitigate threats.

⚙️ Features

- ✅ Reads IP addresses from a file (`malicious_ips.txt` by default)
- 🚫 Skips empty lines and comments for clean input handling
- 🔒 Adds UFW rules to deny all incoming traffic from listed IPs
- 🔄 Reloads UFW to apply changes immediately
- 🔐 Checks for root privileges before execution

📦 Skills Demonstrated

- Linux firewall management with UFW
- Bash scripting for automation
- Input validation and error handling
- Security hardening techniques

🚀 Usage

1. **Install and Enable UFW**

```
sudo apt update

        sudo apt install ufw

        sudo ufw enable
```

2. **Prepare the IP List**

Create a file named `malicious_ips.txt` with one IP per line:

```
192.168.1.100
203.0.113.45
# This is a comment
```

3. **Save and Run the Script**

Save the script as `ip_blocker.sh` and make it executable:

🔧 Configuration

- **IP_LIST_FILE**: Path to the file containing IP addresses (default: `malicious_ips.txt`)
- Ensure the file exists and contains valid IPs only

📝 Sample Output

```
🔥 Starting IP blocking process...
Reading IPs from: malicious_ips.txt
-------------------------------------------------
Blocking IP: 192.168.1.100
Blocking IP: 203.0.113.45
-------------------------------------------------
✅ IP blocking script finished.UFW rules have been reloaded.
```

Lessons Learned

- **Root privileges are mandatory**: UFW commands require elevated permissions
- **Input validation prevents errors**: Skipping empty lines and comments avoids unnecessary failures
- **Reloading UFW is essential**: Changes don't take effect until the firewall is reloaded
- **Automation saves time**: Blocking multiple IPs manually is error-prone and slow
- **Logging is helpful**: Printing actions provides visibility and troubleshooting ease
- **Security hygiene**: Regularly review and update the IP list to avoid blocking legitimate traffic

Disclaimer

Use this script responsibly. Blocking IPs without proper verification may disrupt legitimate traffic. Always validate your IP list before applying firewall rules.