Echowall Honeypot System

EchoWall Honeypot System

Overview

EchoWall is a lightweight active-defense honeypot designed to detect and respond to potential intrusions via ICMP (ping) and SSH. It is optimized for Linux environments and sends real-time alerts to Telegram, logs attacker information, and blocks malicious IPs automatically.

Features

- Listens for ICMP echo requests (pings) and replies with customized warning messages
- Monitors TCP port 22 (SSH) and responds with a fake SSH banner
- Performs GeoIP lookup for every connection
- Sends alerts to Telegram with IP, location, and time
- Blocks IPs using iptables after detection
- Logs all activity locally

Components

1. ICMP Honeypot (Ping Trap)

- Uses Scapy to sniff for ICMP echo requests
- Sends custom echo replies with warning messages
- Logs IP, TTL, and number of pings
- Blocks repeated pingers
- Sends alert via Telegram

2. SSH Honeypot (TCP Trap)

- Uses Python sockets to simulate an SSH server
- Sends a fake banner on connection
- Logs the attacker's IP and GeoIP info
- Sends Telegram alert
- Blocks the IP using iptables

Configuration

Environment Requirements:

- Python 3.6+
- Linux OS (Debian, Kali, Ubuntu)
- iptables installed and active

Required Python Modules:

pip3 install scapy requests colorama

Telegram Setup

1. Create a bot via @BotFather
2. Get your BOT_TOKEN
3. Start a chat with the bot and use @userinfobot to get your CHAT_ID
4. Add both to the Python script

Running EchoWall

ICMP Trap

sudo python3 echowall_icmp.py

SSH Trap

sudo python3 fake_ssh_trap.py

Make sure no real SSH server is running (or switch to another port) if you're testing the fake SSH trap.

Unblocking an IP

List iptables rules:

sudo iptables -L INPUT -n --line-numbers

Delete a rule by number:

sudo iptables -D INPUT <rule_number>

Or delete by IP:

sudo iptables -D INPUT -s <ip_address> -j DROP

Log Files

- honey_icmp_log.txt – ICMP ping activity
- honey_tcp_log.txt – SSH connection attempts

The lesson I practiced

1. How ICMP Works
2. Private vs. Public IPs
3. TCP Socket Programming
4. Firewall Rules with iptables
5. GeoIP & Fingerprinting
6. Telegram Bot API Integration

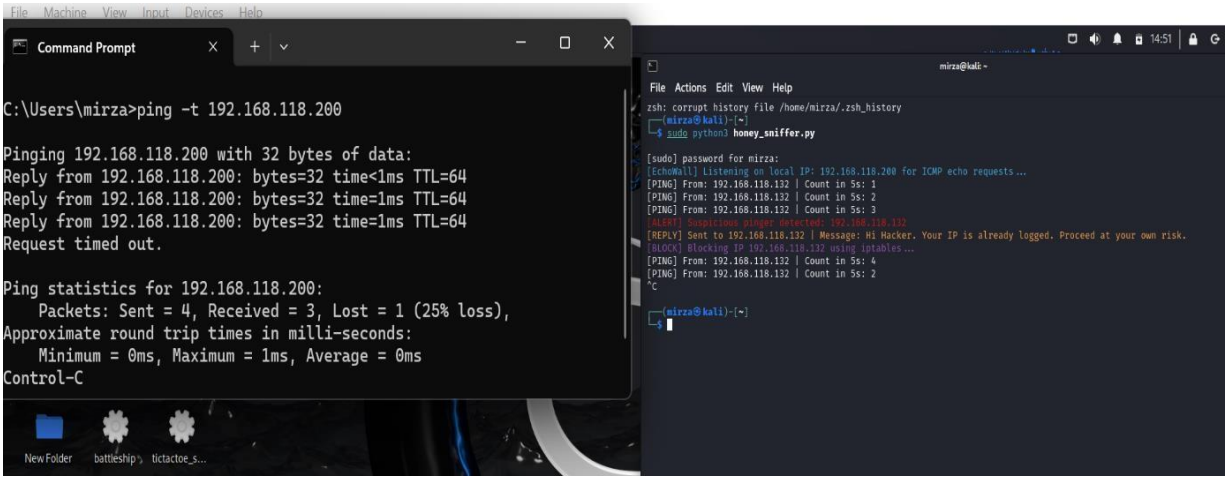
Author

Created by Mirza, 2025. EchoWall is part of a cybersecurity learning initiative and red-team/blue-team experimentation project.

Step-by step Explanation

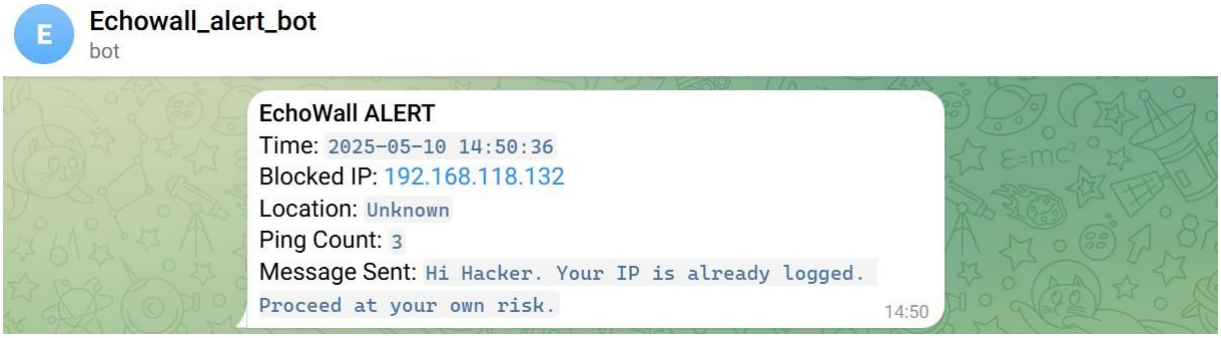
EchoWall (ICMP)

ICMP Trap Activation



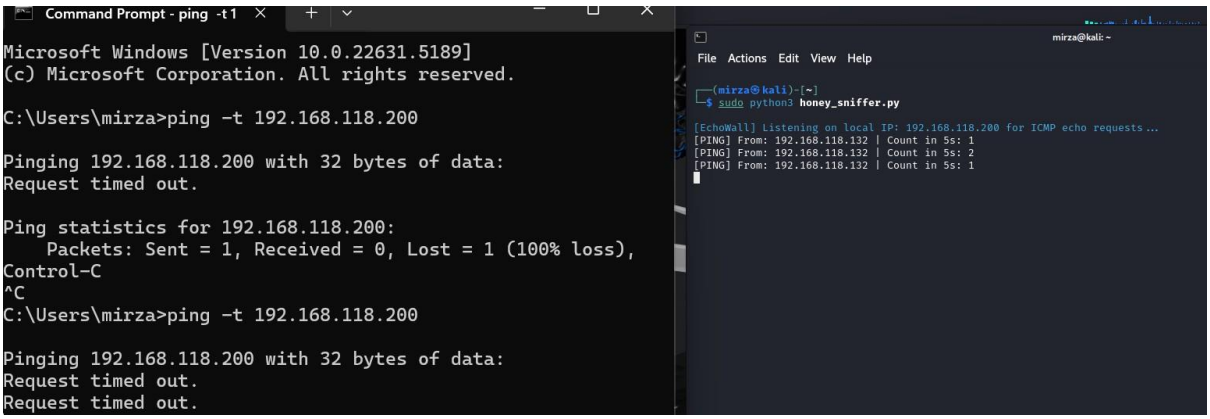
Here, you can see that I pinged my IP address. The honey_sniffer.py script was automatically activated, blocked the IP address, and sent the data to my Telegram bot.

Here’s our lovely alert message.



Let’s check one more time if the ip address blocked or not

iptables Block Confirmation



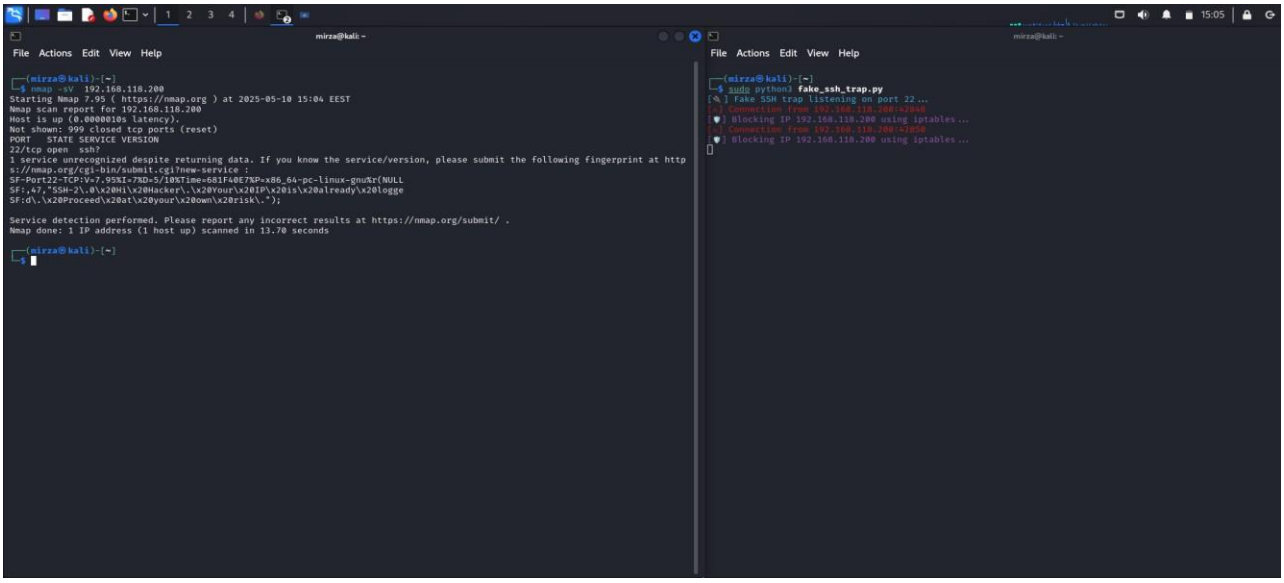
It is blocked, so any traffic from that IP address will no longer receive a response from our Kali machine. ✅

SSH Trap

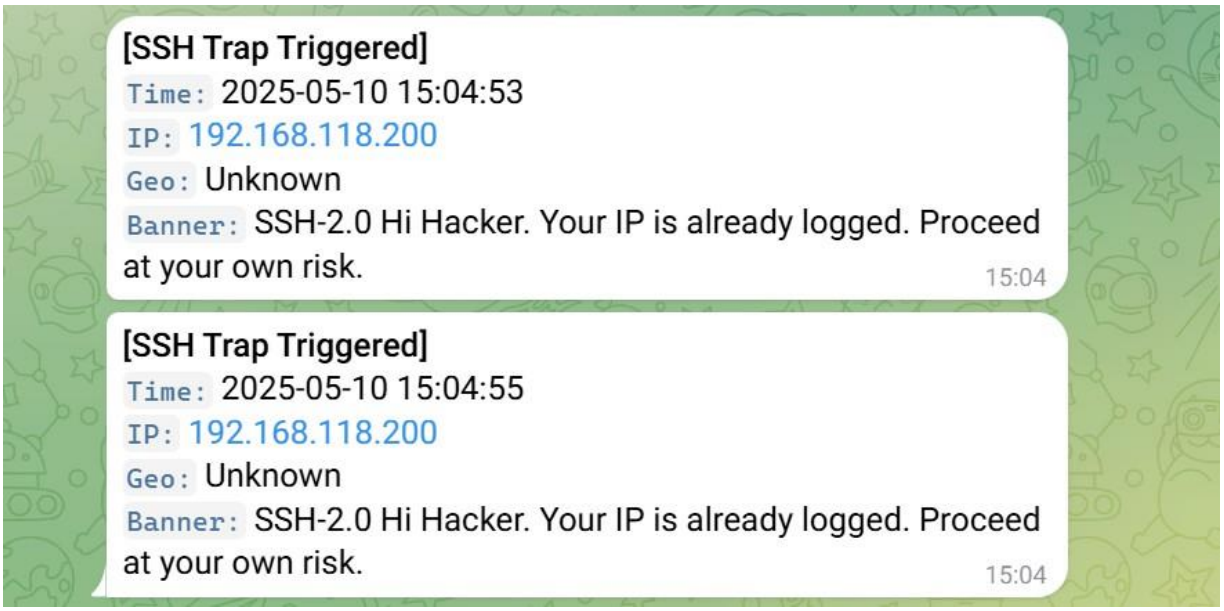
Here, I applied the same idea for Nmap users by opening a fake SSH port. If an attacker scans the system with Nmap, they'll fall into the trap.

Here you can see the message I sent to the attacker: *"Hi Hacker. Your IP is already logged. Proceed at your own risk."*

"SSH Trap Message + Telegram Alert"

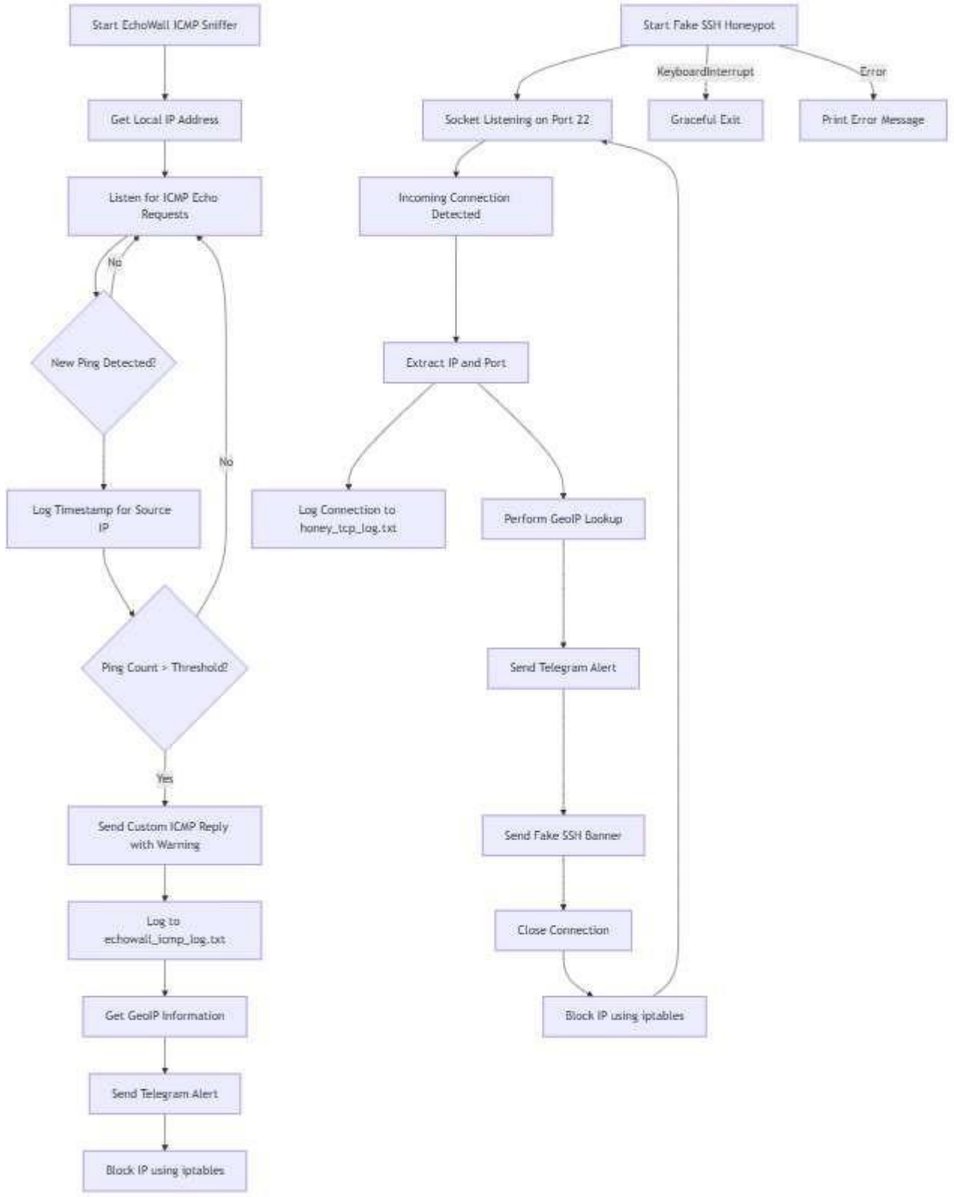


And here is the Telegram message i received.



Thank you for reading and for your support. I tried to be creative with this project, and I hope to develop and make even more innovative and exciting projects in the future.

Lastly, I am adding diagrams for better understanding


Start EchoWall ICMP Sniffer
Get Local IP Address
Listen for ICMP Echo Requests
No
New Ping Detected?
No
Log Timestamp for Source IP
Ping Count > Threshold?
Yes
Send Custom ICMP Reply with Warning
Log to echowall_icmp_log.txt
Get GeoIP Information
Send Telegram Alert
Block IP using iptables
Start Fake SSH Honeypot
KeyboardInterrupt
Error
Socket Listening on Port 22
Graceful Exit
Print Error Message
Incoming Connection Detected
Extract IP and Port
Log Connection to honey_tcp_log.txt
Perform GeoIP Lookup
Send Telegram Alert
Send Fake SSH Banner
Close Connection
Block IP using iptables