

Hi Hacker.  
Your IP is already  
logged Proceed  
at your own risk.



# Echowall Honeytrap 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

---

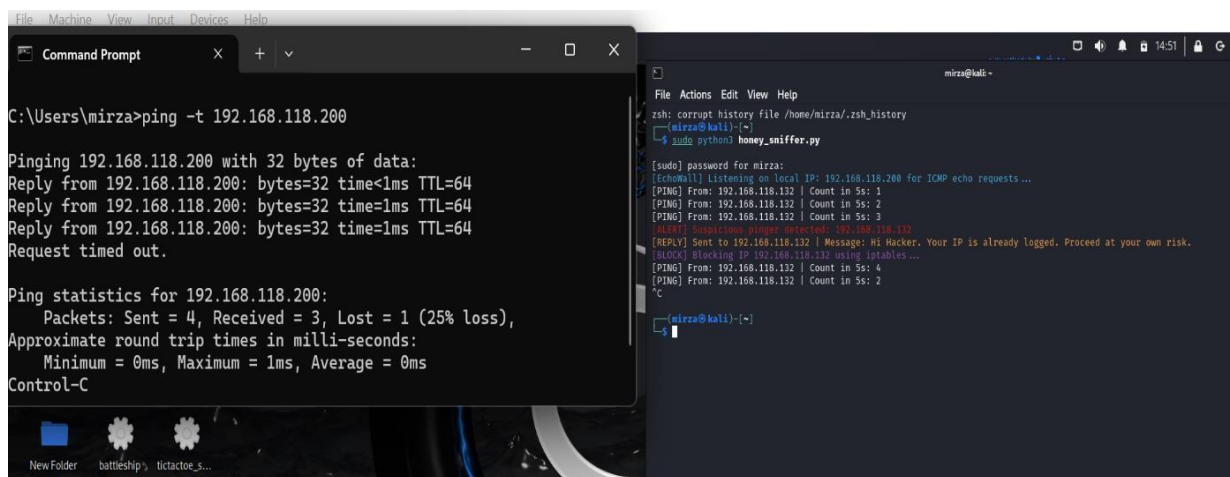
## Author

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



The screenshot shows two windows side-by-side. The left window is a Windows Command Prompt with the following text:

```
C:\Users\mirza>ping -t 192.168.118.200

Pinging 192.168.118.200 with 32 bytes of data:
Reply from 192.168.118.200: bytes=32 time<1ms TTL=64
Reply from 192.168.118.200: bytes=32 time=1ms TTL=64
Reply from 192.168.118.200: bytes=32 time=1ms TTL=64
Request timed out.

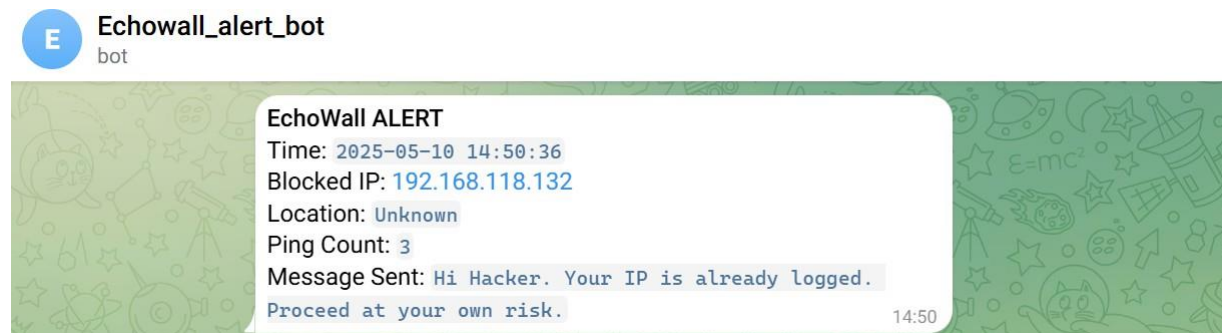
Ping statistics for 192.168.118.200:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
```

The right window is a terminal window with the following text:

```
mirza@kali:~$ python3 honey_sniffer.py
[sudo] password for mirza:
[EchoWall] Listening on local IP: 192.168.118.200 for ICMP echo requests...
[PING] From: 192.168.118.132 | Count in 5s: 1
[PING] From: 192.168.118.132 | Count in 5s: 2
[PING] From: 192.168.118.132 | Count in 5s: 3
[ALERT] Suspicious ping detected: 192.168.118.132
[REPLY] Sent to 192.168.118.132 | Message: Hi Hacker. Your IP is already logged. Proceed at your own risk.
[Block] Blocking IP 192.168.118.132 using iptables...
[PING] From: 192.168.118.132 | Count in 5s: 4
[PING] From: 192.168.118.132 | Count in 5s: 2
```

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*

A screenshot showing two terminal windows side-by-side. The left window is a Windows Command Prompt titled 'Command Prompt - ping -t 1'. It shows the command 'ping -t 192.168.118.200' being executed. The output indicates that the ping request timed out and that 100% of packets were lost. The right window is a Kali Linux terminal titled 'mirza@kali: ~'. It shows the command 'sudo python3 honey\_sniffer.py' being executed. The output of the script shows it is listening on local IP 192.168.118.200 and receiving ping requests from 192.168.118.132.

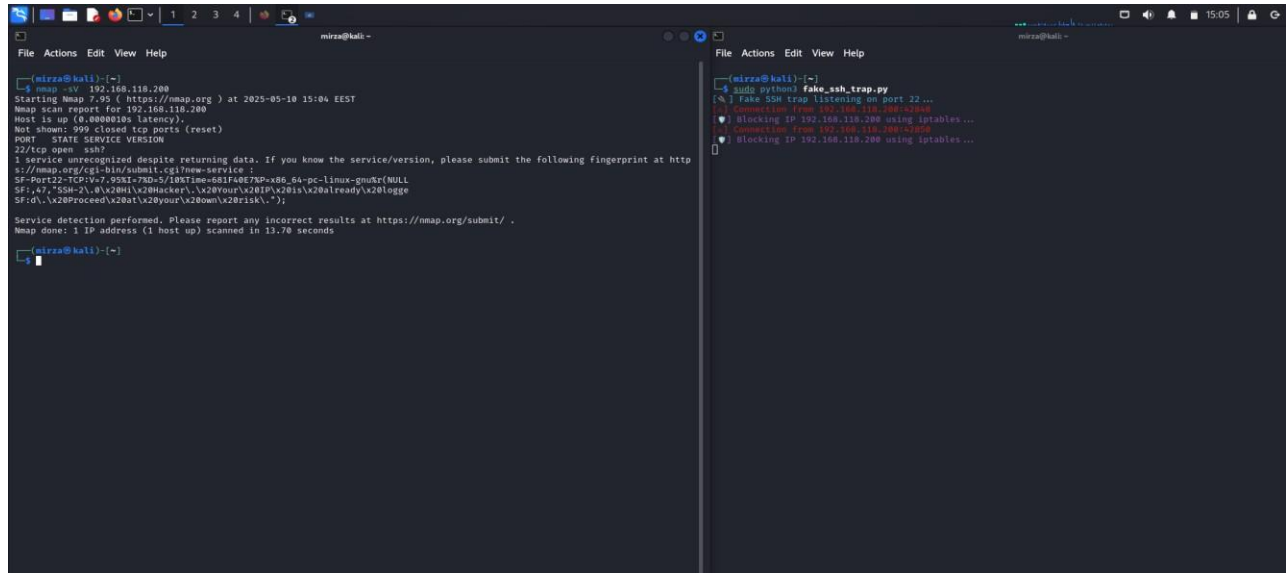
It is blocked, so any traffic from that IP address will no longer receive a response from our Kali machine. ✓

## 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."*

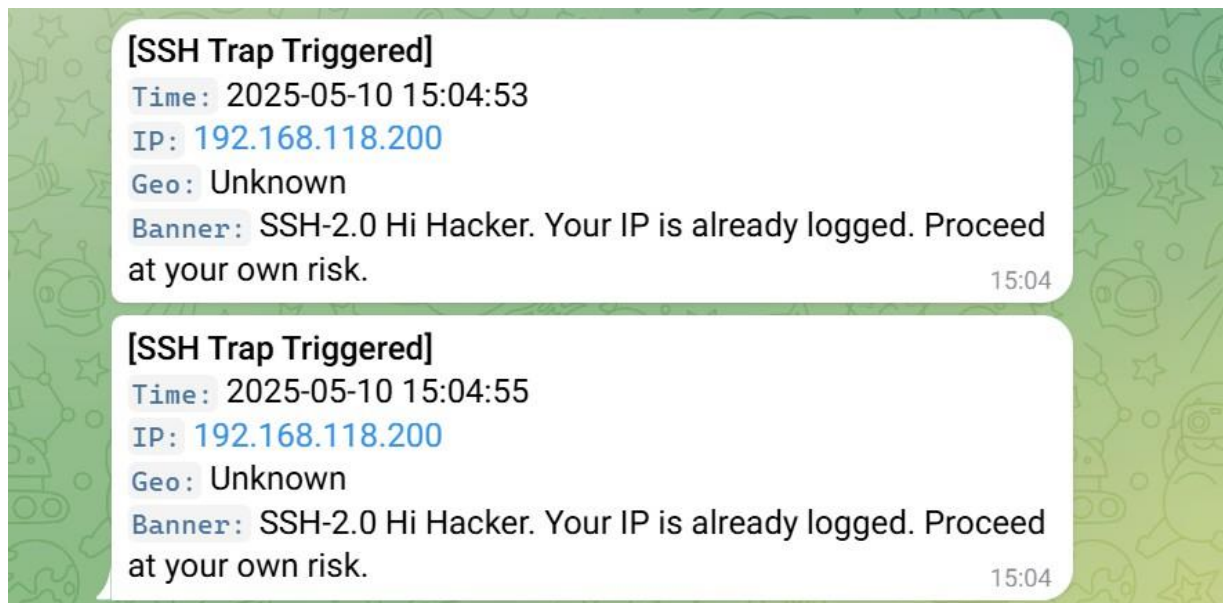
*"SSH Trap Message + Telegram Alert"*



The image shows two terminal windows. The left window displays the output of an Nmap scan for IP 192.168.118.200. It shows that port 22 is open and the service is SSH. The right window shows a Python script named 'fake\_ssh\_trap.py' which is designed to listen on port 22, detect an Nmap scan, and send a message to the attacker.

```
(mirza@kali) ~  
$ nmap -sV 192.168.118.200  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 15:04: EEST  
Nmap scan report for 192.168.118.200  
Host is up (0.000000ms latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF:Port22-TCP:V=7.95I=702S=100Time=68140873P=>x86_64-pc-linux-gnuTr(MULL  
SF: 47,"SSH-2.0_@x20Hi(x20Hacker)\x20Your\x20IP\x20is\x20already\x20logge  
SF:d.\x20Proceed\x20at\x20your\x20own\x20risk\x20").  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 13.70 seconds  
(mirza@kali) ~  
(mirza@kali) ~  
$ sudo python3 fake_ssh_trap.py  
[N] fake SSH trap listening on port 22 ...  
[I] Connection from 192.168.118.200:42004  
[I] Blocking IP 192.168.118.200 using iptables ...  
[I] Connection from 192.168.118.200:42004  
[I] Blocking IP 192.168.118.200 using iptables ...
```

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

