Firewall Configuration & Analysis Guide

For Ethical Hackers

Why This Matters

Firewalls are everywhere. Every network you test has them. Understanding how to configure and bypass them is essential for ethical hackers.

UFW Essential Commands

Basic Setup

```
sudo apt install ufw
sudo ufw enable
sudo ufw status verbose
sudo ufw --force reset          # Reset all rules
```

Allow/Deny Rules

```
# Allow specific ports
sudo ufw allow 22               # SSH
sudo ufw allow 80               # HTTP
sudo ufw allow 443              # HTTPS

# Allow from specific IP
sudo ufw allow from 192.168.1.100

# Allow IP to specific port
sudo ufw allow from 192.168.1.100 to any port 22

# Block traffic
sudo ufw deny 23                # Block Telnet
sudo ufw deny from 192.168.1.50 # Block IP

# Remove rules
sudo ufw delete allow 80
sudo ufw delete 3               # Delete rule number 3
```

Advanced Rules

```
sudo ufw limit ssh                  # Rate limiting (anti-brute force)
sudo ufw allow 1000:2000/tcp        # Port ranges
sudo ufw default deny incoming      # Default policies
sudo ufw default allow outgoing
```

Log Analysis

UFW Logs

```
# View live logs
sudo tail -f /var/log/ufw.log

# Find blocked attempts
sudo grep "BLOCK" /var/log/ufw.log

# Count blocks by IP
sudo grep "BLOCK" /var/log/ufw.log | awk '{print $12}' | sort | uniq -c | sort -nr
```

Reading Log Entries

```
[UFW BLOCK] SRC=192.168.1.100 DST=192.168.1.1 PROTO=TCP DPT=22

SRC = Source IP (attacker)
DST = Destination IP (target)
DPT = Destination Port (what they wanted)
```

Testing Firewalls

From External Host

```
nmap -sS target-ip              # TCP scan
nmap -sU target-ip              # UDP scan
nc -zv target-ip 22             # Test specific port
```

Local Testing

```
sudo ufw status numbered        # Check rules
```

```
sudo netstat -tlnp              # Check listening ports
sudo ss -tuln                   # Alternative to netstat
```

Common Scenarios

Web Server

```
sudo ufw --force reset
sudo ufw default deny incoming
sudo ufw allow 22
sudo ufw allow 80
sudo ufw allow 443
sudo ufw limit ssh
sudo ufw enable
```

Database Server (restricted access)

```
sudo ufw --force reset
sudo ufw allow from 192.168.1.0/24 to any port 3306
sudo ufw allow 22
sudo ufw limit ssh
sudo ufw enable
```

Emergency Block

```
sudo ufw deny from 203.0.113.100    # Block attacker immediately
sudo tail -f /var/log/ufw.log | grep BLOCK  # Monitor attacks
```

Troubleshooting

Service Won't Connect

```
sudo systemctl status ssh       # Check service
sudo ufw status verbose         # Check firewall
sudo netstat -tlnp | grep :22   # Check if listening
nc -zv localhost 22             # Test locally
```

Rules Not Working

```
sudo ufw status numbered          # Check rule order
sudo ufw --force reset            # Reset if needed
```

Quick Reference

Enable/Disable:

- `sudo ufw enable` - Turn on firewall
- `sudo ufw disable` - Turn off firewall
- `sudo ufw status verbose` - Check current rules

Common Rules:

- `sudo ufw allow 22` - Allow SSH
- `sudo ufw deny from IP` - Block IP
- `sudo ufw limit ssh` - Rate limit SSH
- `sudo ufw delete allow 80` - Remove rule

Monitoring:

- `sudo tail -f /var/log/ufw.log` - Watch logs
- `nmap target-ip` - Test from outside
- `sudo netstat -tlnp` - Check listening ports