Dionaea Honeypot
Complete Installation & Testing Guide

Prepared for: Red Team Lab / Threat Intelligence Testing

This document provides a fully validated step-by-step guide to install, configure, troubleshoot, and test Dionaea honeypot with all modules enabled.

1. Installation & Setup

```
1. Update system and install dependencies:

    sudo apt update && sudo apt upgrade -y
    sudo apt install -y git build-essential cmake libcurl4-openssl-dev
libglib2.0-dev libpcap-dev libnl-3-dev libnl-genl-3-dev python3 python3-dev
python3-pip libssl-dev libtool autoconf automake libudns-dev libev-dev libemu-dev
sqlite3 libsqlite3-dev libreadline-dev libtool-bin cython3 python3-setuptools
python3-wheel

2. Clone Dionaea source code:

    cd /opt
    sudo git clone --recursive https://github.com/DinoTools/dionaea.git
    cd dionaea

3. Compile Dionaea:

    mkdir build && cd build
    cmake ..
    make -j$(nproc)
    sudo make install

4. Resolve Python module error:

    - Find compiled core.so:
     find /opt/dionaea/build -name "core*.so"
    - Create folder & move core.so:
     sudo mkdir -p
/opt/dionaea/build/modules/python/build/lib.linux-x86_64-cpython-312/dionaea
     sudo mv
/opt/dionaea/build/modules/python/build/lib.linux-x86_64-cpython-312/dionaea/
     sudo touch /opt/dionaea/build/modules/python/build/lib.linux-x86_64-cpython-312
/dionaea/__init__.py

5. Copy default configuration:

    sudo cp /opt/dionaea/etc/dionaea/dionaea.cfg.dist
/opt/dionaea/etc/dionaea/dionaea.cfg

6. Start Dionaea:

    sudo
PYTHONPATH=/opt/dionaea/build/modules/python/build/lib.linux-x86_64-cpython-312
/opt/dionaea/bin/dionaea -c /opt/dionaea/etc/dionaea/dionaea.cfg -D
```

2. Module Testing Checklist

No.	Module	Service/Protocol	Test Command	Status
1	p0f	Passive OS Detection	nmap -sS <IP>	
2	ftp	FTP (21/tcp)	ftp <IP>	
3	tftp	TFTP (69/udp)	tftp <IP> get file	
4	http	HTTP (80/tcp)	curl http://<IP>	
5	smb	SMB (445/tcp)	smbclient -L //<IP>	
6	mssql	MSSQL (1433/tcp)	nmap -p 1433 --script ms-sql* <IP>	
7	mysql	MySQL (3306/tcp)	mysql -h <IP> -u root -p	
8	echo	Echo (7/tcp)	telnet <IP> 7	
9	sip	SIP (5060/udp)	sipvicious -i <IP> -m REGISTER	
10	upnp	UPnP (1900/udp)	gssdp-discover -i eth0	
11	shellcode	Shellcode emulation	nc <IP> 21 < shellcode.bin	
12	logsql/pcap	Logging & Packet Capture	Check /opt/dionaea/var/dionaea/	

3. Monitoring & Operations

```
3. Monitoring and Log Paths

- Real-time process check:
    ps aux | grep dionaea | grep -v grep

- Check listening ports:
    sudo lsof -i -n -P | grep dionaea

- View logs:
    tail -f /opt/dionaea/var/dionaea/dionaea.log

- Malware sample storage:
    /opt/dionaea/var/dionaea/binaries/

4. Notes:

- Do NOT run Dionaea as root in production. Always create an unprivileged user.
- Test in isolated VM or container environment.
- Combine Dionaea logs with ELK / Wazuh for advanced threat intelligence workflows.
```