

Prerequisiti Sistema

```
# Su Ubuntu/Debian
sudo apt update
sudo apt install python3 python3-pip python3-tk

# Su CentOS/RHEL
sudo yum install python3 python3-pip tkinter

# Su Arch Linux
sudo pacman -S python python-pip tk
```

Installazione Dipendenze Python

```
# Installa le librerie necessarie
pip3 install scapy netifaces

# Alternative con virtual environment (raccomandato)
python3 -m venv venv_rete
source venv_rete/bin/activate # Linux/macOS
# venv_rete\Scripts\activate   # Windows
pip install scapy netifaces
```

Preparazione File

1. Salva il codice in un file chiamato `scoperta_rete.py`
2. Rendi il file eseguibile: `chmod +x scoperta_rete.py`

Esecuzione

```
# Su Linux (richiede privilegi root per cattura pacchetti)
sudo python3 scoperta_rete.py

# Su Windows (esegui come Amministratore)
python scoperta_rete.py
```

Risoluzione Problemi Comuni

Errore "Permission denied":

- Linux: Usa `sudo` per privilegi di cattura pacchetti
- Windows: Esegui il prompt come

Risoluzione Problemi Comuni (continuazione)

Errore "Permission denied":

- Linux: Usa `sudo` per privilegi di cattura pacchetti
- Windows: Esegui il prompt come Amministratore

Errore "No module named 'netifaces'":

```
# Installa manualmente  
pip3 install netifaces --user
```

Errore "Sniffing failed":

- Verifica che l'interfaccia selezionata sia attiva
- Su Windows: installa Npcap (<https://npcap.com/>)
- Su Linux: verifica che libpcap sia installato: `sudo apt install libpcap-dev`

Interfacce non visibili:

```
# Verifica interfacce disponibili  
ip link show # Linux  
ipconfig     # Windows
```

Funzionalità del Software

Scheda "Scoperta Rete":

- Auto-rileva il range di rete della tua interfaccia
- Esegue scansione ARP per trovare dispositivi attivi
- Mostra IP, MAC, hostname e vendor di ogni dispositivo


Scheda "Monitor Comunicazioni":

- Cattura traffico di rete in tempo reale
- Mostra matrice comunicazioni (chi parla con chi)
- Conta pacchetti per ogni comunicazione

Scheda "Analisi Pacchetti":

- Analisi dettagliata dei pacchetti catturati
- Selezione per tipo di comunicazione
- Visualizzazione timestamp e payload summary

Note di Sicurezza

 **Importante:** Utilizza questo strumento solo su reti di tua proprietà o con esplicita autorizzazione. L'uso non autorizzato costituisce violazione della privacy e può essere illegale.

Utilizzi Legittimi:

- Amministrazione della propria rete domestica/aziendale
- Security assessment autorizzati
- Troubleshooting di rete
- Formazione in ambiente lab controllato

Estensioni Possibili

Il codice è strutturato per permettere facilmente:

- Integrazione con database OUI completo per vendor identification
- Export dei risultati in CSV/JSON
- Integrazione con threat intelligence feeds
- Alerting automatico per comunicazioni sospette
- Geolocalizzazione IP esterni
- Analisi protocolli specifici (HTTP, DNS, etc.)

Questo strumento fornisce una base solida per l'apprendimento delle tecniche di network discovery e packet analysis, elementi fondamentali della cybersecurity operativa.