



# MANUALE DI INSTALLAZIONE

**NetGun**

<b>Versione</b>	0.2
<b>Data</b>	15/02/2023
<b>Destinatario</b>	Professore Carmine Gravino
<b>Presentato da</b>	Carlo Colizzi, Giulio Incoronato, Antonio Mazzearella

## Revision History

---

Data	Versione	Descrizione	Autori
10/02/2023	0.1	Stesura del Manuale di installazione	Tutto il gruppo
15/02/2023	0.2	Revisione Totale	Tutto il gruppo

## Team Members

---

Nome	Informazioni di contatto
Carlo Colizzi	c.colizzi@studenti.unisa.it
Giulio Incoronato	g.incoronato2@studenti.unisa.it
Antonio Mazzearella	a.mazzearella5@studenti.unisa.it

## Sommario

<b>1 Introduzione</b>	<b>2</b>
1.1 Scopo del Sistema	2
1.2 Scopo del documento	3
1.3 Relazione con altri documenti	3
<b>2 Prerequisiti per l'installazione</b>	<b>3</b>
<b>2.1 Open Source Program</b>	<b>4</b>
2.2 Database	4
<b>3 Installazione</b>	<b>4</b>

# 1 Introduzione

---

## 1.1 Scopo del Sistema

NetGun ha l'obiettivo di essere un tool per il Penetration Testing (Testing Black Box di infrastrutture in rete).

È possibile racchiudere il sistema in 3 componenti principali. La componente per lo scanning, la componente per l'enumerazione dei dati raccolti, e le utilities che assistono l'utente in tutte le fasi del pre e post scanning.

Inoltre ha l'obiettivo di facilitare una pratica complessa come i Penetration Test, così da permettere ai Penetration Tester di concentrarsi su aspetti più delicati, automatizzando e velocizzando le task alla base di questo tipo di Testing.

## 1.2 Scopo del documento

Lo scopo di questo documento è quello di mostrare i passaggi necessari alla corretta installazione del sistema.

## 1.3 Relazione con altri documenti

Di seguito l'elenco di tutti i documenti in relazione con il manuale:

- [Requirements Analysis Document \(RAD\)](#)
- [System Design Document \(SDD\)](#)
- [Object Design Document \(ODD\)](#)
- [Test Plan \(TP\)](#)
- [Test Case Specification \(TCS\)](#)
- [Codice Sorgente](#)
- [Matrice di tracciabilità](#)

## 2 Prerequisiti per l'installazione

---

Per l'installazione del sistema è necessario avere un sistema Linux, in particolare un debian-based come:

- Ubuntu
- Kali linux
- Parrot OS
- Linux Mint

Si raccomanda tra tutti Kali Linux, sistema sul quale è stato maggiormente testato, poiché presenta di default il software **Nmap**.

Se si tratta di un sistema diverso da Kali si raccomanda l'installazione di **Nmap**.

Fondamentale per l'installazione è avere sulla macchina un interprete **Python3**.

### 2.1 Open Source Program

NetGun è un software applicativo per sistemi linux, che si pone come utility durante le analisi di rete ed infrastrutture informatiche. Utilizza come linguaggio **Python** per semplificare la comprensione e la modifica del codice, ricercando così il contributo della community open source.

### 2.2 Persistenza

Il software utilizza file **XML** per lo storage e file di configurazione **.ini** per consentire agli utenti una facile personalizzazione del software. Inoltre utilizza una tecnica di passivazione ed attivazione dei dati in memoria di massa, pensata per migliorare i tempi di avvio del software.

## 3 Installazione

---

Per la seguente guida all'installazione verrà considerato esclusivamente il sistema operativo Kali Linux.

1. Prima di tutto è necessario **scaricare** il file **.deb** disponibile al seguente link Github: [NetGun<release\\_number>.deb](#)

2. Entrare da terminale nella cartella **Downloads**
3. Procedere con il comando:  
`sudo apt install ./NetGun<release_number>.deb`
4. Scrivere dal terminale NetGun, e si avvierà il programma.

Tutte le **dipendenze**, le **API** necessarie, le **variabili di ambiente**, i file di **persistenza** saranno gestiti automaticamente durante l'installazione.

## 4 Glossario

---

**.deb:** è il formato, nonché estensione, dei pacchetti utilizzati dalla distribuzione Debian e dalle sue derivate.

**XML:** (Extensible Markup Language) si intende il linguaggio di markup che fornisce regole per definire qualsiasi dato.

**Nmap:** è un software libero rilasciato sotto licenza GNU GPL ed è stato sviluppato proprio per avviare attività di port scanning, sia in locale che in remoto.

**API:** acronimo di Application Programming Interface (interfaccia di programmazione delle applicazioni), indica un insieme di definizioni e protocolli per la creazione e l'integrazione di applicazioni software.

**Python:** Python è un linguaggio di programmazione ampiamente utilizzato nelle applicazioni Web, nello sviluppo di software, nella data science e nel machine learning (ML). Gli sviluppatori utilizzano Python perché è efficiente e facile da imparare e può essere eseguito su diverse piattaforme.

**Testing Black Box:** Il black-box testing è una metodologia di test che presuppone un punto di vista esterno rispetto al codice testato. In altre parole non viene presa in considerazione alcuna informazione/conoscenza rispetto al funzionamento interno dell'applicazione.