MONIN
Database Managed Services

# MONIN'S DB. INSPECTOR

Handleiding

Jonas Willems - Jonas.Willems@monin-it.be

T 03/450 67 89
E info@monin-it.be
W www.monin-it.be
BE 0879.917.484

MONIN nv.
Prins Boudewijnlaan 41
2650 Edegem

MONIN

# INHOUD

# 1 INLEIDING

## 1.1 Monin's DB. Inspector

### 1.1.1 INTRODUCTIE

Monin's DB. Inspector is een Python-script dat specifiek is ontworpen voor het efficiënt identificeren en beoordelen van databases binnen een netwerkomgeving. Met deze tool kun je niet alleen de achterliggende database services en versies detecteren, maar biedt het ook de mogelijkheid om beveiligingstests uit te voeren op diverse protocollen, zoals SSH en FTP. De beveiligingstests worden uitgevoerd met behulp van de bekende tool thc-hydra en een eigen wordlist, waarmee het script probeert toegang te verkrijgen tot de beveiligde services door verschillende combinaties van gebruikersnamen en wachtwoorden te testen. Bovendien maakt Monin's DB. Inspector gebruik van Nmap om uitgebreide informatie over hosts en services binnen het netwerk te verzamelen, waardoor het een allesomvattende tool is voor database-identificatie en beveiligingsbeoordelingen.

# 2 TECHNISCHE INFORMATIE

## 2.1 Programmeertaal

Monin's DB. Inspector is ontwikkeld in Python3, een veelgebruikte programmeertaal in het domein van netwerkbeveiliging en systeembeheer. Python staat bekend om zijn eenvoudige syntax, uitgebreide bibliotheekondersteuning en brede inzetbaarheid in diverse toepassingen.

## 2.2 Gebruikte Bibliotheken

### 2.2.1 OS:

De os-module communiceert met het besturingssysteem en beheert taken zoals bestandsbeheer en commando-uitvoering. Het wordt gebruikt voor mapcreatie en algemene interacties met het besturingssysteem.

### 2.2.2 JSON:

json wordt gebruikt voor het lezen en schrijven van JSON-geformatteerde bestanden. Hiermee slaat het script scanresultaten op en laadt het bestaande scans in.

### 2.2.3 TQDM:

tqdm biedt een visuele voortgangsbalk voor langlopende taken zoals het scannen van hosts. Deze functie verbetert de gebruikerservaring door de voortgang van taken duidelijk weer te geven.

### 2.2.4 PING3:

ping3 maakt het mogelijk om ping-opdrachten uit te voeren in het script. Het wordt gebruikt om de bereikbaarheid van systemen binnen het netwerk te controleren en actieve hosts te identificeren.

### 2.2.5 DATETIME:

De datetime-bibliotheek wordt gebruikt voor het vastleggen van tijdstempels. Dit is essentieel voor het genereren van timestamps in het script.

### 2.2.6 IPADDRESS:

De ipaddress-module valideert en manipuleert IP-adressen. Het draagt bij aan de nauwkeurigheid en betrouwbaarheid van het script bij het verwerken van verschillende IP-adresformaten.

### 2.2.7 SUBPROCESS:

De subprocess-module start en beheert externe processen, zoals het aanroepen van thc-hydra voor beveiligingstests. In het script wordt subprocess gebruikt om externe commando's uit te voeren en de uitvoer ervan vast te leggen.

#### 2.2.8 NMAPTHON2:

nmapthon2 fungeert als een wrapper voor de Nmap-tool. Het vereenvoudigt het gebruik van Nmap in het script voor gedetailleerde netwerkanalyses en het identificeren van services op hosts.

### 2.3 Integratie van Externe Tools

#### 2.3.1 THC-HYDRA:

thc-hydra is een geavanceerde tool voor wachtwoordkraken. In het script wordt thc-hydra gebruikt voor het identificeren van zwakke wachtwoorden bij beveiligingstests. Het wordt opgeroepen met behulp van de subprocess-module om aanvallen uit te voeren op services zoals SSH en FTP.

#### 2.3.2 NMAP:

Nmap is een krachtige netwerkscanner die wordt ingezet voor het ontdekken van hosts en services binnen een netwerk. In dit script maakt de toepassing gebruik van Nmap via de nmapthon2-module als een wrapper om uitgebreide informatie over het netwerk te verzamelen. Nmap speelt een cruciale rol bij het identificeren van open poorten en services, inclusief hun versies

### 2.4 Bestandsstructuur

Het project heeft de volgende bestandsstructuur:

- Monin.py: Het kernscript van Monin's DB. Inspector.
- Wordlist/: Bevat lijsten met wachtwoorden voor beveiligingstests.
- Scans/: Map waarin scanresultaten worden opgeslagen.
- requirements.txt: Lijst van vereiste Python-bibliotheken voor het script.

# 3 WERKING

Monin's DB. Inspector biedt een gestructureerde workflow, waarbij elke stap ontworpen is om gebruikers in staat te stellen nauwkeurige database-informatie te verkrijgen en beveiligingsbeoordelingen uit te voeren. Hier volgt een beschrijving van hoe het script werkt.

## 3.1 Nieuwe Scan Aanmaken of Laden

Bij het starten van het script wordt de gebruiker begroet met het hoofdmenu. Hier heeft de gebruiker de keuze om een nieuwe scan aan te maken of een bestaande scan te laden. Wanneer een nieuwe scan wordt aangemaakt, wordt de gebruiker gevraagd een naam op te geven, die als identificatie voor de scan zal dienen.

Na het opgeven van een scannaam verschijnt het scanmenu met de volgende opties: "1. Zoek Database Systemen" en "2. Security Beoordelingen".

## 3.2 Nieuwe Scan: Zoek Database Systemen

De gebruiker selecteert "1. Zoek Database Systemen" om het proces van database-detectie te starten. Hier wordt de gebruiker gevraagd hoe ze het IP, IP-bereik of netwerk willen invoeren. Na het verstrekken van deze informatie, start het script automatisch de zoekopdracht naar databases op de gedetecteerde actieve hosts.

Het script maakt gebruik van ping3 om actieve hosts te detecteren en Nmap via de nmapthon2-module om databases op deze hosts te identificeren. Alle resultaten worden automatisch opgeslagen in een JSON-bestand met de opgegeven scannaam in de "Scans/"-map.

## 3.3 Security Beoordelingen

Na succesvolle database-detectie biedt het menu de optie "2. Security Beoordelingen". Hier kan de gebruiker beveiligingstests uitvoeren op specifieke services, zoals SSH en FTP, om zwakke wachtwoorden te identificeren. Bij het selecteren van deze optie krijgt de gebruiker een lijst met hosts uit de opgeslagen scans. Door een host te selecteren, kan de gebruiker beveiligingstests uitvoeren op de gekozen host, waardoor een holistische benadering van netwerkbeveiliging mogelijk is.

Dit uitgebreide proces biedt niet alleen een effectieve methode om databases te detecteren, maar integreert ook beveiligingstests om kwetsbaarheden bloot te leggen. Monin's DB. Inspector is ontworpen om een allesomvattende en gebruiksvriendelijke ervaring te bieden voor het identificeren en beoordelen van databases binnen netwerkomgevingen.

# 4 INSTALLATIE

## 4.1 Vereisten:

Besturingssysteem: Kali Linux 2023.4.

Software:

- Python3
- Nmap
- thc-hydra

## 4.2 Installatiestappen:

### 4.2.1 UPDATE HET SYSTEEM EN INSTALLEER VEREISTEN:

```
sudo apt update && sudo apt upgrade -y && sudo apt install python3 nmap
hydra -y
```

### 4.2.2 CLONE DE REPOSITORY EN NAVIGEER NAAR DE MAP:

```
git clone https://github.com/Sm3ll1w/Monin-s-DB.-Inspector.git
cd Monin-s-DB.-Inspector/
```

### 4.2.3 INSTALLEER VEREISTE BIBLIOTHEKEN:

```
pip install -r requirements.txt
```

# 5 GEBRUIK

Hier is een stapsgewijze handleiding om gebruikers door het Monin's DB. Inspector-script te leiden, zodat ze moeiteloos databases kunnen detecteren en beveiligingsbeoordelingen kunnen uitvoeren.

## 5.1 Stap 1: Start het Script

- Open een terminalvenster op je Kali Linux systeem.
- Navigeer naar de map waarin Monin's DB. Inspector is gekloond:
- Start het script

```
cd pad/naar/Monin-s-DB.-Inspector/
python Monin.py
```

## 5.2 Stap 2: Nieuwe Scan Aanmaken of Laden

- Optie 1: Maak een nieuwe scan aan
  Voer een unieke scannaam in en druk op Enter.
- Optie 2: Laad een bestaande scan

  Selecteer een eerder aangemaakte scan.

## 5.3 Stap 3: Zoek Database Systemen

- Kies in het hoofdmenu "1" om naar de zoekdatabase-opties te gaan.
- Selecteer de methode om IP's in te voeren:
- "1" voor CIDR-notatie (bijv. 192.168.1.0/24).
- "2" voor een lijst met IP-adressen. (Gescheiden door een komma “,”)
- "3" voor een IP-bereik met een streepje (bijv. 192.168.1.1-192.168.1.10).
- "4" voor een enkel IPv4-adres. ()
- Voer de benodigde IP-informatie in volgens de gekozen methode.

Het script initieert automatisch een zoekopdracht naar actieve hosts door middel van ping-requests en identificeert vervolgens databases met behulp van Nmap. Alle gedetecteerde resultaten worden nauwkeurig vastgelegd en opgeslagen in een JSON-bestand voor latere raadpleging.

## 5.4 Security Beoordelingen

- Navigeer naar Security Beoordelingen:
  Kies in het hoofdmenu "2" om naar het submenu voor security-beoordelingen te gaan.
  Het script laadt automatisch de opgeslagen scanresultaten en toont een lijst met de gevonden databasesystemen.

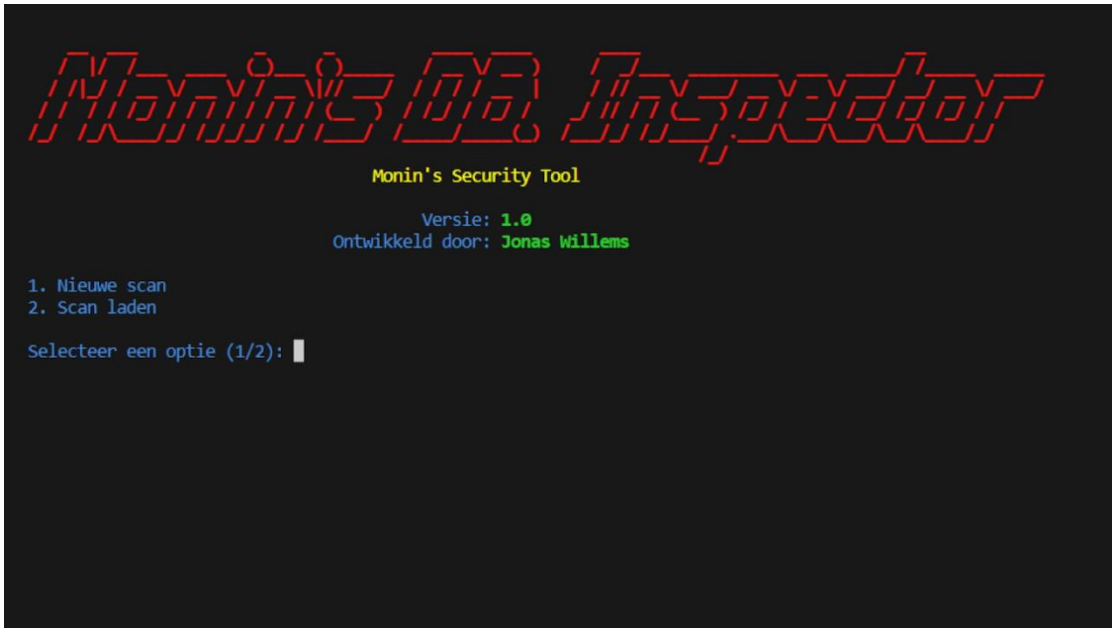
- Selecteer een Host:
  Voer het ID in van de host waarop je beveiligingstests wilt uitvoeren.
  Het script geeft gedetailleerde informatie weer over de geselecteerde host.
  Zoals bijvoorbeeld de aanwezige services.

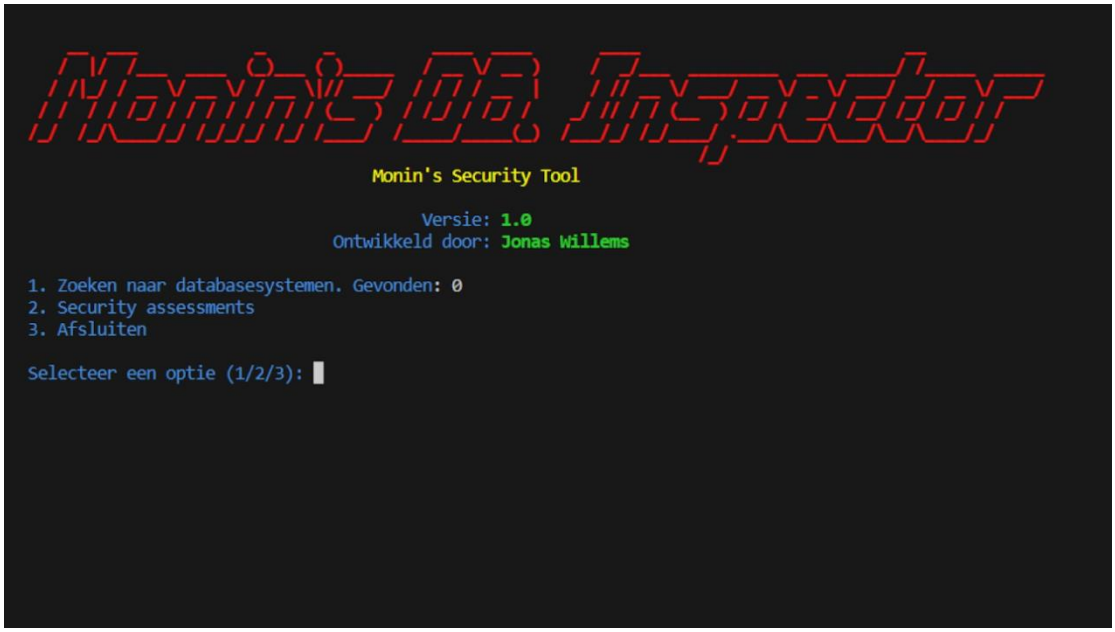
- Kies het Type Beveiligingstest:
  Het script biedt opties om beveiligingstests uit te voeren op specifieke services zoals SSH en FTP.
  Selecteer het gewenste testtype op basis van de services die op de host draaien.

- Invoeren van Testparameters:
  Volg de instructies om eventuele testparameters in te voeren, zoals een gebruikersnaam.
  Het script maakt gebruik van thc-hydra.

- Analyse van Resultaten:
  Bekijk de resultaten van de beveiligingstests om zwakke punten in de beveiliging te identificeren.

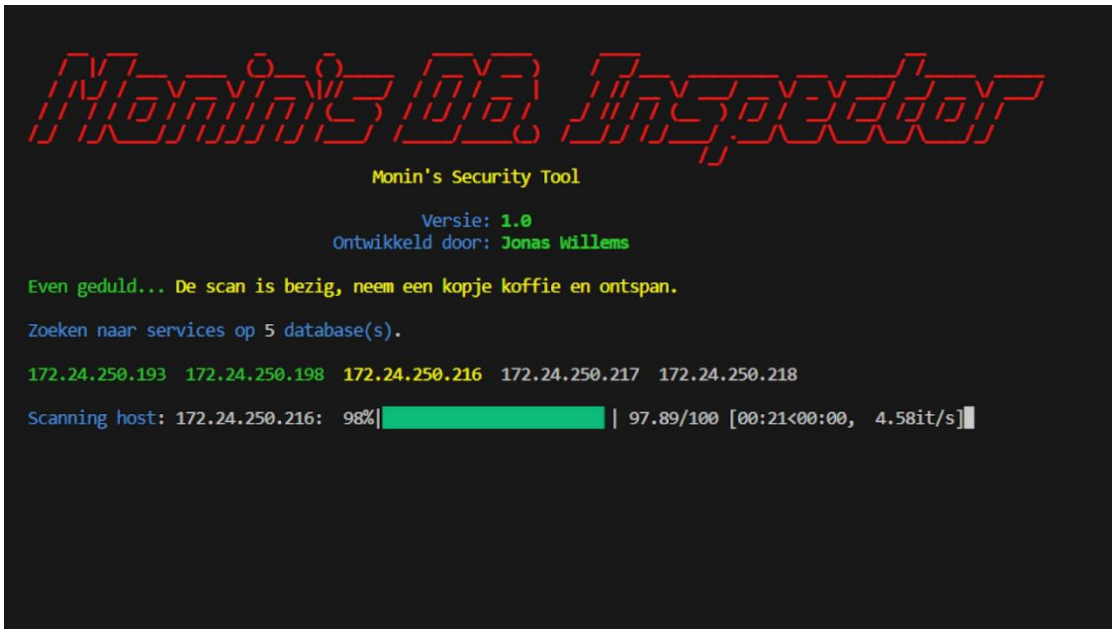
# 6 AFBEELDINGEN



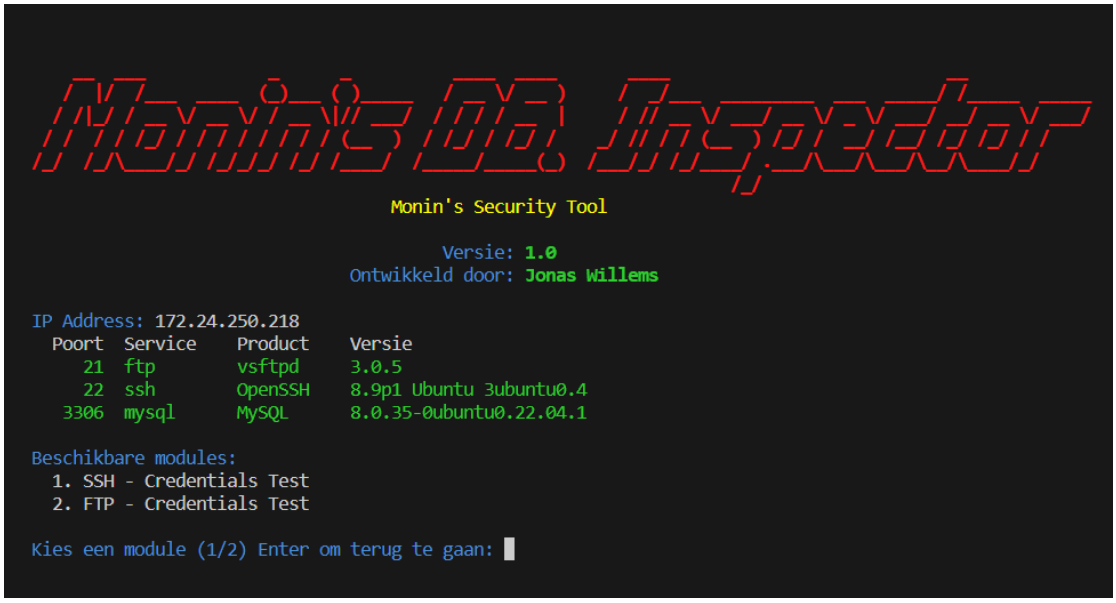



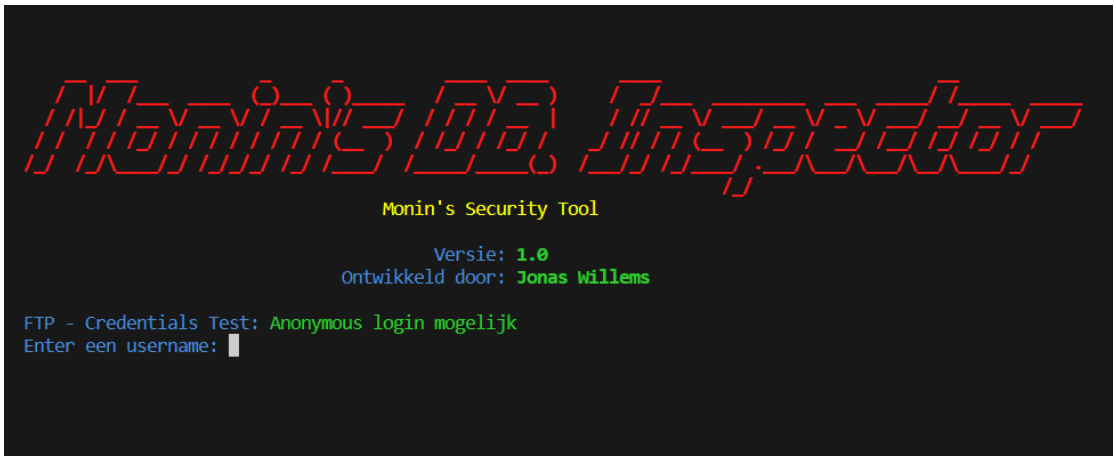

Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
Opties voor het zoeken:
1. Heel netwerk (CIDR-notatie bv. 192.168.1.0/24)
2. Meerdere IP's (gescheiden met komma's (,) bv. 192.168.1.1,192.168.1.5)
3. IP-bereik (gescheiden met streepje (-) bv. 192.168.1.0-192.168.1.5
4. Enkele host (bv. 192.168.1.5)
Selecteer een optie (1/2/3/4): Enter om terug te gaan:

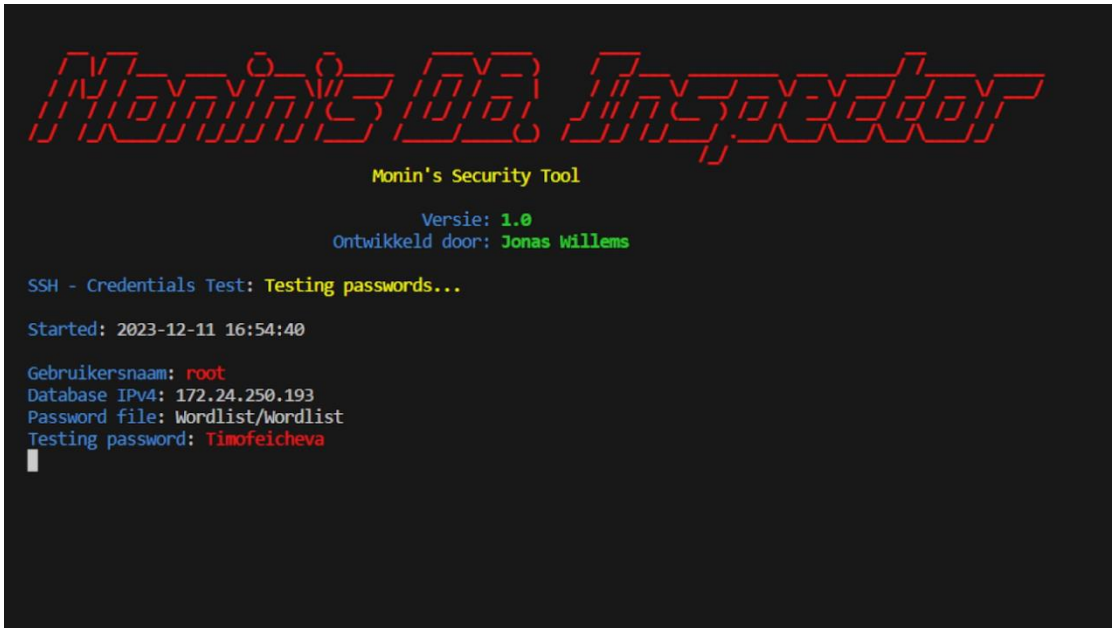

Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
Even geduld... De scan is bezig, neem een kopje koffie en ontspan.
Zoeken naar databases over 5 host(s): Gevonden: 3
172.24.250.193 172.24.250.198 172.24.250.216 172.24.250.217 172.24.250.218
Scanning host: 172.24.250.217: 0%| | 0/100 [00:00<?, ?it/s]

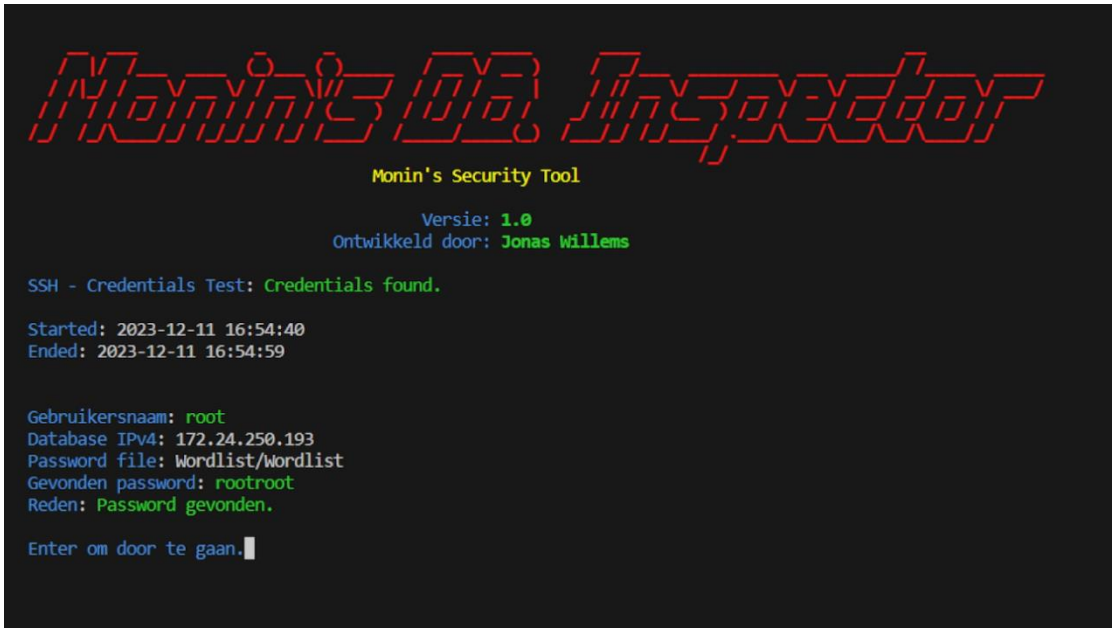

Monin's DB Inspector
Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
Even geduld... De scan is bezig, neem een kopje koffie en ontspan.
Zoeken naar services op 5 database(s).
172.24.250.193 172.24.250.198 172.24.250.216 172.24.250.217 172.24.250.218
Scanning host: 172.24.250.216: 98%| | 97.89/100 [00:21<00:00, 4.58it/s]


Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
Gevonden op: 2023-12-11 10:14:00
Oracle Database(s):
ID IP Poort Product Versie
1 172.24.250.193 1521 Oracle TNS listener
Microsoft SQL Server Database(s):
ID IP Poort Product Versie Naam
3 172.24.250.199 1433 Microsoft SQL Server 16.00.4075.00
5 172.24.250.217 1433 Microsoft SQL Server 2019 15.00.2000.00; RTM WIN-JOGGSUTBLA6
PostgreSQL Database(s):
ID IP Poort Product Versie
2 172.24.250.198 5432 PostgreSQL DB 9.6.0 or later
MySQL Database(s):
ID IP Poort Product Versie
4 172.24.250.216 3306 MariaDB 11.0.3
6 172.24.250.218 3306 MySQL 8.0.35-0ubuntu0.22.04.1
ID om een host te selecteren, enter om terug te gaan:


Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
IP Address: 172.24.250.218
Poort Service Product Versie
21 ftp vsftpd 3.0.5
22 ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4
3306 mysql MySQL 8.0.35-0ubuntu0.22.04.1
Beschikbare modules:
1. SSH - Credentials Test
2. FTP - Credentials Test
Kies een module (1/2) Enter om terug te gaan:


Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
FTP - Credentials Test: Anonymous login mogelijk
Enter een username:


Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
SSH - Credentials Test: Testing passwords...
Started: 2023-12-11 16:54:40
Gebruikersnaam: root
Database IPv4: 172.24.250.193
Password file: Wordlist/Wordlist
Testing password: Timofeicheva


Monin's Security Tool
Versie: 1.0
Ontwikkeld door: Jonas Willems
SSH - Credentials Test: Credentials found.
Started: 2023-12-11 16:54:40
Ended: 2023-12-11 16:54:59
Gebruikersnaam: root
Database IPv4: 172.24.250.193
Password file: Wordlist/Wordlist
Gevonden password: rootroot
Reden: Password gevonden.
Enter om door te gaan.

# 7 TO-DO

## 7.1 Uitbreidingen

- Gevonden credentials opslaan in de JSON-file.
- MSDAT en OSDAT integratie.
- Het ondersteunen van meerdere protocollen.
- Het genereren van een HTLM-rapport.

# 8 CONTACT

## 8.1 E-mail:

- Jonas.Willems@monin-it.be

## 8.2 GitHub-repository:

- jonaswillems/Monin-s-DB.-Inspector (github.com)