# Language

change to Shell

change name of the tool

check if automatic

# Summary

The main goal for this script is to automate the process of enumeration & recon that is run every time, and instead focus our attention on real pentesting.

This will ensure two things:

1. Automate nmap scans.
2. Always have some recon running in the background.

Once initial ports are found 'in 5-10 seconds', we can start manually looking into those ports, and let the rest run in the background with no interaction from our side whatsoever.

# Features

## Scans

Network**: Shows all live hosts in the host's network (~15 seconds)**

Port**: Shows all open ports (~15 seconds)**

Script**: Runs a script scan on found ports (~5 minutes)**

Full**: Runs a full range port scan, then runs a thorough scan on new ports (~5-10 minutes)**

UDP**: Runs a UDP scan "requires sudo" (~5 minutes)**

**Vulns : Runs CVE scan and nmap Vulns scan on all found ports (~5-15 minutes)**

**Recon : Suggests recon commands, then prompts to automatically run them**

**All : Runs all the scans (~20-30 minutes)**

**Note: This is a reconnaissance tool, and it does not perform any exploitation.**

## Automatic Recon

**With the recon option, nmapAutomator will automatically recommend and run** the best recon tools for each found port.  
If a recommended tool is missing from your machine, nmapAutomator will suggest how to install it.

Runs on any shell

nmapAutomator is 100% POSIX compatible, so it can run on any sh shell, and on any unix-based machine (*even a 10 YO router!*), which makes nmapAutomator ideal for lateral movement recon.

# Requirement

In general, most of the requirements should be already installed, especially in Kali OS. However, If Auto-Nmap Analyzer recommends installing any extra tool, user will be notified. Tools that need to be installed are:

Ffuf; sudo apt install ffuf -y

Gobuster; sudo apt install gobuster -y

# Installation

git clone https://github.com/21y4d/nmapAutomator.git

sudo ln -s $(pwd)/nmapAutomator/nmapAutomator.sh /usr/local/bin/

# Usage

./nmapAutomator.sh -h

Examples:

./nmapAutomator.sh --host 192.168.100.1 --type All

./nmapAutomator.sh -H 10.10.10.10 -t network -s ./nmap

﻿nmapAutomator.sh -H/--host <TARGET-IP> -t/--type <TYPE>

﻿nmapAutomator.sh --host 192.168.100.16 --type Network