FORMAN CHRISTIAN COLLEGE
(A CHARTERED UNIVERSITY)

Spring 2022 (2022SP)

COMP421: Information Security | Section A

Course Project Proposal

Project Title: D9scan

Group Members:

Ossama Bin Raza (22-10162)

Muhammad Waleed (22-11081)

Abdul Rauf (22-10586)

Submitted to: Dr. Saad Bin Saleem

Introduction

The ‘d9scan’ tool is a script written in Python3 that allows port scanning and backdoor detection on networks. The program is interactive and simply requires it to be run on Kali Linux. A set of commands along with the target IP address are passed inorder to begin the scanning process. Once the program starts, open ports are detected and a number of scripts are available that may be executed depending on the user. All the scripts in the program are backed by NMAP.

The program uses numerous Python3 libraries that include, socket, OS, time, sys, argpass, subprocess and requests. There are two major functions, generalScan() and automate(). The ‘generalScan’ function scans the target IP using Nmap. The ‘automate’ function gives users multiple scanning options that include, suggested Nmap scan, FTP backdoor detection, HTTP dlink backdoor detection. Almost all scripts in this program are backed by Nmap.

Problem Statement + Solutions:

The d9scan program is run on Kali Linux terminal making it difficult to be used by beginners. Python GUI using tkinter or QtPy may be added to the project for ease of usability.

A few bugs were also discovered in the program, the major one being that multiple attacks cannot be performed on a single IP as an error message is displayed and the program crashes. This bug can be fixed so a target IP can be thoroughly scanned without encountering errors.

The output of the program is displayed on the console and there is no option to save the output for later inspection/use. The output of the program may be saved onto the Desktop or any other directory as the IP address along with the time/date of the scan.

Additional features and commands such as ‘WHOIS’ could be added to the existing program for added functionality. More of such features can be added to the program depending on the available time frame.

The architecture of the code is poorly designed and it is difficult to understand because of minimal documentation and no comments in the code. These aspects of the code could be improved so that it is easier for new users to understand and potentially work on this program.

The program could be reworked so that it works on Windows, however, it may require multiple third party softwares and disabling windows security features. The whole process could be counterintuitive as it may end up leaving the user completely vulnerable to a cyberattack.

Reference(s)

Github: D9scan

sbinsaleem/d9scan: Network Scanner with Backdoor Detection, other Nmap resources and syn-protection detection (github.com)