Application of NMAP for Information Gathering in Penetration Testing

Kashija J., *Student*; Tewolde V., *Student*
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
Blekinge Tekniska Högskola, Karlskrona, Sweden

Penetration testing is a technique to help secure a network or application by highlighting its vulnerabilities by simulating a real attack under specific pre-decided circumstances [1, 2]. By identifying an environment's flaws, it becomes easier to protect it against potential attacks directed at these weaknesses.

There are several automated software tools for different functionality. One essential purpose of the tools is to gather information about the environment to get an idea of how the system is built. NMAP (Network Mapper) is a tool that scans a targeted network to detect open ports and running services [1, 2]. Prior to the development of its GUI called ZENMAP NMAP is a command line utility and some Linux distributions such as Kali Linux come pre-installed by default. Some of the techniques used by NMAP to scan target networks include: -sS (TCP scan), -sT (TCP connect scan), -sU (UDP scans), -p (for port ranges) --exclude-ports <port rage> (excludes ports) [3].

The first step of penetration testing is reconnaissance. This step requires the tester to obtain as much information about the target environment as possible. Scanning the network with NMAP allows the tester to see what ports are open, closed, filtered, unfiltered open|filtered and closed|filtered [3]. This is valuable data to plan future steps. However, [1] claims that NMAP is considered a noisy tool, which could lead to being detected by an Intrusion Detection System and Intrusion Prevention System, consequently being blocked out of the system.

Adviser: Yeremenko O.S., *Dr.Eng.Sc., Assoc. Prof.*

1. S. Rahalkar, *Quick Start Guide to Penetration Testing* (Apress: 2018).
2. R. Messier, *Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems* (Apress: 2016).
3. G. Lyon, *Nmap security scanner* (2014). Available: http://nmap.org/.