NMAP SCAN REPORT

Conducted by: Riddhi Bagri

Risks: nmaping someone's private or unauthorised is illegal.

Introduction:

-NMAP stands for Network Ma**p**per.

-It is a tool used for Host Discovery (which ports are open), Port Scanning and OS detection.

-It is written in C, C++ and Python.

Commands Performed:

1) nmap -V

   Shows details about the nmap software, including it's version number and software details.

2) nmap -F scanme.nmap.org

   -F tells nmap to perform a Fast Scan on the host scanme.nmap.org displaying details of ports that are open and service.

3) Ifconfig wlan0

   Shows the IP of the current system

4) nmap –F 192.168.56.1

   Shows the ports open on the current system.

5) cat/root/Desktop/target.txt
6) nmap –iL root/Desktop/target.txt

   We can nmap under a specific file too.

Learning:

-Ports 0-1023 (well known ports), Ports 1024-49151 (registered ports/vendors use for applications) and Ports>49151 (dynamic/private ports).

-HTTP mainly runs on 80,8080 and HTTPS runs on 443.