SYSTEM PENETRATION TESTING

INTRODUCTION

A Penetration testing is the most commonly used security testing technique for web applications. Web Application Penetration Testing is performed by simulating unofficial attacks internally or externally to get access to sensitive data. A penetration helps end user find out the possibility for a hacker to access the data from the internet, find about the security of their email servers and also get to know how secure the web hosting site and server are. Importance and the need for Web App Pen Testing:

1) Penetration testing helps in identifying unknown vulnerabilities.

2) Helps in checking the effectiveness of the overall security policies.

3) Help in testing the components exposed publicly like firewalls, routers, and DNS.

4) Lets user find out the most vulnerable route through which an attack can be made.

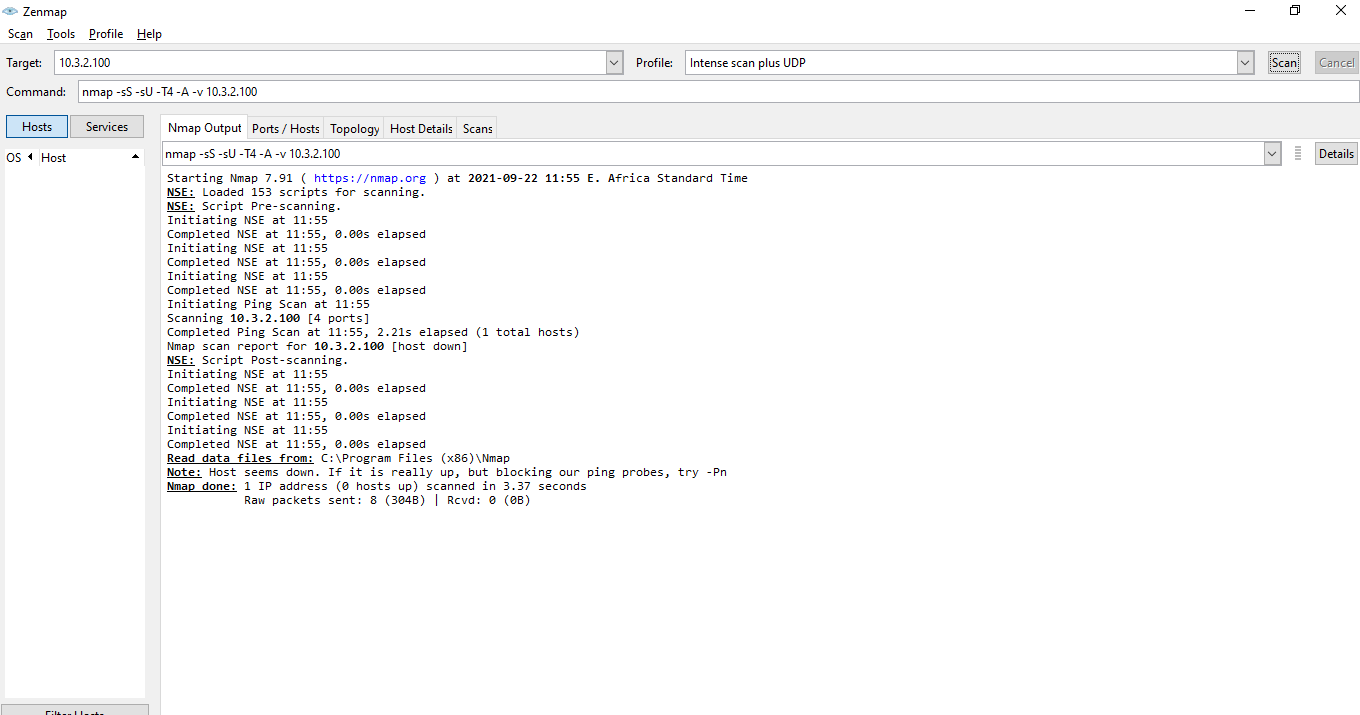
5) Helps in finding the loopholes which can lead to theft of sensitive data.

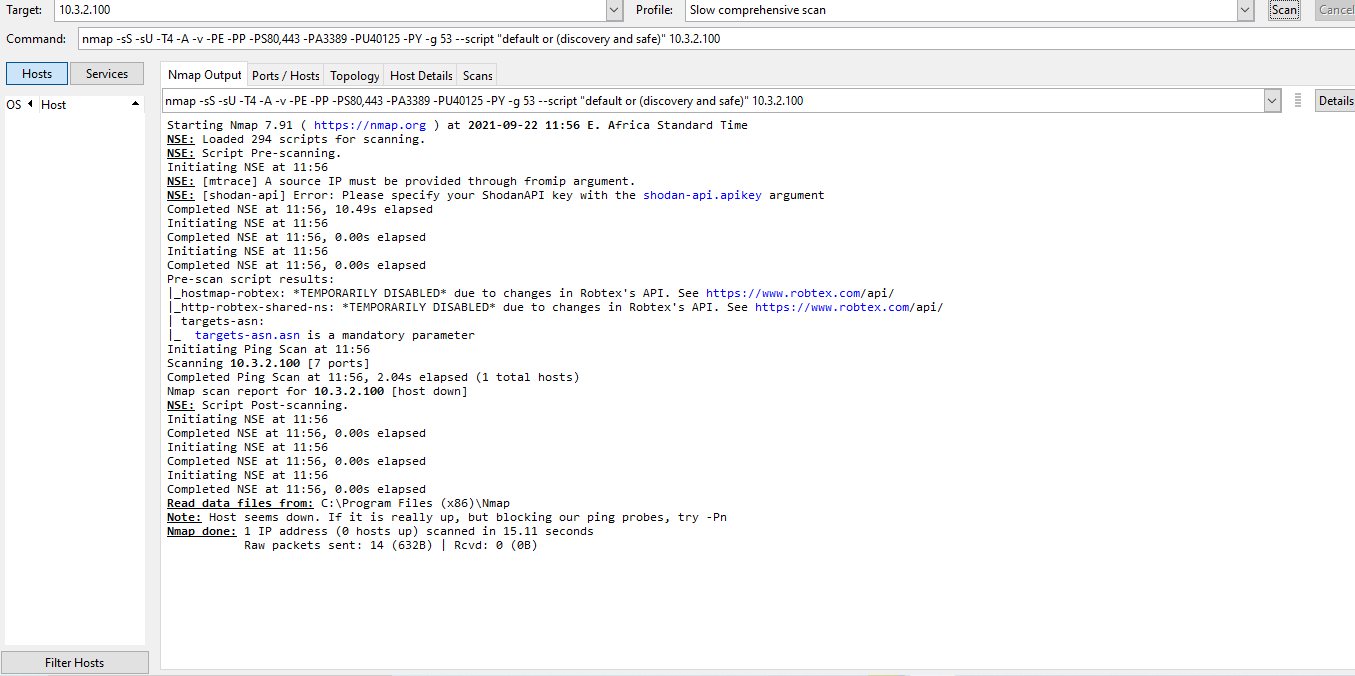
This project deals with preventing the potential errors while developing a basic victim domain in order to prevent it from possible cyber-attacks. The attack will not be able to harm from the secured website (like fetching data etc.) while it may be able to harm the other one, so this will clearly elaborate what are the important points which must be taken care of while developing any basic website to make it secure.

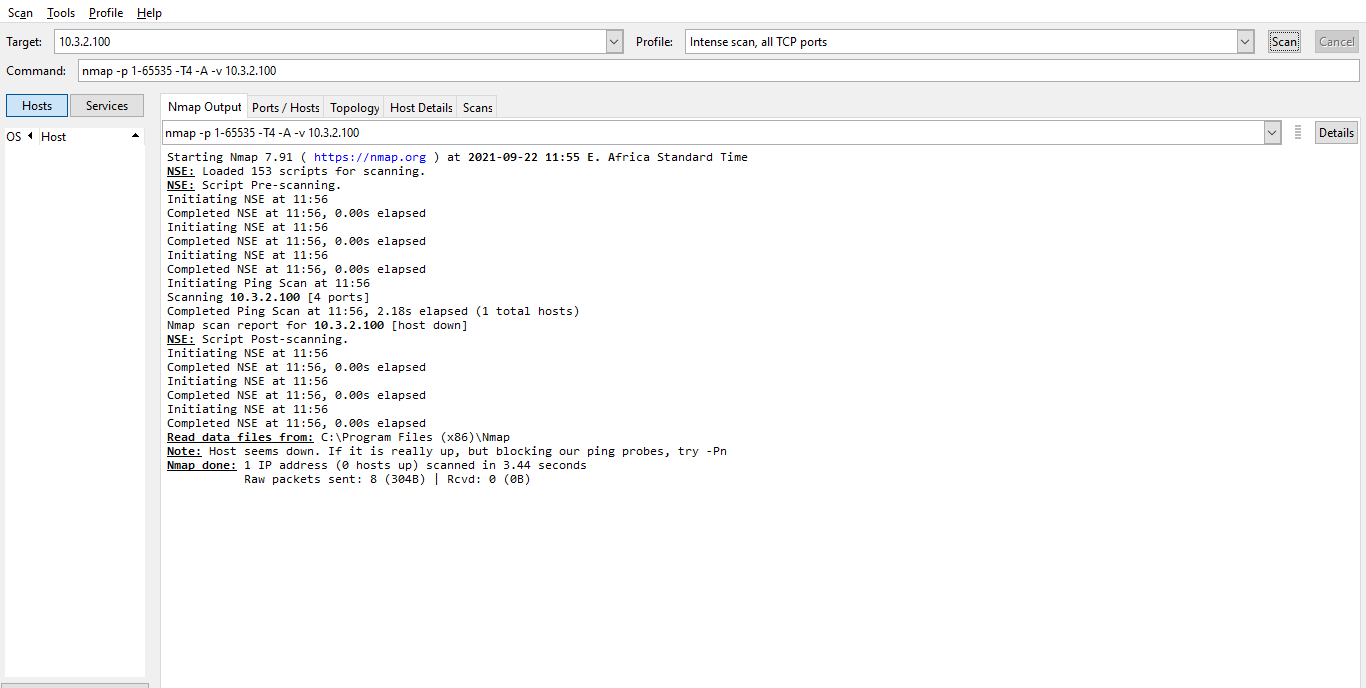
VULNERABILITY TEST

1.ZenMap Scan

Images of the Zen-map Scan of the victim machine







3.Open Socket Analysis of the Ports

Ncat is a feature-packed networking utility which reads and writes data across networks from the command line. Ncat was written for the Nmap Project as a much-improved reimplementation of the venerable Netcat. It uses both TCP and UDP for communication and is designed to be a reliable back-end tool to instantly provide network connectivity to other applications and users. Ncat will not only work with IPv4 and IPv6 but provides the user with a virtually limitless number of potential uses.

Among Ncat’s vast number of features there is the ability to chain Ncats together, redirect both TCP and UDP ports to other sites, SSL support, and proxy connections via SOCKS4 or HTTP (CONNECT method) proxies (with optional proxy authentication as well). Some general principles apply to most applications and thus give you the capability of instantly adding networking support to software that would normally never support it.