IT-Security 2019

Exercises: Information Gathering :

Exercise 1: Identify open and close ports

In this exercise use a Port scanning tool of your choice and scan the web application http://scanme.nmap.org/ which is a intentionally vulnerable application developed for training purposes. Please restrict the scan to only the URL provided and do not attempt it on publicly known web application.

The exercise answer you must include: 1) briefly describe the tools, the installation of the associated tools and and methodolgy used to scan 2) Explain the different scan types used for the reconnisance. 2) State the findings on open and close ports and which possible applications are running on http://scanme.nmap.org/

Exercise 2: Port Scanning

As a network administrator provide detailed steps to avoid port scanning of the public facing interfaces in your network.

Exercise 3: Anonymity tools

TOR is often the choice to surf the internet anonymously. However, alternatives to TOR exist, for example Open VPN hosters like *IPredator*. Both systems provide bundles/installers or standard configuration tutorials. Explain what the differences between TOR and IPredator are. For each system, provide a detailed attack that potentially could deanonymize users in the system.