FOOTPRINTING, RECONNAISSANCE, SCANNING AND ENUMERATION TECHNIQUES OF COMPUTER NETWORKS

DR. HIDAIA MAHMOOD ALASSOULI

Footprinting, Reconnaissance, Scanning and Enumeration Techniques of Computer Networks

By
Dr. Hidaia Mahmood Alassouli
Hidaia_alassouli@hotmail.com

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Footprinting, Reconnaissance, Scanning and Enumeration Techniques of Computer Networks

Written by Dr. Hidaia Mahmood Alassouli.

1. Introduction:

Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible.

Footprinting refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization. Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected.

Network scanning is used to recognize available network services, discover and recognize any filtering systems in place, look at what operating systems are in use, and to protect the network from attacks. It can also be used to determine the overall health of the network.

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

The objective of the report is to explain to the user Footprinting, Reconnaissance, Scanning and Enumeration techniques and tools applied to computer networks

The report contains of the following parts:

- Part A: Lab Setup
- Part B: Foot printing and Reconnaissance
- Part C: Scanning Methodology
- Part D: Enumeration

You can download all hacking tools and materials from the following websites

http://www.haxf4rall.com/2016/02/13/ceh-v9-pdf-certified-ethical-hacker-v9-courseeducatonal-materials-tools/

www.mediafire.com%2Ffolder%2Fad5szsted5end%2FEduors_Professional_Ethical_Hacker&h=gAQGad5Hf