Introduction to Ethical Hacking

Importance of Networking essentials in Ethical Hacking.

Samarendranath B

CONTENTS

- What is Ethical Hacking?
- Penetration Testing
- Role of the Ethical Hacker

What is Ethical Hacking?

- It refers to the act of locating weaknesses and vulnerabilities of computer and information system by replicating the intent and actions of malicious hackers.
- It is also referred as penetration testing, intrusion testing or red teaming.

Introduction to Ethical Hacking

- Ethical Hackers
  - Employed by company to do penetration testing
- Penetration Test
  - Legal attempt to break into company's network to find the weak links.
  - Tester only report findings, does not provide any solutions.
- Security test
  - Also includes analyzing company's security policy and procedures.
  - Tester offers solutions to secure or protect the network

Some Terminologies

- Hacking: Showing computer expertise.
- Cracking: Breaching security on software or systems.
- Spoofing: Faking the originating IP address in a datagram.
- Denial of Service (DoS): Flooding a host with sufficient network traffic so that it cannot respond anymore.
- Port Scanning: Searching for Vulnerabilities.

Gaining Access

- Front door
  - Password guessing
  - Password/key stealing
- Back door
  - Often left by original developers as debug and/or diagnostic tool
- Trojan horses
  - Usually hidden inside of software that we download and install from the network.
  - Many install backdoors
- Software Vulnerability Exploitation
  - Often advertised on the OEMs website along with security patches.
  - Fertile ground for script kiddies looking for something to do.

Once inside, hacker can …

- Modify logs
  - To cover their tracks
- Steal files
  - Sometimes destroy after stealing
  - An expert hacker would steal and cover their tracks to remain undetected.
- Modify files
  - To let you know they were there.
  - To cause mischief.
- Install back doors
- Attack other machines

The Role of Security and Penetration Tester

- Script kiddies or packet monkeys
  - Young and inexperienced hackers
  - Copy codes and techniques from knowledgeable hackers
- Experienced penetration testers write programs or scripts using
  - C, C++, python, JavaScript, Visual Basics, Pearl, SQL…..

Penetration Testing Methodologies

- Tiger box
  - Collection of OS's and hacking tools.
  - Usually on a laptop.
  - Helps penetration testers and security testers conduct vulnerabilities assessments and attacks.
- White box model
  - Tester is told everything about the network topology and technology.
  - Tester is authorized to interview IT personal and employees of the organization.
  - Makes tester job little easier.

Penetration Testing Methodologies

- Black box model
  - Tester is not given details about the network.
  - Burden is on the tester to find out the details.
- Gray box model
  - Hybris of the white and black box model.
  - Company gives tester partial information.

What You Can Do Legally

- Laws involving technologies changes as rapidly as technology itself.
- Find what is legal for you locally.
  - Law changes from place to place.
- Be aware of what is allowed and what is not allowed.

Laws of the Land

- Tools on your computer might be illegal to possess.
- Contact local law enforcement agencies before installing hacking tools.
- Written words are open to interpretation.
- Govt are getting more serious about punishment for cybercrimes.

What You Cannot Do Legally

- Accessing a computer without permission is illegal.
- Other illegal actions:
  - Installing worms and viruses.
  - Denial of Service attack.
  - Denying user access to network resources.
- Be careful your actions do not prevent customers from doing their jobs.

Ethical Hacking in a Nutshell

- What it takes to be a security tester?
  - Knowledge of the network and computer technologies.
  - Ability to communicate with management and IT personnel.
  - Understanding of laws.
  - Ability to use necessary tools.

We Shall Cover

- Networking Essentials
- Information Gathering
- Exploitation and clear the trace
- Evading Security Systems
- Incident Response