
Ethical Hacking

Loophole with Ethical Hacking and Penetration Testing

Duration

Lecture and Demonstration: 15 Hours
Security Challenge: 01 Hours

Introduction

Security can't be guaranteed. As Clint Eastwood once said, "If you want a guarantee, buy a toaster." The only secure system is one that's unplugged, turned off, and in a locked room.

As it's not practical to leave our systems turned off, we need to understand the risks to our systems and prepare ourselves to defend them. Preparation begins with understanding — and that's where awareness comes in.

With all the news stories about hackers, botnets, and breaches involving personal information, it's easy for the security message to sound over-used and tired. It's easy for people to say, "It won't happen here." Yet, studies and surveys repeatedly show that: the human factor (what employees do or don't do) is the biggest threat to information systems and assets.

The best way to achieve a significant and lasting improvement in information security is not by throwing more technical solutions at the problem — it's by raising awareness and training and educating everyone who interacts with computer networks, systems, and information.

Module Structure

Loophole, Ethical Hacking and Penetration Testing workshop, aims to educate users of digital media of the threats, risks and privacy concerns that go with using them. The other goal of this training module is to expose issues and vulnerabilities to drive the digital media industry to create solutions to these problems.

Detailed Module

ISMS with Concept of Hacking

Duration: 30 minutes

(based on GT101: Foundation of Information Security)

Elements of Information Security

- Information Security Supports the Mission of the Organization
- Information Security Should Be Cost-Effective
- Responsibilities and Accountability Should Be Made Explicit
- Owners Have Security Responsibilities Outside Organizations

Roles and Responsibilities

- Senior Management
- Program and Functional Managers/Application Owners
- Users

Common Threats: A Brief Overview

- Fraud and Theft
- Employee SabotageLoss of
- Physical and Infrastructure Support
- Threats to Personal Privacy

Indian Cyber Law

Duration: 30 minutes

(based on GT115: Getting Familiar with Indian Cyber Law)

Information Technology Act 2000-2008

- Introduction to IT Act 2000
- Amendment 2008
- Under Umbrella of IT Act 2000
    - Cyber Crimes
    - Intellectual Property
    - Data Protection and Property
- Limitations of Indian IT Act

Web Application Penetration Testing

Duration: 120 minutes

(based on SE118: Essentials of Web Application Penetration Testing)

Introduction to Penetration Testing

- Legal and Ethical Implications
- Types of Penetration Testing
    - White Box Penetration Testing
    - Black Box Penetration Testing
    - Grey Box Penetration Testing

Setting Up Web Application Penetration Testing Lab

- Collecting and Installing PenTest Tools
- Flexible Browser with Security Add-ons
- Setting up Browser Proxies

Beginning Application Penetration Testing

- Identification of Application Entry Points
    - Get and Post Parameters
- Testing for Security Vulnerabilities
    - SQL Injection
    - Cross Site Scripting
    - Session Hijacking
    - Local and Remote File Inclusion Attacks
    - Parameter Tampering

Basics of Secure Programming

Duration: 30 minutes

(based on GT122: Secure Coding Practices\ for Applications)

Use Cryptography for Application Security

- Hashes
- Secure Key Storage
- Weak Practices in Cryptography

Data Validation Strategies

- Where to include Data Validation
- Prevent Parameter Tampering
    - Hidden Fields
- Encoded Strings
    - HTML and URL Encoding
    - Delimiter and Special Characters

Session Management

- Session ID Generation
- Session Handling
    - Regeneration of Session Tokens
    - Session Validation
    - Session Bruteforcing
- Session Termination

Hacking Emails and Social Networks

Duration: 90 minutes

(based on GT102: An Eye Opener to Cyber Social Media Security)

Cyber Social Media Threats

- Social Engineering
    - Human Based Social Engineering
    - Computer Based Social Engineering
- Fake Emails
- Keystroke Loggers
- Phishing
- Identity Theft

Securing Your Cyber Social Life

- Awareness is the Key
- Email Security
    - Detecting Fake Emails
    - Creating Account Filters
- Online Account Security
    - Strong Password Setup
    - Designing Account Recovery Mechanism
    - Secure Logout
    - Browser Remember Password
- Recognizing Phishing Websites

Google Hacking

Duration: 30 minutes

(based on GT121: Google Best Friend of a Hacker)

Working of Google and its methodology

- Introduction to Crawlers, Bots
- Caching Process of Crawlers

Various Roles of Google as a Friend of Hacker

- Advance Google Search Operators
- Directory Traversal Tool
    - Finding Directory Listings
    - Locating Specific Directories
- Vulnerable Website Locator
    - Locating via Company Tags
    - Locating via Web Applications
    - Locating via Common Names

Various Attacks with the help of Google

- Password Harvesting
- Controlling CCTV Camera

Data Security and Recovery

Duration: 60 minutes

(based on GT117 - Data Recovery and Backup)

Data Security with Cryptography

- Securing Data by Using EFS and BitLocker
- File and Folder Permissions
- Alternate Data Streams
- Encrypting Office Documents

Recovering Techniques

- Corrupt Partitions
- Corrupt File System
- Media Errors
- Overwritten Damage

Data Acquisition

- OS Volume Information
- Disk Imaging

World of Digital Virtualization

Duration: 30 minutes

(based on GT105: Concepts of Computer Virtualization)

Introduction to Virtual Machines and Virtualization

- Concept of Virtualization
- Need and Advantages of Virtualization

Installation and Configuration

- Hardware and Software Requirements
- Installation and Configuration

- Performance Optimization
  - CPU & Memory Performance
  - Network Performance Optimization
    - Host to Host Networking
    - Host to LAN Networking
  - Storage Performance

Hacking and Securing Windows Systems

Duration: 120 minutes

(based on GT108: Beginning with Windows Security)

Introduction to Windows Security

- Overview of Windows OS
- Windows File System
- Security Architecture in Windows
  - Local Security Authority
  - Security Account Manager
  - Security Reference Monitor

User Account Security

- Password Attacks in Windows
  - Bruteforcing, Dictionary and Rainbow Table Attacks
- Account Security Strengthening
  - Strong Password Policy
  - Additional Security: Syskey Encryption
  - User Account Control : Parental Controls
  - Restricting BIOS Setup

Services, Port and Protocol Security

- Auditing and Monitoring Network Connections
- Restricting Ports, Protocols and Services
- Windows Firewall with Advanced Restrictions

Security Applications in Windows

- Auditing and Monitoring Windows Auto Startup
- Defending Windows via Windows Defender
- Policy Management with MBSA
- File and Folder Scanning with MSSE

Malware: Attack, Detect and Defend

Duration: 90 Minutes

(based on GT110: Computer Malware: Detection and Defense)

Introduction to Computer Malware

- Overview Malware: Malicious Software
- Proliferation and Purposes
- Types of Malware
- Virus: Vital Information Resources Under Seize
- Worm: Write Once Read Multiple
- Trojan Horse, RootkitSpyware, Keystroke Logger

Virus and Worm: Infectious Malware

- Significance of Virus and Worm
- Behavioral Activity of Virus and Worm
- Virus and Worm Development
    - By Automated Tools
    - Coding own Viruses and Worms

Trojan Horse: Concealment

- Overview of Trojan
- Trojan Attack
    - Direct Connection
    - Reverse Connection
- Injection in System Files

Detection and Removal

- Anti Malware Tools
- Manual Removal of Malwares

Software Cracking: Product Key Generation

Duration: 60 minutes

(based on GT111: Application Reverse Engineering)

Introduction to Assembly Language

- Role of Assembly Language in Reverse Engineering
- Concept of Debuggers and Dis-assemblers

Understanding Data Flow

- "Step Over" view of Data flow
- "Step Into" view of Data flow

Principles of Software Security

- Encryption
- Online Key Checking
- Fake Checking Points
- DLL Breakpoints

Mini Chakravyuh – Security Challenge

Duration: 60 minutes

(based on Password Cracking and Product Key Generation)

Requirements

- Computer Device (Bring Your Own Device)
- Windows Operating System
- Working CD/DVD Drive
- Removable Storage Media (Pen Drives 1GB)
- Battery Backup for 60 minutes

Challengers will be asked to install Virtual PC in their machines so that they can use the challenge machine.

Level 1: Windows Password Cracking

Windows virtual machine will be password protected. Challengers will be required to recover the password of the administration user account using the password cracking techniques demonstrated during the workshop.

Level 2: Product Key Generation

Windows virtual machine will carry a software setup. Challengers will be required to generate a valid product key against their name.

Target application will be with the Loophole Software Toolkit

Demonstration

Winners will be required to demonstrate the solution of both the levels to all the participants of the workshop to declare their win.

Mobile Hacking Techniques and Security Concepts

Duration: 30 minutes

(based on GT116: Vulnerabilities in Mobile & VOIP Security)

Attacks for Faking Caller ID

- via Softphones
- via Websites

Attacks for SMS Technology

- Faking Sender ID: Fake SMS
- Faking Sender ID: Fake MMS

Mobile Security Kit

- Anti Virus
- Key Guard
- Secure Password Setup
- Threats Posted by Third Party Application