Suggested Teaching Guideline for

Security Concepts PG-DITISS September 2022

Duration: 84 classroom hrs + 96 lab hrs (Total: 180 Hrs)

Objective: To introduce the student to issues related to application security and ethical Hacking.

Prerequisites: Knowledge of database concepts

Evaluation method: Theory exam – 40% weightage
Lab exam – 40% weightage
Internal Assessment – 20% weightage

List of Books / Other training material

Courseware: Gray Hat Hacking: The Ethical Hackers Handbook by Shon Harris
Reference: Python for Unix and Linux System Administration

Application Security

(MySQL): (20 hrs)
Session 1:

- Introduction to MYSQL
- Installing and Configuring MYSQL
- Creating and Dropping Database
- Queries in MYSQL

Lab Assignment:

- Create a MYSQL user.
- Create a database add tables and then add data into those tables.
- Delete/Modify a Table or Database.

Session 2 & 3:

- Web Application Security Risks
- Identifying the Application Security Risks
- Threat Risk Modelling
- Other HTTP fields

Lab Assignment:

- Identify all risks and vulnerabilities of web applications using tools.

Session 4 & 5:

- Data Extraction
- Advanced Identification/Exploitation

Lab Assignment:

- Find vulnerability of data extraction/exploitation of a web application.
- Find vulnerabilities of HTTP Methods (1.0 & 1.1).
- Analyse web application with the help of Wireshark.

(Web Application Security): (20hrs)

Session 6 & 7:

- OWASP Top 10 – 2021
- Injection and Inclusion
- Cross Site Scripting
- Injection in stored procedures

Lab Assignment:

- Give SQL queries to bypass authentication.
- Make your own cross site script and apply in any web application.

Session 8:

- Denial of Service
- Buffer Overflows and Input Validation
- Access Control

Lab Assignment:

- Try DOS attack to denial a service of any server.
- Try to do input validation to get access in vulnerable application.

Session 9:

- DevOps Security
- API Security
- OWASP top 10 Cloud security Risks
- Secure Code Review

Session 10:

- SAST and DAST tools
- Case Study On Web Application Framework
- Use browser-jsguard Firefox add-on also to detect Malicious and Suspicious Webpages.

Lab Assignment:

- Try to do static and Dynamic application security testing by SAST and DAST tools.

(Python) 24 Theory + 30 Lab

Session 11:

- Installing Python
- Your First Python Program
- Declaring Functions
- What's an Object?
- Indenting Code
- Testing Modules
- Native Data types

Lab Assignment:

- Try to install Python in windows and Linux (if by default not installed)
- Do practice of all data types questions?
- Make small program to print Hello Word
- Make a script file in Python and run that script.
- Take an input from user while running the program and print the output.
- Use for/while loop and If-else condition in program.

Session 12 & 13:

- Introducing Dictionaries
- Defining Dictionaries
- Modifying Dictionaries
- Deleting Items from Dictionaries
- Files
- Introducing Lists
- Defining Lists
- Adding Elements to Lists
- Searching Lists
- Deleting List Elements
- Using List Operators

Lab Assignment:

- Create a dictionary, print that dictionary.
- Use for/while loop while running the programme.
- Insert/delete an item in dictionary.

Session 14:

- Introducing Tuples
- Declaring variables
- Referencing Variables
- Assigning Multiple Values at Once
- Formatting Strings
- Mapping Lists
- Joining Lists and Splitting Strings
- Historical Note on String Methods

Lab Assignment:

- Create a tuple, print that tuple.
- Use for/while loop while running the program.
- Insert/delete an item in tuple.

Session 15:

- Using Optional and Named Arguments
- Using type, str, dir, and Other Built-In Functions
- Object References
- Socket with Python

Lab Assignment:

- Append/insert/extend/remove/sort/reverse a list.
- Append/insert/extend/remove/sort/reverse a string.
- Use Built-in functions.

Session 16:

- Regular Expressions Using python
- Scripting in Python
- Functions and Functional Programming

Lab Assignment:

- Use regular expression to take a regular expression and search any pattern.
- Do all of these with the help of regular expression.
    - Match a single character except newline.
    - Match a word.
    - Match a Decimal word.
    - Match a single whitespace character.
    - Match any Non-whitespace character.

Session 17:

- Object Oriented Linux Environment
- Classes, Objects and OOPS concepts

Lab Assignment:

- Do practice of memory management questions.
- To find out Current directory of a file
- To find out all folders & files inside given folder.
- To find out absolute path and relative path.
- To check if a file or folder exists or not.
- To create/remove a Directory.
- To check the permissions.

Session 18 & 19:

- File Handling
- Directory Access Permissions
- Controls Socket
- Libraries and Functionality Programming
- Servers and Clients Arch
- Web Servers and Client scripting
- Introduction to Python web development framework

Lab Assignment:

- To read or write a file using python.
- Print everything written in a file.
- Count, how many lines are there in a file?
- Count, how many words are there in a file
- To read a web page content

Session 20:

- Libraries and Functionality Programming
- Servers and Clients Arch
- Web Servers and Client scripting

Lab Assignment:

- Create a socket between a server and a client then analyse and monitor all activity done by client.

Session 21:

- Exploit Development techniques
- Writing plugins in Python

Lab Assignment:

- With the help of socket programming try to exploit.

Session 22:

- Exploit analysis Automation Process
- Debugging basics

Ethical Hacking (30 hrs Theory+ 36 hrs Lab)

Session 23:

- Security Management Concepts & Principles
- Human side of Information Security's
- Threats of Information System
- Threats and attacks
- Classification of Threads and attacks

Session 24:

- Protecting Information System Security
- Security in Mobile and Wireless Computing
- Credit card frauds in mobile and wireless Computing
- Information Security Management
- Fundamentals of Information Security

Session 25:

- Cyber Crimes
- Understanding Cyber Crimes in context of Internet
- Legal aspects of open communications
- Indian Penal Law & Cyber Crimes Fraud Hacking Mischief
- International law
- Obscenity and Pornography Internet

- Introduction to Ethical Hacking
- Understanding Ethical Hacking Terminology
- Identifying Different Types of Hacking Technologies
- Understanding the Different Phase Involved in Ethical Hacking

Session 26:

- Types of Hacker Classes
- Red team , Blue Team ,Grey Team
- Ethical Hackers and Crackers
- Goals of Attackers
- Security, Functionality and Ease of Use Triangle
- Defining the Skills Required to become an Ethical Hacker

Session 27:

- How to Conduct Ethical Hacking
- Creating a Security Evaluation Plan
- Types of Ethical Hacks
- Foot-printing and Social Engineering
- Understand How Traceroute Is Used in Foot-printing
- Define the Terms Port Scanning, Network Scanning and Vulnerability Scanning
- Understand various Scanning Methodologies
- SYN, Stealth, XMAS, NULL, IDLE and FIN Scans

Lab Assignment:

- Use NMAP, WHOIS for Reconnaissance.
- Open-source Intelligence Gathering tool:
    - Netcraft, Shadon, Google Dorks, Recon-Ng
- Use traceroute in footprinting.
- Use FOCA for finger printing.
- Use Tree Pad tool for reporting

Session 28:

- TCP Communication Flag Types
- Banner Grabbing and OS Fingerprinting Techniques
- How Proxy servers are used in launching an Attack?
- Http tunneling Techniques
- IP Spoofing Techniques
- Enumeration
- Password-cracking Techniques
- Cracking Windows Passwords
- Redirecting the SMB Logon to the attackers
- SMB Redirection, SMB Relay MITM Attacks and Countermeasures
- NetBIOS DOS Attacks
- DDos Attack

Lab Assignment:

- Do all these practical of following;
  - Ip spoofing
  - DNS Reconnaissance
  - DNS Enumeration
  - Host and Port Discovery (using NMAP) etc.
- Use Nessus also to find Vulnerability.

Session 29:

- Password-Cracking Countermeasures
- Active/Passive online Attacks
- Offline Attacks
- Keyloggers and other Spyware Technologies
- Trojans and Backdoors
- Overt and Covert Channels
- Types of Trojans
- Reverse-connecting Trojans
- Netcat Trojan
- Indications of a Trojan Attacks

Lab Assignment:

- Use KALI operating system tools to crack password

Session 30:

- Wrapping
- Trojan Construction Kit and Trojan Makers
- The countermeasure Techniques in Preventing Trojans
- Trojan-Evading techniques
- System File Verification

Session 31:

- Difference between a Virus and a Worm
- Types of Viruses
- Antivirus Evasion Techniques
- Virus Detection Methods

Session 32:

- Protocols Susceptible to Sniffing
- Active and Passive Sniffing
- ARP Poisoning
- Ethereal Capture and Display Filters
- MAC Flooding
- DNS Spoofing Techniques
- DNS hacking
- Describe Sniffing Countermeasures

Session 33:

- Types of DOS Attacks
- How DDos Attacks Work
- How BOTs/BOTNETs work

- Smurf Attacks
- SYN Flooding
- Spoofing vs Hijacking
- Types of Session Hijacking
- Steps to perform session Hijacking
- Prevention of session Hijacking

Session 34:

- Hacking Web Servers
- Web Application Vulnerabilities
- Web-Based Password Cracking Techniques
- Wireless Hacking
- WEP, WPA Authentication Mechanisms and Cracking Techniques
- Wireless Sniffers and Locating SSIDS, MAC spoofing
- Wireless hacking Techniques
- Methods used to secure Wireless Networks

Session 35:

- Backdoor Devices
- Distributed Dos attacks
- Biometric Spoofing
- Linux Hacking
- Linux Backdoors
- IDSs, Honeypots and Firewalls

Lab Assignment:

- Use NAGIOS, SNORT as IDS/IPS
- Try to install DMZ in your infrastructure.

Session 36:

- Physical Security
- Overview of Physical Security
- Need of Physical Security
- Factors Affecting Physical Security
- Penetration Testing Methodologies

Lab Assignment:

- Use Metasploit framework for penetration testing.

Session 37: Malware Reverse Engineering

- Types of Malware
- Malicious code Families
- Latest Trends in Malware
- Analysis of Malware

Lab Assignment:

- Do analysis of a Malware use tools of Static and Dynamic analysis.
- Case Study
- Malware Analysis Scenario – Case Study

Note: We can use **USB Pratirodh** and **AppSamvid** tools for System security**.**

Mobile Security: (20 hrs)

Session 38:

- Introduction to Android Architecture
- Android File Structure
- Android Build Process
- Android App fundamentals
- Android Security Model
- Device Rooting

Lab Assignment

- Android Emulator setup

Session 39:

- Android Debug bridge
- Penetration Testing Tools

Lab Assignment

- Lab based on Android Debug Bridge

Session 40:

- OWASP Top 10 Mobile App vulnerabilities
- Attacks on Android Apps

Lab Assignment

- Lab based on Reverse Engineering
- Lab based on Smishing attack

Session 41:

- Web based attacks on Android devices
- Networks based attacks
- Social Engineering attacks

Lab Assignment

- Lab based on MITM Attacks
- Packet Sniffing using Wireshark
- Lab based on Phishing Attack

Session 42:

- Overview of Mobile Malware
- Android App Analysis

Lab Assignment

- Static and Dynamic Analysis of Android Apps using MobSF