Ethical Hacking

Content Outline

Session 1

Ethics & Hacking
Hacking history : How it all begin
- Why is security needed?
- What is ethical hacking?
- Ethical Hacker Vs Malicious hacker
- Types of Hackers
- Building an approach for ethical hacking
- Steps in Ethical hacking

Basics of Internet, Networking & Hacking
- What is a Network?
- Types of network – LANs, WANs & WLANs
- What is Internet?
- History of the Internet
- Basic Structure
- What is a Server?
- What is an IP Address?
- What is a domain name?
- IP-Domain Relation
- Client-Server Relationship Model
- Internet networking
- What is a port?
- What is Programming?
- Types of programming languages.
- What is a Programming loophole or error?

Session 2

Information gathering & Google Hacking
- Whois access (Demo)
- Maltego (Demo)

- 123people.com (Demo)
- Ip scaning (Demo)
- Port scaning (Demo)
- Network scaning & its tools (Demo)
- What is Google and how does it work?
- Google tricks (Demo)
- Basic hacks (Demo)
- How can Google hacking help an Ethical Hacker? (Demo)
- Accesing online remote cameras

Windows security
- Windows security (Demo)
- Registry (Demo)
- Port & Services (Demo)

Session 3

SQL injections attacks (Practical)
- Introduction of SQL
- What is SQL injection
- Checking SQL injection vulnerability (demo)
- Basic strategy of SQL injection (Demo)
- Getting login credientials using SQL injections (Live Demo)
- Using SQL to login via middleware language (Demo)
- URL and Forms (Demo)
- SQL Query SELECT, DROP etc. (Demo)
- SQL cheat sheets (Demo)
- Using source changes to bypass client side validation (Demo)
- Live demonstration of the attack (Demo)
- Using SQL injection tools (Demo)
- Importance of server side validation (Demo)
- How to protect your system from SQL Injections (Demo)

Man-in-the-middle attack (MITM Attack) (Practical)
- What is Man-in-the-middle attack?
- What is Backtrack linux (Most common unix system for ethical hacking)?
- Preparation for Man-in-the-middle attack (Demo)

Identifying victim (Demo)
- Cache poisining (Demo)

- Routing table modification (Demo)
- Eveasdroping (Demo)
- Countermeasures against MITM attack (Demo)

Session 4

Phishing, Trojan & Viruses
- What is phishing?
- Social engineering used in phishing (Demo)
- Phishing attack (Demo)
- Phishing sites (Demo)
- Protection against phishing (Demo)
- Viruses: Trojans, Worms, Malware, Spyware
- Modes of spreading
- Different Ways a Trojan can Get into a System (Demo)
- Creation of Trojan using cybergate (Demo)
- Attacking a system using our created trojan (Demo)
- Indications of a Trojan Attack (Demo)
- Some Famous Trojans and Ports They Use (Demo)
- How to Detect Trojans? (Demo)
- How to Determine which Ports are Listening (Demo)
- Netstat

Session hijacking & Cookie grabbing
- What are cookies? (Demo)
- Reading and writing cookies (Demo)
- Passive Vs Active session hijack (demo)
- TCP sessions and HTTP sessions (Demo)
- TCP session hijacking: Telnet (Demo)
- Stealing Cookies to hijack session using: XSS (Demo)
- Sniffers (Demo) - Spoofing (Demo)
- Spoofing Vs Hijacking
- Types of Hijacking
- Protection against session Hijacking (Demo)

Session 5

Social Network Attacks (Facebook, WhatsApp & Gmail)
- Overview of Social Engineering - Case Study
- Example of Social Engineering Attack
- Java Applet Attack (Demo) -WhatsApp Security -Facebook Security -Gmail Security

Call & SMS Spoofing
- What is Fake SMS & Call?
- Method of generating fake SMS & Calls (Demo)

DNS Spoofing:
- What is DNS Spoofing?
- How does it work?
- How to secure yourself?
- DNS Spoofing (Demo)

Session 6

Email Forging & Tracing
- How does an email work?
- Tracing an email (Demo)
- Spam

Firewalls & Keyloggers (Demo)
- Detecting fake emails (Demo)
- What is a firewall? & How can it help you
- How a firewall works
- What are key loggers? (Demo)
- Types of key loggers? (Demo)

Session 7

Understanding of an Organization's IT Environment
Concept of Zoning – Demilitarized Zone
Militarized Zone Basic Servers being used in the IT Environment
Positioning in different Zones
Brief Insight of the IT Security Devices used
What is Computer Forensics all about?
Difference between Computer Crime & Un-authorized activities
6 steps involved in Computer Forensics
Description of what is to be carried in each step

Need for forensics investigator

Session 8

Security Incident Response
What is a Security Incident?
Role of the Investigator in investigating a Security Incident Evidence Control and Documentation
Skills and Training of a Forensics Investigator
Technical, Presentation, Professional

Number of Team Members: 1