[1.] Hacking Psychology — 3 Hours

The next section will explain the purpose of ethical hacking and exactly what ethical hackers do. As mentioned earlier, ethical hackers must always act in a professional manner to differentiate themselves from malicious hackers. Gaining the trust of the client and taking all precautions to do no harm to their systems during a pen test are critical to being a professional.

(1.) Concept of Ethical Hacking: Legal or illegal??
(2.) Categories of Hackers(As per Knowledge)
(3.) Categories of Hackers(As per Working)
(4.) How to secure yourself from Attackers
(5.) How to Stop Attackers
(6.) Indian Cyber Law

[2.] E-Mails: Exploitation and Security — 4 Hours

Forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. The main protocol that is used when sending e-mail -- SMTP -- does not include a way to authenticate. There is an SMTP service extension (RFC 2554) that allows an SMTP client to negotiate a security level with a mail server. But if this precaution is not taken anyone with the know-how can connect to the server and use it to send spoofed messages by altering the header information.

(1.) What is an E-mail
(2.) Working of E-mail
(3.) Traveling of an E-Mail
(4.) Email Servers
(5.) E-mail Forgery and Spamming
(6.) Security to Anonymous Mailing
(7.) Attacks on E-Mail Password
(8.) Securing the E-Mail Passwords
(9.) Email Forensics

Typical email security products didn't. Phishing emails that link to infected websites cause many of today's information security breaches. Yet typical email security products use outdated methods from phishing's early days, when hackers attached viruses to emails. They can't catch blended email/web threats that can lead to malware infection. And they can't detect employee activities that can lead to data loss.

[3.] *Operating System Hacking & Security* *4 Hours*

Hacking systems and planting and or sending malicious content are the two most performed actions by hackers. As an ethical hacker, it will be your responsibility to test systems against hacking and to be prepared for the different types of malicious content that hackers will try to get into your network environment. This course examines password cracking methodologies and tools, privilege escalation, rootkits, steganography and backdoor types and tools, and different types of viruses and worms and their countermeasures.

1. **Introduction to System Software's**
2. **Windows Security Components and Working**
3. **Introduction to Virtual Machines**
4. **Implementation of Virtualization**
5. **Windows**
6. **Linux**
7. **Attacks on Windows Login Password**
8. **Other Security Measure**
9. **Windows Inbuilt Flaws and Security Loopholes**
10. **Invading into Computer System**
11. **Optimizing Windows Computer System**
12. **Restrict Hackers into box**

A technical background with a solid understanding of networks and networking concepts, such as IP, IP Routing, and LAN Switching, as well as Windows and/or UNIX/LINUX operating systems.

[4.] *Malwares: Trojan, Viruses & Worms* *6 Hours*

Malware, short for **malicious software**, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Named after the Trojan Horse of ancient Greek history, a **Trojan** is a network software application designed to remain hidden on an installed computer. Trojans generally serve malicious purposes and are therefore a form of **Malware**, like viruses.

1. **What are malwares?**
2. **Trojan**
3. **Trojan Attack Methods**
4. **Some Well Known Trojans**
5. **Detection of Trojan**
6. **Viruses**
7. **Working and Functionality of Viruses**
8. **Development**
9. **Development of Folder lockers**
10. **Registry tweaks and Tricks**
11. **Developing Professional Security too**
12. **Detection and Manual Removal**

A **computer virus** is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

[5.] *Attacks Related to Network & Security (LAN/WLAN)* *4 Hours*

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

1. **Introduction to the LAN (Local Area Networks)**
2. **Back-Track: Penetration Tool**
3. **Secure Network Configuration**

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

[6.] Web Server Attacks & Security 4 Hours

The HTTP (or HTTPS) protocol is the standard that makes it possible to transfer web pages via a request and response system. Mainly used to transfer static web pages, the web has quickly become an interactive tool making it possible to provide on-line services. The term "web application" refers to any application whose interface can be accessed on the web from a simple browser. Now the basis for a certain number of technologies (SOAP, Javascript, XML-RPC, etc.), the HTTP protocol plays an undeniable strategic role in information system security.

1. **Introduction to Web Application Security**
2. **Understanding Attack Vectors**
3. **Web Application Attacks**
4. **SQL Injection**
5. **Google Dorks – Using Google as an Expert**
6. **Cross Site Scripting: XSS**
7. **Directory Traversal Attacks**
8. **Putting breaks on Web Application attacks**
9. **Mozilla Firefox as a Hacking tool**

10. **Bypassing Proxy – Intermediate**
11. **Using Google as Proxy**
12. **Remote File Inclusion for Opening Blocked Websites**
13. **Creating your Own Proxy Server**

Attacks on web applications are always harmful since they give the company a bad image. A successful attack can have any of the following consequences:

- Website defacement;
- Stolen information;
- Modification of data, and particularly modification of users' personal data
- Web server intrusion.

[7.] *Software Reverse Engineering and Attacks on Demand* *3 Hours*

Software Reverse Engineering (SRE) is the practice of analyzing a software system, either in whole or in part, to extract design and implementation information. A typical SRE scenario would involve a software module that has worked for years and carries several rules of a business in its lines of code. Unfortunately the source code of the application has been lost; what remains is “native” or “binary” code. Reverse engineering skills are also used to detect and neutralize viruses and malware, as well as to protect intellectual property. It became frighteningly apparent during the Y2K crisis that reverse engineering skills were not commonly held amongst programmers.

1. **What is Reverse Engineering**
2. **Software – Definition**
3. **Disassembling the Software's**
4. **Software Cracking & Serial Key Phishing**
5. **Software Patching**
6. **Applying Application Security**
7. **Attacks on Demand**

Since that time, much research has been undertaken to formalize just what types of activities fall into the category of reverse engineering so that these skills could be taught to computer programmers and testers. To help address the lack of software reverse engineering education, several peer-reviewed articles on software reverse engineering, re-engineering, reuse, maintenance, evolution, and security were gathered with the objective of developing relevant, practical exercises for instructional purposes. The research revealed that SRE is fairly well described and most of the related activities fall into one of two categories: software development-related and security-related.