Name of Course	Applied Cybersecurity Track
PRELIMINARY SKILLS - (PREREQUISITES & PROGRAMMING)	• Module 1: Introduction to Pentesting and Information Security • Module 2: Networking • Module 3: Bash Scripting • Module 4: Web Applications
Lessons	**Outline**
Module 1: Introduction to Pentesting and Information Security	In this module, we will answer fundamental questions like: What is Information Security? Who are penetration testers? How do they perform their tasks? What methodology do they follow? Skills and methodology are what differentiate a real professional from an amateur. This module also explains what methodology to use during an engagement, from the initial engaging phase to the final reporting and consultancy phase. • Introduction to Information Security • nformation Security Attacks and Information Security Controls • Hacking Concepts • Introduction to Penetration Testing • Lifecycle of a Penetration Test • Engagement, Information Gathering, Footprinting and Scanning, Vulnerability Assessment, • Exploitation and Reporting. • Examples of the Vulnerability • Red Team && Blue Team • Capture The Flag (CTF)
Module 2: Networking	This module provides a broad overview of networking, covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective. This module focuses on the various protocols used at each layer, with a particular focus on the Networking layer.

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 2: Networking	• Network • Types Of Network • Network Topologies • The 7 Layers Of The OSI Model • Layer 7 - Application • Layer 6 - Presentation • Layer 5 - Session • Layer 4 - Transport • Layer 3 - Network • Layer 2 - Data Link • Layer 1 - Physical
Module 3: Bash Scripting	• Introduction to Bash • Linux commands • Linux File Permissions • Programming using Bash • Variables and Read from user • Shell Programming - Arithmetic Operators
Module 4: Web Applications	Web Applications are more complex and pervasive than what many think; this module explains the protocols and technologies behind web applications and prepares students for web application penetration testing topics. Students will learn how to study a web application and use the information collected to mount attacks. • Introduction • HTTP Protocol Basics • HTTP Cookies • Sessions • Same Origin Policy • Burp Suite

Name of Course	Applied Cybersecurity Track
PENETRATION TESTING	• Module 5: Reconnaissance & Information Gathering • Module 6: Footprinting and Scanning • Module 7: Advanced Scanning Techniques • Module 8: Vulnerability Assessment • Module 9: Network Attacks • Module 10: Anonymity • Module 11: System Attacks • Module 12: Web Attacks • Module 13: Next Steps • Module 14: Penetration Testing and Capture the Flag Labs
Lessons	**Outline**
Module 5: Reconnaissance & Information Gathering	Information gathering is the most important phase of the overall pentesting engagement. A penetration tester will use the information collected during this phase to map the attack surface and increase their chances to breach the organization in the same way criminals do. Students will see how to use different sources to perform the information gathering phase. • Information Gathering Introduction • Types of Information Gathering • Open-Source Intelligence (OSINT) • Advanced Google Hacking Techniques • Search Engines and Advanced Google Search Operators • Social Networks Information Gathering and Social Engineering • Public Sites Information Gathering • Metadata, METAGOOFIL and theHarvester • Infrastructure - Domain • WHOIS • DNS Enumeration • SHODAN and Maltego • Subdomain Enumeration • The Importance of Information Gathering

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 6: Footprinting and Scanning	This module covers infrastructural information gathering. Remotely identifying operating systems, server applications, and clients is of paramount importance to widen the attacksurface and prepare the penetration tester for the vulnerability assessment activity and the following exploitation phase. • Network Discovery and Mapping • Scanning Goals and Types • Mapping a Network • Why Map a (Remote) Network • Network sweeping • Ping Sweeping • Nmap Ping Scan • Network Fingerprint • Possibly identify operating system • Active Fingerprinting - Passive Fingerprinting • Network Scanning • Port Scanning (TCP Port Scanning - UDP Port Scanning) • Services Scanning (Nmap - Metasploit - Netcat)
Module 7: Advanced Scanning Techniques	This module, We are going to look at some more advanced Nmap commands.Sometimes it is necessary to perform scans that will do something other than the TCP scan that Nmap is doing by default. Those more advanced commands are used to detect exotic services or to evade firewalls. • Wireshark for the Pen Tester • Firewall / IDS Evasion Techniques • Timing Options • Bypass by Fragment Packets • Bypass Firewall by Specify a Specific MTU • Bypass by Decoys • Bypass by Source Port Number Specification • Bypass by Append Random Data • Bypass by Send Bad Checksums • Bypass by Idle Zombie Scan

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 8: Vulnerability Assessment	Vulnerability Assessment is the process through which a penetration tester uncovers all the vulnerabilities in a computer system or application. This module explains how vulnerability assessment can be carried out using automatic tools or manual investigation. • Vulnerability Assessment • Vulnerability Scanners • Manual Testing • Nessus • OpenVAS • NMAP Scripting Engine • Under the Hood of a Vulnerability Scanner • Port Scanning • Service Detection • Vulnerabilities Database Lookup
Module 9: Network Attacks	This module provides a comprehensive explanation of the most common and historical remote attacks. Students will learn attacking techniques against authentication services,Windows file sharing, and network devices. Every attacking technique can be tested in a hands-on lab. The last two chapters explain in theory and practice, how to use Metasploit and Meterpreter to automate attacks and penetration testing techniques. **9.1 Authentication Cracking** • Brute Force vs. Dictionary Attacks • Weak and Default Credentials • Installing Dictionaries • Authentication Cracking Tools • Hydra • Telnet Attack Example • HTTP Basic Auth Attack Example

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 9: Network Attacks	**9.2 Windows Shares** • NetBIOS • Shares • UNC Paths • Administrative Shares • Badly Configured Shares **9.3 Null Sessions** • Enumerating Windows Shares • Checking for Null Sessions • Checking for Null Sessions with Windows • Checking for Null Sessions with Linux • Exploiting Null Sessions **9.4 ARP Poisoning** • ARP Poisoning Actors • Gratuitous ARP Replies • Forwarding and Mangling Packets • Local to Remote Man-in-the-Middle • Dsniff Arpspoof **9.5 Metasploit** • MSFConsole • Identifying a Vulnerable Service • Searching • Configuring an Exploit • Configuring a Payload • Running an Exploit **9.6 Meterpreter** • Bind and Reverse • Launching Meterpreter • Sessions • Information Gathering with Meterpreter • System Information • Network Configuration • Routing Information • Current User

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 9: Network Attacks	**9.7 Privilege Escalation** • Bypassing UAC • Dumping the Password Database • Exploring the Victim System • Uploading and Downloading files • Running an OS Shell **9.8 Antivirus Evasion**
Module 10: Anonymity	• Using of Anonymity During Testing of Networks • Browsing Anonymously • HTTP Proxies • ProxyChains • Tunneling for Anonymity • SSH Tunneling
Module 11: System Attacks	From malware, through password cracking attacks, up to buffer overflows, students will learn the most common attack vectors used against computer systems nowadays, as well as which malware they can use during an engagement. In the Password Attacks, we explain how to recover passwords from a compromised machine. Then, we conclude this module with an entire chapter dedicated to buffer overflows, one of the most used attack vectors against applications and operating systems. **11.1 Malware** • Viruses • Trojan Horses • Backdoors • Firewalls vs. Backdoors • Firewalls vs. Connect-back Backdoors • Rootkits • Bootkit • Adware • Spyware • Greyware • Dialer • Keylogger • Hardware Keyloggers • Rootkit Keyloggers • Bots • Ransomware • Data-Stealing Malware • Worms

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 11: System Attacks	**11.2 Password Attacks** • Cryptography • Types of Cryptography • Password Attacks • Dictionary Attacks • Installing Password Dictionaries • Brute Force Attacks and Algorithm • Crack Hash By John The Ripper • Hash-Identifier • Hash Type is used by GNU/Linux and Windows • Crack Linux Hash and Windows Hash By John The Ripper • Rainbow Tables • Ophcrack Tool to Crack Hash Windows • Network Service Attack By Hydra Tool • Pass The Hash Attack **11.3 Buffer Overflow** • How to Hack any Application in the World ? • Understand the Computer Working • Stack Buffer Overflow • Buffer Overflow Attacks • Buffer Overflow Example • How Buffer Overflow Attacks Work

Name of Course	Applied Cybersecurity Track
Lessons	**Outline**
Module 12: Web Attacks	This module dissects and explains the most widespread web application vulnerabilities. Students will study the most common web application attacks, starting from the information gathering phase to the exploitation phase. Additionally, students will learn how to perform attacks manually and then learn how to automate them by utilizing the most commonly used tools. • Introduction • Web Server Fingerprinting • HTTP Verbs • Directories and File Enumeration • Google Hacking • Cross-Site Scripting • SQL Injections
Module 13: Next Steps	This module is a summary of the course. It contains useful advice and information about how to continue learning in the field of IT Security in the most efficient way. Also, students can test their skills against special lab challenges, which are very similar to real-life penetration testing scenarios.
Module 14: Penetration Testing and Capture the Flag Labs	