

CYBER SECURITY TRAINING BROCHURE

IGNITE TECHNOLOGIES

Academy for Hackers



"We do not provide just knowledge; rather, we train you to use your knowledge to become a PROGAURD for an organization"

About Company

Our aim at the IGNITE TECHNOLOGIES Institute is to provide businesses military, organizations, and government bodies with cutting-edge information security knowledge and skills necessary to defend their people and assets.

IGNITE offers more than 15 distinct courses, all of which are aligned with the most prevalent security team roles, responsibilities, and disciplines. Our courses equip students to deal with today's risks and tomorrow's difficulties.

Background

Our students are placed in the MNC and are capable of executing fantastic jobs safeguarding the organization's and clients' networks' security posture. Ignite Certified students were able to earn Hall of Fame status from organisations such as Facebook, Twitter, Swiggy, and Uber.

OBJECTIVE

IMPROVE THE RESISTANCE OF YOUR DEFENSIVE CAPABILITY TO SOPHISTICATED CYBER-ATTACKS.

At Ignite Technologies we aim to train students in attack and defence techniques in the cyber security domain. It will allow you to obtain the knowledge and expertise to evaluate, design and build secure computer systems, processes and people that are involved in cyber security. It covers the theory and practice of designing and building secure systems and gives you a firm grounding in cryptography, network security and secure programming, as well as optional modules in topics such as hardware and cloud security, operating systems and incident management and forensics.

With increasing awareness and concern over the growing cyber threats facing organizations, governments and individuals alike, many universities and colleges have created new graduate degree programs in cybersecurity.

Companies including Microsoft, Vodafone, E&Y, KPMG, IBM and Adobe come onto campus for placement drive.

Tech giants like Google, Microsoft, Facebook, and others offer bug bounties to people who can hack their software and help them fix security flaws. In 2019, for example, Tesla offered 900,000 USD and a free car to anyone who could hack their Tesla Model 3.

CYBERSECURITY FAST FACTS

- Every minute, \$17,700 is lost due to phishing attacks.
- 94% of malware is delivered via email.
- 63% of companies said their data was potentially compromised within the last year.
- 60% of data breaches involve vulnerabilities that could have been avoided if an available security update or patch had been applied.

TRAINING PROGRAM LEVELS



■ Ethical Hacking, Bug Bounty,
Infrastructure Pentest, Wireless Hacking

LEVEL 1

■ API security Assessment, Android
Application pentesting, Advanced
Burp Suite, Capture the Flags

LEVEL 2

■ Privilege Escalation, MITRE Red Team,
Active Directory, MSSQL Security
Assessment

LEVEL 3

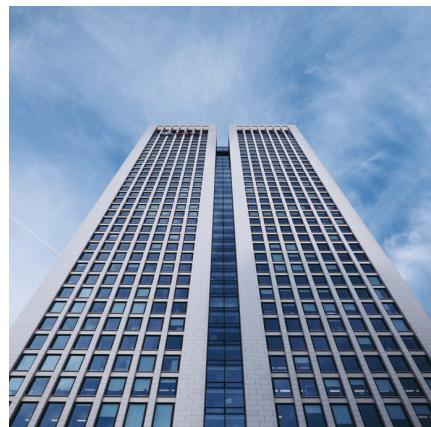
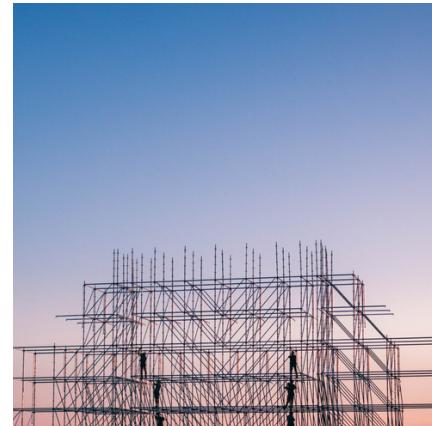
TIMEFRAME

2022 TO 2023

LEVEL 1- Beginners + Professional

At this level, the applicant will learn the fundamentals of cyber security, IT infrastructure, application and network design, and secure implementation and configuration.

120 +
Hours



LEVEL 3- EXPERT

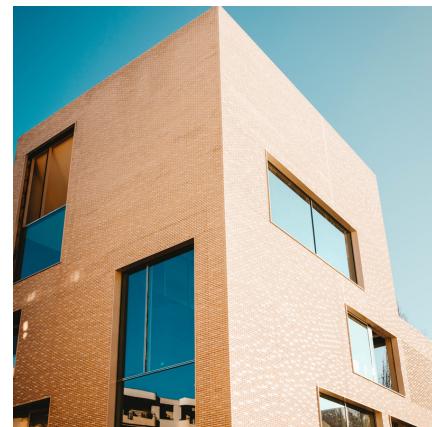
At this level, the candidate will develop an expert understanding of how to evaluate business risk consequences produced by a threat following exploitations, threat modelling, and hunting for indicators of compromised systems.

90+
Hours

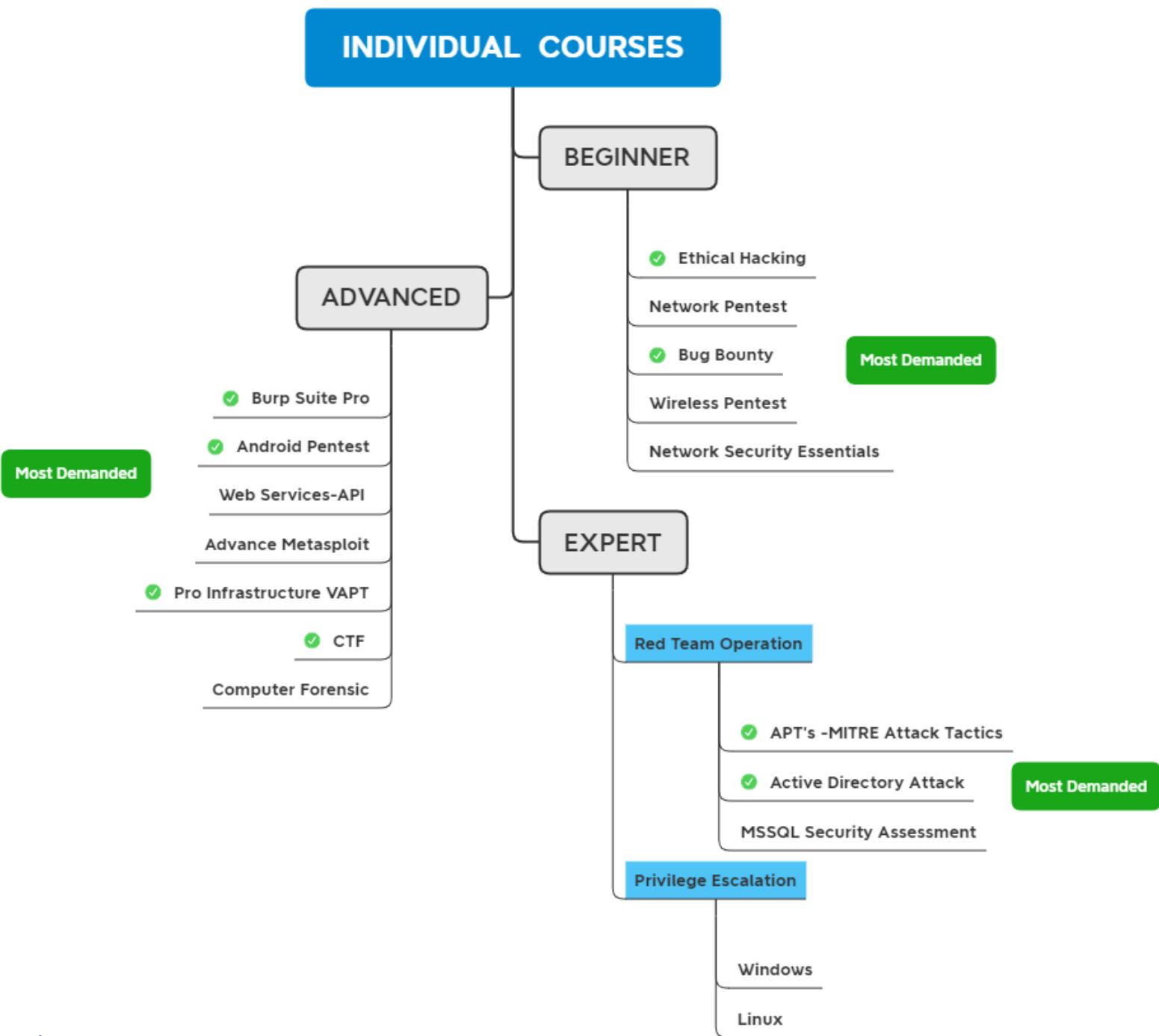
LEVEL 2- ADVANCED

At this level, the applicant will acquire additional hands-on approaches based on industry requirements for identifying key vulnerabilities and bugs in IT networks and applications.

100+
Hours



ALL COURSES



TRAINING FRAMEWORK

OWASP

The Open Web Application Security Project (OWASP) is a "best practice" penetration testing framework that users can implement in their own organizations and a "low level" penetration testing guide that describes techniques for testing most common web application and web service security issues

NIST

NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks. A 2016 study found that 70% of organizations surveyed see the NIST Cybersecurity Framework as a popular best practice for computer security.

MITRE ATT&CK

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

IN 2019, THE VALUE OF THE HEALTHCARE CYBERSECURITY MARKET WAS 9.78 BILLION AND THIS IS PROJECTED TO RISE TO \$33.65 BILLION BY 2027

(GLOBENEWSWIRE, 2020)

WHY TO CHOOSE US?

- Ignite Technologies trainers are experts in conducting proactive live training sessions
- Simulate a real-time scenario to mimic real-time threat and risk impact.
- Focused on personalized training as per individual skills.
- Less than 10 students in a group
- Ignite offers 1-year Diploma course that has more than 2000 practical sessions.
- Job Assurance for Diploma Holders
- Experience in training 10000+ students around the globe
- Community of more than 50,000+ individuals
- Ignite is highly adaptable in offering Online, weekend, and weekday programs according to students' available time windows.
- Ignite provides free access to the Ignite library, which contains a variety of e-books and lab manuals.
- After completing Ignite's Level 1 program, they were awarded a scholarship for Level 2.
- Ignite offered a Diploma and Postgraduate Diploma in Cyber Security to applicants who completed ALL levels of Training.
- Ignite Provided Diploma and PG Diploma Holders with 6-Month or 1-Year Training and Internship Letters.



SCHOLARSHIP PROGRAM

Ignite encourages your interest in hacking with its scholarship programme. Candidates enrolled in the Level 1 Program are eligible to participate in the Level 2 Scholarship Program.

Level 2 is comprised of Advanced Topics that enable candidates to conduct more thorough Penetration Testing on a network, web application, Web API sockets, and Android.

In addition, Level 2 focuses on Capture the Flag training in order to provide candidates seeking industry-recognized certification with hands-on training.

Scholarship Criteria for Level 2 Program

PARTICIPANTS	SCORE	DISCOUNT
Winner	100	100%
1st Runner-up	85	50%
2nd Runner-up	75	25%

ETHICAL HACKING

By opting to pursue this course, you will learn the fundamentals of hacking, penetration testing, network security, web application security, wireless security, auditing and much more.

Prerequisites: Basic in Computer and Networks (Optional)

System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

M1-Introduction
M2-OLD School Learning
M3-Basic of Networks
M4-Recon- Foot printing
M5-Recon- Network Scanning
M6-Recon – Enumeration
M7-System Hacking
M8-Post Exploitation & Persistence
M9-Webservers Penetration Testing
M10-Website Hacking

M11-Malware Threats
M12-Wireless Networks Hacking
M13-Cryptography & Steganography
M14-Sniffing Attack
M15-Denial of Service
M16-Evading IDS, Firewalls & Honey Pots
M17-Social Engineering
M18-Hacking Mobile Platforms

 DOWNLOAD

Durations: 32 Hours

NETWORK PENTESTING

This course has been devised to upskill the security competency of an IT professional/individual by imparting knowledge on the basics as well as advanced concepts of Network Security & Organizational Infrastructure. One of the benefits of opting for this course is the flexibility of the course structure which allows even an individual with little to no technical skills to easily grasp the knowledge.

Prerequisites: Candidate should be aware of Ethical Hacking (Optional)

System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

M1-Introduction Network Security
M2-Penetration Testing Framework
Kali Linux
M3-Analyzing Network Traffic
M4-Packet Analysis with Tshark
M5-Detecting Live Systems and
Analyzing Results
M6-Nmap Advance Port Scan
M7-Metasploit Framework
M8-Dictionary & Passwords Attacks
M9-FTP Penetration Testing
M10-SSH Penetration Testing
M11-Telnet Penetration Testing
M12-SMTP Penetration Testing
M13-DNS & DHCP Pentesting
M14-NetBIOS & SMB Penetesting

M15-MySQL Penetration Testing
M16-Remote Desktop Penetration Testing
M17-VNC Penetration Testing
M18-Credential Dumping
M19-Socks Proxy Penetration Testing
M20-Sniffing & Spoofing
M21-DOS Attack Penetration Testing
M22-Covering Tracks & Persistence
M23-Honeypots
M24-Firewall
M25-Intrusion Detection System
M26-Vulnerability Assessment Framework

 DOWNLOAD

Durations: 32 Hours

BUG BOUNTY

Companies sponsor bug bounty programmes to allow security researchers and pentesters from all over the world to prove their abilities and uncover weaknesses in their websites. Depending on the severity of the bug reported, they are either compensated or recognised as a token of appreciation.

This course will build an understanding of application security vulnerabilities and penetration testing.

Prerequisites: Know about Ethical Hacking. Additionally, the candidate should be familiar with frontend and backend web development concepts (optional).

System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

M1-Introduction to WAPT & OWASP	M12-OS Command Injection
M2-Pentest Lab Setup	M13-Open Redirect
M3-Information Gathering & Reconnaissance	M14-Unrestricted File Upload
M4-Netcat For Pentester	M15-PHP Web Shells
M5-Configuration Management Testing	M16-HTML Injection
M6-Cryptography	M17-Cross-Site Scripting (XSS)
M7-Authentication	M18-Client-Side Request Forgery
M8-Session Management	M19-SQL Injection
M9-Local File Inclusion	M20-XXE Injection
M10-Remote File Inclusion	M21-Bonus Section
M11-Path Traversal	

 DOWNLOAD

Durations: 32 Hours

ADVANCED BURP SUITE

Bug Bounty without Burp Suite? Is it even possible? That is completely out of the question!! Testing for vulnerabilities in web applications is currently regarded as one of the most important subfields within the broader domain of information security. However, within all of this, Burp Suite plays a significant part. Whether it's a basic web application scan or the exploitation of the vulnerabilities that have been uncovered, burp suite can handle it all.

The course's holistic framework and real-world practice with Burp Suite Professional Edition's Basic to Advanced features make it a worthwhile investment. The training is meant for both beginners and professionals who wish to improve their Web-Application Penetration Testing skills.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty

System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

M1-Introduction to Burp Suite

M2-Burp Suite Fundamentals

M3-Burp Suite's Vulnerability Scanner

M4-Advanced Fuzzing

M5-The Burp Collaborator

M6-The Burp's Hack Bar

M7-Top 10 Vulnerability Plugins

M8-Burp Suite Encoder & Decoder

M9-Payload Processing

M10-Engagement Tools

 DOWNLOAD

Durations: 20 Hours

ANDROID PENTESTING

This course will focus on code-level security, which means that you will now understand the working of codes on the backend of the mobile applications and then be able to determine the type of attacks that can be performed on the application. The information gained from performing the pentests can help devise proper mitigation strategies to secure the Android applications.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty

System Configuration: 8 GB RAM & i5 Processor

TABLE OF CONTENTS

M1-Basic Understanding & Lab Setup

M2-Android Application Static Testing

M3-Android Application Dynamic Testing

M4-Android Application Web & API Testing

 DOWNLOAD

Durations: 25 Hours

INFRASTRUCTURE VULNERABILITY ASSESSMENT & PENETRATION TESTING

Infrastructure penetration testing is discovering and probing vulnerabilities and faults in computer systems and devices connected to a network, cloud, or Servers. It is the process of discovering security vulnerabilities in an organization's security framework.

Typically, it is performed in conjunction with other approaches, such as External, Internal, Wireless, Cloud, and Virtualization Penetration Testing.

This course will instruct you on how to construct secure networks and systems for an organization's infrastructure.

Prerequisites: Candidate should be aware of Ethical Hacking

System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

- M1-Pre-engagement Interactions
- M2-Internal & External Penetration Scanning
- M3-Application Server Mapping
- M4-Linux for Pentester
- M5-Windows for Pentester
- M6-Microsoft Database Penetration Testing
- M7-Docker for Pentester
- M8-Network Device Security Audit
- M9-Android Pentesting

 DOWNLOAD

Durations: 50 Hours

CAPTURE THE FLAG (CTF)

Capture the Flag is an information security competition that is an amalgamation of various challenges that applies concepts like Reverse engineering, Web Applications, Binary, Network, Cryptography, Forensics, etc. Each challenge holds a certain number of points based on its difficulty level. The idea behind these CTFs is to provide an individual with practical knowledge of the different kinds of attacks and issues in the real world.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty

System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

- M1-Introduction
- M2-Linux for Pentester
- M3-Windows for Pentester
- M4-Kali Linux
- M5-Enumeration
- M6-Port Scanning with Nmap
- M7-Web Based Attack
- M8-Passwords Attack
- M9-Active Directory Attack
- M10-Powershell Empire
- M11-Port Forwarding & Tunneling
- M12-Pentesting Tools
- M13-File Transfers

- M14-Introduction to Overflows
- M15-Windows Buffer Overflow
- M16-Vulnerability Scanning
- M17-Finding Public Exploits
- M18-CTF Bonus Section
- M19-Exploiting Container| CI | CMS
- M20-Linux Privilege Escalation
- M21-Windows Privilege Escalation
- M22-Capture the Flag Challenges
- M23-Finding Public Exploits
- M24-Bonus Section

 [DOWNLOAD](#)

Durations: 45 Hours

APT'S MITRE ATTACK

RED TEAM TACTICS

To help organizations assess the scale and level of preparedness for a cyberattack, Red Team Operations simulates a meticulously orchestrated cyberattack. In-depth testing of an organization's detection and response capabilities over a long period of time

The training includes attacker simulators and attack frameworks like Cyber Kill Chain, Attack Tree, and MITRE ATT&CK Framework. Candidates can act as an adversary and use local tools to achieve corporate goals while avoiding detection. The training also focuses on using open-source tools and scripts and customizing them to meet an organization's needs.

Prerequisites: Candidate should be aware of Ethical Hacking & Bug Bounty

System Configuration: 16 GB RAM & i7 Processor

TABLE OF CONTENTS

- M1 Introduction
- M2 Initial Access & Delivery
- M3 Weaponization to Obfuscate Payload
- M4 Command & Control
- M5 Escalate Privileges
- M6 Credentials Dumping

- M7 Active Directory
- M8 Lateral Movement
- M9 Establishing Persistence
- M10 Data Exfiltration
- M11 Defense Evasion
- M12 Reporting

 [DOWNLOAD](#)

Durations: 50+ Hours

ACTIVE DIRECTORY ATTACK

RED TEAM TACTICS

Professionals who want to learn about the most common risks can benefit from this course. To begin, you'll do a sneak reconnaissance and enumeration of hosts, servers, services, and privileged users to identify them. To wrap things up, you will learn how to conduct red team attacks on Active Directory by targeting common misconfigurations and leveraging genuine Windows/Active Directory features.

Prerequisites: Candidate should be aware of Ethical Hacking

System Configuration: 16 GB RAM & i7 Processor

TABLE OF CONTENTS

- M1 Introduction to AD and Domain Network
- M2 Initial AD Exploitation
- M3 Active Directory Post Enumeration
- M4 Abusing Kerberos Authentication
- M5 Domain Persistence
- M6 Privilege Escalation
- M7 Lateral Movement
- M8 Bonus Section

 DOWNLOAD

Durations: 30+ Hours

MSSQL SECURITY ASSESSMENT

RED TEAM TACTICS

This Security Assessment will examine SQL Server instance discovery, inadequate configuration auditing, and privilege escalation at scale. Penetration testers and red teams are the primary targets of this operation. However, manual assessment supports a number of methods that administrators may utilise to inventory the SQL Servers in their ADS domain.

Additionally, a company can use this approach to define the risk factor and ensure compliance with information security policies. They can also use it to assess their level of reaction to any cyber-based threats.

Prerequisites: Candidate should be aware of Ethical Hacking

System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

- M1-LAB SETUP
- M2-Enumeration
- M3-Privilege Escalation
- M4-Database Link Abuse
- M5-Gaining Access
- M6-Command Execution
- M7-Persistence

 [DOWNLOAD](#)

Durations: 20+ Hours

WINDOWS PRIVILEGE ESCALATION

The Privilege Escalation Training curriculum consists of approaches that help students comprehend how an adversary gains access to higher-level privileges on a system or network. A network's adversaries are often able to go around within the system without proper credentials.

As part of your cybersecurity strategy, this course explains how to protect user accounts in your systems and web application.

Prerequisites: Candidate should be aware of Ethical Hacking

System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

- M1-Introduction & Lab Setup
- M2-Exploiting Scheduled Tasks
- M3-Weak Services/Permissions
- M4-Kernel Exploits
- M5-Logon Autostart Execution
- M6-Passwords Hunting
- M7-Bypass ACL
- M8-Automated Tools

 DOWNLOAD

Durations: 20+ Hours

LINUX PRIVILEGE ESCALATION

The Privilege Escalation Training curriculum consists of approaches that help students comprehend how an adversary gains access to higher-level privileges on a system or network. A network's adversaries are often able to go around within the system without proper credentials.

As part of your cybersecurity strategy, this course explains how to protect user accounts in your systems and web application.

Prerequisites: Candidate should be aware of Ethical Hacking

System Configuration: 12 GB RAM & i5 Processor

TABLE OF CONTENTS

M1-Linux Fundamental

M2-Writable Files

M3-Misconfigured NFS

M4-Abusing Sudo Rights

M5-SUID Binaries

M6-Capabilities

M7-Groups

M8-Exploiting Cron jobs

M9-Kernel Exploit

M10-Automated Script

M11-Shell Escaping

M12-Password Hunting

 DOWNLOAD

Durations: 20+ Hours

Contact US



PHONE

📞 +91-9599387841 | +91 11 4510 3130

WHATSAPP

💬 <https://wa.me/message/HIOPPNENLOX6F1>

OFFICE

📍 26, Pusa Rd, Block 1, WEA
Karol Bagh, New Delhi, 110005



EMAIL ADDRESS

✉️ info@ignitetechnologies.in

WEBSITE

🌐 www.ignitetechnologies.in

BLOG

🌐 www.hackingarticles.in

LINKEDIN

🌐 <https://www.linkedin.com/company/hackingarticles/>

TWITTER

🐦 <https://twitter.com/hackinarticles>

GITHUB

<https://github.com/Ignitetechnologies>