BLACK BEAR
ACADEMY

Certified Pentester

This course is not your traditional ethical hacking training program. Lessons range from in country laws and regulations showcasing the importance of VAPT towards driving compliance. Build your own infosec team and strategically position VAPT as part of your Red Team initiatives. Review your gaps by assessing your own security controls to actual hands on by penetrating into systems using our virtual labs. Determine your organization's future state by participating in workshops about threat modeling and maturity models.

Agenda:

This course provides participants with the essential skills and knowledge to conduct thorough network and web application penetration tests. It emphasizes core concepts, effective methodologies, vulnerability identification, and exploitation techniques using industry-standard tools. The training also covers planning, scoping, and reporting VAPT engagements while applying best practices in practical, real-world scenarios.

Audience:

- Network Administrators
- Security Analysts
- IT Security Professionals
- Penetration Tester Enthusiast
- Individuals preparing for ethical hacking certifications
- Anyone interested in network and web application security testing

Course Qualifications:

- Basic understanding of networking and operating systems (Linux and Windows)
- Familiarity with common cybersecurity concepts
- Experience with command-line tools (optional but beneficial)
- Prior exposure to programming or scripting (helpful, but not required)
- Interest in ethical hacking, penetration testing, or cybersecurity roles

Day 1: Introduction and Foundation

1. **A Day in the Life of an Ethical Hacker**
   Gain insights into the daily activities, responsibilities, and mindset of an ethical hacker. Understand the challenges and rewards of working in cybersecurity.

2. **What is VAPT?**
   Explore the concepts of Vulnerability Assessment and Penetration Testing (VAPT), including their significance in maintaining cybersecurity and compliance.

3. **Basics Overview**
   Review foundational concepts of basic networking, Linux, and web applications. This includes understanding IP addressing, subnetting, network protocols (TCP/IP, DNS, HTTP/HTTPS), and network devices (routers, switches, firewalls). Learn Linux fundamentals such as file system navigation, command-line tools, permissions, process management, and scripting basics. Additionally, cover the basic structure and functionality of web applications, including HTTP methods, sessions, and cookies.

4. **Planning and Scoping**
   Learn the critical steps involved in planning and scoping a VAPT engagement, including defining objectives, understanding client requirements, and setting boundaries for both network and web application testing.

Day 2: Methodologies and Tools

5. **Methodology | Phases**
   Understand the structured phases of VAPT, including reconnaissance, scanning, exploitation, post-exploitation, and reporting. Both network and web application methodologies will be discussed.

6. **Information Gathering**
   Discover techniques for collecting valuable data about targets using open-source intelligence (OSINT) and other information-gathering tools. This will include identifying technologies and infrastructure used in both networks and web applications.

7. **Vulnerability Assessment**
   Delve into methods for identifying and assessing vulnerabilities in systems, including automated scanning and manual analysis. Techniques applicable to both network and web application environments will be covered.

8. **Vulnerability Identification**
   Learn how to categorize and prioritize vulnerabilities based on their risk level, potential impact, and exploitability. This includes network vulnerabilities like open ports and services, as well as application vulnerabilities such as insecure inputs.

Day 3: Hands-On Practice and Reporting

9. **Attacks and Exploits**
   Explore common attack vectors and exploitation techniques used by ethical hackers. Both network-level and application-level attacks will be demonstrated, including exploiting misconfigurations and vulnerabilities.

10. **Penetration Testing Tools**
    Get hands-on experience with popular penetration testing tools and frameworks for both network and application testing. Tools like Nmap, Burp Suite, and Metasploit will be included in practical exercises.

11. **Report and Communication**
    Understand the importance of clear and concise reporting in VAPT. Learn how to document findings, provide remediation advice, and communicate results to stakeholders in a comprehensive manner.

12. **Certification**
    Review the various certifications available for ethical hackers and VAPT professionals and discuss the value they add to a cybersecurity career.

Certification Exam:

- The exam environment will be accessed via VPN.
- The exam will follow a black-box approach.
- The exam must be completed within a 4-hour window.