iGNITE Technologies

INFRASTRUCTURE

Penetration Testing

INFRASTRUCTURE
Penetration Testing

This is exclusive training provided by Ignite technologies worldwide to provide realistic exposure for Vulnerability Assessment and Penetration Testing as per Industry requirements.

A detailed, step-by-step penetration testing technique that is well-known in the industry is included with the training. This enables a learner to enhance their capacity for using new abilities acquired through rigorous practical workshops and challenges.

The course will complete a focused manual Penntesting to identify the logical threats that cannot be identified by automated tools.

Designed based on the most common penetration testing services provided by the penetration testing service providers and consulting firms in the market including Network, Application, Android, Database, Docker, and CTFs.

To become a Red Teamer the candidate should be capable of penetrating the target environment the infrastructure VAPT course is a step towards it. It's a bridge between ethical hackers and Red Teamers.

iGNITE Technologies

HOW WE FUNCTION

TRAINING TYPE

Type 1

A GROUP SESSION will have a maximum of 10 candidates.

Pros: 1) Less Expensive than Type 2. 2) Get a chance to build connections across the world.

Type 2

A PERSONALISED SESSIONS will one-on-one session

Pros: Flexible slot as per candidate availabilities.

iGNITE Technologies

iGNITE Technologies

WHAT YOU WILL ACHIEVE

OUR FOCUS

- Level up all candidates from the various domains to make the curriculum cohesive.
- Learn Techno Commercials and Secure Implementation of Servers, Network Devices & Applications.
- Give the hands-on experience of Real-Time Pentesting .
- Meet The Business Standards of Report Deliverables Maintain the security posture by adhering to industry best practices.
- Work-in Professional Red Teamers and Pentesters around the world will be conducting all sessions live.
- Follow OWASP and NIST standards for how to respond to the attack.

And Much More.....

WHO CAN ?

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide realtime exposure.
- Get a training certificate of participation.

PREREQUISITES

In order to initiate the vulnerability Assessment & pen-testing Training, the Candidate should be aware of the basic concepts of Ethical Hacking. This course is for beginners and needs to know setting up vmware and kali linux

COURSE DURATION: 45 HOURS

INFRASTRUCTURE ROADMAP

Module 1

Rule of Engagement

Module 2

Internal & External Network Pentest

Module 3

Web Application Pentest

Module 4

Windows for Pentester

Module 5

Linux for Pentester

Module 6

MSSQL Grey Box Testing

Module 7

Network Device security Aduit

Module 8

Android Pentesting

Bonus Section
Advance Nmap
Advanced Metasploit

FREE SESSION DOCKER CONTAINER SECURITY

iGNITE Technologies

MODULE 1

Rule of Engagement

The Rules of Engagement (RoE) is a document that outlines how the penetration test should be carried out. Before beginning the penetration test, certain guidelines that should be included in RoE are as follows:

Learning Objectives

- Establishing Goals, Objectives, and Deliverables for Penetration Testing Engagement
- Scoping Technical Aspects of the Engagement and Questionnaires
- Outlining Scope for Lines of Business, Third Parties, and Structuring Compensation and Metrics For Time Estimation
- Establishing Communication Plans and Engagement
- Standards Of Operations
- Testing Check List
- Standard Business VAPT Report. (Executive and Technical)

MODULE 2

Internal and External Network Pentest

There are several factors that might warrant an internal and external network penetration study for your firm or organisation. Reducing and perhaps even minimising the adverse effects on your information assets is the main goal. An unscrupulous hacker will locate and take advantage of a flaw in your network if they have enough time, sophisticated tools, and expertise.

A penetration test is a comprehensive, expert-driven procedure designed to find all potential entry points that an attacker may use to access the network. It detects not only the vulnerabilities but also the possible harm.

iGNITE Technologies

Learning Objectives

- Strategically Approach of Network VAPT
- Information Gathering
- Map The Internal Network
- Utilization of Nmap in Expert Mode
- VAPT of Well Know Ports
- OS & Service Fingerprinting
- Man-in-the-Middle Attack
- Hands-on Ideal Vulnerability Assessment Tools
- Network Report Writing by defining real risk impact with CVSS and CWE

MODULE 3

Web Application Pentest

Web application penetration testing is a systematic process that includes a number of phases with the goal of learning about the target system, identifying its flaws or vulnerabilities, and looking into potential exploits that might take advantage of those flaws or vulnerabilities to breach the web application.

Learning Objectives

- OWASP Top 10 and WSTG Testing Guide, Principal of testing and approach.
- Manual Vulnerability Assessment with Burp Suite and OWASP ZAP
- Information Gathering and Application Fingerprinting
- Configuration and Deployment Management Testing
- Code Injection Testing-OS, SQLi, XSS, LFI and etc.
- Automated Vulnerability Scanning and Fuzzing
- SSL/TLS Security Testing
- Web Report Writing by defining real risk impact with CVSS and CWE
- Challenge 1: CMS Penetration Testing
- Challenge 2: Web Server Hacking

iGNITE Technologies

MODULE 4

Windows for Pentester

During the threat modelling phase, the organisation may engage a pentester to do authenticated testing in order to verify an account's authorization and identify internal threats brought on by illegal access. The teacher will concentrate on internal threats throughout the lesson and attempt to map the threats by providing CTFs to enhance the expertise.

Learning Objectives

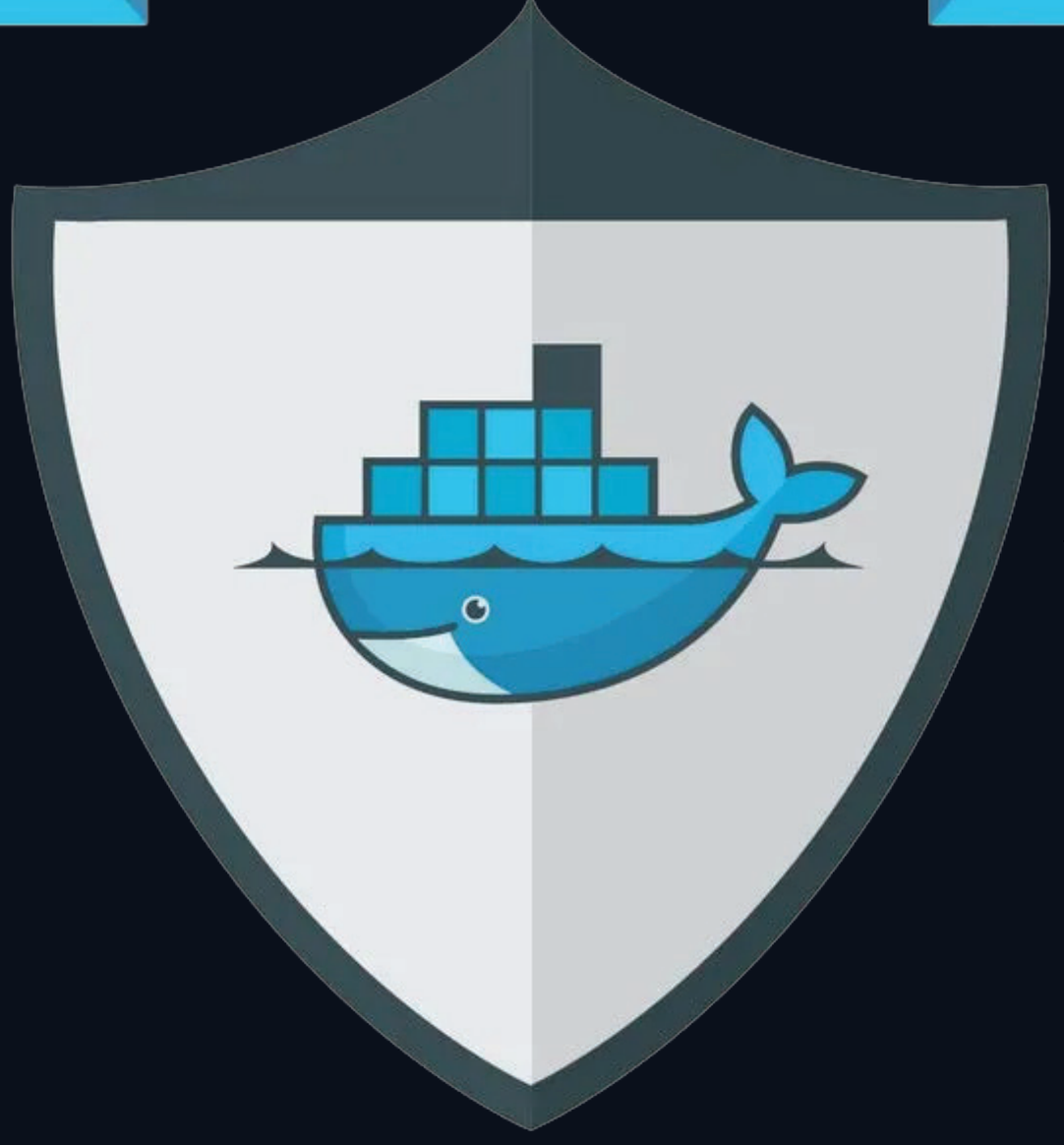
- Remote Connection via SMB in multiple methods.
- Pentesting with PowerShell Empire
- Bypasses Whitelisting Programs
- Reporting Dangerous Misconfiguration
- Privilege Escalation-Automated Script
- Privilege Escalation-Manual
- Lateral Movement

iGNITE Technologies

BUY 1 GET 1

FREE!

Docker Container Security



HURRY UP!

Enroll NOW

iGNITE Technologies

MODULE 5

Linux for Pentester

During the threat modelling phase, the organisation may engage a pentester to do authenticated testing in order to verify an account's authorization on a Linux platform and identify internal threats brought on by illegal access. The teacher will concentrate on internal threats throughout the lesson and attempt to map the threats by providing Linux-based CTFs to enhance the expertise.

Learning Objectives

- Fundaments of Linux permission and privileges
- One-liner Reverse Shell
- File Transfer Technique
- Abusing Network Shares
- Bypass Restricted Shell
- Privilege Escalation
- Abusing Sudo Rights
- Misconfigured Suid Permissions
- Abusing Network File Share Misconfiguration
- Pivoting & Tunnelling

iGNITE Technologies

MODULE 6

Network Device Security Audit

Organisations engage a pentester with endpoint as an end device auditing where a pentester may have to schedule an automated network scanning as well as secure config review. Moreover, pen-testing of routers, switches, and printers as per industry standards could be added to the scope.

A pentester with limited knowledge may face challenges to meet the business requirement. Here the instructions will provide cooked steps to follow the industry's best practices for Network Security Audits.

Learning Objectives

- Router vulnerability assessment and config review
- Switches vulnerability assessment and config review
- Firewall vulnerability assessment and config review
- Printers vulnerability assessment and config review
- Secure configuration auditing
- Concept to bypass data leak prevention (DLP)

MODULE 7

Android Pentesting

just like other platforms, android pen-testing is demanded by many organisations because The privacy and security of Android users are at risk from unreliable applications. Furthermore, using these apps may lead to financial losses. The openness of the Android ecosystem is mostly to blame for this. Cyberattacks are more likely to target mobile applications than ever before. Android penetration testing is one of the finest techniques to enhance an android app's security.

iGNITE Technologies

Learning Objectives

- Fundamental Of Android Framework
- Implementing a Simulator for Lab setup
- Genymotion
- Testing Owasp Top 10
- Secure Code Analysis

MODULE 8

Bonus Section

The Bonus section will provide in-depth knowledge of industry-leading tools without them penetration is impossible. The instructor-led training will ensure the to provide the capability of these tools and automate manual pen-testing through them.

Learning Objectives

- Nmap NSE Scripts
- Metasploit Framework and WorkSpace
- Powershell Empire for Red Teamers
- Responder
- Impacket python libraries
- BurpSuite
- OwaspZap

iGNITE Technologies

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

WhatsApp

https://wa.me/message/HIOPPNENLOX6F1

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

iGNITE Technologies