SkillsDA®
Center for advance training

futureskills®
A NASSCOM initiative

COURSE NAME

APPLICATION HARDENING AND DEPLOYMENT CONFIGURATION FOR MINUMUM APPSEC VULNERABILITIES

SFNOS 0910

THEORY

- Identify & secure web servers and web | Review all applications for valid credentials | Review systems and applications to reduce the chance of exploitation | Apply access controls to applications and databases | Ensure patches for all web servers, web applications and databases
- Ensure STIGs for compliance with best practices | Review logs for web attacks and identify signs of compromise
- Implement defences such as firewalls & load balancer | Ensure that all applications connect with least privilege | Limit and monitor file creation in network | Configure application securely for minimum exposure and weaknesses | Secure applications via application testing, code review, WAF, etc.
- Check platforms for reported vulnerabilities and available patches
- Work on the established guidelines for security configuration and hardening | Establish mechanism and measures to ensure patches on all application assets
- Define security baseline for malware protection | Make business users aware of application vulnerability and patch requirements | Define strategy for management of patches and updates
- Identify a patch management life cycle process | Integrate patch management with the IT infrastructure management | Ensure that infrastructures are reengineered for patch management requirements
- Research best practices in hardening applications | Document the outcome of the tools and solutions

Course Theory Duration - 11.5 Hours
Course Practical Duration – 38 Hours

Duration of quizzes/knowledge check - 160 minutes
No. of Quizzes/knowledge checks - 8
Total no. of questions/Knowledge checks - 20
No. of quiz attempts given to user - 3 attempts

Course Overall Duration – 49.5 Hours

Criteria for for awarding E-Certificate
80% course completion and Scoring 70% in Knowledge check

COURSE Fee:

₹ 5000 + GST

Access Duration

6 Months

Pre Requisites for learners: Learners should have an understanding of how the web works, and the basics web technologies and web development languages

PRACTICALS

LAB MANUAL

Web application vulnerability scanning - Security breach prevention - Web application security techniques - Application vulnerability management techniques - Hardening techniques and standards - Application security and patch management - Managing patches and updates in web application - DAST techniques

TOOLS/TECHNIQUES

Manual - Arachni - Metasploit OWASP - Wireshark - Nmap - Manual - Nagios - pfsense OpenVAS - Metasploit - Snort - Nmap - OSSEC - Cryfs - Kali Linux - Skipfish - Oracle Traffic Director - Blackfire - Tideways - Splunk - Loggly - Papertrail - Netsparker - PCI Requirement - Fireeye - Open SSH - SolarWinds Patch Manager - Manageengine - WSUS RSI Secuirty - Appknox - Veracode - Netsparker