

Nikhil Waghlikar – Practice Lead - Security Assessment

<p>Summary</p>	<p>Nikhil W. is a Vulnerability Assessment, Penetration Testing and Information Security Auditor expert at NII. He is also a Certified Ethical Hacker, and has performed vulnerability assessment, penetration testing and security auditing exercises for some of NII’s premier customers. He has consistently impressed clients with his ability to think out of the box, and creatively attack systems and applications. He is well-versed with the OWASP, OSSTMM and ISO 27001 Standards.</p> <p>He currently serves as Practice Lead – Security Assessment at NII Consulting focusing on Penetration Testing, Vulnerability Assessment and Information Security Audits.</p> <p>His technical abilities span a very wide range of technologies across networks, operating systems, databases, web servers, mail servers, and applications; however his specialization is web applications and UNIX systems. He possesses strong analytical skills and is at the forefront of the research activities that NII undertakes.</p>
<p>Educational Qualification</p>	<ul style="list-style-type: none"> • Bachelors Engineering in Electronics and Telecommunication University of Mumbai, India
<p>Certifications</p>	<p>➤ List of certifications</p> <ul style="list-style-type: none"> ○ Certified Ethical Hacker ○ ISO 27001 LA
<p>Detailed Experience & Expertise</p>	<p>➤ Application Security</p> <ul style="list-style-type: none"> ○ Expertise in Threat Modeling, web application testing, and operational environment audit. ○ Well-versed with the Open Web Application Security Project Top Ten security vulnerabilities. <p>➤ Network Security</p> <ul style="list-style-type: none"> ○ Worked on security for a range of operating systems, databases, web servers, mail servers, directory services and applications ○ Experience with an extensive range of security systems and solutions. ○ In-depth knowledge of TCP/IP fundamentals <p>➤ Compliance & Guidelines</p> <ul style="list-style-type: none"> ○ Is well versed with ISO/IEC 27001 Standards ○ OECD Guidelines for the Security of Information Systems ○ NIST & Microsoft guidelines for Windows Server Security ○ MNSCU guidelines for UNIX Security
<p>Technical Skills</p>	<p>➤ Operating Systems: Windows 9x/NT/2000/XP/2003/2008/Vista, Linux, UNIX</p> <p>➤ Servers: Domain controllers (Active Directory), DNS (Microsoft DNS, BIND), DHCP, Mail Servers (QMail, Microsoft Exchange, Sendmail), Web Servers (Microsoft IIS, Apache), FTP (Microsoft FTP, vsftp, wu-ftp), Proxy Servers (Microsoft ISA, SQUID), File Servers (Microsoft built-in, SAMBA)</p> <p>➤ Databases: MS-SQL, Oracle, MySQL</p> <p>➤ Network components: Firewalls, Routers, VPN, Switches, WLAN access points</p> <p>➤ Security tools: Nmap, Nessus, Fport, Ethereal, Hping, tcpdump, whisker, nikto, ethereal, WebGoat, SARA, Netcat, Superscan, Snort, firewall, Achilles, brutus, Paros, HTTPPrint, WinHTTrack, Sam Spade, Cain and Abel, L0phcrack, Crack, WEPCrack, Kismet, forceSQL,</p>

<p>Business Skills</p>	<p>SQLPing, John the Ripper, Dsniff, windump, Xavior etc.</p> <ul style="list-style-type: none"> ➤ Languages: C, Shell Scripting, Windows Script Host, Perl, HTML. ➤ Firewalls: Cisco PIX, Forti-gate, Juniper ➤ Communication and Interpersonal <ul style="list-style-type: none"> ○ Have good communication skills by virtue of being a public speaker and trainer ○ Experience in project management, and client interactions ○ Experience in dealing with senior and middle management, system administrators, auditors, business partners, clients, customers, employees, etc. ➤ Project Management <ul style="list-style-type: none"> ○ Have led many of the projects executed by the company ➤ Very strong commitment to quality of deliverables
<p>Training</p>	<p>He delivers training on:</p> <ul style="list-style-type: none"> • Certified Ethical Hacking (CEH) • Operating System Security • Network Security • Database Security • Wireless Network Security • Auditing and compliance • Application Security
<p>Security Articles & Research</p>	<p>Security Articles</p> <ul style="list-style-type: none"> ➤ Universal Extractor ➤ Dare to delete my files <p>http://www.niiconsulting.com/checkmate/</p> <ul style="list-style-type: none"> ➤ Network Performance Audit (2 Part Article) <p>Article 1: Assessing Bandwidth Use as a Function of Network Performance Link: http://www.theiia.org/ITAuditArchive/index.cfm?catid=21&iid=571</p> <p>Article 2: Essential Aspects of an Effective Network Performance Audit Link: http://www.theiia.org/ITAuditArchive/index.cfm?iid=575&catid=21&aid=2901</p> <p>Research</p> <p>Vulnerability disclosure of clear text password dumped in memory in ThunderBird Email client.</p>
<p>Significant InfoSec projects</p>	<ul style="list-style-type: none"> • Penetration and Web Application Testing for: <ul style="list-style-type: none"> • India's largest online share trading website • One of the largest online gifting websites • Law firm in Riyadh • Matrimonial and dating website • Zahid Tractor • One of the largest Telecom company in Bahrain • One of the largest Airlines Company at US • Two of the leading Public Sector Unit • Two of the India's largest BPO

- One of Asia Middle East's leading IT Security Service provider.
- One of Asia Middle East's government educational organization.
- One website hosting company.
- One of the Government Owned Manufacturing Organisation.

- **Wireless Penetration Testing for:**
 - One of Largest banks in Middle East
 - One of Asia Middle East's leading IT Security Service provider

- **Vulnerability Assessment Testing for:**
 - Two of the India's largest BPO
 - One of India's largest banking sector
 - India's largest online share trading company
 - One of India's Mail service provider company
 - One of Asia Middle East's leading IT Security Service provider

- **Information Security Auditing for:**
 - One of India's sports company
 - One of India's largest banking sector
 - One of India's Mail service provider company
 - One of India's largest online share trading company
 - One of Asia Middle East's leading IT Security Service provider

- **ISO27001 Implementation for:**
 - One of India's online share trading company
 - One of India's Third Party revenue collection company
 - One of Asia Middle East's government educational organization
 - One of Asia Middle East's leading IT Security Service provider

- **Network Performance Audit for:**
 - One of India's largest chemical engineering service provider

- **Mail Server Setup:** Setup and configure a "QMail" Mail server based on Linux. QMail is considered much stable and secured Mail server in Linux world and is used by major commercial mail service providers like Gmail and Yahoo.
- **Domain Controller:** Setup, configure and manage Windows based Domain controller (Active Directory), its policies, auditing etc.
- **Linux Based Firewall:** Setup, configure and manage IPCOP. IPCOP is a specialized Linux based Firewall for protecting all kind of networks.
- **UNIX/Linux Audit:** Performed a comprehensive audit of UNIX/Linux Operating System.
- **Security Hardening of Systems:** Written scripts that would hack proof completely Oracle Database, and various Operating Systems and databases.