Deepak Modi

Sr. Information Security Analyst

Deepakmodi411@gmail.com +91 861-980-3101 Chennai, India

Summary:

An information security professional with 2.9 years of experience in- Security Analysis, Penetration Testing, CEH, VAPT,SAST, DAST, Firewall & Network Troubleshooting

Extensive experience in vulnerability assessment, vulnerability management and manual pen- testing. Assisted in more than 70 VAPT consulting assignments and was adjudged as 'Threat Hunter" by multiple companies for my support in finding vulnerability & security from outside intruders.

Technical Skills:

VAPT Tools	Burp Suite, Acunetix, IBM Appscan, HP Fortify Code Analyser, Nmap, Nessus, Sqlmap, Maltego, OWASP ZAP, Curl, Netcat, Hping3, Metasploit, CheckMarx, Openvas, WPscan, Routersploit, NSE Scripts, DirBuster, MassDNS, Nikto, Nexpose.
Network Analysis Tools	Wireshark, Snort, TCPDump, Splunk, ELK, AlienVault.
Security Standard	OWASP, PTES, OSSTMM, OSINT,SAST, DAST.
Scripting Languages	Unix Shell Scripting, Python, SQL/MySQL, Java Script
Programming Languages	Knowledge of Python, C/CPP, Java, Sql.
Operation System	Mac OS/Linux/Windows.
Industry knowledge:	Palo Alto TAC, internal network security audit, External network security audit, Web application penetration testing, Mobile penetration testing, Cyber forensics analysis, Incident handling and response management
Routing & Switching	Static Routing, RIP, OSPF, BGP.TCP/IP, NAT, VLAN, Inter-VLAN Routing.
Security	Vulnerability Assessment Penetration Testing, WAPT, Network Penetration Testing, Black Box Testing. Network Security, SSL VPN, IPsec VPN. Layer 7 Inspection and security.

Cyber Security Projects:

Title	**Web Application Vulnerability Assessment & Penetration Testing (30+ Projects)**
Role	Sr. Security Analyst
Tools/Technologies:	Acunetix, HP Fortify Code Analyzer, Nessus Professional, Burp Suite, Metasploit, NSE Script, Python Scripting, Shell Scripting.
Responsibilities:	• Prepared testing checklist, policies, use cases and documented the requirements from the client. • Developed threat and vulnerability management policies and defined ROE (Rule of engagement). • Performed validation checks on different servers, found loopholes and customized the code. • Ensured that the development is at par with the detailed design. Ensured that the code developed is in compliance with quality standards. • Performed static as well as dynamic vulnerability analysis. • Manually handled the identification/analysis of critical vulnerabilities and exploited them in a non-destructive manner. Provided vulnerability assessment report to client as per requirement.

Title	**Internal and External Network Security Assessment Test (VAPT) for Many SME/Enterprises and Government Organization. (20+ Projects)**
Role	Sr. Security Analyst
Tools/Technologies:	Nessus Professional, Burp Suite, TestSSL, RouterSploit, Iotsploit, Metasploit, NSE Script, Python Scripting, Shell Scripting.
Responsibilities:	• Prepared testing checklist, policies, use cases and documenting the requirements from the client. • Developed threat and vulnerability management policies and define Scope & ROE (Rule of engagement). • Performed validation checks on different servers and find loopholes and customize the code accordingly. • Identification of security flaws present in the environment. • Understanding the level of risk for the organization. • Help address and fix identified network security flaws. Manually handle the identification/analysis of critical vulnerabilities and exploiting them in a non-destructive manner. Provide vulnerability assessment report to client as per requirement in a non-destructive manner. Provide vulnerability assessment report to client as per requirement.

Title	**Enterprise Security & Risk Management**
Role	Sr. Security Analyst
Tools/Technologies:	Rapid7 Insight, Nmap, Burp Suite, Nessus Professional, Metasploit, Kali Linux Tools
Responsibilities:	• Performed static, dynamic, port, process and registry Analysis. • Prepared testing checklist based on OWASP Top 10 and policies as per the requirement. • Static and dynamic application security testing (SAST & DAST). • Identify the Malicious process and trying to kill the process and provide solutions for system flaws. • Conducted Security Assessment Test for Internal Network, External Network. • Knowledge of protocols such as HTTP, FTP, DNS, DHCP, SMTP. • Accomplished project goals on time, on budget and in alignment with corporate objectives.

Title	**Mobile Application Security Assessment Test VAPT (10+ projects Using OWASP guidelines)**
Role	Sr. Security Analyst
Tools/Technologies:	SANTOKU O.S, BURP suite Professional, Genny Motion, Apktool adb, JD-gui, dex2jar, Andrototak, APKscan, Drozer, MOBSF.
Responsibilities:	• Created the threat model for an application • Performed static, dynamic testing. • Prepared testing checklist based on OWASP Top 10 and policies as per the requirement. • Static and dynamic application security testing. • Acting upon discovered vulnerabilities for gaining sensitive information or performing malicious activities. • Demonstration of the identified vulnerability for gaining privileges and attempting to become the super user. • Created the detailed report about discovered vulnerabilities, such as overall risk rating, the associated technical risk, and description etc.

Title	**CERT-IN Implementation**
Role	Sr. Security Analyst
Tools/Technologies:	Nessus Professional, Burp Suite, Metasploit, Rapid7 Insight, Acunetix
Responsibilities:	• Conducted Security Assessment Test. • Report Writing and Risk ratings. • Presented the findings with CERTIN team. • Incident Triage, Evidence Gathering and analysis, Data ingestion and Data Analytics using System logs and event logs

Career Progression:

CSS Corp: Network Engineer **(July 2019 - Present)**

Responsibilities-

- Working as Tier2 TAC engineer for Palo Alto. Hands-on experience with troubleshooting PAN-OS 7.0.x, 7.1.x, 8.0.x, 8.1.x, 9.0. x.
- Help customers with debugging issues.
- Proficient handling of Threat and vulnerability signatures.
- Help customers with debugging issues related APP-ID, USER-ID, GLOBAL PROTECT, SSL-DECRYPTION, IPSEC VPN
- Provide customized solution for customers security measures
- Help identify packet drop, latency using Wireshark captures and debug flow basic, tcp basic, ssl basic, tunnel flow
- Proficient in handling Panorama related assistance
- Proving RCA for unexpected reboot, high Management/Data Plane CPU, High Memory, Process Crash.
- Analyze logs, packet captures to resolve support cases escalated from Level 2 support team, pertaining to enterprise switches, firewalls and wireless solutions.

Kantag Solutions: Sr. Information Security Analyst **(Dec 2017- July 2019)**

Responsibilities-

- Conducted Vulnerability Assessment and Penetration Testing (VAPT), on various Infrastructure and Applications.
- Internal and external Network VAPT,
- Conducted source code review, mobile application assessment with Mobsf.
- Identifying all the potential loopholes within the Network and show the potential impact of all those threats & loopholes by exploiting them.
- Ran vulnerability and compliance scanning on test machines and reviewed security standard and minimum-security baseline for the client.
- Performed penetration testing for thin & thick client-based application.
- Performed live packet data capture with Wireshark to examine security flaws. Used LDAP injections techniques of exploiting Web application that use client supplied data.
- Port scan servers using NMAP and close all unnecessary ports to reduce the attack surface.
- Performed dynamic and static analysis of web application using IMB Appscan, acunetix. Analyze systems for potential vulnerabilities that may result from improper system configuration, hardware, software, operational or network flaws.

Training / Achievement:

- Achieved HOF (Hall of Fame) by Accenture for finding vulnerability.
- Achieved Appreciation Letter by Miniorange for finding vulnerability.
- Achieved CSAT Championship Certificate and Amazon gift card from Palo Alto.
- Completed PAN-OS 9.2 Release Training Assessment for TAC.
- Certified in **ICSI | CNSS Certified** Network Security Specialist certification.
- Certified in **CEH (Certified Ethical Hacker)**.
- Certified in **Qualys Web Application Scanning & Vulnerability Management.**

Academic Qualification:

Course	Board/University	Year
B. Tech. (CSE)	Madhav University, Rajasthan	2017
Diploma	Sunrise University	2014
12th	Saint N.N RSV	2011
10th	Jesus & Mary school	2009

Declaration:

I hereby declare that the above information furnished by me is true to the best of my knowledge.

Date: 12/10/2020 (Deepak Modi)