AVINASH KUMAR THAPA
OSCP, OSCE
Mobile: - +971523557045, +918968912648, +917042732190
E-mail:-avinash_thapa@outlook.com

PERMANENT ADDRESS:
House no.152, Street no. 2, Ward no.5,
Dharampal Coloney, Dhayansar, Kartholi, B.D
Bari.
NH-Jammu 181133

CORRESPONDANCE ADDRESS
Flat No. 405, E-Tower,
Satyam Appartments,
Swastik Vihar, Patiala Road
Zirakpur

CAREER OBJECTIVE

To work in a firm with a professional work driven environment where I can utilize and apply my knowledge, skills which would enable me to grow while fulfilling organizational goals.

EXPERIENCE

- Serving as **Senior Information Security Analyst** in Network Intelligence India Pvt. Ltd.
- **1 Year** and **10 Months** as **Information Security Analyst** in Network Intelligence India Pvt. Ltd.
- Total Experience of **2 Years and 7 month**.
- Handled numerous projects on different technologies as mentioned in further section.

CERTIFICATIONS

- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional (OSCP)
- Certified Professional Hacker(CPH NxG)
- Certified Information Security Consultant(CISC)
- Certified Professional Forensics Analysis (CPFA)

PROJECTS HANDLED

- **Network Security Assessment**
  - ✓ Executed the network performance and IT infrastructure security assessment projects for one of the Pharmaceuticals companies and one of the Home appliances Manufacturer Company.
  - ✓ Performed IT infrastructure Security and Network Performance Audit for one of the largest manufacturing company of India.
  - ✓ Performed IT infrastructure Security and Network Performance Audit for one of the MNC in financial and for one of the leading pharmaceutical Companies.
  - ✓ Performed IT Infrastructure audit for one of the state Telecom Company in India
  - ✓ Conducting various Network Security Audit project of one of the largest PSU in India.
  - ✓ Executed Security Assessment project for one of the largest search engine of the India and Other corporate clients.
  - ✓ Conducted network Security assessment project for Indian Banks
  - ✓ Conducted network security assessment for largest internet service providers
  - ✓ Conducted network security assessment for telco digital transformation company.
  - ✓ Performed network switches auditing for Indian government Clients
  - ✓ Performed overseas assessment for electronics security system companies.
- **Application Assessment**
  - ✓ Performed Web application penetration testing for Indian Banks
  - ✓ Performed **ATM whitelisting assessment** for various Indian Banks
  - ✓ Performed web application testing for telecom companies

- ✓ Performed Web application Penetration testing for Mutual fund website
- ✓ Performed Web application penetration testing for global Infrastructural Company
- ✓ Performed Web application Pentesting of CORE Banking Application.

❖ **Forensics (RAM forensics, Image Analysis)**

- ✓ Conducted headers analysis project for government clients

❖ **PCI-DSS (Segregating Testing)**

- ✓ Performed segregation testing on Compliance Projects of online wallets websites

❖ **Mobile Application Pentesting**

- ✓ Performed Mobile Application Penetration testing for Indian Banks
- ✓ Performed IOS Mobile Application testing for Overseas Banks

❖ **Active Directory Configuration Review**

- ✓ Performed active directory configuration review for various overseas client

❖ **Virtualization Configuration Review**

- ✓ Reviewed virtualization configuration (Hyper-V and LDOM) for overseas Clients.

CORPORATE TRAININGS

Along with execution of projects, I have performed corporate training for reputed clients and details for these trainings are mentioned below:

- ❖ Penetration Testing with Kali Linux (Overseas trainings in Kuwait)
- ❖ Certified Information Security Consultant (For Governments Clients)
- ❖ Assembly Language and Advance Exploit Development trainings.

ONLINE PUBLICATIONS

- ❖ Stored Cross-site Scripting Flaw Reported and exploit Present in Exploit-db.com
  http://www.exploit-db.com/exploits/35266/
- ❖ Multiple Vulnerabilities Reported on WordPress Platform
  http://1337day.com/exploit/22362
- ❖ Buffer Overflow Bug in Brasero DVD/CD Burner (Pre-Installed on Kali Linux)
  http://www.exploit-db.com/exploits/36388/
- ❖ i.FTP 2.21 - SEH Overflow Crash PoC
  https://www.exploit-db.com/exploits/36847
- ❖ UniPDF Version 1.2 - 'xml' Buffer Overflow Crash PoC
  https://www.exploit-db.com/exploits/36841/
- ❖ WIRESHARK <=1.12.4 Access Violation and Memory Corruption PoC
  https://www.exploit-db.com/exploits/36840/
- ❖ Created CTF For Ethical Hackers
  https://www.vulnhub.com/entry/acid-server-1,125/
- ❖ Created CTF For Ethical Hackers
  https://www.vulnhub.com/entry/acid-reloaded,127/
- ❖ Remote Code Execution
  https://www.exploit-db.com/exploits/39161/

HALL OF FAME

- ❖ Hall of Fame in Apache friends (for Vulnerabilities in XAMPP)
  https://www.apachefriends.org/about.html
- ❖ Hall of Fame in Coinbase
  https://hackerone.com/coinbase/thanks
- ❖ Hall of Fame in HackerOne
  https://hackerone.com/acid_creative
  https://hackerone.com/acid_creative/thanks

TECHNICAL EXPERTISE

Exploit Writing	• Assembly Language in Intel & AT&T syntax • Buffer Overflows (stack, arithmetic, heap) • Writing Shell codes • Exploit Writing with Python Programming • Bypassing Buffer Overflow Protection
Network Security	• Reconnaissance of Network Services • Eavesdropping the network traffic • Denial of Service • Security Audit on Network Device • Configuration Review • Firewall Security Auditing • VPN Security • Exploiting Network Services
Tools : Nmap, Superscan, Netcat, Hping3, Wireshark, TCPDump, Brutus, Cain & Abel, Nipper, Nessus, Metasploit	
Operating System Security	• Fingerprinting Operating System • Vulnerability Scanning • Patch Management • Windows Server Security • Linux Server Security • Account Policy Security
Tools: Nmap, NAT, Superscan, Nessus, Metasploit, GFI Languard.	
Database Security	• DB Enumeration • Database Security Parameters • Auditing DB Roles & privileges • Oracle Security • MS SQL Server Security
Tools: Nmap, OSScanner, Sqlmap.	
Application Security	• OWASP TOP 10 • WASC TC • Business Logic Testing • WAF Identification and Bypass Methods
Tools: Burp Suite, BeEF, SQLmap, havij, FuzzDB, FOCA, GHDB, W3AF, Netsparker, Nikto.	
Digital Forensics	• Disc Imaging • Image Analysis • Network Forensics

	• Live Forensics
Mobile Security	• Mobile Owasp top 10 • Vulnerability Assessment and Penetration Testing of Mobile Applications.(All Platforms)

GENERAL I.T PROFICIENCY

Virtualization	VM Ware, Virtual Box, Oracle Virtual Box
Programming Languages	C#, C++, Python, Shell Scripting , Assembly Language, PHP
Database Tools	SQL
Operating systems	Windows NT, Linux, Backtrack, Kali Linux
Web technologies	PHP,HTML, JavaScript,JSON
Software tools	MS Office, Various Antivirus tools
Hardware Knowledge	Assembling and Dismantling machines, Configuring LANs
Exploitation Skills	Buffer Overflow and working with Exploit Writing.

BASIC ACADEMIC CREDENTIALS

Qualification	Board/University	Year	Percentage
B.Tech (ECE)	Kurukshetra University	2010-2014	First Division
12th Class	Kendriya Vidhayala Nagrota (CBSE Board)	2010	72.6%
10th Class	Kendriya Vidhayala Nagrota (CBSE Board)	2008	73%

INTERPERSONAL SKILL

- ❖ Ability to rapidly build Relationship and set up trust.
- ❖ Confident and determined.
- ❖ Ability to cope up with different situations.

DECLARATION

I do hereby declare that the above information is true to the best of my knowledge.

Place: Chandigarh

Avinash Kumar Thapa

Date: 16th November'2016