HARSH SHRIVASTAVA

Harsh.Shrivastava08@gmail.com www.linkedin.com/in/hrshshrivastava
(509)715-7149 2030 8th Ave., Seattle, WA

EDUCATION

M.S., Information Technology/Cyber Security, *University of Texas San Antonio, TX* *Dec '16*
B.E., Computer Science, *Rajiv Gandhi Technical University, Bhopal, India* *Jun '13*

Relevant Coursework: Secure Network Design, Operating Systems, Compiler Design, Analysis and Design of Algorithms, Principles of Information Security, Computer Architecture, Advanced Topics In Cyber-Security.

EXPERIENCE

Research Assistant, *University of Texas at San Antonio, TX* *May '17- Present*
- Researching American Invention Act connecting the Patent Life Cycle with the Technology Development Process.

Software Developer, *Skip Analytics, San Antonio, TX* *May '15 - Oct '15*
- Designed an iOS scan& shop app allowing shoppers to skip billing queues and purchase items by scanning barcodes.
- Implemented client side payment system using Stripe API.
- Built location tracking intelligence and integrated it into this app
- Analyzed the app for cyber-security vulnerabilities.

CERTIFICATIONS

EC- Council's Certified Ethical Hacker (CEH), *Entersoft Labs, India* *active till '19*
*Score: **93%***
- Certified in Ethical Hacking, Backtrack Operating Systems, Metasploit, Nessus, Wireshark.

EC- Council's Certified Hacking Forensic Investigator (CHFI), *Net conclave Systems, India* *active till '19*
*Score: **90%***
- Certified in forensics, use of forensic tools like Encase, CAINE, SANS Investigative Forensics Toolkit.

PROJECTS

Web Application Penetration Testing *Aug '17*
- Performed Black Box vulnerability testing on Bug Tracking web application. Tested for OWASP top 10 and some other known vulnerabilities. Used tools like Burp Suite, SQL map, ZAP, Samurai WTF.

Secure Network Design *Jan '16*
- Designed and implemented dev network comprised of routers & servers.
- Enforced policies using firewalls to segregate zones: DMZ, prod and dev.
- Used Snort for Intrusion Detection at the network periphery.

Security Incident Response, University of Texas San Antonio *May '15*
- Analyzed a compromised virtual machine and tried to find who was behind the compromise by using incident response rules and tools, such as SANS Investigative toolkit, Encase, nmap, malware finders.

TECHNICAL SKILLS

Programming-	Basic Python, C/C++, Swift, GDB, Xcode 8.
Web App Penetration Testing -	Burp Suite, Zed Attack Proxy, AppScan, SQLmap, b33f framework
Networking Protocols-	HTTPS, SSL, TLS, IPsec, TCP/UDP, ARP, DNS, OSI and TCP/IP model.
Linux -	RHCE and RHCSA (3 months training), Kali Linux, Ubuntu.
More -	Troubleshooting (Network and System), LAN/WAN, Environments and IP addressing, Active Directory, Snort IDS, Wireshark, pFsense Firewall.