Kul P. Subedi

Professional Summary

Highly experienced and skilled Offensive Security Researcher focus on finding vulnerabilities with a strong record of excellent teamwork and successful completion of product hacking in time-boxed environment. Specialized in problem identification, analytical ability and performance tuning experience to drive change and improve the overall security posture of software product.

Teaching Experience

Part-time Cyber Security Instructor. ThriveDX (formerly HackerU), Miami, FL 33134

Lead Cyber Security Instructor **August 2022 to till date**

- Teach courses related to cyber security such as ethical hacking, cloud security, network security, linux security, cyber infrastructure and technologies.
- Perform hands on lab on each course.

Part-time Computer Science Lead Instructor. Christian Brothers University, Memphis, TN 38104

Lead Instructor **Jan 2022 to till date**

- Teach courses in computer science such as cloud security, cyber ethcis, and computer network and cyber security.
- Perform hands on lab on each course - AWS, Azure.
- Manage content of the courses in Canvas platform.

Professional Experience

Senior Security Researcher. Microsoft, Mountain View, CA 95110

Senior Security Researcher **Feb 2023 to till date**

- Analyzing vulnerabilities in software and services to determine their root cause, severity, and security impact.
- Identifying variants of vulnerabilities and discovering new vulnerabilities.
- Building tools and inventing new approaches to automate the discovery analysis of vulnerabilities.
- Analyzing trends in vulnerabilities being discovered to spot patterns.
- Researching, developing, and deploying mitigations for common patterns of vulnerabilities.
- Performing penetration testing, offensive security research, and red teaming activities.

Application Security Researcher. Adobe Inc., San Jose, CA 95110

Application Security Researcher **May 2021 to Jan 2023**

- Perform full-scope security reviews for Adobe products to ensure design and implementation are secure before production release.
- Provide recommendation for product teams in report with complete walkthrough and proof-of-concept exploits.

- Develop automation projects that reduce attack surface of the Adobe products from external world as well as insider threat.
- Perform internal red teaming to get the real-world risk associated in Adobe products.
- Research on different security techniques to find vulnerabilities in Adobe products: fuzzing with winAFL, libFuzzer, OneFuzz, AFL++ - discoverd zero-day vulnerabilities in many code and binary analysis projects for clinets, dynamic testing, software composition analysis, and static analysis.

Red Teaming and Adversary Simulation. VDA Labs, Grand Rapids, MI 49525

Senior Security Engineer **October 2020 to May 2021**

- Simulated advanced persistent threat activities and techniques during multi-day opposing force exercise against Cyber Protection Teams. Provided frequent briefings and delivered quality reporting.
- Performed numerious full-scope projects involving social engineering, network, wep application, native application, IoT, and internal pentesting for very satisfied clients with well-known names across commercial and government sectors.
- Reverse engineered and exploited products, e.g., full remote compromise of a drone via RF attack surface and developing bypasses for common endpoint protection suites.
- Developed zero-day techniques, attribution minimizing infrastructure, and collection systems to ensure mission success.
- Performed fuzzing with winAFL, libFuzzer, OneFuzz, AFL++ - discoverd zero-day vulnerabilities in many code and binary analysis projects for clinets.
    i. Advanced harnessing of compiled binaries using hooking and patching techniques.
- Enhanced team expertise through research, documentation, and collaboration.

Design and develop cloud native applications using Spring Boot. FedEx Services, Collierville, TN 38017

DevSecOps III **January 2020 to October 2020**

- Implemented front-end single page application that helped sorting, track package information, and monitor to sort packages in Hub using Spring framework.
- Developed components in Angular JS to provide flexible User Interface, e.g. HTML/HTML5, CSS, Javascript, Typescript, Angular, jQuery.
- Implemented the publisher JMS component using Tibco API to push status of sort system and sort line control system.
- Implemented file manager application using custom protocol used in Sort Controller to allow delete, update, copy, and view the files.
- Experience in using Developer Tools in different browsers and Firebug for debugging and troubleshooting the code.
- Expertise in creating user validation forms and sending data to server using RESTful services, e.g., Postman, Swagger, and Springfox.

- Experience with versioning, continuous integration (CI), and continuous delivery (CD), e.g., Git/GitLab, Jenkins, Nexus Repository Manager.
- Experience with monitoring and alerting framework, e.g. Splunk, AppDynamics, Kenna.
- Participation in peer reviews on specifications, design, and code.
- Exceptional ability to quickly master new concepts and capable of contributing individually or as part of a team with excellent communication skills.

Provide object-oriented software (OOS) design for one of the telecommunication industry's leading telecommunication expense management and mobility service platforms (TEMMS). Develop and customized software for diverse client base.

Tangoe US Inc, Memphis, TN 38119

Software Engineer **August 2016 to January 2020**

- Contributed software engineering expertise in the development of products through the software lifecycle, form requirements definition through successful deployment.
- Facilitated customization of account payable and general ledger systems by encouraging software engineering team to adopt emerging standards for software application development architecture and tools.
- Developed automation process to dispute charges using Grails, Angular JavaScript, and Helium.
- Implemented new customer requirements under strict deadlines.
- Provided support to the customer's technical team to upgrade, deploy, configure, and setup different components of TEMMS application in their infrastructure.
- Configured, installed, and deployed a report system based on Jasper Report Server.
- Involve in finding vulnerabilities on authentication, authorization, access control, input validation, and boundary validation in TEMMS application.
- Performed SQL tuning for customized SQL scripts used by clients and increased the performance 40 percent.
- Designed and implemented customized bash script to automate the account payable and general ledger file generation process.

Deja vu Security, Seattle, WA 98122

Associate Security Consultant **February 2016 to June 2016**

- Experienced in Performing Security testing for large scale Software Systems e.g. Amazon Inspector , Amazon Payments, and Market Place Web Services. (Worked in **Amazon** Client Site).
- Perform penetration testing from the perspective of design, implementation, cryptography of web applications, native applications, web services, and protocols.
- Perform source code review from the security perspective.
- Perform configuration review.
- Develop pits for Peach Fuzzer.

- Execute security test plan.
- Involve in finding vulnerabilities on authentication, authorization, access control, input validation, and boundary validation.
- Proof-of-Concept Exploit development.

The University of Memphis, Memphis, TN USA

Graduate Research Assistant **August 2012 to February 2016**

- Password Immunizer: Negative Authentication System, a joint work with Geospatial Data Center, Massachusetts Institute of Technology (MIT)
  Developed a negative authentication architecture for web clients and Windows clients.
- Software Security Researcher
  Perform security analysis of software using different approaches such as static analysis, dynamic analysis. Perform security analysis of InfiniBand protocol using in HPC infrastructure.
  Installation, Configuration, and OS upgrades on RHEL 5.X/6.X, SUSE 10.X, 11.X to perform software security analysis
  Implemented and administered VMware ESX 3.5, 4.x for running the Windows, Centos, SUSE, Red Hat Linux Servers on development, and test servers.
  Creating volume groups, Logical volumes, and extending them using LVM.
  Working with HP XEN Blade Servers. Attaching disk space from DL-360 blade servers to VMs.
  Responsible for setting up new instances, migrating existing services from physical servers to AWS cloud.
  Configure, monitor, and maintain AWS VPC environment.
  Working with SAN team for exporting shared volumes and mounting shared volumes.
  Installing and Configuring Puppet for configuration management. Responsible for configuring networking concepts like NIS, NFS, SAMBA, LDAP, SSH, SFTP, SNMP, DNS, DHCP, troubleshooting network problems such as TCP/IP, and support users in solving their problems.
  Configuring, Managing, and Scheduling CRONTABs for App Accounts and Backup management on a regular basis.
  Designing, implementing, and updating the web application for the Cyber Summit, Center of Information Assurance.
- nulltester
  Team Captain (A Cyber-Security focused student group)

Nepal Telecom, Jawalakhel, Lalitpur, Nepal

Senior Software Engineer/Database Administrator **January 2010 to July 2012**

- Developed Web Application using J2EE Spring Framework to expose services for multi-tenant telecommunication customers.
- Developed PL/SQL procedures, triggers for database constraints.

- Performed administration of Oracle 10g Production on the telecom billing database with 40TB+.
- Performed administration of Production Servers with Oracle 10g, Oracle 9i and MySQL Servers 5.1.
- Performed deployment of major and minor releases in database level production servers.
- Carried out performance monitoring and tuning of database system.
- Deployed projects such as ERP, Convergent Billing System.
- Database backup tools: datapump, manual backup, RMAN backup.
- Provided daily support to the developers, managers in technical issues in production environment.
- Performed backup and recovery of overall database in production line.

Linux System Engineer **October 2008 to December 2009**

- Performed Linux Systems Administration for 25+ Enterprise RedHat Enterprise Linux Systems.
- Maintained Linux infrastructure environment at Nepal Telecommunication data centers during business hours and off-hours; performed technical resolution procedures on Linux networking services and protocols: TCP/IP, DNS, NFS, FTP, SSH, SMTP, SSL and HTTP.
- Installed, configured and maintained Linux server equipment, disk arrays, tape libraries, virtual tape libraries, and terminal servers.
- Performed routine backup and recovery for data protection and integrity for 25+ Linux servers; monitored Linux infrastructures consisting of complex sets of equipment and system software.
- Performed proactive monitoring for system data protection, backup and recovery, user account management, disk storage management, hardware and OS maintenance, and application maintenance: Linux storage environment using Logical Volume Manager, RAID.

Government of Nepal, Ministry of Health and Population, Matepani, Pokhara, Nepal

Software Developer/Information Technology Officer **August 2007 to September 2008**

- Designed and implemented web application using J2EE technology and client side HTML, CSS, JavaScript.
- Researched existing Customer Relationship Management technologies for feature enhancement.
- Participated in new feature development and bug fixing in Health Inventory Management System.

Professional Certification

Software Security Practitioner - Defending C++, SSP C++.
Offensive Security Cerified Professional (OSCP) (OS-101-27048), OSCP: OS-101-27048.
RedHat Certified Engineer, RedHat Enterprise Linux 4, Certification Number: 110-098-233

Professional Training

Offensive Security Web Expert (OSWE), Offensive Security, OS-13082. Training completed.
Offensive Security Exploit Development (OSED), Offensive Security, OS-13082. Training completed.
NE40E–X8 Router and iManager U2000, Training Center, Nepal Telecom, Huawei Technologies Co., Ltd.
Advanced Oracle DBA, NIIT, New Delhi, India.
System and Network Administration and Security, Red Hat India.
Cisco Certified Network Associate (CCNA),Computer Point Nepal.

Academic Experience

Advanced College of Engineering and Management, Lalitpur, Nepal

Computer Lecturer **December 2005 to August 2007**

- Taught Computer Network, Operating System, Computer Architecture, TCP/IP Protocol Stack, Data Structure and Algorithm using C/C++
- Carried out the hands-on lab for Data Structure and Algorithm, Computer Network, Operating System

Computer Point Nepal, Jame Market, Kathmandu, Nepal

RedHat Enterprise Linux Instructor **April 2007 to June 2007**

- Taught Red Hat Enterprise Linux System Administration I, II, III.
- Conducted hands-on lab for RHEL Sample Exam.

Education

The University of Memphis, Memphis, TN USA Overall GPA:3.8

Ph.D. in Computer Science, Computer Science(August 2012 – Dec 2018)

- Advisor: Professor Dipankar Dasgupta
- Area of Study: A Framework for Analyzing Advanced Malware and Software

M.S. in Computer Science, Computer Science(August 2012 – August 2016)

- Advisor: Professor Dipankar Dasgupta
- Area of Study: Building Secure and Reliable Software System

Advanced College of Engineering and Management, Lalitpur, Nepal GPA:3.98

B.E., Computer Engineering, August 2001 – November 2005

- Computer Engineering specialization with Computer Network, Operating System

Skillsets

Extensive system development and software engineering experience in application development and information technology

Programming Languages

- Java, Groovy, Ruby on Rails, C, C++, Python, PHP, Perl, UNIX/Linux shell scripting, SQL, PL/SQL.

Software Development Frameworks and Tools

- Spring, Grails, Angular JS, Rails, Django.
- RESTful web services, Object Relational Mapping (ORM) - Hibernate.
- Oracle Database, Postgres Database, MySQL Database.
- HTML-5, CSS, JavaScript.
- Gradle, Maven, Ant, GNU make.
- ESXi, Docker, XEN.
- Git, Svn, Mercurial.

Security Tools

- *Network Tools*: Snort, Wireshark, Tcpdump, Netfilter, Packet Filter (pf), NMAP
- *Fuzzing Frameworks*: Sulley, Peach, SPIKE
- *Penetration Testing Tools*: Kali Linux, Scapy, sqlmap, Metasploit Framework, Debuggers Ollydbg, Immunity Debugger, GNU Debugger (GDB), Evans Linux Debugger (EDB), IDA Pro, Tamper Data, Burp
- *Networking services and protocols*: TCP/IP protocol stack, DNS, NFS, FTP, SMTP, SSL, HTTP/HTTPS, routing protocols (RIP, OSPF, BGP), Windows Active Directory Server 2012, Samba 3 and Samba 4
- *Digital Forensic Tools*: EnCase v7, Autopsy and Sleuth Kit, WinHex

Operating Systems

- Linux, OpenBSD, other UNIX variants, and Microsoft Windows family.
- Linux Server Administration.
- OpenStack Cloud Operating System.

Network and Internet Technology

- Networking TCP/IP Protocols (ARP/RAPR, IP, UDP, TCP, DNS, HTTP, FTP, SSH), Services (Apache, HTTP Proxies, MySQL, POP, IMAP, SMTP, DNS), Cloud services (OpenStack).
- InfiniBand Protocols.
- Applied Crypotography.

Big Date Technologies

- Hadoop Ecosystems: HDFS, MapReduce, HBase, Pig, Hive.

Mathematics

- Abstract Algebra, Applied Mathematics, Applied Statistical Analysis, Discrete Probability.

Publication

- S. Poudyal, K. P. Subedi, and D. Dasgupta. A framework for analyzing ransomware using machine learning. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1692–1699, 2018
- Kul Prasad Subedi, Daya Ram Budhathoki, and Dipankar Dasgupta. Forensic analysis of ransomware families using static and dynamic analysis. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 180–185. IEEE, 2018
- Kul Prasad Subedi, Daya Ram Budhathoki, Bo Chen, and Dipankar Dasgupta. Rds3: Ransomware defense strategy by using stealthily spare space. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–8. IEEE, 2017
- K. P. Subedi, D. Dasgupta, and Bo Chen. Security analysis on infiniband protocol implementations. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–7, Dec 2016
- Dipankar Dasgupta, Denise Ferebee, Sanjib Saha, Abhijit Kumar Nag, Kul Prasad Subedi, Alvaro Madero, Abel Sanchez, and John Williams. G-nas: A grid-based approach for negative authentication. In *Computational Intelligence in Cyber Security (CICS), 2014 IEEE Symposium on*, pages 1–10. IEEE, 2014

Technical Report

- Dipankar Dasgupta, Denise Ferebee, Abhijit Kumar Nag, Sanjib Kumar Saha, Kul Subedi, Alvaro Madero, Abel Sanchez, and John R. Williams. Design and implementation of negative authentication system. Technical Report CS-14-001, University of Memphis, feb 2014
- Dipankar Dasgupta, Denise Ferebee, Sanjib Kumar Saha, Abhijit Kumar Nag, and Kul Subedi. A deterministic grid-based approach for negative authentication system (g-nas). Technical Report CS-13-005, University of Memphis, aug 2013

Awards and Paper Presentation

- Participated in Capture the Flag Challenge hosted at CSI CyberSEED University of Connecticut, Cyber Readiness Challenge by Symantec, October 29-30, 2015.
- **Second Place** in Cyber Defense Competition Cyber Defense Competition @CANSec 2015 hosted in University of Arkansas at Little Rock on October 24, 2015.
- Played Boston Key Party CTF 2015 Boston Key Party CTF 2015, Feb. 27, 2015, 10 p.m. – March 1, 2015, 5 p.m.

- Participated in Capture the Flag Challenge hosted at CSI CyberSEED University of Connecticut, Cyber Readiness Challenge by Symantec, October 20-21, 2014.
- **First Place** in Capture the Flag competition hosted at MTSU's Cyber Summit, May 5-6, 2014.
- Gave a talk in Computer Science Colloquium on Dive into Big Data, The University of Memphis, March 28, 2014.
- Gave a talk in Kennesaw State University on Applying Puzzle Based-Learning to Cyber-Security Education, October 12, 2013.
- Undergraduate Scholarship, Advanced College of Engineering and Management, 2001-2005
- Outstanding Student Stipend, Advanced College of Engineering and Management, 2001-2005

References

References will be provided upon request.