Osama Nusair
Cyber Security Researcher

Cyber Security researcher with an experience of 4 years in the web, network and cloud security. Major work in the field of smartphone forensics and minor roles in web and software development for windows & linux operating systems. Winner of 1st Digital Pakistan Cyber Security Hackthon 2021 securing top positions in Programming and Network Security.

Contact

Phone
+44-745-9822875

Email
xamaa6@gmail.com

Address
6 Sandbourne Road, B8 3NT,
Birmingham, UK

Education

2018 - 2022
BS Cyber Security
Air University, Islamabad

2013 - 2015
FSc - Pre Engineering
Fauji Foundation HSS, Attock

2013 - 2015
Matriculation
Fauji Foundation HSS, Attock

Expertise

- VAPT
- Smartphone Digital Forensics
- Computer Networks & Security
- C/C++/C#
- Python
- Django/Flask
- IDS/IPS

Language

English

Urdu

Pashto

Experience

BS Scholar

National Centre for Cyber Security, Islamabad
- Android Forensics Tool Development
- iOS Forensics Tool Development
- ext4 Filesystem Data Recovery
- Python/Flask

NAVTTC Instructor
- Introduction to Linux
- Network Scanning
- Penetration Testing tools and techniques
- OWASP Top 10 Vulnerabilities
- Intrusion Detection & Prevention System (Snort)
- Red Team Exercises

Founder AirOverflow
- Cyber Range
- Pakistan Cyber Security Challenge (PCC)
- Cyber Siege CTF
- VAPT for Pakistan Bureau of Statistics
- VAPT for Ministry of Planning, Development & Special Initiatives
- Workshops on Ethical Hacking & Defense
- Sandbox - Malware Analysis in sandbox environment

Achievements

★ Founder & CEO AirOverflow

★ President of Air University Cyber Security Society (AUCSS)

★ Orgaized multiple events such seminars, workshops, webinars & trainings under the flag of AUCSS

★ Won Digital Pakistan Cyber Security Hackathon 2021

★ Team lead from Air University for hackthebox Uni CTF'20

★ Lead host for E-Gaming event at Air Nexus'19

★ Multiple Speed programming competitions

Projects

Cyber Range - AirOverflow

Cyber Range is a virtual environment used for cyber security trainings. In cyber range, we are able to emulate real life cyber attack scenarios where red & blue teams can practice their skills and learn in a safe virtualized environment. This project is under development and uses multiple technologies such as Cloud, VPN, Software Defined Networks and Nested Virtualization technologies.

LogBeats - A SIEM Solution

During my Final Year Project, I chose SIEM Solution. As per my supervisor, I was to develop a basic structure of a security information and events management solution in python. I successfully developed and tested a SIEM solution capable of collecting, parsing and storing events and logs from multiple sources. This solution used both techniques of agent based and agentless log collection. Agent was developed in C# for windows OS. Agentless collection was tested by collecting logs from linux OS using rsyslog. Network devices such as routers and firewalls were also tested and successfull.

Android Smartphone Forensics - NCCS

During my work at National Centre for Cyber Security (NCCS), I worked as a digital forensics tool developer. Python3 was the primary programming language being used. For Android forensics, I automated the process of rooting android 5 and lower versions automatically with a single click. Moreover, worked with a few other android technologies, such as recovering and shredding data.

iOS Smartphone Forensics - NCCS

At NCCS, I was assigned the task of iOS forensics for which I developed an extensive solution capable of live data acquisition from Apple smartphone. It included phones application data, social media, contacts, apple accounts, gmail accounts, and many more. This tool was developed and tested on iOS v13.

Data Recovery - NCCS

Data recovery is the process of recovering deleted files in digital forensics. I developed multiple solutions to recover deleted data including images, microsoft documents (word, excel, etc), zip files, mp3, mp4, text and many other files. This task also led me to understanding of ext3 and ext4 linux file system structure and how data is stored on the hard drive.

Other Projects

- Automatic Email Setup & Bulk Sender - AirOverflow
- Snort IDS/IPS
- LAN IP changer with GUI in C#
- Ransomware Techniques in C++

VAPT

Vulnerability Assessment and Penetration Testing (VAPT) has been our major service at AirOverflow. VAPT services were provided to the following government bodies:

- Ministry of Planning, Development & Special Initiatives
- Pakistan Bureau of Statistics

Events

PCC - AirOverflow/NCCS

Pakistan CyberSecurity Challenge (PCC) was a hackathon event held in 2022 by NCCS & AirOverflow as part of a growing cyber security challenge in the country. Students from all across Pakistan were invited to attend and participate in the event and prizes were distributed among the winners. About 120+ teams having 360+ participants was a successful and an exceptional event in the cyber security of Pakistan.

Workshops - AirOverflow

AirOverflow held workshops for practical hands-on cyber security trainings on multiple occasions. Some significant workshops include Introduction to Linux, Digital Forensics, Web App Exploitation and Password Cracking.

Cyber Siege CTF - AirOverflow

A capture-the-flag event was held exclusively for Air University Students in order to practice their skillset. Awards were distributed among the winners. This event accommodated 100+ teams and 300+ participants.

Talk - AirOverflow/IRS

Invited as a guest speaker by the Institute of Regional Studies (IRS) to have a table talk on the topic, "Cyber Security & the Role of Corporate Sector".

Guest Lecture - AirOverflow/Connected Pakistan

A guest lecture on the topic, "Cyber Security Trends" at an E-Mustakbil event hosted by Connected Pakistan in collaboration with AirOverflow.