RAYHAN BAIG

rayhanbaig@gmail.com +1(585)2692416 Rochester, U.S.A linkedin.com/in/rayhan-baig
github.com/Rayhan2525

EDUCATION

Bachelor of Science in Cybersecurity 05/2019 – 05/2024
Rochester Institute of Technology Rochester, U.S.A
- Academic scholarship.
- CGPA: 3.72/4.00 (*Magna Cum Laude*).

TECHNICAL SKILLS

- **Hacking Tools:** Metasploit, Nmap, Hydra, Hashcat, Burp Suite, John the Ripper, Wireshark, Responder.
- **Programming Languages:** Python, Java, Assembly language, HTML, CSS, Rust, PHP, JavaScript.

PROFESSIONAL EXPERIENCE

Information Technology Network Co-Op (Internship) 05/2023 – 12/2023
Wegmans Food Markets Inc. Rochester NY, U.S.A
- Managed IT systems and network infrastructure of Wegmans Food Markets.
- Utilized problem-solving skills to troubleshoot and resolve complex network issues.
- Collaborated with IT security team to mitigate security vulnerabilities and implement security controls.
- Configured Palo Alto firewalls to maintain secure web traffic flow.
- Worked with security monitoring tools such as Forescout and Crowdstrike to implement security controls.

Software and Systems Engineer (Internship) 05/2022 – 08/2022
Neutral Fuels LLC. Dubai, U.A.E
- Automated data scraping from web portals using Python scripts.
- Developed Python scripts for company data processing and visualization.
- Built cross-platform mobile app with Flutter for enhanced business connectivity.
- Designed user-friendly front-end, integrated Microsoft authentication, and utilized Firebase database for app development.

PROJECTS

Cybersecurity Capstone Project: Stepping Stone Data Collection
- Built a functional network infrastructure and installed network services and vulnerabilities into the machines.
- Conducted a competition to have students attack the network and gathered network traffic using Wireshark.
- Programmed scripts using Python and worked with Python libraries to detect stepping stone attack pattern.

Cybersecurity Projects
- Member of the R.I.T Security Club. Participated in penetration testing and ethical hacking events.
- Attended BsidesROC 2024 Cybersecurity conference. Participated in MetaCTF competition. Solved web, binary, and SQL injection challenges.
- Participated in DICE CTF and 0xL4ugh CTF competitions. Solved web, binary, and SQL injection challenges.
- Participated in Incident Response Security Competition (IRSeC) as a White Team member, and provided hardware and technology support to Blue Team.
- Performed Red Team penetration testing operations on Linux and Windows OS. Exploited binary, web, and OS vulnerabilities to gain root access.
- Performed Password brute force attacks on Windows Active Directory applications using Hydra, and Patator.
- Utilized Nmap to perform extensive network scans and identify hosts and vulnerabilities.
- Exploited vulnerabilities on machines using Metasploit sessions.
- Utilized tools such as Burp Suite to set up proxy interception and exploit web vulnerabilities.
- Built a Flask web app with user authentication via Microsoft Azure AD using MSAL, enhancing security and user management.
- Automated asset discovery on Linux and Windows machines using Ansible and OSQuery for risk management reporting.