Murat Zamir

OBJECTIVE

Constantly enhancing skillset on penetration testing, web application security, and network security. Looking for a summer 2023 internship.

EDUCATION

Purdue University, West Lafayette, IN — August 2020 - May 2024
Bachelor of Science in Cybersecurity | Purdue Polytechnic Institute — GPA: 3.53/4.0

- b01lers CTF (Capture the Flag) | Member
    - Learning Cryptography, Web Exploitation, Penetration Testing within the lab environment

Relevant Coursework: Software Development Concepts, System Development, Cybersecurity Fundamentals, Cryptography, UNIX Fundamentals, Policy, Regulations and Ethics in IT, Bar Codes to Biometrics, Network Engineering Digital Forensics, Systems Programming (ANSI C/C++), Network Administration

SPECIALIZATIONS

Technical Skills: Penetration Testing, Network Security, Web Application Security, Digital Forensics, Python, SQL, Linux, React
Tools: Burp Suite, Nmap, Metasploit, Wireshark, Autopsy, AccessData FTK Imager/Registry Viewer, pfSense firewall, BIG-IP F5 LTM

WORK EXPERIENCE

Infrastructure & Network Engineer | Internship | Purdue University — April – August 2022

- Contributed to a **real-life cyberattack remediation** and **recovery phase** by conducting **malware scanning** on 200+ infected external drives and kept logs of every step in the **incident recovery** phase for the head of IT department
- Maintained accurate records of the telecommunication infrastructure and maintained proper connectivity throughout Purdue campus
- Installed, configured, and troubleshooted network equipment such as Cisco **Switches, UPSs,** and **WAPs**

PROJECTS

DevOps Pipeline | Medium Article — March 2023

- Possessed knowledge of analyzing source code and version control systems, including **security considerations**, **dependency management**, and **automated testing**.
- Acquired knowledge on DevOps environments, including in-depth analysis of **CI/CD pipeline**
- Discussed various pipeline environments and their specific use cases regarding different security postures

Enterprise Network Administration | Lab Project - Purdue University — February 2023

- Created an enterprise IT network infrastructure by a secure firewall solution that allows unsolicited traffic to reach Internet servers
- Set up **pfSense firewall** with 4 different zones, allowed mail exchange through **Postfix** server, manage SPAM with **Spamassassin**
- Deployed external/internal **DNS** services to forward recursive queries across the network utilizing **DNS records** (A, MX, CNAME)
- Hosted secure web servers (**Apache2**) using SSL based sites and a transparent proxy server (**Squid**) in the **DMZ** zone
- Implemented an **application delivery system** using Big-IP LTM to **load balance** and **fail over** across the web servers

The Cyber Range (Defender 302) | cyberTAP — October 2022

- Monitored and analyzed live malicious network traffics using **SIEM** tools (IBM QRadar, Zenoss, Palo Alto Firewall)
- Enhanced defensive security operation skills including **incident response** frameworks, the cyber **kill chain**, and **SOC operations**
- Prepared cyber incident reports covering the CIA triad impact, attacker profile, threat hunting, recovery, remediation, prevention.

AWS Home Lab | Automated w/ Terraform — August 2022

- Created a **VPC** environment, assigned **IPv4 CIDR block** for subnet, associate **subnet** with **routing table**, created security groups to allow port forwarding, assigned **elastic IP** to host an **Ubuntu** web server by installing **Apache2**
- Securely controlled access to AWS resources by implementing **IAM** users, security groups, principals, and roles
- Set alarms using **CloudWatch** to notify admin when a specified metric reaches a threshold

The Cyber Kill Chain | Medium Article — November 2022

- Explained all 7 layers of the Cyber Kill Chain
- Analyzed several weaknesses and possible protections for organizations to apply their network infrastructure

RELEVANT COURSE WORK

Jr. Penetration Tester | THM Path — August 2022

- Performed **content discovery, subdomain enumeration, authentication bypass** using vulnerable web applications
- Exploited websites by testing for **IDOR, file inclusion, XSS** and **SQL injection** vulnerabilities as well as learned remediation process of the **OWASP Top 10**

Practical Ethical Hacking | TCM Security — July 2022

- Performed **security assessment** testing for vulnerable software by using industry trusted **penetration tools** and application
- Developed proficiency in **reconnaissance** and information gathering, including network and web application security analysis
- Examined **threat models** and **vulnerability assessment** through the use of **scanning tools** and **enumeration** strategies