BERK POLAT

COMPUTER ENGINEERING

CONTACT

☎ +905533477165

✉ berkopolat@gmail.com

Gümüşpınar Mah. Millet Cd.
Istanbul/Kartal

www.github.com/berkpolatCE

EDUCATION

2022 - ONGOING
ISTANBUL OKAN UNIVERSITY

- Computer Engineering (English)

SKILLS

- Advanced C++ and Python
- Intermediate Level Java and Lua
- Advanced Proficiency in Linux and Windows environments.
- Knowledge on common cybersecurity tools (nmap, metasploit framework, sqlmap, web proxies)
- Understanding of Computer Networks, Web Applications, HTTP/HTTPS protocols, Web Security
- Network Traffic Analysis
- Vulnerability Assessment

LANGUAGES

- Turkish (Native)
- English (C1, 8.0 IELTS Score)

PROFILE

A dedicated and passionate Computer Engineering student currently in the third year at Istanbul Okan University. Possesses advanced proficiency in C++ and Python, with intermediate skills in Java and Lua. Specializes in cybersecurity, actively engaging in practical learning and challenges on Hack The Box to enhance hands-on experience. Demonstrates advanced knowledge of both Linux and Windows operating systems. Eager to apply technical expertise and problem-solving skills in cybersecurity and software development roles.

CYBERSECURITY EXPERIENCE

Hack The Box
Active Learner and Practitioner (2022 - Present)

- Engaged in various cybersecurity challenges and labs to enhance practical skills.
- Developed expertise in areas such as network enumeration, web application attacks, and command injections.
- Applied knowledge in real-world scenarios to identify and exploit vulnerabilities.

CYBERSECURITY PROJECTS

Web Application Security Assessments

Utilized knowledge from Hack The Box modules like SQL Injection Fundamentals, Cross-Site Scripting (XSS), and File Inclusion to assess and strengthen web application security. Identified vulnerabilities and recommended mitigation strategies to enhance protection against common web attacks.

Network Enumeration and Analysis

Applied skills from Network Enumeration with Nmap and Introduction to Networking to conduct thorough network scans and analyses. Mapped out network structures and identified potential security weaknesses using tools like Nmap and custom Python scripts.

Penetration Testing Simulations

Leveraged modules such as Penetration Testing Process, Attacking Common Services, and Command Injections to perform simulated penetration tests. Gained hands-on experience with tools like the Metasploit Framework and SQLMap to exploit vulnerabilities and understand attack vectors.