Cansu Kayalar

About

I am Cansu Kayalar. Driven by my deep curiosity about the world of cybersecurity, I am constantly developing myself and actively producing projects. With my open approach to learning and analytical perspective, I prioritize putting my theoretical knowledge into practice. I aim to specialize in Penetration Testing (Pentest) and deepen my expertise in this field to shape my career. With my strong communication skills, I want to create value in both individual and team work and contribute to a secure digital future by using innovative technologies.

Contact

cansukayalar5@gmail.com
cansukayalar.com

LinkedIn:
https://www.linkedin.com/in/cansu-kayalar-b55839294/
Github:
https://github.com/jansudo/

Project

Cypture – Web Application Scanner
GitHub: https://github.com/jansudo/cypture
A security scanning tool developed to identify vulnerabilities in web applications.

CTFc – Free CTF Platform Template (CTFd Alternative)
GitHub: https://github.com/jansudo/CTFc
An open-source and free template for organizing Capture The Flag (CTF) competitions.

LLM-Sec-Tool – Prompt Injection Detection Tool
GitHub: https://github.com/jansudo/llm-security-tool
An AI-based security tool aimed at detecting prompt injection vulnerabilities in Large Language Models.

TextoJi – AES-Based Data Hiding Platform
Website: https://textoji.introvert.team
A web platform that allows hiding data inside emojis using AES encryption.

mewith.me – Anonymous Sharing Platform
Website: https://mewith.me
A web application that enables users to share thoughts freely and anonymously.

introvert.team Blog – Cybersecurity & Cloud Blog
Website: https://blog.introvert.team
A blog platform co-developed with a teammate where I regularly publish articles on cybersecurity and cloud technologies.
Sample topics include AWS EC2 attacks and defense, Azure fundamentals, cloud security, and XSS vulnerabilities.

Experience

Threat Intelligence Specialist Intern *ThreatMon | [Oct 2025] – [Dec 2025]*

- Played an active role in monitoring the cyber threat landscape, collecting data on potential threat actors and emerging attack vectors.
- Conducted threat analysis using Open Source Intelligence (OSINT) techniques within the **Cyber Threat Intelligence (CTI)** lifecycle and contributed to actionable intelligence reporting.
- Tracked malware campaigns and ransomware groups to support the development of proactive defense strategies.
- Developed insights into Threat Hunting concepts to assist in mitigating organizational risks and enhancing situational awareness.

Cyber Security Intern T.C. İletişim Başkanlığı | *[Jul 2025] – [Sept 2025]*

- Assisted in securing corporate network infrastructure, gaining in-depth proficiency in **Network Security** protocols and architecture.
- Gained hands-on experience in network traffic analysis, Firewall management, and Intrusion Detection/Prevention Systems (IDS/IPS).
- Participated in identifying network vulnerabilities against potential cyber-attacks, contributing to the hardening of defense mechanisms.
- Experienced processes compliant with national security standards regarding the protection of critical public data and secure data transmission.

PSA Teknoloji Cyber Security Expert | *Jan 2026 – Present*

- Conducted comprehensive web and mobile application penetration testing to identify security vulnerabilities.
-
- Analyzed system and network logs to detect suspicious activities and potential security threats.
- Performed manual and automated vulnerability assessments to improve overall security posture.
- Documented and reported technical findings with actionable remediation steps.

Education and Certifications

Karadeniz Technical University | *Trabzon, Turkiye* **B.Sc. in Computer Engineering** | *[2022] – Present (Expected: 2027)*

- **3rd Year Student** (Junior)
- **Relevant Coursework:** Computer Networks, Operating Systems, Data Structures & Algorithms, Introduction to Cyber Security.
- **English Proficiency:** B2 Level (Upper Intermediate) supported by technical coursework

Siber Vatan Cyber Security Bootcamp | *Republic of Türkiye Ministry of Industry and Technology*

- *Prestigious Training Program:* Selected through a competitive process for Turkey's leading government-backed cyber security capability building program.
- *Core Competencies:* Gained advanced hands-on experience in offensive and defensive security operations, malware analysis, and incident response via intensive bootcamps.
- View Credential

Certified Associate Penetration Tester (CAPT) | *Hackviser*

- *Hands-on Proficiency:* Demonstrated ability to identify and exploit vulnerabilities in realistic network environments through a purely practical, performance-based exam.
- *Focus Areas:* Network penetration testing, privilege escalation, and manual vulnerability verification.
- View Credential

Certificate of Ethical Hacker | *Cisco*

- *Comprehensive Ethical Hacking Skills:* Covered the complete lifecycle of penetration testing from reconnaissance to reporting.
- **Key Technical Competencies:**
  - **Exploitation:** Exploiting Applications, Exploiting Networks, Social Engineering.
  - **Assessment & Security:** Vulnerability Assessment, Vulnerability Scanning, IoT Security.
  - **Operations:** Penetration Testing, Pentesting Tools, Professional Reporting.
- View Credential

Web Attack Detection and Analysis | *LetsDefend*

- *Blue Team Operations:* Specialized training on detecting, analyzing, and mitigating web-based cyber attacks using real-world log analysis techniques.
- View Credential

Advent of Cyber 2025 | *TryHackMe*

Security Bootcamp: Completed a 24-day intensive program covering a broad spectrum of offensive and defensive security domains through daily real-world scenarios.

Key Technical Competencies:

- **AppSec & Cloud:** IDOR, XSS, Prompt Injection, Race Conditions, AWS Security, and Containers.
- **Blue Team & Forensics:** SOC Operations (Splunk), Digital Forensics, Malware Analysis (YARA), and C2 Detection.
- **Infrastructure:** Linux CLI, Network Discovery, and ICS/Modbus Security.

View Credential

Technical Proficiencies

- **Programming Languages:** Python, Go (Golang), C, C++, JavaScript.
- **Cyber Security Tools:** Burp Suite, Wireshark, Nmap, Metasploit, SQLMap etc.
- **Infrastructure & Systems:** Docker, Linux Administration, Network Security Protocols.

Core Competencies (Soft Skills)

- **Innovative Ideation:** Recognized for generating creative solutions and strategic ideas in collaborative environments ("Idea Generator").
- **Communication & Collaboration:** Strong interpersonal skills with a proactive approach to team synergy and professional networking.

- **Adaptability:** Quick to learn and implement emerging technologies in dynamic project requirements.

- **Technological Innovation:** Passionate about exploring cutting-edge technologies and adapting them to security workflows.
- **Professional Networking:** Actively engaging in tech communities, cybersecurity summits, and collaborative workshops.
- **Continuous Learning:** Solving CTF challenges and following global cybersecurity trends to stay ahead of threat vectors.