Burak Baris

Cyber Security Expert

Address Istanbul, Turkey 34734

Phone +90 501 579 18 57

E-mail contact@burakbaris.com

Dynamic cybersecurity professional with a robust foundation in red team penetration testing and a strong emphasis on blue team operations, including incident response, threat detection, and security monitoring. Proven expertise in identifying attack vectors, privilege escalation paths, and lateral movement techniques, effectively translating findings into actionable defensive controls and detection logic. Hands-on experience includes vulnerability assessment, network security, and adversary simulation, supported by practical engagement in Capture The Flag (CTF) environments. Committed to advancing cybersecurity knowledge through the creation of technical content, including educational materials and blog posts focused on ethical hacking and defensive security practices.

Websites, Portfolios, Profiles

- https://www.linkedin.com/in/burak-baris/

Skills

Security Operations & Blue Team

- Incident response, threat detection, and log analysis
- SIEM usage and detection logic development (KQL, query-based analysis) using Splunk Enterprise Security, Microsoft Sentinel
- Threat management, mitigation, and risk assessment processes
- Security risk register maintenance and review

Offensive Security & Adversary Simulation

- Penetration testing across web, network, and wireless environments
- Tooling: Metasploit, Burp Suite, Nessus, OWASP ZAP, Nmap
- Credential attacks and hash cracking (NTLM, SHA family) using Hashcat, John the Ripper

- Network exploitation and traffic interception (Netcat, Ettercap, Wireshark)
- Wireless security testing (WEP, WPA, WPA2)
- Social engineering attack simulation

Detection, Analysis & Reverse Engineering

- Real-time network traffic analysis with Wireshark
- Malware analysis, reverse engineering, and binary exploitation using Ghidra, Radare2, GDB
- Low-level analysis (assembly, memory debugging, CPU-level behavior)

Cloud & Infrastructure Security

- Cloud security architectures in Amazon Web Services and Microsoft Azure
- Virtualization and lab environments: KVM, VMware, VirtualBox, Hyper-V
- Linux/Unix systems (Arch, Debian, Red Hat) administration and security hardening

Programming & Automation

- Python, Bash, PowerShell (automation, scripting, security tooling)
- C, C++, Java, JavaScript (secure coding and low-level analysis)

Technical Communication

- Penetration testing reporting and security documentation
- Writing technical content (blogs, educational material) explaining vulnerabilities and mitigations

Experience

Dec 2023 - Sep 2024

Cyber Security Consultant

ITserv Technology, Istanbul

Conducted penetration testing and adversary simulations across client environments to identify vulnerabilities, privilege escalation paths, and lateral movement risks

- Delivered post-engagement remediation aligned with deployed security products, improving secure configuration and reducing attack surface

- Designed and developed an internal CERT capability for real-time incident detection and coordinated response across company and customer infrastructures
- Built customized endpoint protection solutions, reducing malware infections and strengthening endpoint security posture in client environments
- Translated offensive findings into defensive controls and detection strategies, supporting blue team operations and improving threat visibility

Education

Jan 2023 **Bachelor of Science: Computer Systems Cyber Security**

Nottingham Trent University - United Kingdom - Nottingham

- Some Key Modules I studied to intensify my skill set:
- - Advanced Networking Information Security
- - Network Design & Administration
- - Service-Centric and Cloud Computing
- - Digital Investigations and Forensics
- - Distributed Network Architecture and Operating Systems
- - Advanced Topics in Cyber Security
- - Security in Practice
- - Operating Systems and Architecture
- Degree Awarded with 1st Class with Honors

Jan 2019 **High School Diploma**

Istanbul Anatolian High School - Istanbul

GPA: Graduated with AAB equivalent

PROJECTS

PROJECTS & PUBLIC WORK

Security Research & Content

- **KnuckleSecurity Blog** — IT and cybersecurity-focused technical writing covering offensive techniques, defensive practices, and vulnerability analysis

Security Tools & Offensive Research

- **Bbcap** — Network traffic analysis tool inspired by Wireshark, designed for packet inspection and analysis in controlled environments
- **KnuckleVault** — API-based open-source password manager focusing on secure credential storage and access control mechanisms
- **UncleBob Vulnerable Machine** — Custom vulnerable lab (targeting Hack The Box publication) focused on horizontal privilege escalation and binary exploitation techniques

Applications & Systems Development

- **Knuckle Travel** — Full-stack web application with user registration and real-time communication features; includes authentication and session management design
- **Weighted Round Robin Load Balancer** — Reverse proxy implementation for distributing external traffic across internal services using load balancing algorithms

Infrastructure & System Tools

- **KryArch** — Automated Arch Linux installation and configuration tool for rapid system provisioning and reproducible setups
- **thinkpadfan-gui** — System-level utility for hardware control and monitoring on Linux-based environments