Burak Baris

SECURITY SPECIALIST

Istanbul, Turkey · contact@burakbaris.com · +90 501 579 18 57 · linkedin.com/in/burak-baris · burakbaris.com · github.com/burakbaris0x01

PROFESSIONAL SUMMARY

Security Specialist with hands-on experience in penetration testing, adversary simulation, vulnerability assessment, and defensive security operations. Skilled in identifying attack paths, privilege escalation risks, and lateral movement opportunities, and translating offensive findings into defensive controls and detection strategies. Background includes client-facing security consulting, incident detection capability development, endpoint protection improvement, and practical security research.

CORE SKILLS

Security Operations	Incident Response · Threat Detection · Log Analysis · Security Monitoring · Risk Assessment
SIEM & Detection	Microsoft Sentinel · Splunk · KQL · Detection Logic
Offensive Security	Penetration Testing · Vulnerability Assessment · Adversary Simulation · Web / Network / Wireless
Tools	Burp Suite · Nessus · OWASP ZAP · Nmap · Metasploit · Wireshark · Hashcat
Systems & Cloud	Linux · Windows · AWS · Azure · VMware · Active Directory
Programming	Python · Bash · PowerShell · JavaScript · C · C++
Analysis	Malware Analysis · Reverse Engineering · Ghidra · Radare2 · GDB

PROFESSIONAL EXPERIENCE

Cyber Security Consultant · ITserv Technology — Dec 2023 – Sep 2024 · Istanbul, Turkey

- Conducted penetration testing and adversary simulation across client environments to identify vulnerabilities, privilege escalation paths, and lateral movement risks.
- Delivered remediation guidance aligned with deployed security products, improving secure configuration and reducing attack surface.
- Supported the design and development of an internal CERT capability for real-time incident detection and coordinated response across company and customer infrastructures.
- Improved endpoint protection posture through customized security configurations, malware prevention controls, and defensive hardening recommendations.
- Translated offensive security findings into defensive controls, detection strategies, and blue team operational improvements.
- Produced technical security documentation and client-facing reports with clear findings, risk explanations, and remediation steps.

EDUCATION

Bachelor of Science — Computer Systems Cyber Security
Nottingham Trent University · 1st Class Honours
Awarded Jan 2023
Nottingham, UK

Advanced Networking Information Security · Network Design & Administration · Service-Centric & Cloud Computing · Digital Investigations & Forensics · Distributed Network Architecture · Advanced Topics in Cyber Security

SELECTED PROJECTS

Security Blog	Technical cybersecurity writing covering offensive techniques, defensive practices, vulnerability analysis, and mitigation guidance.
BBCap	Network traffic analysis tool inspired by Wireshark, designed for packet inspection and analysis in controlled environments.
KnuckleVault	API-based open-source password manager focused on secure credential storage, authentication, and access control mechanisms.
UncleBob Vulnerable Machine	Custom vulnerable lab focused on horizontal privilege escalation and binary exploitation techniques.
Weighted Round Robin LB	Reverse proxy implementation for distributing external traffic across internal services using load balancing algorithms.

CERTIFICATIONS & DEVELOPMENT

Currently Preparing Cisco CCNA · CompTIA CySA+ · Microsoft SC-200