Furkan Goksel

furkan.goksel27@gmail.com   in linkedin.com/in/frkngksl/   ○ github.com/frkngksl

Education

Middle East Technical University   2016-2021
Bachelor of Science in Computer Engineering (GPA: 3.88 / 4.00)   *Ankara, Turkey*

Experience

Picus Security   March 2021 – Present
Senior Red Team Engineer   *Ankara, Turkey*
- Transformed Exposure Management outputs into actionable attack paths, showcasing end-to-end compromise scenarios to prioritize real-world risk across enterprise environments.
- Simulated lateral movement in Microsoft Active Directory and crafted endpoint attack scenarios across Windows, Linux, and macOS, targeting MITRE ATT&CK TTPs and evading EDR/EPP defenses.
- Performed internal Red Teaming operations and Penetration Tests to assess organizational resilience against real-world attack vectors.

Purdue University   July 2020 – Oct 2020
Undergraduate Student Researcher   *West Lafayette, USA*
- Co-authored *"On the Safety Implications of Misordered Events and Commands in IoT Systems" (IEEE SafeThings 2021)*, demonstrating how adversaries can exploit misordered legitimate IoT events to violate safety properties.

Secrove Information Security Consulting   March 2020 – Sept 2020
Security Researcher   *İstanbul, Turkey*
- Developed a custom Linux Endpoint Detection and Response system leveraging Ptrace system calls to monitor and intercept process behaviors for real-time threat detection and analysis.

Secrove Information Security Consulting   March 2019 – Sept 2019
Intern   *İstanbul, Turkey*
- Performed Mobile and Web Application penetration testing for clients, identifying security vulnerabilities and providing actionable remediation guidance in real-world environments.

Projects

Shoggoth | *BlackHat Europe 2022 Arsenal Presentation*
- Engineered polymorphic encryptor to convert COFF, BOF and PE files into shellcode that consists of polymorphically encrypted payloads and their corresponding loaders for enabling in-memory payload execution across Windows systems.
- Implemented with the AsmJit JIT compilation framework to dynamically generate machine code for encryption/decryption routines and garbage instruction stubs targeting x86/x64 architectures
- Integrated advanced garbage instruction generation for evasion, including side-effect-preserving sequences, no-op jumps, and fake call patterns to confuse static analysis.

WAFADM | *Best Senior Design Project at METU CENG Demo Day 2021*
- Enhanced ModSecurity Web Application Firewall by implementing custom rule compilers, rule generators, access zones, and extending core functionalities for Web Application attack detection and mitigation.

Process Tracer | *BSCon2020 Presentation*
- Developed a browser-based interface for monitoring and manipulating Linux process system calls, enabling interactive analysis of suspicious programs for research and security purposes.

Achievements

Certificates: Certified Red Team Professional (CRTP), OffSec Certified Professional (OSCP), Certified Red Team Operator (CRTO)
CVEs: CVE-2022–34008, CVE-2022-31464, CVE-2021-30461, CVE-2020-35597
Publications: AgriLoRa: A Digital Twin Framework for Smart Agriculture, On the Safety Implications of Misordered Events and Commands in IoT Systems