



Can ("John") Kurnaz

Technical Security Consultant, Nixu Cybersecurity

Experience

- 12.2019–Present **Technical Security Consultant,**
NIXU CYBERSECURITY, Amsterdam/Netherlands.
- Planning and conducting penetration tests, vulnerability assessments, architecture reviews and configuration reviews both for Information Technology (IT) and Operational Technology (OT) (e.g. Industrial Control Systems (ICS)).
 - Handling Incident Response cases for both IT and OT.
 - Threat Hunting for IT and OT.
 - Contributing to Red Team assessments.
 - Supporting customers during OT monitoring systems architecture design decision process for their ICS networks, supporting on deployment and fine-tuning of OT Monitoring systems.
- 09.2018–12.2019 **Senior Consultant (Cybersecurity),**
KPMG, Amstelveen/Netherlands.
- Conducting penetration tests to external and internal networks, web applications, WiFi, IoT and ICS/SCADA systems and components.
 - Conducting vulnerability assessment and architecture review of Industrial Control Systems.
 - Supporting Incident Response cases.
 - Presenting reports to the customers.
- 10.2017–09.2018 **Penetration Tester,**
EUROPEAN NETWORK FOR CYBER SECURITY (ENCS), The Hague/Netherlands.
- Conducting robustness tests and penetration tests for IT and OT infrastructure such as smart meters, electric vehicle charging points and ICS/SCADA systems and components.
 - Working on physical security assessments of IT/OT hardware, servers, computer systems, and networks.
 - Instructing "Red Team – Blue Team Training for Industrial Control Systems and Smart Grid Cybersecurity".
 - Maintaining RT–BT Hands-on Simulation Lab environment.
- 01.2015–10.2017 **Penetration Tester,**
BARIKAT CYBER SECURITY B.V., Ankara/Turkey.
- Planning and conducting penetration tests to external and internal networks, web applications and WiFi networks.
 - Planning and conducting DDoS and load tests for availability assessment.
 - Working on physical security assessments of server rooms, computer systems, networks and physical assets including buildings.
 - Presenting penetration test results to customers.
 - Scheduling, prioritizing and distributing the projects and/or tasks for penetration testing team members.

Certifications

- 05.2020 **Nozomi Networks Certified Engineer**, Nozomi Networks, May 2020 - May 2022.
- 09.2019 **Global Industrial Cyber Security Professional (GICSP)**, SANS - GIAC, Sep 2019 - Sep 2023.
- 06.2018 **Offensive Security Certified Professional (OSCP)**, Offensive Security, OS-101-014130.
- 05.2018 **Offensive Security Wireless Professional (OSWP)**, Offensive Security, OS-BWA-035948.
- 04.2018 **Certified Ethical Hacker (CEH)**, EC-Council, ECC96879536854, Apr 2018 – May 2021.

Voorhout – The Netherlands

📞 [REDACTED] • ✉ [can.kurnaz\[at\]gmail.com](mailto:can.kurnaz[at]gmail.com) • 🌐 <https://can.github.io>

1/2

Education

- 2016–... **Master's Degree, Cybersecurity**, *Middle East Technical University*, Ankara/Turkey.
2009–2014 **Bachelor's Degree, Computer Engineering**, *Ondokuz Mayıs University*, Samsun/Turkey.
2011–2012 **Computer Science**, *Linnéuniversitetet / Linnaeus University*, Växjö/Sweden.
Erasmus Exchange Programme Student

Communication Skills and Publications

- 08.2020 Accepted Presentation: "DeTT&CT for ICS" at Black Hat USA 2020 (Arsenal), Virtual Event.
08.2019 Presentation: "Get your next Europe trip for free! Long live the vulnerable EV charging points!" at DEFCON 27 (IoT Village), Las Vegas/USA.
08.2019 Presentation: "Wi-Fi Threat Modeling and Monitoring" at DEFCON 27 (Packet Hacking Village), Las Vegas/USA.
08.2019 Presentation: "WTS: Scenario-Based WiFi Network Threat Simulation" at Black Hat USA 2019 (Arsenal), Las Vegas/USA.
02.2019 Publication: ICS CERT Advisory (ICSA-19-059-01) Multiple PSI GridConnect GmbH Products | Cross Site Scripting Vulnerability (CVE-2019-6528) (<https://www.us-cert.gov/ics/advisories/ICSA-19-059-01>).
10.2018 Publication: ICS CERT Advisory (ICSA-18-305-03) Circontrol CirCarLife | Found zero-day vulnerabilities in an EV charging point. (CVE-2018-17918 and CVE-2018-17922) (<https://ics-cert.us-cert.gov/advisories/ICSA-18-305-03>).
08.2018 Presentation: "WiPi-Hunter - It Strikes against Illegal Wireless Network Activities (Detect and active response)" at DEFCON 26 (Demo Labs), Las Vegas/USA.
03.2018 Publication: Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module < 4.25 - Denial of Service Exploit (<https://www.exploit-db.com/exploits/44103>) and Metasploit Module (<https://github.com/rapid7/metasploit-framework/pull/9692>).

Languages

Turkish	Native	C2
English	Advanced	C1
Dutch	Elementary	A2

References

[REDACTED], Please send me an e-mail if you want to see my resume with my references.