Fabio Carretto

ESPERIENZA LAVORATIVA

Founder e Amministratore, Penetration Tester e Ethical Hacker
Soter IT Security S.r.l. [02/2021 – Attuale]

Città: Torino

Sono uno dei creatori e amministratori dell'azienda Soter IT Security S.r.l. dove svolgo attività di Penetration Test, Vulnerability Assessment e più in generale attività di Offensive Security su Software e Hardware.
Inoltre, in qualità di CTO mi occupo di gestire l'infrastruttura aziendale e della configurazione di rete e dispositivi.
Mi occupo anche di sviluppare soluzioni software inerenti al campo della sicurezza, faccio attività di ricerca nel campo della Cyber-Security e mi occupo anche di corsi di formazione.

Software Security Consultant
IMQ Minded Security [04/2020 – 02/2021]

Penetration Test e Vulnerability Assessment su applicazioni WEB, Mobile e Network.
Attività di source-code analysis.

Penetration Tester / ICT Security Specialist
Certimeter Group [03/2019 – 05/2020]

Città: Torino

Vulnerability Assesment e Penetration Test su Applicazioni WEB, Networks (infrastrutturali) e Mobile (Android, IOS).
Attività di ricerca di vulnerabilità su software disponibili online o proprietari

IoT Security - Stage curriculare (Laurea Magistrale)
Certimeter Group [11/2018 – 04/2019]

Città: Torino

Ricerca sulla sicurezza dei dispositivi IoT e della loro interconnesione.
Analisi e approfondimento Firmware Exploitation.
Scoperte gravi vulnerabilità su Domoticz, pubblicati relativi CVE ed exploit.

Software Developer - Stage curriculare (Perito)
Oasis srl [05/2010 – 07/2010]

Città: Torino

Sviluppo software per applicazioni web.
Analisi e uso di Content Management System.

ISTRUZIONE E FORMAZIONE

Dottore Magistrale in informatica con 110/110
Università degli Studi di Torino. Dipartimento di Informatica [2015 – 2019]

Percorso carriera magistrale: Reti e Sistemi.
Particolare attenzione su argomenti di: Sicurezza informatica, Machine Learning e Reti Neurali, Reti complesse.

Dottore in informatica con voto 107/110
Università degli Studi di Torino. Dipartimento di Informatica [2011 – 2016]

Percorso Reti e Sistemi
Tesi: Rilevamento Defacement in tempo reale e adattabile

Perito in Elettronica e Telecomunicazioni. Voto 92/100

J.C. Maxwell, Nichelino (TO) [2005 – 2011]

Progetto finale: sistema embedded con microcontrollore pilotabile tramite usb in grado di gestire sistemi di illuminazione complessi.
Attività da sistemista: Network setup and management in una scuola.
Installazione di firewall, server proxy e filtri contenuti web.
Assemblaggio e configurazione di computer.

COMPETENZE LINGUISTICHE

Altre lingue:

inglese

ASCOLTO B1 **LETTURA** B1 **SCRITTURA** B1

PRODUZIONE ORALE B1 **INTERAZIONE ORALE** B1

Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato

PUBBLICAZIONI

Pubblicazioni

F. Bergadano, F. Carretto, F. Cogno, D. Ragno - Defacement Response via Keyed Learning, 8th IEEE IISA Conference, 2017.

F. Bergadano, F. Carretto, F. Cogno, D. Ragno - Defacement Detection with Passive Adversaries, Algorithms, 2019.

PATENTE DI GUIDA

Patente di guida: B

CYBER-SECURITY PROFILE

Cyber-Security Profile

Il mio nickname è bytevsbyte, twitter @bytevsbyt3. Sono attivo su diversi piattaforme di hacking, cerco vulnerabilità su portali di bug bounty o in software disponibili online.
Profilo HTB: www.hackthebox.eu/profile/27835
CVE pubblicati:
- CVE-2019-10664 - SQL Injection Domoticz
- CVE-2019-10678 - Command Injection Domoticz
- CVE-2019-10767 - Directory Traversal on ioBroker (snyk.io)
- CVE-2019-10765 - Directory Traversal on ioBroker (snyk.io)
- CVE-2019-10771 - Reflected XSS on ioBroker (snyk.io)

Exploit pubblici: Unauthenticated Remote Command Execution on Domoticz <= 4.10577

Nel 2018 ho creato, insieme ad altri, il team beerpwn, con il quale partecipo a competizioni Capture The Flag (CTF). Alcuni riferimenti: ctftime.org/team/53094, beerpwn.it, github.com/beerpwn, www.hackthebox.eu/teams/profile/608. Alcuni write-up relativi a challenge che ho risolto: Crond Writeup (Linux challenge), Beginner's Luck Writeup (web challenge), Black Echo (binary exploitation)

CERTIFICAZIONI

Certificazioni

2022 - OSWE (Offensive Security Web Expert)

2020 - OSCP (Offensive Security Certified Professional)

2011 - MTA (Microsoft Technology Associate), MOS (Microsoft Office Specialist), MCAS Vista

2010 - Cisco CCNA Discovery 2

2009 - Cisco CCNA Discovery 1

2007 - ECDL

ALTRE CAPACITÀ

Altre Capacità

Ottima capacità di spiegazione grazie alle numerose lezioni personali impartite.
Buona predisposizione al team working.
Prediligo ambienti di lavoro collaborativi dove si adotti una politica di condivisione del sapere.

TRATTAMENTO DEI DATI PERSONALI

Trattamento dei dati personali

Autorizzo il trattamento dei dati personali contenuti nel mio curriculum vitae in base all'art. 13 del D. Lgs. 196/2003 e all'art. 13 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Autorizzo il trattamento dei miei dati personali presenti nel CV ai sensi dell'art. 13 d. lgs. 30 giugno 2003 n. 196 - "Codice in materia di protezione dei dati personali" e dell'art. 13 GDPR 679/16 - "Regolamento europeo sulla protezione dei dati personali".