Antonio Squillace

Nazionalità: Italiana **Data di nascita:** 31/08/1997 **Sesso:** Maschile

Numero di telefono: (+39) 3335719248

Abitazione: Via T. Campanella 3, 88831 San Mauro Marchesato (Italia)

PRESENTAZIONE

Sono un professionista nel campo della sicurezza informatica con un'esperienza biennale come tester di penetrazione, specializzato nella valutazione di vulnerabilità, test di intrusione e nella redazione di report dettagliati sui rischi per la sicurezza. La mia esperienza include la progettazione e l'attuazione di test di penetrazione mirati, attraverso i quali ho efficacemente identificato e contribuito a mitigare minacce significative alla sicurezza IT di diverse organizzazioni. Dotato di una forte passione per l'innovazione e l'apprendimento continuo, sono costantemente alla ricerca di nuove sfide che mi permettano di espandere le mie conoscenze e competenze nel settore. Agile nell'adattamento a contesti diversificati, valorizzo il lavoro di squadra e la collaborazione come elementi chiave per il successo dei progetti di sicurezza informatica.

ESPERIENZA LAVORATIVA

Analista di Sicurezza Applicativa

[2024 – Attuale]

- Analisi statica e dinamica di file eseguibili, librerie software e applicazioni mobili per identificare comportamenti sospetti o malevoli
- Attività di reverse engineering su software e componenti per comprendere logiche di funzionamento interne e individuare vulnerabilità non documentate
- Utilizzo di debugger, disassemblatori (come IDA Pro, Ghidra) e sandbox per l'analisi approfondita del codice e del suo comportamento a runtime
- Documentazione tecnica delle vulnerabilità scoperte (es. buffer overflow, race condition) e stesura di report dettagliati con relative prove

Sviluppatore Backend

[2024 – Attuale]

- Sviluppo e manutenzione di applicazioni backend robuste, scalabili e performanti
- Progettazione e implementazione di API RESTful sicure per l'integrazione tra servizi
- Containerizzazione di applicazioni tramite Docker
- Conduzione di attività di code review per identificare e mitigare vulnerabilità di sicurezza, secondo le pratiche di sviluppo sicuro (Secure SDLC)
- Integrazione di controlli di sicurezza nel ciclo di vita dello sviluppo per la prevenzione di attacchi comuni (es. OWASP Top 10)

Poste Italiane

Penetration Tester

[01/05/2022 – 31/12/2023]

- Scansioni di Vulnerability Assessment mediante tool automatici
- Attività di Penetration Test infrastrutturali/applicativi
- Verifiche dello stato di sicurezza dei sistemi in ambiente di produzione e certificazione
- Attività di reportistica

Ministero della Giustizia

Security Assessment Consultant

[01/12/2022 – 30/06/2023]

- Attività di PT a livello applicativo
- Attività di reportistica
- Attività condotte su sistemi in certificazione

Università LUMSA ROMA

Security Assessment Consultant

[01/05/2023 – 30/11/2023]

- Rientro vulnerabilità
- Progettazione e gestione SOC
- Orchestratione e monitoraggio
- Attività di verifica

ISTRUZIONE E FORMAZIONE

Laurea Magistrale in Ingegneria Informatica

Università della Calabria [15/12/2022]

Città: Rende | **Paese:** Italia | **Campi di studio:** Cybersecurity | **Voto finale:** 110 | **Tesi:** Un sistema cyber range basato su digital twin per l'analisi di attacchi informatici a sistemi di controllo industriale

Il lavoro di tesi mira a utilizzare l'analisi dei processi per scoprire modelli comportamentali che consentiranno il rilevamento di attacchi informatici che modificano il flusso di controllo normale di un sistema cyber-fisico. Per fare ciò, si utilizza il Process Mining, un insieme di tecniche tradizionalmente utilizzate per il miglioramento dei processi aziendali ma che possono essere usate per il rilevamento di anomalie nei sistemi di controllo industriale. Un ulteriore attività condotta in questo lavoro di tesi, ha riguardato la realizzazione di uno scenario operativo immersivo che consiste di componenti emulative e simulative di sistemi cyber fisici per il testing e la verifica di eventuali vulnerabilità (applicando le suddette tecniche) in ambienti completamente isolati e controllati. Più precisamente, ci si è occupati della progettazione e implementazione di un sistema cyber range in grado di ospitare scenari che integrano digital twin (DT) sia per i sistemi IT ma anche per i sistemi ICS. Il DT utilizzato in questo studio è basato su un impianto di simulazione di un sistema di palletizzazione, i cui elementi principali sono: un braccio meccanico, una rulliera, un sensore e i pacchi. L'approccio di analisi utilizza questo gemello digitale per modellare ed eseguire diversi scenari realistici di attacco consapevole del processo e generare un set di dati che riflettono le misurazioni del processo, in condizioni di normale operatività e in scenari di attacco.

Laurea Triennale in Ingegneria Informatica

Università della Calabria [16/09/2019]

Città: Rende | **Paese:** Italia | **Voto finale:** 96 | **Tesi:** Attacchi informatici basati su tecniche basate su Return Oriented Programming

Il lavoro di tesi si propone di esplorare e analizzare in dettaglio la Return Oriented Programming (ROP), una tecnica avanzata di sfruttamento della memoria che consente agli aggressori di eseguire codice arbitrario nei sistemi vulnerabili. Attraverso un'indagine approfondita delle varie sfaccettature della ROP, il testo si addentra nelle metodologie con cui gli attaccanti possono eludere le moderne misure di sicurezza, quali la non esecuzione di codice (NX) e la randomizzazione dello spazio degli indirizzi (ASLR), dimostrando l'importanza di sviluppare e implementare strategie di difesa sempre più robuste e sofisticate.

Certified Ethical Hacker (CEH)

EC-Council [2024]

Corso di formazione Splunk Enterprise

5 Emme Informatica [2024]

Auditor/Lead Auditor per i Sistemi di Gestione della Sicurezza delle Informazioni IT (ISO/IEC 27001:2022)
DIMITTO CERTIFICATION SERVICES [2023]

Lead Auditor/Auditor ISO 27001:2017
DIMITTO CERTIFICATION SERVICES [2023]

Metodologie di audit secondo le norme ISO/IEC 17021-1:2015 – ISO 19011:2018
DIMITTO CERTIFICATION SERVICES [2023]

Mastering CVSS v3.1
FIRST Learning [2023]

Autopsy Training Course
Basis Tech [2020]

CyberChallenge.IT Training Course
Cybersecurity National Lab [2019]

Città: Rende | **Paese:** Italia

COMPETENZE LINGUISTICHE

Lingua madre: italiano

Altre lingue:

inglese

ASCOLTO B2 **LETTURA** B2 **SCRITTURA** B1

PRODUZIONE ORALE B1 **INTERAZIONE ORALE** B1

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

COMPETENZE

Competenze informatiche di base

Elaborazione testi (Buona) / Programmazione (Ottima) / Sistemi operativi (Ottima),

Linguaggi di Programmazione

Java / Python / C / Assembly / MySQL / Javascript / Scripting in Python, Bash e shell Windows / Typescript-base

Sistemi Operativi

Linux / MacOS / Windows / Android / iOS

Web Development

JavaEE servlet e jsp / Conoscenza del framework (Spring, Hibernate, JPA) / Gatsby JS

Cloud Services

Terraform / Ansible / Packer / Vault / Cloud-init

Simulatori

Factory I/O / OMNeT++

CyberSec Tool

Nmap / Frida (Mobile) / Nikto / Hashcat / BurpSuite / Scrapy / WFuzz / TcpDump / Netcat / Dirbuster / FUFF / Hydra / John / Metasploit / Wireshark / Ghauri / SQLmap / Dirb / Tracee / Fiddler / Ida

Compliance, normative, regolamenti, framework e standard

Cyber Security PTES,NIST,ISSAF,OSSTMM,WASC,OWASP,CVSS. / General Data Protection Regulation (GDPR) / Iso / Iec 27001 / Nist Csf / Dora / Uni En Iso 19011 / CSA

Ambienti di virtualizzazione

vmWare Workstation / VirtualBox / vmWare esXi / WSL / QEMU

CONTRIBUTI

[2023 – 2024]

Attività di Bug Bounty

- [**LVE-2023-0153**] Administrator account information exposure vulnerability in “LG SuperSign CMS”
- [**LVE-2023-0154**] Encrypted information exposure vulnerability in “LG SuperSign CMS”
- [**LVE-2023-0155**] RCE possible vulnerability by connecting bind shell in “LG SuperSign CMS”

Link: https://lgsecurity.lge.com/bulletins/idproducts#updateDetails

---