europass

Stefan Sabin Nicula

Date of birth: 21/12/1994 | **Nationality:** Romanian | **Sex:** Male | **Phone:** (+40) [redacted] | **Email:** niculastefan13@stud.ase.ro | **Website:** https://onexploit.com/

WORK EXPERIENCE

01/08/2022 – CURRENT Remote, Belgium

SENIOR PENETRATION TESTER SONY

- Web application and API Penetration Testing
- Source code review
- Mobile application review
- Cloud confi guration security review (AWS, GCP, Azure)

01/08/2019 – CURRENT Remote, United States

FREELANCE PENETRATION TESTER HACKERONE, 7ASECURITY, COBALT LABS INC.

https://hackerone.com/snicula
https://app.cobalt.io/snicula

- Leading project-based Penetration Testing engagements for complex customer solutions.
- Working on Penetration Testing projects for web applications, infrastructure, web services, APIs, and mobile applications.
- Manual and automated source code review.

01/07/2019 – 01/08/2022 Bucuresti, Romania

SENIOR THREAT RESEARCHER AVIRA/NORTONLIFELOCK

- Exploit development, vulnerability research and fuzzing on Windows
- Perform advanced static and dynamic malware analysis for PE, non-PE and Android malware
- Reverse engineering malware & exploits to understand their inner workings
- Researching new malware trends and incorporate new detection methodologies
- In-depth analysis for malware outbreak incidents & CVEs
- Responsible for internal training sessions and workshops for PE malware analysis and FP fi xing, Windows internals and Android internals

01/08/2016 – 01/07/2019 Bucuresti, Romania

SENIOR PENETRATION TESTER KPMG ROMANIA

- Participate in penetration testing engagements (web application,network confi guration & internal infrastructure, mobile application & API's,embedded systems security, code review, red teaming activities)
- Experience in operating systems internals & tools
- Provide technical vulnerability guidance by communicating risks andremediation strategies to infrastructure groups and developmentteams
- Develop custom tools for current engagements or long term tools tobe used in future projects or as Proof of Concept
- Experience in programming languages and development framework(Java, C#, C, Android Studio, Python)

EDUCATION AND TRAINING

01/10/2018 – CURRENT Bucuresti, Romania

PHD INFORMATION SECURITY Faculty of Cybernetics, Statistics and Economic Informatics

Level in EQF EQF level 8

08.08.2024 [redacted]

01/10/2016 – 01/06/2018 Bucuresti, Romania

IT&C SECURITY MASTER Faculty of Cybernetics, Statistics and Economic Informatics

Level in EQF EQF level 7

01/10/2013 – 01/06/2016 Bucuresti, Romania

BACHELOR'S DEGREE IN INFORMATICS Faculty of Cybernetics, Statistics and Economic Informatics

Level in EQF EQF level 6

TRAININGS/COURSES

01/05/2021 – 01/06/2021

Windows Kernel Exploitation Advanced

Upon completion of this training, participants will be able to learn:

- Exploit development process in kernel mode
- Mitigation bypasses
- Pool internals & Feng-Shui
- Arbitrary Read/Write primitive

Link https://hacksys.io/trainings/windows-kernel-exploitation-advanced

01/07/2020 – 01/08/2020

Advanced fuzzing and crash analysis

This training class is designed to introduce information security professionals to the best tools and technology available for automating vulnerability discovery and crash triage.

Link https://www.fuzzing.io/

01/09/2020 – 01/10/2020

Windows internals training

Understand the underlying mechanism and advanced services of the Windows OS and use that knowledge to write better and more efficient programs on Windows 7 and later.

Link https://github.com/zodiacon/syllabi/blob/main/Windows Internals.pdf

01/02/2019 – 01/03/2019

Advanced Exploit Development

Students will get the opportunity to learn how to write heap exploits for the Windows platform, using Windows 7, Windows 10, and Windows 11 as the example platform, but mostly focusing on learning & applying generic techniques that can be applied to other operating systems and heap implementations.

Link https://www.corelan-training.com/index.php/training/heap/

PROJECTS

01/08/2019 – 01/10/2023

Microsoft MAPP Partner

Researcher on Microsoft Active Protections Program, reverse engineer exploits, write detection rules, and implement hunting techniques to identify potential ITW exploit usage.

Link https://www.microsoft.com/en-us/msrc/mapp

01/10/2017 – 03/10/2017

IoT security/Speaker @Defcamp8

Research project focused on testing the security of an IoT robot. Technically specific in vector of attacks, entry points, and device hijacking opportunities.

Links https://securitycafe.ro/2017/09/22/robot-hacking-research/ | https://def.camp/speaker/stefan-nicula/

01/10/2017 – 03/10/2017

Weaponized RaspberryPi in Red Team Engagements

Contributed in creating a Raspberry Pi with Wi-Fi attacking capabilities and reverse SSH tunneling for acting like a pivot inside compromised networks. Used in Red Team engagements.

Link https://github.com/Matasareanu/RPI-weaponized/

PUBLICATIONS

2023

ValleyFall Spyware in the wild – From one sample to a hive of malware servers

Uncovered a new spyware named ValleyFall, identifi ed in the wild in mid-2023. This malware can infect people with a remote-control component also focused on password stealing and keylogging.

2022

Anatomy of an exploit in Windows win32k – CVE-2022-21882

Research about the CVE identifi cation, its impact, and how to analyze it. Includes technical details about the exploitation process, samples identifi ed in the wild and exploitation techniques.

Public Penetration Testing reports

Various public Penetration Testing reports on complex solutions:

- https://7asecurity.com/reports/pentest-report-minivpn.pdf
- https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

2020

Principles of Heap-based exploits on Windows

Differences between the Windows Heap Manager of Windows 7 & 10, browser-specific memory corruption exploits, heap-based vulnerabilities, and exploitation techniques such as heap spraying, LFH vs BEA, vtable pointers.

2020

EXPLOITING STACK-BASED BUFFER OVERFLOW USING MODERN-DAY TECHNIQUES

Database Systems Journal, vol. XI, nr. 2, pg. 99-108, ISSN 2069- 3230

2021

TECHNICAL AND ECONOMICAL EVALUATION OF IOT ATTACKS AND THEIR CORRESPONDING VULNERABILITIES,

INFORMATICA ECONOMICA JOURNAL, vol. 25, nr. 1, pg. 31-41, ISSN 1453-1305

2021

PE MALWARE TRIAGING AND EFFICIENT FALSE- POSITIVE CLASSIFICATION

International Journal of Economics, Commerce and Management United Kingdom, vol. IX, nr. 1, pg. 325-332, ISSN 2348-0386

2021

CHAINING LOW-RISK ISSUES INTO HIGH-RISK WEB APPLICATION VULNERABILITIES

International Journal of Economics, Commerce and Management United Kingdom, vol. IX, nr. 2, pg. 307-316, ISSN 2348-0386,

ANALYSIS OF HEAP MANAGER FOR WINDOWS 7 & 10 FROM AN EXPLOITATION PERSPECTIVE

International Journal of Economics, Commerce and Management United Kingdom, vol. IX, nr. 5, pg. 213-222, ISSN 2348-0386

CONFERENCES & SEMINARS

2021 Bucuresti, Romania

AN ANALYSIS OF DIFFERENT BROWSER ATTACKS AND EXPLOITATION TECHNIQUES

The 20th International Conference on Informatics in Economy, Education, Research & Business Technologies, IE 2021

2020 Romania

IOT SECURITY, ASSOCIATED MALWARE TRENDS AND VULNERABILITIES

The 19th International Conference on Informatics in Economy 2020, IE2020

2019 Comibra, Portugal

EXPLOITING STACK-BASED BUFFER OVERFLOW USING MODERN DAY TECHNIQUES

Procedia Computer Science The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2019),

LANGUAGE SKILLS

Mother tongue(s): **ROMANIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C2	C2	C2	C2	C2
FRENCH	A1	A1	A1	A1	A1
SPANISH	A1	A1	A1	A1	A1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user

08.08.2024