

## PERSONAL INFORMATION

Dragoş-George Ionică



Sex Male | Date of birth | Nationality Romanian

## POSITION

Cyber Security Senior Consultant

## WORK EXPERIENCE

23 Apr 2019–Present

**Senior Consultant**

Deloitte, Bucharest (Romania)

Penetration Testing

- Web applications
- Red Team Operations
- Infrastructure (network, operating systems, Wi-Fi)
- Mobile applications

1 Feb 19–22 Apr 19

**Cyber Security Senior Advisor (Vulnerability Management)**

Secureworks Europe, Bucharest (România)

- Vulnerability Management (Identify vulnerability in Core Banking Systems)
- Client Reporting
- Develop strategies for red-team assessments

1 Nov 17–31 Jan 17

**Team Leader (Online Operations)**

National Cyberint Centre, Bucharest (Romania)

- Development of tactical solutions used in Red-Team assessments
- Development of BigData data correlation solutions
- Researching vulnerabilities in critical applications and systems

1 Nov 13–31 Oct 17

**Cyber Security Expert**

National Cyberint Centre, Bucharest (Romania)

- Penetration Testing &amp; Red Team:

- Web applications
- Network Infrastructure
- Operating Systems
- Industrial networks (ICS/SCADA)
- Wi-Fi networks

- Cyber Security Exercises

- Scenario Development
- Infrastructure deployment (mass VM deployment)
- Virtual Machines automatic customization

- Infrastructure Monitoring
- Red Team operations
- HelpDesk Support during the execution period

- Incident Response engagements by being part of the CERT-RO team for multiple incidents of cyber critical infrastructures (network & hosts forensic).

1 Feb 12–13 Sep 13

### Digital Marketing Specialist

SC Dunarea SA, Galați (Romania)

- Web developing and maintaining websites
- Managing marketing campaigns (AdWords, Facebook)
- Online Marketing (SEO)

## EDUCATION AND TRAINING

---

### Jul 2021 ARM Exploit Development Training | SANS SEC661

Working with ARM (Tools and Techniques)

Debugging ARM

Branching

Exploiting Stack Overflows

Shellcode

Firmware Extraction

Netgear Exploit

ROP

Dlink Exploit

64-bit ARM

### Jun 2021 Web application Penetration Tester eXtreme – eLearnSecurity

eWPTXv2 Certification

Penetration testing processes and methodologies

Web application analysis and inspection

Advanced Reporting skills and Remediation

Advanced knowledge and abilities to bypass basics advanced XSS, SQLi, etc. filters

Advanced knowledge of different Database Management Systems

Ability to create custom exploits when the modern tools fail

### Mar 2021 – Apr 2021 Certified Penetration Testing eXtreme – eLearnSecurity – CPTX

eCPTX Certification

Advanced penetration testing processes and methodologies

Advanced Exploitation using Metasploit and Empire

Network/traffic manipulation

Pivoting

Advanced Lateral Movement (WMI, PS Remoting, DCOM, etc.)

Advanced Active Directory Information Gathering, Enumeration and

Reconnaissance  
Custom Attack Vector Development  
Deep knowledge of Active Directory and Windows internals  
Knowledge of Windows authentication weaknesses  
Web application Manual exploitation  
Stealthy Scanning and Profiling the target  
Advanced Persistence / Backdooring  
Privilege escalation

Mar 2021 – Apr 2021 **Certified Red Team Expert – Pentester Academy – CRTE**  
**Windows Red Team Lab – CRTE Certification**  
Practice various attacks in a fully patched real world Windows environment with Server 2012, Windows 10 and SQL Server 2017 machines.  
Understand concepts of well known Windows and Active Directory attacks.  
Execute and visualize the attack path used by the modern adversaries.  
Learn to use Windows as an attack platform and using trusted features of the OS like PowerShell and others for attacks.  
Try scripts, tools and new attacks in a fully functional AD environment.

Dec 2020 – Jan 2021 **Offensive Security Advanced Pentesting Training – OSEP**  
**Evasion Techniques and Breaching Defenses**  
Client Side Code Execution With Office  
Client Side Code Execution With Jscript  
Process Injection and Migration  
Advanced Antivirus Evasion  
Application Whitelisting  
Bypassing Network Filters  
Linux Post-Exploitation  
Windows Credentials  
Windows Lateral Movement  
Linux Lateral Movement  
Active Directory Exploitation

Jun 9 – Jun 12 2020 **Adversary Tactics: Red Team Operations – Specter Ops**  
**CRTO (Certified Red Team Operator)**  
Privilege Escalation  
Credential Abuse  
Payloads & Lateral Movement  
SQL Abuse  
Domain Trust  
Silver & Golden Tickets  
Kerberos Delegation  
DPAPI

22 Feb – 22 Mar 2020 **Red Team Ops - ZeroPointSecurity**

	<p>CERTO (Certified Red Team Operator)</p> <ul style="list-style-type: none"> <li>Local Privilege Escalation</li> <li>Domain Reconnaissance</li> <li>Lateral Movement</li> <li>Kerberos Abuse</li> <li>MS SQL Server Abuse</li> <li>Domain Dominance</li> <li>Bypassing Defences</li> </ul>
07 – 26 Jan 2020	<p><b>Offensive Security Web Expert - OSWE</b></p> <p>AWAE (Advanced Web Attacks and Exploitation)</p> <ul style="list-style-type: none"> <li>Persistent Cross-Site Scripting</li> <li>.NET Deserialization</li> <li>Data Exfiltration</li> <li>Blind SQL Injections</li> <li>Bypassing File Upload Restrictions</li> <li>Bypassing Character Restrictions</li> <li>Debugging .NET Assemblies</li> </ul>
Sep–Oct 2019	<p><b>Offensive Security Certified Expert - OSCE</b></p> <p>CTP (Cracking The Perimeter)</p> <ul style="list-style-type: none"> <li>Windows applications exploit development</li> <li>Antivirus evasion/bypass</li> <li>Web applications penetration testing</li> </ul>
Feb–May 2019	<p><b>Offensive Security Wireless Professional - OSWP</b></p> <p>OSWP Online Training, București (România)</p> <ul style="list-style-type: none"> <li>Identify vulnerabilities in Wi-Fi networks</li> <li>Specific password-cracking techniques for Wi-Fi networks</li> <li>Wi-Fi network security</li> </ul>
Sep 2018	<p><b>Red Team Live Operations</b></p> <p>Bucharest, Romania</p>
Jan 2015–May 2015	<p><b>Offensive Security Certified Professional - OSCP</b></p> <p>PWK (Penetration Testing and Ethical Hacking with Kali Linux), Bucharest (Romania)</p> <ul style="list-style-type: none"> <li>Web &amp; Infrastructure Penetration Testing (web applications, networking, operating systems, pivoting, AntiVirus bypass)</li> </ul>
Mar 2015–Apr 2015	<p><b>GIAC Exploit Researcher and Advanced Penetration Tester - GXPN</b></p> <p>SANS 660, Munich (Germany)</p> <ul style="list-style-type: none"> <li>Exploit development (buffer overflows, bypass canaries, DEP, ASLR)</li> <li>Advanced Penetration Testing (VLAN Hopping, SNMP)</li> </ul>
Feb 2015–Mar 2015	<p><b>GIAC Penetration Tester - GPEN</b></p>

- SANS 560, Bucharest (Romania)  
Infrastructure penetration testing (web, network, operating systems, wi-fi)
- Jan 2015–Feb 2015 **GIAC Web Application Penetration Tester - GWAPT**  
SANS 548, Bucharest (Romania)  
Web application security and penetration testing
- 1 Oct 2013–1 Jul 2015 **Master's Degree (MSc)**  
Polytechnic University of Bucharest (Romania)  
- Cyber security (web, network, operating systems, Wi-Fi)  
- eGovernment  
- Project Management
- 1 Oct 09–1 Jul 13 **Bachelor's Degree in Telecommunications Software and Networking**  
University of Galati (FACIEE), Galați (Romania)  
- C / C ++ and Java programming  
- Computer networks  
- Development of complex software applications
- 15 Sept 05–15 Jun 09 **High School Graduation**  
Colegiul Național Mihail Kogălniceanu (România)  
Math and Computer Science (databases, programming)

**PERSONAL SKILLS**

Mother tongue(s) Romanian

Foreign language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C1	C1	C1	C1
French	A1	A1	A1	A1	A1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user  
Common European Framework of Reference for Languages

Communication skills - Good technical communication skills

Organisational / managerial skills From the position of team leader I was the manager of a team of four people, which had the objective of carrying out activities with offensive/red team operations within networks or cyber infrastructures, the study of vulnerabilities of such networks, and the development of tactical solutions, used in Red-Team assessments.

Job-related skills - Good penetration testing (internal networks, external networks, web applications) and technical reports writing skills

Digital skills

SELF-ASSESSMENT

Information processing	Communication	Content creation	Safety	Problem solving
Proficient user	Proficient user	Independent user	Proficient user	Proficient user

Digital skills - Self-assessment grid