24/09/2024

**Curriculum Vitae**

Gert Nelen

August Van Doorslaerlaan 55

1860 Meise

+32 474 86 19 44

gert.nelen@g3rt.be

https://www.g3rt.be

**Tuition**

1999-2002: Applied Computer Science – Rega-instituut KHL

1997-1999: Psychology – Catholic University Leuven

1991-1997: Latin/Sciences – College van het Eucharistisch Hart (Essen)

**Courses**

ISC² Member ID: 784520

2024: Brucon Spring Advanced Incident Response in the MS Cloud, Brucon Autumn A quick, efficient, yet not entirely sane, primer on Cyber Deception

2023: SANS SEC699: Advanced Purple Teaming - Adversary Emulation & Detection Engineering, Brucon 2023 IoT Security Bootcamp

2022: GDAT certification – GIAC Defending Advanced Threats, SANS SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses, Brucon 2022 Linux Forensics Inspection and Incident Response at scale

2021: CCSP certification – Certified Cloud Security Professional, Brucon 2021 Operational Threat Intelligence

2020: CISSP certification – Certified Information Systems Security Professional

2013-2019: Brucon 2019– Full Stack Exploitation, Brucon 2018, Network Data Exfiltration Techniques-Post Exploitation, SANS SEC560 Network Penetration Testing and Ethical Hacking, SANS SEC660 Advanced Penetration Testing, Exploit Writing and Ethical Hacking, SANS SEC575 Mobile Device Security and Ethical Hacking, SANS SEC760 Advanced Exploit Development for Penetration Testers, Suricata Intrusion Detection Training, SANS SEC511 Continuous Monitoring and Security Operations

I regularly visit LEA-only (Law Enforcement Agency) or other security-conventions/seminars (ICCS, ISS world, Black Hat, Brucon, ...) to keep me informed of the latest developments in the field.

2009-2013: Ethical Hacking (tailor-made) by John Cordier Academy, Fortinet Professional by Exclusive Networks, Fortinet Specialist by Fortinet, Juniper JNCP, VMWare ESXi 5.5 configure and install, Powershell, SANS FOR500 Windows Forensics Analysis, SANS FOR508 Advanced Digital Forensics, Incident Response and Threat Hunting, SANS FOR572 Advanced Network Forensics and Analysis, SANS SEC503 Intrusion Detection In-Depth

2007-2009: Internship-training VS/SE comprising people skills, research techniques, security principles, arms handling, (inter)national law, ...

2002-2007: Managing Active Directory, Exchange mail server, Linux (beginner/advanced), Extreme Networks management, VMWare GSX

**Job Experience**

3/2018 - present: Security Consultant at g3rt – Long Term Assignments:

1/3/2018 – 31/8/2019 @ BNP-Paribas-Fortis – SOC start-up Project, Threat Management Capability, Incident Response Tier 3, Threat Hunting

5/8/2019 – 12/2020 @ PWC incident team – Asco industries– Translate business needs into a network security strategy to re-establish a secure environment after a cyber-incident.

3/1/2021 – 12/2024 @ Colruytgroup – Security Operations Team Coach - assist Colruytgroup from an operational pov in their evolution towards a layered, in-depth security model within the organization and the professionalization of Security Operations within that model.

10/2007-2/2018: Operator at the Belgian Civil Intelligence Service (VS/SE) in the Operational IT-departement

8/2002-10/2007: CIBG, fulltime consultant as network – and systemadministrator at Vlaamse Gemeenschapscommissie

1/2002-5/2002: schooling internship at Flemish Parliament – java developer dynamic Oracle database

**Languages/Extra**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Reading** | **Conversation** | **Writing** |
| Dutch | Native Tongue | Native Tongue | Native Tongue |
| English | Excellent | Fluent | Excellent |
| French | Excellent | Fluent | Good |

Thorough understanding of both legal and technical language in both dutch and english.

**Experience/Skills/Projects**

2021-2024:

In january 2021 I start as a team coach and senior analyst in Colruytgroup’s security operations. My mission is to improve security operations and the integration within the security model of the organization as well as facilitate the formation and evolution toward a consistent layered (cyber)defense model. Incident Response, detection engineering and threat intel capabilities are developed with a sliding role assignment to optimize the team’s productivity. Advise about security control improvements and build and share knowledge about forensic acquisitions, investigation methodologies, playbook and rule developement, purple teaming, threat reporting, ...

2020:

Since the beginning of 2020 I’m hired directly by Asco to ensure the continuity of the G2G (go to green) and further continue my mission. Most projects are gradually reaching the end by the end of the year and responsibilities are handed over to Asco.

2019-2020:

In the wake of a heavy-impact cyber incident I’m hired by PWC to strengthen their international response (and rebuild) team at Asco. I get the responsibility to re-design the network-level security of this aviation-giant – and morph the network to accommodate the expected operation – and function as a team lead for all network security related matters. The greenfield approach is chosen and our team manages to create a well defendable, controllable and clear network design, integrating all different system-, network-, iot- and ot-components, where the separation between green, amber, red and black is enforced through all the layers of security in order to to limit the margin for human error and prevent further incidents with similar impact from happening.

2018-2019:

By the end of 2018 I shift within the SOC team towards the Incident Response team in response to the needs of BNPPF. I handle Tier 3 incidents and do Threat hunting when no incidents need handling. I make use of the different security technologies within the bank’s infrastructure (F5 reverse proxies, McAfee & Bluecoat Proxy, Cisco Netwerk producten, Fortinet en Palo-alto Firewalls, Infoblox, IDS, Qualys, ArcSight, Splunk, Archer, EagleEye ...). I also do forensic analysis of both systems and networks when needed.

2018:

As a security consultant I am hired by BNP Paribas Fortis to assist in the start-up of a fully functional SOC (Security Operations Center). More specifically I focus on the Threat Management capability of the team, outlining the processes and procedures to streamline the cyber defence posture of this big bank. Absorbing threat intelligence and converting it to actionable indicators that can be deployed directly to the different levels of security controls is the main challenge. Analysing new threats and the implications related to the client’s infrastructure, reporting to involved parties and testing the resilience against new (and old) TTP’s (Tools Techniques and Procedures) is part of my daily work.

2010-2018:

*In 2010 a reorganization of the IT-services is initiated based on the new Belgian law on Special Intelligence Methods (BIM). This will form the legal framework that allows our service to obtain exceptions on regular law in order to facilitate gathering certain types of intelligence in specific conditions and within a tightly controlled framework. Given my extensive knowledge on networking I am tasked to the Operational Branch.*

* In 2010 we design a new network and its security for our service. Initially we try to limit the previous multitude of vendors and build around a limited set of products and technologies. The major corner stones are products of Fortinet, Juniper, Cisco and Barracuda.
* Regular forensic research on computer systems as well as network infrastructure, obtained from both external as company owned sources.
* Further extension, deepening and widening of the connected networks, with as most difficult challenge achieving the best possible accessibility while still meeting the required individual security standards.
* Design, testing and installation of a Knox-based solution from Samsung to replace the existing Blackberry system. A close international cooperation with Samsung SDS/Electronics is key to success in this project. Strongly encrypted dialup-IPSEC tunnels from Android devices provide a permanent secure access to the corporate network to facilitate the access to much needed operational services and programs as well as encrypted communication for agents in the field.
* Further build-up and extension of a competent Red Team with its primary mission to penetrate computer systems from a distance and write or modify exploits to ensure continuous access. We mostly use a multitude of scripting and programming languages (e.g. powershell, python, c#, perl, wmi). A close cooperation with friendly foreign services helps to hone each other’s expertise and skills as quickly as possible. Extensive experience with frameworks and tools like metasploit, cobalt strike, empire, dnscat2, burp, scapy, …
* The expertise and know-how from both red and blue teams is used to start redesigning an entire new network and its defenses in 2016. Because of the multitude of diverse external connections and external relations everything needs to be meticulously segmented with a complex but performant and future-proof network design as a result. Different layers of security within many diverse functional segments form the core of the network, augmenting security, logic and manageability. Dozens of (virtual or other) firewalls and other security components filter and monitor on all layers of the OSI model any data passing through this network.

2007-2010:

* Internship at the Belgian Civil Intelligence Service (VS/SE). I learn a lot of skills that are not directly related to IT, but fit in the bigger security picture, e.g. law, intelligence working fields, security principles, international (co)operation...
* After 1 year of (operator-) training I start my intership within the IT-division, which is tasked to provide support and fulfil in the IT-needs of the service. I inherit a network with many different connections with other government agencies and intelligence services from other nations. The multitude of different databases, security restrictions, techniques and formats proves a sound training ground. One year later I pass the final tests of my internship and I am assigned as operator with the IT-department.
* Set-up of secure mobile connections using Blackberry and matching AD and Exchange configuration and hardening.
* Professionalize Internet access, with centralized security and gradual roll-out to all desktops.

2002-2007:

* Migrate Old Token Ring network to a new Ethernet-based network with switches and routers (of the Extreme brand), L2TP –like connections between the different branches.
* Set-up and management of sendmail mail server, providing mail services for all personnel and students in Brussels. Set-up and management of bind dns-server.
* Secured connections with all external (dutch) entities in Brussels (like schools, community centers, administration houses,...). Introduction of functional segmented networks, secured with iptables and snort.
* Setup, secure and manage a new Apache web server for the dutch schools in Brussels.
* Design, setup and manage Active Directory and Exchange for all administrions.
* Starting 2005 the open source firewall is replaced by a firewall cluster of Vasco.

**About Myself**

Hobbies: listening/making music, watching a good movie or making an adventurous journey can soothe my soul. I’m a passionate skier and enjoy the peace and quiet of a scuba dive in tropical waters. I regularly make time to finish a private project where I get to challenge and work with my hands, like building robots, building and designing a terrarium or automating an aquarium with a raspberry PI. I’m interested in new technological novelties and advances and sometimes am called ‘Mr. Gadget’ by my friends.

I am passionate and motivated and can comprehend complex problems and situations. I can deep dive into a specific problem without losing oversight of the final goal. I don’t quit before reaching the required result. A downside to this is my disability to let problems go and sometimes I tend to take them home. I can deal with pressure and a high workload although I sometimes need some time for myself. Spending time with my family is also very important to me.

I can cope with repetitive and less challenging tasks, as long as they are a means to an end and limited in time. I can work well in a team, although I sometimes have little patience with lack of benevolence/spirit from my team-members.

I have a broad experience and can manage people from a diverse (technical and social) background. I have experience with managing larger projects within different types of corporate structures and frameworks. I’m a good communicator and an excellent (written) reporter, especially in more technical fields (though I’m not a captive presenter).

I possess an analytical mind and a good memory which combine into a large problem-solving ability. Combined with my thorough knowledge of computer networks and ip-packets there is seldom a mystery in a network that will go unexplained, let alone unsolved. I have an in-depth understanding of many offensive techniques and strategies, which I use to devise targeted defenses and adaptations to existing security controls and policies to improve their security and/or their effectiveness (purple-team tactics).

My years of experience in many layers of security, conducting investigations and operations, participating in several incident investigations and re-builds, securing complex networks and working in a SOC have given me a unique skill-set that might spark your interest to explore a further cooperation.