Resume PenTest Career by Joas A Santos

https://www.linkedin.com/in/joas-antonio-dos-santos

Fundamentals

Computer Network

- Network basics: Understanding the purpose, advantages, and types of networks (e.g., LAN, WAN, PAN, MAN) as well as their topologies (e.g., bus, star, ring, mesh).
- Network hardware: Exploring the physical devices that make up a network, such as switches, routers, hubs, bridges, and network interface cards (NICs).
- Network protocols: Learning about the rules and conventions that govern network communication, such as TCP/IP, UDP, HTTP, FTP, and SMTP.
- Network architectures: Studying the design principles and models for organizing networks, including the OSI model and the TCP/IP model.
- Network addressing: Understanding IP addressing (IPv4 and IPv6), subnetting, and the Domain Name System (DNS).
- Network security: Learning about methods for securing networks, such as firewalls, intrusion detection systems (IDS), encryption, and virtual private networks (VPNs).
- Wireless networking: Exploring the principles and technologies behind wireless communication, including Wi-Fi, Bluetooth, and mobile networks.
- Network management: Learning about tools and techniques for monitoring, maintaining, and troubleshooting networks, such as Simple Network Management Protocol (SNMP), network analyzers, and performance monitoring.
- Network services: Understanding the various services provided over networks, such as file sharing, email, web hosting, and remote access.
- Network applications: Studying the software and applications that utilize networks, such as web browsers, email clients, and file transfer programs.

Programming Language

- Variables and data types: Understanding how to declare and use variables, as well as the different data types (e.g., integers, floats, strings, booleans) available in a programming language.
- Operators: Learning about arithmetic, comparison, logical, and assignment operators to perform operations on data.
- Control structures: Understanding how to use conditional statements (e.g., if, else, elif) and loops (e.g., for, while) to control the flow of a program.
- Functions and methods: Learning about writing reusable code blocks (functions) and methods to improve modularity, maintainability, and readability.
- Data structures: Studying different ways to organize and store data, such as arrays, lists, dictionaries, sets, and tuples.
- Object-oriented programming (OOP): Learning about the principles of OOP, such as encapsulation, inheritance, and polymorphism, and how to create and work with objects and classes in a programming language.
- Error handling and debugging: Understanding how to handle errors and exceptions in code, as well as techniques for debugging and troubleshooting.
- Algorithms: Studying common algorithms (e.g., sorting, searching) and their implementation, as well as understanding algorithm complexity and efficiency.

Cyber Security

- Security fundamentals: Understand core security concepts, such as confidentiality, integrity, availability (CIA triad), and risk management.
- Encryption and cryptography: Learn about encryption algorithms, public and private keys, symmetric and asymmetric encryption, digital signatures, and certificates.
- Network security: Study various network security protocols, firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs).
- Application security: Learn how to secure software applications by understanding common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and buffer overflows, as well as secure coding practices and frameworks.
- Endpoint security: Study techniques for securing end-user devices, such as antivirus software, patch management, and mobile device management (MDM).
- Access control: Learn about different access control models, such as role-based access control (RBAC), discretionary access control (DAC), and mandatory access control (MAC), as well as authentication and authorization mechanisms.
- Cloud security: Understand the unique security challenges associated with cloud computing, such as data privacy, compliance, and securing cloud infrastructure.
- Incident response: Learn about creating and implementing incident response plans, digital forensics, and techniques for mitigating and recovering from security breaches.
- Security policies and compliance: Study the importance of creating and enforcing security policies, as well as adhering to legal and regulatory requirements, such as CDPR, HIPAA, and PCI DSS.
- Social engineering and phishing: Understand the psychological aspects of cybersecurity, including techniques used by attackers to manipulate individuals into revealing sensitive information or granting unauthorized access.
- Ethical hacking and penetration testing: Learn how to identify vulnerabilities in systems by simulating real-world cyberattacks and performing security assessments.
- Security awareness training: Study the importance of creating a culture of security awareness within an organization and educating employees on best practices for maintaining security.

Certifications (It's not in order)

- Security+ — Cybersecurity Concepts
- eJPTv2 (INE/eLearnSecurity) — Fundamentals PenTest
- eWPT (INE/eLearnSecurity) — Fundamentals Web PenTest
- PenTest+ (CompTIA) — PenTest and Vulnerability Management
- CEH (EC-Council) — PenTest and Countermeasures
- OSCP (Offensive Security) — Professional PenTest
- PNPT (TCM Security) — Professional PenTest
- CRTO (Zero Point Security) — Red Team Operations and Adversary Emulation
- CRTP (PenTest Academy / Altered Security) — Professional PenTest
- eWPTX (INE/eLearnSecurity) — Web PenTest Professional
- OSEP (Offensive Security) — Evasion PenTest
- OSWA (Offensive Security) — Web PenTest Professional
- CRTE (PenTest Academy / Altered Security) — Professional PenTest
- AWS PenTest (CyberWarFareLabs) — AWS PenTest

PenTest Study

General

- Pentesting methodologies: Learn about common penetration testing methodologies and frameworks, such as the Penetration Testing Execution Standard (PTES), the Open Source Security Testing Methodology Manual (OSSTMM), and OWASP Testing Guide.
- Each pentest environment is different, saying to master everything is impossible, however you can choose an area that attracts you and go deeper. Whether PenTest Web, Mobile, OT, Network Infrastructure or another area
- Learn to write documentation and reports, it will help you professionally and develop your technical skills
- Legal and ethical considerations: Study the legal and ethical aspects of penetration testing, including obtaining permission, defining the scope of a test, and following responsible disclosure practices.
- Practice in labs and CTFs, this will help you to further improve both your performance and theory skills
- Certifications are important not just for defining skills, but for compliance and based on trade agreements
- A strong desire to learn and stay up-to-date with the latest security trends, technologies, and threats, along with the ability to adapt to new challenges and situations quickly.
- Effective verbal and written communication skills for conveying technical information to non-technical audiences, creating clear and concise reports, and collaborating with colleagues and clients.
- Building a professional network and engaging with the cybersecurity community through conferences, forums, and social media can help you stay current with industry trends and advance your career.
- Develop self-taught thinking, research and go after it, do not stand still and do not depend only on your own tools

Try Harder Philosophy and Mindset in OSCP

- Be persistent. Penetration testing often involves encountering roadblocks and dead ends. The "Try Harder" concept emphasizes the importance of not giving up when faced with challenges and encourages students to keep pushing until they find a solution.
- Think creatively. The "Try Harder" mindset promotes thinking outside the box to find unique and innovative solutions to problems. It encourages students to explore alternative approaches and develop their problem-solving skills.
- Be resourceful. The OSCP course intentionally provides limited guidance, forcing students to rely on their research skills and ability to find information independently. The "Try Harder" concept emphasizes the importance of self-reliance and resourcefulness in a penetration tester's toolkit.
- Learn from failure. The "Try Harder" mindset encourages students to view failure as a learning opportunity. Instead of being discouraged by setbacks, they should analyze their mistakes and use the experience to improve their skills and understanding.
- Develop a strong work ethic. The OSCP course is demanding and requires dedication, discipline, and a willingness to invest time and effort. The "Try Harder" concept reminds students that becoming a skilled penetration tester takes hard work and commitment.

Laboratory

General

- Attack-Defense - https://attackdefense.com
- Alert to win - https://alf.nu/alert1
- Bancocn - https://bancocn.com
- CTF Komodo Security - https://ctf.komodosec.com
- CryptoHack - https://cryptohack.org/
- CMD Challenge - https://cmdchallenge.com
- Exploitation Education - https://exploit.education
- Google CTF - https://lnkd.in/e46dnbz8
- HackTheBox - https://www.hackthebox.com
- Hackthis - https://www.hackthis.co.uk
- Hacksplaining - https://lnkd.in/eABSCSTA
- Hacker101 - https://ctf.hacker101.com
- Capture The Flag - Hacker Security - https://lnkd.in/ex7R-C-e
- Hacking-Lab - https://hacking-lab.com/
- HSTRIKE - https://hstrike.com
- ImmersiveLabs - https://immersivelabs.com
- NewbieContest - https://lnkd.in/ewBk6fUS
- OverTheWire - http://overthewire.org
- Practical Pentest Labs - https://lnkd.in/esq9VuvS
- Pentestlab - https://pentesterlab.com
- Hackaflag BR - https://hackaflag.com.br/
- Penetration Testing Practice Labs - https://lnkd.in/e6wVANYd
- PentestIT LAB - https://lab.pentestit.ru
- PicoCTF - https://picoctf.com
- PWNABLE - https://lnkd.in/eMEwB3zn
- Root-Me - https://www.root-me.org
- Root in Jail - http://rootinjail.com
- SANS Challenger - https://lnkd.in/e5TAMawK
- SmashTheStack - https://lnkd.in/eVn9rP9p
- The Cryptopals Crypto Challenges - https://cryptopals.com
- Try Hack Me - https://tryhackme.com
- Vulnhub - https://www.vulnhub.com
- Vulnmachine - https://lnkd.in/e32e_kD
- W3Challs - https://w3challs.com
- WeChall - http://www.wechall.net
- Websploit - https://websploit.org/
- Zenk-Security - https://lnkd.in/ew25rNx2
- Cyberdefenders - https://lnkd.in/dVcmjEw8
- LetsDefend- https://letsdefend.io/