Penetration Testing Career – JR to Specialist

Joas Antonio

Detalhes

- Esse pdf tem como objetivo apresentar os conhecimentos necessários para atuar como PenTester;
- Conhecimentos baseados na exigências do mercado de trabalho em muitas vagas;
- Utilizei vagas tanto aqui no Brasil como no Exterior;

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

Details

- This pdf aims to present the necessary knowledge to act as PenTester;
- Knowledge based on the demands of the job market in many vacancies;
- I used vacancies both here in Brazil and abroad;

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

PenTest JR

- Conhecimentos em padrões e politicas de segurança da informação (ISO 27001, LGPD/GDPR, PCI-DSS, HIPAA, NIST, FISMA e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF e etc);
- Conhecimentos em Gestão de Riscos;
- Conhecimentos em Gestão e Analise de Vulnerabilidades;
- Conhecimentos em Ferramentas de PenTest;
- Conhecimentos em Linguagens de Programação (Ex: Python, Ruby, C, C#, GO, PHP, JavaScript e etc);
- Conhecimentos em sistemas operacionais e administração (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD e etc...);
- Conhecimentos Fundamentais em Redes de Computadores;
- Conhecimentos em Hardening e Mitigação de Riscos;
- Conhecimentos em PenTest em Aplicações Mobile, Web, Cloud, Redes e IoT;
- Conhecimentos em Black Box, White Box e Gray Box Testing;
- Auxiliar na elaboração de Relatórios Técnicos e Gerenciais;

PenTest JR - ENGLISH

- Knowledge of information security standards and policies (ISO 27001, LGPD / GDPR, PCI-DSS, HIPAA, NIST, FISMA and etc);
- Knowledge of PenTest methodologies (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF and etc);
- Knowledge in Risk Management;
- Knowledge in Management and Analysis of Vulnerabilities;
- Knowledge in PenTest Tools;
- Knowledge in Programming Languages (Ex: Python, Ruby, C, C #, GO, PHP, JavaScript and etc);
- Knowledge of operating systems and administration (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD and etc ...);
- Fundamental Knowledge in Computer Networks;
- Knowledge in Hardening and Risk Mitigation;
- Knowledge in PenTest in Mobile Applications, Web, Cloud, Networks and IoT;
- Knowledge in Black Box, White Box and Gray Box Testing;
- Assist in the preparation of Technical and Management Reports;

PenTest PL

- Conhecimentos em padrões e politicas de segurança da informação (ISO 27001, LGPD/GDPR, PCI-DSS, HIPAA, NIST, FISMA e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF e etc);
- Conhecimentos em Gestão de Riscos;
- Conhecimentos em Gestão e Analise de Vulnerabilidades;
- Conhecimentos em Ferramentas de PenTest (Best Tools);
- Conhecimentos em Linguagens de Programação (Ex: Python, Ruby, C, C#, GO, PHP, JavaScript e etc);
- Conhecimentos em sistemas operacionais e administração (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD e etc...);
- Conhecimentos Fundamentais em Redes de Computadores ;
- Conhecimentos em Hardening e Mitigação de Riscos;

PenTest PL (CONT)

- Conhecimentos em PenTest em Aplicações Mobile, Web, Cloud, Redes e IoT;
- Conhecimentos em desenvolvimentos de Scripts e melhorias de ferramentas;
- Técnicas avançadas de PenTest, sem a utilização de ferramentas automatizadas;
- Desenvolvimento e elaboração de relatórios executivos e técnicos;
- Conhecimentos e experiência em PenTest Black Box, Gray Box e White Box;

PenTest PL - ENGLISH

- Knowledge of information security standards and policies (ISO 27001, LGPD / GDPR, PCI-DSS, HIPAA, NIST, FISMA and etc);
- Knowledge of PenTest methodologies (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF and etc);
- Knowledge in Risk Management;
- Knowledge in Management and Analysis of Vulnerabilities;
- Knowledge in PenTest Tools (Best Tools);
- Knowledge in Programming Languages (Ex: Python, Ruby, C, C #, GO, PHP, JavaScript and etc);
- Knowledge of operating systems and administration (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD and etc ...);
- Fundamental Knowledge in Computer Networks;
- Knowledge in Hardening and Risk Mitigation;

PenTest PL (CONT) - ENGLISH

- Knowledge in PenTest in Mobile Applications, Web, Cloud, Networks and IoT;
- Knowledge in developing Scripts and improving tools;
- Advanced PenTest techniques, without using automated tools;
- Development and preparation of executive and technical reports;
- Knowledge and experience in PenTest Black Box, Gray Box and White Box;

PenTest SR AND SPECIALIST

- Conhecimentos em padrões e politicas de segurança da informação (ISO 27001, LGPD/GDPR, PCI-DSS, HIPAA, NIST, FISMA e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF e etc);
- Conhecimentos em Gestão de Riscos;
- Conhecimentos em Gestão e Analise de Vulnerabilidades;
- Conhecimentos em Ferramentas de PenTest (Best Tools);
- Conhecimentos em Linguagens de Programação (Ex: Python, Ruby, C, C#, GO, PHP, JavaScript e etc);
- Conhecimentos em sistemas operacionais e administração (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD e etc...);
- Conhecimentos em Hardening e Mitigação de Riscos;
- Conhecimentos em Arquitetura e Soluções de Segurança da Informação;
- Conhecimentos em PenTest em Aplicações Mobile, Web, Cloud, Redes e IoT;

PenTest SR AND SPECIALIST (CONT)

- Conhecimentos em desenvolvimentos de Scripts e melhorias de ferramentas;
- Técnicas avançadas de PenTest, métodos de exploração avançados e etc;
- Técnicas de Pós Exploração Avançado;
- Conhecimentos em Buffer Overflow e Desenvolvimento de Exploits;
- Conhecimentos em Mitre Att&ck and Advanced Persistent Threat (APTs);
- Desenvolvimento e elaboração de relatórios executivos e técnicos;

PenTest SR AND SPECIALIST - ENGLISH

- Knowledge of information security standards and policies (ISO 27001, LGPD / GDPR, PCI-DSS, HIPAA, NIST, FISMA and etc);
- Knowledge of PenTest methodologies (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF and etc);
- Knowledge in Risk Management;
- Knowledge in Management and Analysis of Vulnerabilities;
- Knowledge in PenTest Tools (Best Tools);
- Knowledge in Programming Languages (Ex: Python, Ruby, C, C #, GO, PHP, JavaScript and etc);
- Knowledge of operating systems and administration (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD and etc ...);
- Knowledge in Hardening and Risk Mitigation;
- Knowledge in Architecture and Information Security Solutions;
- Knowledge in PenTest in Mobile Applications, Web, Cloud, Networks and IoT;

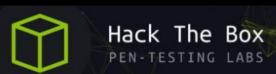
PenTest SR AND SPECIALIST (CONT) – ENGLISH

- Knowledge in developing Scripts and improving tools;
- Advanced PenTest techniques, advanced exploration methods and etc;
- Advanced Post Exploration Techniques;
- Knowledge in Buffer Overflow and Development of Exploits;
- Knowledge in Miter Att & ck and Advanced Persistent Threat (APTs);
- Development and preparation of reports and technicians;

Skills Development - Labs

- Hackthebox;
- Vulnhub;
- Try Hack Me;







Skills Development - Certifications

- eLearnSecurity;
- EC-COUNCIL;
- Offensive Security;
- Sans;
- CompTIA;



Roadmap Certifications

IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at: CompTIA.org/CertsRoadmap



Certifications validate expertise in your chosen career. CompTIA A+ certification CompTIA has helped launch over ADVANCED EXPERT Information INTERMEDIATE A+ 1 million IT careers. Security CCIE CCSK IA CISA BEGINNER/NOVICE CENA CompTiA Security+ CCDP CSSLP. SCYBER Solutions Architect - Associate CCNP. MCSE: Server CASP CompTIA Network+ SysOps Administrator - Associate Infrastructure CGEIT Network and CompTiA Server+ CompTIA CySA+ G CCNA CompTIA.A+ CompTIA IT GSLC. CISM. CompTIA. G CCDA CCIA. Cloud Fundamentals+ GCED GCED Penllest+ CISSP CEH! CompTIA Network+ Technologies MR CPTE EG CHFI CompTIA Linux+/LPIC-1 G GCIH CompTIA Cloud+ ED GCPCA Solutions. GSEC. CompTIA IT CompTtA A+ CO HCNA Architect-TER HONE O COL Fundamentals+ GISP MR MICSA GE CCENT Professional LPIC-2 CASP CASP Hardware, CompTIA Cloud MCSA: Windows Server 2012 OpenStack Administrator DevOps ME MICSE Essentials THE HOTE SU SCA Services and Engineer -NO CNE M ASE/CSE Linux Essentials THE RHICSA Professional Infrastructure RH RHCE LPIC-3 ME MIA CCSK RCT. SOL SOL CCDP. ETB REICA CompTIA Server+ O CONP WW VCIX ED SEA CompTIA Network+ G CCP W VCDX CWNA CWNA IT Management CCA. CompTIAIT Comptia A+ CWTS Compilia Project+ Fundamentals+ HDI DST HOLDSM and Strategy Prince2 Foundation ITIL Master HDI SCA ITIL Foundation HDI SCM CAPM. BR MTA III ITIL intermediate MCSA. Salesforce.com ITIL Expert Prince2 Practitioner Storage and Data ME MCSE CCNA CompTIA A+ CompTIAIT CompTIA Server+ Fundamentals+ WED VCA IBM Certified M ACMP ME MIA MCSD: Application Lifecycle Web and Mobile Specialist CCNP Wireless M ASE/CSE Management B MC5A GO OCM CCP-M OCA. Microsoft Specialist OCP WCA Workforce Mobility CompTIAA+ WED VCP CompTIAIT PHP Certification Software CCNP CCNP Fundamentals+ MO ACE ATM SEE MCSE MCSE Development OCMJEA CSP MCSD: Developer - Associate Framework 2 Certification Training Microsoft Specialist ACI. MongoDB Certified MB MTA COMpTIA.A+ CompTIA CTT+ Developer Associate OCAL HDI CI OCPIP DevOps Engineer MB MCSD MCT. OR OCMID Computer literacy certifications validating end user skills include IC3 and ECDL/ICDL Updated 6/2018

Skills Development - Resources

- PenTest Toolkit (https://bit.ly/3fQSOTo)
- Red Team/PenTest Books (https://bit.ly/3ln0cqD)
- PenTest Study Guide (https://bit.ly/33yGXV0)

• STÖK (Fredrik Alexandersson)

https://lnkd.in/djwu5A6

Red Team Village DC Red Team Village

https://lnkd.in/dDhcEa5

InsiderPhD Katie Paxton-Fear

https://lnkd.in/duDph87

Nahamsec Ben Sadeghipour

https://lnkd.in/drBQim3

HackerOne

https://lnkd.in/d7QNQE8

BugCrowd

https://lnkd.in/dAqbA84

The Cyber Mentor Heath Adams

https://lnkd.in/dbYCM5Q

• John Hammond John H.

https://lnkd.in/dAp3xJM

Codingo Michael S.

https://lnkd.in/dpEsrEk

HackerSploit HackerSploit

https://lnkd.in/dGXwDkX

LiveOverflow

https://lnkd.in/dTWHXSD

IPPSec

https://lnkd.in/deCU5YZ

S4vitar Marcelo Vázquez (Spanish Content)

https://lnkd.in/dMjbPft

Zigoo Ebrahim Hegazy (Arabic)

https://lnkd.in/dgQTeuG

ACADI-TI

https://www.youtube.com/channel/UCi8P9S-PW7AF71g8Pi0W6Jw

Michael LaSalvia

https://www.youtube.com/user/genxweb

Wraiith

https://www.youtube.com/user/Wraiith75

Bsides

https://www.youtube.com/channel/UCVImyGhRATNFGPmJfxaq1dw

Vinicius Vieira

https://www.youtube.com/channel/UCySphP8k4rv7Jf-7v3baWIA

Kindred

https://www.youtube.com/channel/UCwTH3RkRCIE35RJ16Nh8V8Q

Bug Bounty Public Disclosure

https://www.youtube.com/channel/UCNRM4GH-SD85WCSqeSb4xUA

- https://www.youtube.com/channel/UCxHzA-Z97sjfK3OISjkbMCQ (RoadSec)
- https://www.youtube.com/channel/UC2QgCedRNj_tLDrGWSM3Gs
 Q (Mindthesec)
- https://www.youtube.com/channel/UCz1Psqlhim7PUqQfuXmD-Bw (Hackaflag)
- https://www.youtube.com/user/BlackHatOfficialYT (Blackhat)

- https://www.youtube.com/channel/UCqGONXW1ORgz5Y4qK-0JdkQ (Joe Grand)
- https://www.youtube.com/user/DEFCONConference (Defcon)
- https://www.youtube.com/channel/UC4dxXZQqofAadUWbqhoceQ (DeviantOllam)
- https://www.youtube.com/channel/UC3s0BtrBJpwNDaflRSoiieQ (Hak5)
- https://www.youtube.com/channel/UCimS6P854cQ23j6c_xst7EQ (Hacker Warehouse)
- https://www.youtube.com/channel/UCe8j61ABYDuPTdtjltD2veA (OWASP)
- https://www.youtube.com/channel/UC42VsoDtra5hMiXZSsD6eGg/featured (The Modern Rogue)
- https://www.youtube.com/channel/UC3S8vxwRfqLBdIhgRIDRVzw (Stack Mashing)

- https://www.youtube.com/channel/UCW6MNdOsqv2E9AjQkv9we7A (PwnFunction)
- https://www.youtube.com/channel/UCUB9vOGEUpw7|KJRoR4PK-A (Murmus CTF)
- https://www.youtube.com/channel/UCND1KVdVt8A580SjdaS4cZg (Colin Hardy)
- https://www.youtube.com/user/GynvaelEN
- https://www.youtube.com/channel/UCBcljXmuXPok9kT_VGA3adg (Robert Baruch)
- https://www.youtube.com/channel/UCGISJ8ZHkmlv1CaoHovK-Xw (/DEV/NULL)
- https://www.youtube.com/channel/UCDbNNYUME_pgocqarSjfNGw (Kacper)
- https://www.youtube.com/channel/UCdNLW93OyL4lTav1pbKbyaQ (Mentorable)

- https://www.youtube.com/channel/UCMACXuWd2w6_IEGog744UaA (Derek Rook)
- https://www.youtube.com/channel/UCFvueUEWRfQ9qT9UmHCw_og (Prof. Joas Antonio)
- https://www.youtube.com/user/ricardolongatto (Ricardo Longatto)
- https://www.youtube.com/user/daybsonbruno (XTREME Security)
- https://www.youtube.com/user/eduardoamaral07 (Facil Tech)
- https://www.youtube.com/channel/UC70YG2WHVxlOJRng4v-CIFQ (Gabriel Pato)
- https://www.youtube.com/user/Diolinux (Diolinux)
- https://www.youtube.com/user/greatscottlab (Great Scott!)
- <u>https://www.youtube.com/user/esecuritytv</u> (eSecurity)
- https://www.youtube.com/channel/UCzWPaANpPISEE_xvJm8lqHA (Cybrary)
- https://www.youtube.com/user/DanielDonda (Daniel Donda)
- https://www.youtube.com/user/ZetaTwo (Calle Svensson)
- https://www.youtube.com/channel/UCNKUSu4TPk979JzMeKDXiwQ (Georgia Wedman)
- https://www.youtube.com/channel/UCqDLY9WFoJWqrhycW8cbv1Q (Manoel T)