

How to start at once in the PenTest/Red Team area?

Joas Antonio



Details

- A lot comes to me with doubts about how to get started in the PenTest/Red Team area, I hope this PDF helps to fully or partially clear these doubts.
- Muitas dúvidas me chegam sobre como iniciar na área PenTest/Red Team, espero que este PDF ajude a esclarecer total ou parcialmente essas dúvidas.

Fundamentals

- Yes, fundamentals are necessary! It's no use wanting to skip processes, if you don't have experience with IT and much less security, you're going to have a lot of difficulties. It would be the same thing as flying an An-225 plane without flying hours
- Sim, fundamentos são necessários! Não adianta querer pular processos, se você não tem experiência com TI e muito menos segurança, vai ter muitas dificuldades. Seria a mesma coisa que pilotar um avião An-225 sem horas de voo

How to acquire fundamentals?

Software and
Hardware Concepts

Network Computer
Concepts and Practical
Configuration Procedures

Logic
Programming

Operation System
(Linux, Windows
and Mac)
Administrator

Cyber Security
Foundations

Where to study fundamentals?

1. Free Courses
2. Technical Courses
3. Graduation
4. YouTube
5. Programming Platforms
6. CTF Platforms

Where to study fundamentals?

1. <https://www.udemy.com/>
2. <https://alura.com/>
3. <https://pt.coursera.org/>
4. <https://www.alura.com.br/>
5. <https://tryhackme.com/>
6. <https://www.edx.org/>
7. https://en.wikipedia.org/wiki/Computer_science
8. <https://codedred.eccouncil.org/>
9. <https://www.analyticsinsight.net/sharpen-your-coding-skills-top-10-coding-challenge-websites/>

How to start in PenTest/Red Team?

- Starting with PenTest you will have several directions, but if you don't know where to go, starting with a fundamentals course is much better and nothing better than starting with eJPT (eLearnSecurity)
- In addition, you can choose to use Try Hack Me as a platform to practice, I recommend signing it, as you will acquire good technical and theoretical skills
- <https://elearnsecurity.com/>
- <https://tryhackme.com/>

How to start in PenTest/Red Team?

Vulnerability
Management
Concepts

Risk Management
Concepts

Network Security
Concepts

Penetration
Testing
Fundamentals

Programming
Language Study
(High Level)

Red Team
Concepts

Mitre Att&ck
Knowledge

Adversary
Emulation
Concepts

Red Team
Operations and
Development

Web Vulnerability
Skills

Network
Enterprise PenTest
Skills

Social
Engineering Skills

Purple Team
Knowledge

Advanced PenTest
Skills

How to start in PenTest/Red Team? - PDFs

- <https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU>
- <https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU>
- <https://drive.google.com/file/d/18Ab78LeA-C2N-WAIZ12JuPTAFXMqi12R/view?usp=sharing>

How to start in PenTest/Red Team? - Certifications

	Forensics		Incident Handling		Penetration Testing				Exploitation			
										OSEE		
	GREM					OSWE	OSCE3	OSEP	OSED			
		CSFA	CFCE		MRT			GXPN				
	MTIA	CAWFE	GCFA	GCTI				GAWN	MCD			
		CFSR	GNFA			eCPTX	eWPTX	CREST CCSAS		CREST CSAM		
			BTL2					CREST CCT				
	eCMAP		GCFE	CEIM	PACES		S-CEHL	CREST CRT		CEREA		
	MTH	GASF	eCTHP				S-EHE			eCRE		
	Cisco CyberOps Pro	CCFE	GCED		PA CRTE	CREST CTIM			OSCP			
		GCDA	CMFE	CCTHP	GCIH			OSWP	MRE			
		CDRP	eCDFP		MDFIR	LPT	PNPT	GCPN	GPEN	GPYC	GMOB	
		CCE	CREST CRIA		CREST RTIA	PA CRTP	GWAPT		GCPT	CREST CWS	CREST CMRE	eCXD
		GBFA	BTL1		MBT	CPENT	ZPRTO	MPT	CREST CWAT	GEVA		
	CREST CHIA	EnCE	ACE	eCIR			eCPPT	eWPT	CEPT			
	Cisco CyberOps Associate		CHFI		ECIH	CJPSH	CMWAPT	CJPTC	CRTOP	CSR		
		CSX-P	CJNFE	GOSI			eMAPT	S-EHP	OPST		CREA	
	MSOAA	MRCI	EDRP		CFR	CTIA	CPT	eJPT	CHAT	CREST CPSA		
	OPSA	CSAE	ASIS PCI			CEH		CJPTC				
		MOIS	CFA		CSA					Pentest+	CREST CSAS	ECES
		CSX-PA		CREST CPIA		CREST CPTIA		CJPEH	GCPEH			
		ECSS	CJVFE	CJDFE		Mile2 Red vs Blue						
	OPSE	CSX-F			CIRM Fdn			EEHF	S-EHF	CHA		
	CSCU	CJSP				CND		CJVA	KLCP			

How to start in PenTest/Red Team? – Certifications Journey

Green = Fundamentals
Red = PenTest
Yellow = Web App Sec
Blue = Extra

Security+ (Fundamentals Security)	eJPT	CEH and CEH Practical	PenTest+	OSCP
eCPPT	eWPT	CRTP	PNPT	CRTE
CRTOP	eWPTX	OSWE	OSEP	OSD
eCPTX	CREST CPSA	OSEE	eCXD	

How to start in PenTest/Red Team? – Certifications Journey - Laboratory

- <https://www.mindmeister.com/pt/1781013629/the-best-labs-and-ctf-red-team-and-pentest>
- <https://tryhackme.com/>
- <http://vulnhub.com/>
- <https://Inkd.in/eYEK8UT>
- <https://Inkd.in/emGNfz7>
- <https://Inkd.in/erQp9cq>
- <https://Inkd.in/eNTFEEC>
- <https://Inkd.in/eJFz5ra>
- <https://ctf.hacker101.com/>
- <https://Inkd.in/eMsrxpQ>
- <https://Inkd.in/ef4kFOX>
- <https://www.hackthebox.eu/>
- <https://Inkd.in/eW776r2>
- <https://Inkd.in/erhJpks>
- <https://Inkd.in/eEvqcJT>
- <https://Inkd.in/e83EfXP>
- <https://Inkd.in/eZD-SFR>
- <https://Inkd.in/e-ghWRZ>
- <https://Inkd.in/eFXvmDj>
- <https://Inkd.in/e9YUSC7>
- <https://Inkd.in/ejVpGGt>
- <https://Inkd.in/esPgayX>
- <https://Inkd.in/e32fMwS>
- <https://Inkd.in/eX4-mK4>
- <https://Inkd.in/e-8YKX5>
- <https://Inkd.in/egim iq>