PENTEST TOOLKIT

Information Gathering

- Osint Framework
- Dig
- Dnsenum
- Sublist3r
- Dnstracer
- Hping3
- Whois
- Nmap
- Google Hacking Database
- Doxing Techniques
- Dnsrecon
- Sslstrip
- Wireshark
- Recon-ng
- Nikto
- Maltego & Casefile
- Meetagofil
- Wafw00f

Scanning & Enumeration

- Nmap
- Nikto
- Dnsenum
- Openvas & Nessus
- Oscanner
- Enum4linux
- PrivescCheck
- LinEnum
- Dnsdumpster
- Sqlninja
- Sqlsus
- Vega
- Wpscan and joomscan
- Dirb
- Gobuster and Wfuzz
- Fimap
- CURL
- Whatweb
- Powershell Scripts

Exploitation and Techniques Red Team

- Metasploit
- Beef
- Exploitdb and Searchsploit
- Routersploit
- Sqlmap
- Hydra and patator
- Github search exploit
- Mitre Att&ck
- Veil-evasion
- Setoolkit & Shellphish
- Unicorn
- LuckyStrike
- Eggshell
- Burp suite
- Exploit pack
- Linux Suggester
- Shellter and Hyperion
- Netcat & cryptcat
- Crunch & Ophcrack & John & Hashcat & Hashid & ncrack

Post-exploitation Tools

- Cobalt Strike & Convenant & Gcat &Trevorc2 & Merlinc2 & dnscat
- Silenttrinity
- Psattack
- LinEnum
- UacMe
- Powerup
- Sherlock
- Tokenvator
- Potato
- PenTest Monkey & Incognition
- Meterpreter & Mimikatz
- Powershell Rat & Responder & Powersploit

Report

- Dradis
- Libre Office & Office 365
- Cherrytree
- Cutycapt
- Pipal
- RDPY
- Nipper-ng
- Google Hacking report template
- Attackforge
- Infection monkey
- IDE Faraday

By Joas Antonio

RED TEAM TECHNIQUES AND TOOLS - LINKS

- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://attack.mitre.org/
- https://github.com/FuzzySecurity/PowerShell-Suite
- https://github.com/Mr-Un1k0d3r/RedTeamPowershellScripts
- https://github.com/threatexpress/red-team-scripts
- https://github.com/SadProcessor/SomeStuff
- https://github.com/rvrsh3ll/Misc-Powershell-Scripts
- https://github.com/enigma0x3/Misc-PowerShell-Stuff
- https://github.com/ChrisTruncer/PenTestScripts
- https://github.com/bluscreenofjeff/Scripts
- https://github.com/xorrior/RandomPS-Scripts
- https://github.com/xorrior/Random-CSharpTools
- https://www.tutorialspoint.com/kali_linux
- https://weibell.github.io/reverse-shell-generator/
- https://github.com/Z4nzu/hackingtool
- https://github.com/enaqx/awesome-pentest
- https://github.com/S3cur3Th1sSh1t/Pentest-Tools
- https://github.com/arch3rPro/PentestTools
- https://github.com/iDigitalFlame/redteam-tools
- https://github.com/d0nkeys/redteam
- https://github.com/sectool/redteam-hardware-toolkit
- https://drive.google.com/drive/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU (My ebooks)
- https://github.com/an4kein/awesome-red-teaming
- https://github.com/mantvydasb/RedTeam-Tactics-and-Techniques
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/emilyanncr/Windows-Post-Exploitation
- https://github.com/mubix/post-exploitation
- https://github.com/swisskyrepo/PayloadsAllTheThings
- https://github.com/SecWiki/windows-kernel-exploits
- https://tools.kali.org/tools-listing
- https://github.com/CyberSecurityUP/information-security-relatory

By Joas Antonio

CENTRO DE TREINAMENTOS

- https://acaditi.com.br/
- https://www.bootsantos.com/
- https://becodoexploit.com/
- https://www.comptia.org/
- https://www.cybrary.it/
- https://desecsecurity.com/
- https://esecurity.com.br/
- https://www.eccouncil.org/
- https://elearnsecurity.com/
- https://www.pentesteracademy.com/
- https://gohacking.com.br/
- https://www.sans.org/
- https://www.offensive-security.com/
- https://specterops.io/
- http://zeropointsecurity.co.uk/
- https://sec4us.com.br/

By Joas Antonio