

Pentest in Office365 and Security

Joas Antonio

Details

- This pdf aims to bring techniques and tools for performing pentesting in Office365 environments

My LinkedIn: <https://www.linkedin.com/in/joas-antonio-dos-santos>

Introduction

- <https://docs.microsoft.com/pt-br/microsoft-365/?view=o365-worldwide>
- <https://docs.microsoft.com/pt-br/office/>
- [https://docs.axway.com/bundle/AMPLIFY Integration Builder allOS en/page/microsoft office 365 api documentation.html](https://docs.axway.com/bundle/AMPLIFY_Integration_Builder_allOS_en/page/microsoft_office_365_api_documentation.html)
- <https://system.suny.edu/userservices/office365-faq/>
- <https://github.com/MicrosoftDocs/microsoft-365-docs>
- <https://techdocs.blogs.brynmawr.edu/6634>
- <https://www.varonis.com/blog/microsoft-office-365-file-sharing/>
- <https://www.youtube.com/watch?v=01T6gSvR0xs>

Introduction

- <https://www.microsoft.com/pt-br/microsoft-365>
- <https://www.microsoft.com/pt-br/microsoft-365/microsoft-office>
- <https://www.microsoft.com/pt-br/microsoft-365/microsoft-365-for-existing-subscribers>
- <https://www.youtube.com/watch?v=HhgpVvqZhzA>
- <https://www.youtube.com/watch?v=zsBt85WjtIY>

PenTest in Office365

- <https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement>
- <https://www.agileit.com/news/pentesting-microsoft-office-365/>
- <https://bond-o.medium.com/microsoft-office-365-enumeration-58f9b5ba21c8>
- <https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/>
- <https://thecyphere.com/blog/office365-security-best-practices/>
- <https://www.imgsecurity.com/will-you-be-pwned-in-an-office-365-brute-force-attack-use-this-free-tool-for-testing/>
- <https://intercom.help/cobalt/en/articles/4641747-network-office-365-penetration-testing>
- <https://www.trustedsec.com/blog/owning-o365-through-better-brute-forcing/>
- <https://www.redscan.com/news/office-365-security-six-ways-to-safeguard-your-environment-against-cyber-attacks/>
- <https://www.kitploit.com/2019/07/o365-attack-toolkit-toolkit-to-attack.html?m=0>

PenTest in Office365

- <https://vapt.ee/offensive-security/penetration-testing/cloud-penetration-testing/office365-penetration-testing/>
- <https://www.blackhillsinfosec.com/tag/office365/>
- <https://github.com/0xZDH/o365spray>
- <https://github.com/S3cur3Th1sSh1t/Pentest-Tools>
- <https://github.com/mdsecresearch/LyncSniper>
- <https://github.com/byt3bl33d3r/SprayingToolkit>
- <https://github.com/sensepost/ruler>
- <https://pentestbook.six2dez.com/enumeration/cloud/azure>
- <https://www.blackhatethicalhacking.com/tools/o365-attack-toolkit/>
- <https://www.cryptron.ch/security-analysis-microsoft-office-365-advanced-threat-protection/>
- <https://securityonline.info/raindance/>
- <https://www.microsoft.com/pt-br/msrc/pentest-rules-of-engagement>

PenTest in Office365

- <https://www.agileit.com/news/pentesting-microsoft-office-365/>
- <https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/>
- <https://thecyphere.com/blog/office365-security-best-practices/>
- <https://www.linkedin.com/pulse/risk-assessment-penetration-testing-microsoft-azure-satinder/>
- <https://www.cryptron.ch/security-analysis-microsoft-office-365-advanced-threat-protection/>
- <https://i.blackhat.com/USA-20/Thursday/us-20-Bienstock-My-Cloud-Is-APTs-Cloud-Investigating-And-Defending-Office-365.pdf>
- <https://i.blackhat.com/USA-19/Wednesday/us-19-Metcalf-Attacking-And-Defending-The-Microsoft-Cloud.pdf>
- <https://www.blackhat.com/docs/us-17/wednesday/us-17-Dods-Infecting-The-Enterprise-Abusing-Office365-Powershell-For-Covert-C2.pdf>
- <https://github.com/Kyuu-Ji/Awesome-Azure-Pentest>
- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md>
- <https://book.hacktricks.xyz/cloud-security/cloud-security-review>
- <https://www.blackhillsinfosec.com/exploiting-mfa-inconsistencies-on-microsoft-services/>
- <https://www.optiv.com/insights/source-zero/blog/go365-office-365-password-spraying-tool>

Phishing Office365

- <https://github.com/duocircle/Office365-Phishing-Rules>
- <https://github.com/AlteredSecurity/365-Stealer>
- <https://github.com/mdsecactivebreach/o365-attack-toolkit>
- <https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?redirectSourcePath=%252fen-us%252farticle%252fSet-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6&view=o365-worldwide#enablemfaoffice365>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/set-up-anti-phishing-policies.md>
- <https://github.com/pentestgeek/phishing-frenzy-templates/tree/master/office365>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/campaigns/m365-campaigns-phishing-and-attacks.md>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/tuning-anti-phishing.md>
- <https://github.com/milo2012/phishing-scripts/blob/master/o365.py>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365.md>

Phishing Office365

- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/attack-simulation-training.md>
- <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/attack-simulator-need-a-real-phishing-template-library-to-be/m-p/1405895>
- <https://staaldraad.github.io/2017/08/02/o365-phishing-with-oauth/>
- <https://medium.com/sekoia-io-blog/analysis-and-detection-of-mitm-phishing-attacks-bypassing-2fa-o365-use-case-cf0ffdae9cae>
- <https://hooksecurity.co/phishing-examples/github-phishing-example>
- <https://otx.alienvault.io/pulse/5df9f836cfe26eacac1703ad>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/attack-simulator.md>
- https://github.com/MicrosoftLearning/MS-500-Microsoft-365-Security/blob/master/Instructions/Labs/MS500T00/LAB_AK_06_Lab1_Ex1_Phishing_attack.md
- https://github.com/MicrosoftLearning/MS-101T00-Microsoft-365-Mobility-and-Security/blob/master/Instructions/Labs/LAB_AK_03_Lab3_Ex1_AttackSim_Phishing_attack.md

Office 365 Security

- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/defender-for-office-365.md>
- <https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Delivery/Open%20email%20link.txt>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/security-recommendations-for-priority-accounts.md>
- <https://docs.microsoft.com/pt-br/microsoft-365/security/defender/overview-security-center?view=o365-worldwide#:~:text=O%20Microsoft%20365%20de%20seguran%C3%A7a,seguran%C3%A7a%20para%20o%20portal%20unificado.&text=As%20fun%C3%A7%C3%B5es%20j%C3%A1%20nos%20produtos,portal%20Microsoft%20365%20seguran%C3%A7a%2C%20automaticamente.>
- <https://www.microsoft.com/security/blog/office-365-security/>
- <https://www.cloudfastpath.com/office-365-migration/top-office-365-security-features-examples/>
- <https://docs.microsoft.com/pt-br/microsoft-365/security/office-365-security/security-dashboard?view=o365-worldwide>
- <https://www.youtube.com/watch?v=eBByRs1GsuA>
- <https://www.youtube.com/watch?v=hl4Kid-uzxY>
- <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-365-security-for-it-pros-2021-edition/m-p/1518661>
- <https://medium.com/falconforce/reducing-your-office365-attack-surface-1073a4d46a7b>
- https://www.beazley.com/documents/TMB/Insights/beazley-bbr-hardening_O365_best_practices_08312018.pdf
- https://www.cisecurity.org/benchmark/microsoft_office/
- <https://static1.squarespace.com/static/5bbb4a7301232c6e6c8757fa/t/603f6ea2dbc4a57691453b61/1614769826578/Office+365+Hardening.pdf>