Plano de Estudos Cyber Security - Parte 1 Red Team

Joas Antonio

Detalhes

- Fiz esse PDF para auxiliar nos estudos em Cyber Security Red Team, com materiais e dicas;
- Não é um guia que vai te tornar um profissional, mas para dar uma direção mesmo;

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

Red Team e Blue Team

Red Team e Blue Team: Conhecimentos Fundamentais

- Você que está iniciando na área de Red Team ou Blue Team, quais conhecimentos possui, já auto se avaliou? É essencial conhecimentos fundamentais antes de tudo, por exemplo:
- Conhecimentos sólidos em Redes de Computadores, Administração de Redes e Segurança de Redes;
- Habilidades e conhecimentos em Execução de comandos (Windows e Linux);
- Lógica da programação aprofundada;
- Conhecimentos em Linguagens de Programação, muitos começam com Python, mas no seu dia a dia, Python e C são os principais requisitos, mas outras linguagens durante o cotidiano será necessário pelo menos entender, por isso a lógica é essencial;
- Conhecimentos em Administração de Sistemas Operacionais Windows e Linux;
- Conhecimentos fundamentais em Segurança da Informação, normas, padrões, metodologias e gestão de segurança;
- Conhecer de arquitetura e soluções de cibersegurança é importante;
- Clouding Computer, IoT e Containers são essenciais, eu recomendo conhecer;

Red Team e Blue Team: Fundamentos (Material)

- http://brasilmaisdigital.org.br/index.php/pt-br/
- https://www.dltec.com.br/
- http://www.eadccna.com.br/
- https://www.udemy.com/
- https://www.youtube.com/user/cursosemvideo
- https://www.youtube.com/user/excriptvideo
- https://4linux.com.br/cursos/cursos-gratuitos/
- https://www.ev.org.br/
- https://www.cisco.com/c/pt_br/training-events/training.html
- https://www.cybrary.it/

Red Team e Blue Team: Fundamentos (Material)

- https://cheatography.com/davechild/cheat-sheets/linux-command-line/
- https://phoenixnap.com/kb/linux-commands-cheat-sheet
- https://www.linuxtrainingacademy.com/linux-commands-cheat-sheet/
- https://www.guru99.com/linux-commands-cheat-sheet.html
- https://github.com/vincenzobaz/Computer-Networks-Notes/blob/master/notes.md
- https://github.com/vincenzobaz/Computer-Networks-Notes
- https://github.com/hasantezcan/computer-networks-notes
- https://github.com/xiedaxia1hao/Computer-Networking-Notes
- https://github.com/changkun/computer-networks
- https://github.com/franciscolfraga/Computer-Networking-Notes/blob/master/README.md

Red Team e Blue Team: Fundamentos (Material)

- https://github.com/ravexina/linux-notes
- https://github.com/mahammad/my-Linux-Notes
- https://github.com/pimterry/notes
- https://github.com/microsoft/WSLab
- https://medium.com/javarevisited/top-5-free-courses-to-learn-docker-for-beginners-best-of-lot-b2b1ad2b98ad
- https://www.youtube.com/watch?v=fqMOX6JJhGo&ab_channel=freeCodeCamp.org
- https://github.com/tmrts/awesome-cloud-computing
- https://github.com/rootsongjc/awesome-cloud-native

Red Team e Blue Team: Fundamentos (Material)

- https://github.com/sbilly/awesome-security
- https://github.com/onlurking/awesome-infosec
- https://github.com/fabionoth/awesome-cyber-security
- https://github.com/joe-shenouda/awesome-cyber-skills
- https://github.com/sobolevn/awesome-cryptography
- https://github.com/inputsh/awesome-linux
- https://github.com/Awesome-Windows/Awesome
- https://github.com/decalage2/awesome-security-hardening

Red Team e Blue Team: Fundamentos (Dicas)

- Caso queira algo mais estruturado, seja para estudar redes, segurança, sistemas operacionais, tenho uma dica:
  - Pegue conteúdos de certificações, de uma olhada na ementa e estude;
  - Não desperdice conteúdos gratuitos, qualquer oportunidade estude;
  - Procure por cheatsheets, notes e awesomes no Google;
  - Canais no YouTube tem uma gama de conteúdo que pode ajudar;
  - Artigos no Medium e LinkedIn tem vastos conteúdos, feitos por profissionais, eu recomendo;
  - Fórum e comunidades ajudam bastante;

RED TEAM

Guia de Estudos

Red Team - Conceitos

- https://medium.com/@antman1P_30185/red-teaming-from-the-military-to-corporate-information-security-teams-408c040bd87e
- https://pt.slideshare.net/JoeGrayCISSPISSMP/red-team-framework
- https://purplesec.us/red-team-vs-blue-team-cyber-security/
- https://www.youtube.com/watch?v=QPmgV1SRTJY&ab_channel=SANSOffensiveOperations
- https://www.youtube.com/watch?v=8a-sBM34BU4&ab_channel=Infosec
- https://www.csoonline.com/article/3267691/what-is-mitres-attandck-framework-what-red-teams-need-to-know.html
- https://www.youtube.com/watch?v=q7VQeK533zI&ab_channel=RaphaelMudge
- https://medium.com/@redteamwrangler/how-do-i-prepare-to-join-a-red-team-d74ffb5fdbe6

Red Team – Conhecimentos Fundamentais

Quais conhecimentos um Red Team deve ter? Agora que você esta aprendendo PenTest, vou dar umas dicas para você se tornar um bom Red Team, lembre-se que aqui já estou partindo para algo mais avançado, antes de tudo tenha fundamentos, pois só ele vai conseguir te desenvolver.

- Conhecimentos em Threat Intelligence;
- Metodologias e Frameworks de Threat Intelligence e PenTest;
- Conhecimentos na estrutura Mitre Att&ck e TTPs;
- Conhecimentos na estrutura Cyber Kill Chain;
- Conhecimentos em Gestão de Vulnerabilidades e Riscos;
- Plano de Remediação;
- Conhecimentos em Resposta a Incidentes de segurança;
- Conhecer o ciclo de vida de um ataque;
- Habilidades com desenvolvimento/programação;
- Conhecimentos em Segurança de Aplicação;

Red Team – Conhecimentos Fundamentais

- Habilidades com Engenharia Reversa e Desenvolvimento de Exploits;
- Habilidades para escrever relatórios técnicos;
- Conhecimentos em Segurança Física;
- Conhecimentos em Engenharia Social;
- Habilidades com treinamento e comunicação;
- E ter uma mentalidade ofensiva, veja que nada é seguro e todo sistema foi feito para funcionar, funcionando está tudo bem. Então desenvolva uma mente Ofensiva e Try Harder, sempre cutuque e pense fora da caixa;

Red Team – Estrutura

- Initial Access
- Network Propagation
- Discovery
- Privilege Escalation
- Persistence
- Defense Evasion and Execution
- Credential Access
- Lateral Movement and Pivoting
- Action on Objectives
- Target Manipulation, Collection, and Exfiltration

Red Team - Dicas e Truques

- Pratique e desenvolva suas habilidades, por exemplo: Se você está estudando Engenharia Reversa, busque CTFs e desafios para você aprimorar suas habilidades, além disso, estude as ferramentas mais utilizadas dentro desse campo. Entender as armas que os criminosos utilizam é essencial para ter uma visão de como eles pensam.
- Investir em uma infraestrutura para suas operações é essencial, principalmente para trabalhar com C2. Além de auxiliar nas pesquisas de segurança, simulando ambientes controlados para caçar 0days ou testar uma vulnerabilidade nova;
- Além disso, aprenda a utilização de mecanismos de proteção como Firewall, IDS, IPS, Proxys e etc. Assim você entende como bypassa-los e como configurar para coibir diversos tipos de ataques e até mesmo detectar um comportamento diferenciado na rede;

Red Team - Dicas e Truques

- Trabalhe com Frameworks voltados a Red Team e pesquise ferramentas que podem ser uteis para cada campo da estrutura envolvida em um ciclo de ataque. O Mitre Att&ck tem uma estrutura de grupos que traz os métodos utilizados pelos principais grupos de APT https://attack.mitre.org/groups eu recomendo dar uma olhada;
- Um C2 ou C3 é essencial para qualquer equipe de Red Team, eu recomendo dar uma olhada nesse projeto https://www.thec2matrix.com/ que traz informações relevantes sobre todos os C2 e C3 disponiveis por ai;
- Assista palestras, participle de comunidades de Red Team, pois é um bom meio de adquirir conhecimentos e trocar informações;
- Um bom Red Team ele tem uma visão de atacante, por isso existem diversos cursos de Red Team Operations que ensinam técnicas diferenciadas para comprometer um alvo, com o foco de ensinar a mentalidade de um atacante. E para isso é necessário que você não apenas como um atacante ele atua, mas como um Host vulnerável pode ser manipulado durante e pós invasão, conheça bem dos principais sistemas utilizados em Empresas, Industrias e até por usuários comuns;

Cursos – Red Team

- https://redteamsecuritytraining.com/
- https://www.pentesteracademy.com/redteamlab
- https://www.sans.org/cyber-security-courses/red-team-exercises-adversary-emulation/
- https://redteamacademy.com/course/certified-red-team-associate/
- https://www.zeropointsecurity.co.uk/red-team-ops
- https://specterops.io/how-we-help/training-offerings/adversary-tactics-red-team-operations
- https://www.fireeye.com/services/training/courses/creative-red-teaming.html
- https://acaditi.com.br/
- http://sec4us.com.br/
- https://gohacking.com.br/
- https://www.iacertification.org/crtop_certified_red_team_operations_professional.html

Fontes de Pesquisas – Red Team

- https://www.blackhat.com/docs/webcast/01182018-Using-Red-Team-for-So-Much-More.pdf
- https://i.blackhat.com/USA-19/Thursday/us-19-Smith-Fantastic-Red-Team-Attacks-And-How-To-Find-Them.pdf
- https://i.blackhat.com/webcasts/2019/BlackhatWebinar-Leveraging-Red-for-Defense-by-David-Kennedy.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Nickels-MITRE-ATTACK-The-Play-At-Home-Edition.pdf
- https://www.blackhat.com/docs/webcast/2018-08-23-handling-vast-amounts-of-threat-intel-via-automation-by-anomali.pdf
- https://media.blackhat.com/bh-us-12/Briefings/Amit/BH_US_12_Amit_Sexy_Defense_WP.pdf

Fontes de Pesquisas – Red Team

- https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Landers-Flying-A-False-Flag-Advanced-C2-Trust-Conflicts-And-Domain-Takeover.pdf
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Rikansrud-Mainframe-[zOS]-Reverse-Engineering-and-Exploit-Development.pdf
- https://i.blackhat.com/eu-19/Thursday/eu-19-Zhang-New-Exploit-Technique-In-Java-Deserialization-Attack.pdf
- 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/executive-interviews/us-20/black-hat-webcast-summary_how-attackers-confuse-investigators-with-cyber-false-flag-attacks_extrahop.pdf

Fontes de Pesquisas – Red Team

- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/an4kein/awesome-red-teaming
- https://github.com/marcosValle/awesome-windows-red-team
- https://0xsp.com/offensive/red-ops-techniques/red-team-cheatsheet
- https://github.com/therealdeho/red-team-cheat-sheet
- https://adsecurity.org/wp-content/uploads/2016/08/DEFCON24-2016-Metcalf-BeyondTheMCSE-RedTeamingActiveDirectory.pdf
- https://arnavtripathy98.medium.com/my-crtp-experience-20076c8c3e26
- https://github.com/Kitsun3Sec/Pentest-Cheat-Sheets

Fontes de Pesquisas – Red Team

- https://stark0de.com/2020/04/30/crtp-review.html
- https://kdpbuster.medium.com/review-advanced-red-team-labs-pentester-academy-b6195109d47f
- https://fiddlycookie.medium.com/my-certified-red-team-professional-journey-2020-review-2f82e60b7958
- https://robsware.medium.com/a-review-of-crtp-and-the-attacking-and-defending-active-directory-course-f66360a26a05
- https://www.amazon.com.br/Tribe-Hackers-Red-Team-Cybersecurity/dp/1119643325
- https://www.amazon.com.br/Red-Team-Development-Operations-practical/dp/B083XVG633
- https://www.amazon.com.br/Hacker-Playbook-Practical-Penetration-Testing/dp/1980901759
- https://redteams.net/redteaming
- https://redteamacademy.com/blogs/
- https://www.ired.team/
- https://medium.com/@ismailtasdelen/red-team-hardware-toolkit-1f8d6737d934

Fontes de Pesquisas – Red Team

- https://medium.com/@dmchell/what-ive-learned-in-over-a-decade-of-red-teaming-5c0b685c67a2
- https://medium.com/@cyb3rops/the-problems-with-todays-red-teaming-7b8ed1e735c9
- https://medium.com/@malcomvetter/how-to-create-an-internal-corporate-red-team-1023027ea1e3
- https://medium.com/@malcomvetter/choose-your-own-red-team-adventure-f87d6a3b0b76

Fontes de Pesquisas – Red Team

- https://ippsec.rocks/?#
- https://www.youtube.com/channel/UCNSdU_1ehXtGclimTVckHmQ
- https://www.youtube.com/c/JohnHammond010
- https://www.youtube.com/user/GynvaelEN
- https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA
- https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w
- https://www.youtube.com/channel/UCCZDt7MuC3Hzs6IH4xODLBw
- https://www.youtube.com/channel/UCQN2DsjnYH60SFBIA6IkNwg
- https://www.youtube.com/channel/UChjC1q6Ami7W0E71TzPZELA
- https://medium.com/ctf-writeups
- https://github.com/enaqx/awesome-pentest
- https://github.com/apsdehal/awesome-ctf

Fontes de Pesquisas – Red Team

- https://github.com/paralax/Awesome-Pentest-1
- https://github.com/x0x8x/awesome-pentester
- https://github.com/CyberSecurityUP/Awesome-PenTest-Practice
- https://github.com/0x4D31/awesome-oscp
- https://github.com.cnpmjs.org/topics/oscp-prep
- https://johnjhacking.com/blog/the-oscp-preperation-guide-2020/
- https://github.com/burntmybagel/OSCP-Prep
- https://cybersecurity.att.com/blogs/security-essentials/how-to-prepare-to-take-the-oscp
- https://medium.com/@galolbardes/passing-the-oscp-while-working-full-time-29cb22d622e0
- https://medium.com/@gavinloughridge/a-beginners-guide-to-vulnhub-part-1-52b06466635d
- https://www.youtube.com/channel/UCXPdZsu8g1nKerd-o5A75vA
- https://www.youtube.com/channel/UC8nq3PX9coMiqgKH6fw-VCQ

Certificações

CONCLUSÃO

- Caso queira mais conteúdos e artigos referente a Red Team e um pouco de Blue Team, acesse meu LinkedIn que lá conto com quase 200 artigos;
- Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/
- Além disso, eu possuo diversos ebooks e documentos como esse, principalmente sobre pentest, caso queira dar uma olhada, segue o link: https://bit.ly/3rQNjKa