A ARTE DO OSINT PARA PENTESTERS

PROF. JOAS ANTONIO

SOBRE O EBOOK

- Feito para profissionais de PenTest e Estudantes
- Dar os fundamentos e as ferramentas necessárias para realizar um reconhecimento mais cabal no sistema
- Ajudar os professores a se aprofundar mais em reconhecimento
- Apresentar metodologias

O QUE É A FASE DE RECONHECIMENTO?

RECONHECIMENTO

- Os Pen Testers realiza o levantamento do máximo de informações possíveis sobre a empresa analisada. Dados como os serviços prestados, os principais gerentes e diretores, localização física, existência de filias e etc.
- Além disso a fase de reconhecimento esta ligada a demonstrar o quanto a empresa fica exposta pela internet.

METODOLOGIA PARA RECONHECIMENTO

METODOLOGIA

- As metodologias são essenciais para a separação de tarefas afim de chegar em um único objetivo
- Sem as metodologias não teríamos a fase de reconhecimento em um PenTest, afinal foram metodologias como OSSTMM e PTES que ajudaram a designar essa fase como uma das essenciais em um PenTest
- Com isso, surgiu a metodologia OSINT

OSINT

- **OSINT** (sigla para Open source intelligence ou Inteligência de Fontes Abertas)
- OSINT é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através desses exemplos, como dados disponíveis para o público em geral, como jornais, revistas científicas e emissões de TV. OSINT é uma das fontes de inteligência.
- O OSINT é essencial sendo a metodologia principal para efetuar reconhecimentos.

ESTRUTURA DE OSINT

ESTRUTURA DO OSINT

1. Username
2. Email Address
3. Domain Name
4. Ip Address
5. Image / Videos / Docs
6. Social Networks
7. Instant Messaging
8. People Search Engine
9. Datin
10. Telephone Numbers
11. Public Records
12. Business Records
13. Transportation
14. Geolocation Tools / Maps

ESTRUTURA DO OSINT

15. Search Engine
16. Forums / Blogs
17. Archives
18. Language Translation
19. Metadata
20. Mobile Emulation
21. Terrorism
22. Dark Web
23. Digital Currency
24. Classifieds
25. Enconding / Decoding
26. Tools

ESTRUTURA DO OSINT

27. Malicious File Analysis
28. Exploits & Advisories
29. Threat Intelligence
30. OpSec

- Essas são as estruturas do OSINT.

COMO TRABALHAR COM O OSINT

EXEMPLO

1. Faça um planejamento, eu recomendo a utilização de ferramentas de Analytics ou de Inteligência para montar um gráfico legalzinho, existe a ferramenta Maltegoce que é sensacional!

Sobre o maltego: https://www.youtube.com/watch?v=sP-PI_SRQVo

2. Após o planejamento, faça o levantamento das informações mais básicas que tem, como número de funcionários, tamanho da empresa, seu faturamento e local aonde reside.
3. Depois procure suas redes sociais e faça levantamento dos sites que ela tem, você pode utilizar ferramentas como o Google Hacking, Whois e o Social Search

https://www.exploit-db.com/google-hacking-database

https://centralops.net/co/DomainDossier.aspx

https://www.social-searcher.com/

EXEMPLO

4. Após isso, procure seus funcionários em redes como LinkedIn ou Facebook, você pode utilizar ferramentas para isso

https://github.com/leapsecurity/InSpy

https://github.com/vysecurity/LinkedInt

5. Com isso você parte para a utilização de mecanismo de buscas mais profundos como o próprio GHDB, Maltego ou Filecase e procure tudo relacionado a uma determinada pessoa
6. Você pode utilizar os domínios e subdomínios para fazer varreduras e verificar o site de hospedagem e o administrador
7. Com informações básicas como email, você pode ir atrás de sites ao qual esse email está registrado

https://emailrep.io/

https://verify-email.org/

http://mailtester.com/testmail.php

EXEMPLO

8. Depois dos levantamentos básicos, você pode partir para as buscas de endereços de Ips
9. Em seguida por número de telefones
10. E depois por dados públicos ligados a um nome, número e afins
11. Após o levantamento de ips, você pode utilizar ferramentas de varreduras para verificar do que se trata tal ip

FERRAMENTAS

Ferramentas? Existem muitas, cada uma tendo uma opção melhor que a outra.

Por isso, eu recomendo esses sites: https://osintframework.com/

https://github.com/jivoi/awesome-osint

POR QUE ESTUDAR OSINT?

- É essencial o estudo do OSINT para possibilitar o levantamento de informações mais detalhadas
- As vezes a chave para um PenTest bem sucedido é o número de informações que você levanta, seja relevantes ou irrelevantes
- Os principais governos do mundo e centro de inteligências, utilizam de OSINT para buscar mais precisamente um alvo e ter mais porcentual de chances de ter um ataque bem sucedido
- Trabalhar com OSINT requer costume, pois ferramentas existem de monte, mas algumas chegam ter opções múltiplas, basta conhece-las e se aprofundar
- A dica que eu dou é realizar um OSINT em você e em seus familiares, tente buscar o maior número de informações possíveis e garanto que você vai se surpreender ao descobrir tanta coisa que é armazenado sobre você na World Wide Web
- Estude essa metodologia profundamente e explore o OSINT FRAMEWORK
- A chave para ser um ótimo PenTester e para realizar de maneira eficaz, é somente o número de informações que você tem.

DICA: ORGANIZAÇÃO

- Muitas informações requer organização, então utilize de planilhas, ferramentas de analise, folhas de papeis, prints e vídeos para a organização
- Separe todo tipo de informação, sendo e-mails, número de telefones, nome de usuários, endereços de ips, arquivos, noticias, históricos, planilhas e afins.
- Todos separados e organizados em pastas ou em ordem para que você não se perca.
- Busque ferramentas para isso é mais fácil e sempre garanta cópias dessas informações, pois as vezes você pode perder algo que nunca mais vai achar.
- O OSINT é essencial e ninguém pode negar, então estude e será o melhor PenTester.