TEMA 09
Footprint – Descoberta de Informações

Habilidades:

- Conhecimento sobre legislação de proteção de dados LGPD.
- Habilidades de conformidade com a LGPD.
- Competência em gestão de riscos de privacidade.
- Sensibilidade para a proteção de dados e privacidade.

Footprint (pegada, em inglês) é **a primeira etapa que um invasor**, seja ético ou não, realiza em um ataque. Este é o momento em que ele faz o reconhecimento e o estudo do alvo, além de levantar as informações necessárias com o auxílio de ferramentas públicas ou privadas, com o objetivo de analisar as possibilidades e preparar sua estratégia e ideias sem o perigo de detecção. Chamamos esta técnica, inclusive, de **pré-ataque**.

São diversas as opções de informações a serem exploradas por um hacker/cracker, como a arquitetura de uma rede, banco de dados, softwares e hardwares, configurações de back e front-end, entre outros.
O footprint (**ou rastreamento**) é uma prática que visa coletar informações e dados sobre uma entidade-alvo, e usa fontes disponíveis publicamente.

Aqui estão alguns tópicos importantes relacionados ao Footprint:

- **Definição:** O Footprint é o processo de rastrear e coletar informações sobre uma entidade, como uma pessoa, organização, sistema ou marca, por meio de fontes abertas, como registros públicos, mídias sociais, sites, fóruns e outras fontes de informação disponíveis publicamente.
- **Objetivos:** O objetivo do Footprint é obter uma visão abrangente e detalhada da entidade-alvo, enquanto coleta informações relevantes que podem ajudar na tomada de decisões informadas, análise de riscos, investigações ou qualquer outra atividade que exija conhecimento prévio sobre a entidade.
- **Fontes de informações utilizadas:** Durante o processo, várias fontes de informações são exploradas, como registros públicos, diretórios, sites de busca, redes sociais, blogs, fóruns, bancos de dados públicos, entre outros recursos disponíveis publicamente.
- **Métodos de coleta de informações:** Existem diferentes métodos para coletar informações durante o Footprint, incluindo pesquisa manual em sites e fontes relevantes, uso de ferramentas de busca especializadas, consulta a registros públicos, análise de perfis de mídias sociais e interação com a entidade-alvo para obter informações adicionais.
- **Tipos de informações coletadas:** No decorrer do Footprint, várias informações são coletadas, como nomes, endereços, números de telefone, endereços de e-mail, registros profissionais, histórico de empregos, relacionamentos, atividades nas mídias sociais, participação em fóruns, eventos passados e qualquer outra informação relevante disponível publicamente.
- **Análise e correlação de informações:** Após coletar as informações, é importante realizar uma análise cuidadosa e correlacionar os dados coletados para obter uma visão mais completa da entidade-alvo. Isso envolve a identificação de padrões, relacionamentos e qualquer outra informação que possa ser útil para entender a entidade em questão.
- **Importância do Footprint em diferentes áreas:** Ele é usado em diversas áreas, como segurança da informação, investigação digital, inteligência de negócios, análise de riscos, **due diligence**, marketing digital, entre outros. Ele fornece uma base sólida de informações para orientar decisões e atividades nessas áreas.

O Footprint é uma prática fundamental para obter informações relevantes sobre uma entidade-alvo

por meio de **fontes disponíveis publicamente**. A coleta e a análise de informações durante o Footprint fornecem uma visão abrangente e embasada da entidade, o que possibilita tomar decisões mais informadas e realizar atividades de forma mais eficiente.

Métodos de Footprint

Para a obtenção dessas informações, o atacante pode usar de diversas ferramentas e pesquisas, específicas ou públicas. Há vários métodos e cabe ao hacker/cracker definir o que usar de acordo com a complexidade do alvo. Vamos aprender alguns destes métodos?

Fingerprint

Definitivamente um dos pontos de partida quando falamos de Footprint. O Fingerprint (impressão digital) é a técnica que tem como objetivo identificar qual sistema operacional, versão e distribuição o alvo utiliza, além de identificar brechas nos protocolos de comunicação dos dispositivos que estão em uma rede, conhecidos como TCP/IP. Ao reconhecer essas informações, o atacante conseguirá optar quais ferramentas para que apresentem um melhor desempenho e compatibilidade.

As ferramentas utilizadas para este método são chamadas de Scanner de Fingerprint, que são separadas entre **Fingerprint ativo** e **Fingerprint passivo**.

O **Fingerprint passivo** atuará como farejador na rede do alvo para identificar o sistema operacional, analisando o formato dos pacotes, detectando a informação. Uma das ferramentas baseadas nesse Fingerprint é a **P0F**, que realiza o reconhecimento do sistema sem precisar enviar nenhum pacote e é capaz de retornar ao atacante a estruturação da rede.

OBS.: O P0f (Passive OS Fingerprinting) foi originalmente desenvolvido para sistemas Unix-like, como Linux e BSD, mas ele pode ser utilizado em outros sistemas operacionais, incluindo Windows, através de algumas soluções alternativas. P0f é uma ferramenta passiva de fingerprinting usada para identificar o sistema operacional, tipo de host e outros detalhes sobre um dispositivo em uma rede, sem enviar pacotes ativos.

Já o **Fingerprint ativo** é um pouco mais complexo, já que o mesmo encaminha pacotes anteriormente manipulados e analisará como a rede responde, que retorna informações para definir qual o sistema operacional a aplicação utiliza.

O mais conhecido fingerprint ativo, sem dúvidas, é o **NMap(Network Mapper – Mapeador de Rede)**, um programa que, além de detectar o sistema operacional, também é capaz de identificar os dispositivos conectados na rede e os serviços que estão sendo executados. Ele também consegue identificar se há portas abertas nesta rede, o que por si só já facilitaria bastante para o atacante.

OBS.: O Nmap (Network Mapper) é uma ferramenta poderosa e popular para exploração de rede e auditoria de segurança. Ele pode ser usado para descobrir hosts e serviços em uma rede, identificar portas abertas, determinar versões de software, detectar sistemas operacionais, entre outras funcionalidades.

Considerações de Uso

Legalidade e Ética: Certifique-se de ter permissão para escanear os hosts e redes. Escaneamento de portas e redes sem autorização pode ser ilegal e considerado como uma tentativa de invasão.

Desempenho: Scans grandes podem ser demorados e consumir muitos recursos. Use as opções com moderação e ajuste a profundidade dos scans conforme necessário.

Whois

O Whois é uma **ferramenta pública de consultas de domínios** que pode ser acessada via terminal/console ou até mesmo via site. Você pode conferir esta ferramenta facilmente em https://registro.br/tecnologia/ferramentas/whois/.
Ela permite a rápida obtenção de **dados do titular do domínio, como nome completo, endereços, telefones e e-mails**. Definitivamente um prato cheio para os atacantes, já que a ferramenta retorna informações de maneira rápida e sem deixar rastros.

IP Location

Funciona basicamente da **mesma forma que o Whois**, as ferramentas de localização via endereço IP permitem a realização de consultas de IP retornando à localização aproximada de endereços públicos. Você pode conferir esta ferramenta em https://iplocation.com .

DIG

A Domain Information Groper, ou pesquisador de informações de domínio, é uma ferramenta para consultar registros de DNS, abreviação de Domain Name System, traduzindo, Sistema de Nome de Domínio e são responsáveis por traduzir os endereços IP dos sites.

OBS.: O DIG (Domain Information Groper) é uma ferramenta de linha de comando usada para realizar consultas de DNS. Ele é amplamente utilizado para resolver nomes de domínio e diagnosticar problemas relacionados ao DNS. O DIG geralmente vem pré-instalado na maioria das distribuições Linux, especialmente em sistemas baseados no BIND (como Ubuntu, Debian).

A consulta de registros DNS (Domain Name System) relacionada ao Footprint é importante porque permite obter informações detalhadas sobre a infraestrutura de rede de uma entidade-alvo. Os registros DNS podem revelar:

1. Mapeamento de Domínios e IPs: A consulta DNS mostra como os domínios estão associados a endereços IP, o que ajuda a identificar servidores específicos, incluindo servidores de e-mail, servidores web e outros serviços associados ao domínio.

2. Identificação de Subdomínios: Muitas vezes, subdomínios podem ser descobertos através de consultas DNS, o que pode expor recursos adicionais da rede que podem ser explorados.

3. Exposição de Infraestrutura: Registros como MX (Mail Exchange) e NS (Name Server) fornecem detalhes sobre a infraestrutura de e-mail e os servidores de nomes utilizados pela entidade. Isso pode ser útil para entender a estrutura e as tecnologias empregadas.

4. Análise de Segurança: Informações obtidas através de consultas DNS podem ser usadas para avaliar possíveis vulnerabilidades, como a exposição de servidores que não deveriam ser públicos, configurações incorretas de DNS, ou a falta de segurança em determinados serviços.

5. Reconhecimento de Rede: A consulta DNS ajuda a construir um mapa da rede, permitindo que um analista (ou invasor) compreenda melhor como a rede da entidade está organizada, facilitando a realização de etapas subsequentes, como a identificação de alvos específicos para ataques.

Em resumo, a consulta de registros DNS é uma etapa crítica no Footprint porque fornece uma visão ampla e detalhada da infraestrutura de rede da entidade-alvo, que pode ser essencial para análises de segurança e preparação de estratégias, tanto defensivas quanto ofensivas.

TraceRoute

Ferramenta que realiza um mapeamento das rotas e topologia de uma rede específica. No Windows, ela vem com o nome de tracert, e pode ser facilmente utilizada **através do console do Prompt de Comando**.

Engenharia Social

Já vimos este nome antes, certo? Definitivamente a **Engenharia Social não poderia ficar de fora da lista de ferramentas mais comuns para Footprint**. Através da manipulação psicológica contra funcionários de uma empresa, por exemplo, o atacante consegue pegar as minúcias e informações valiosas para um ataque futuro.

Fotoprint

Footprint representa uma coleção de instrumentos que possibilitam a um invasor digital, seja ele hacker ou cracker, coletar dados adicionais acerca do seu objetivo. Utilizando-se do Footprint, o indivíduo será capaz de entender a mecânica de determinados serviços e softwares, o que possibilita a ele um aprimoramento de sua estratégia ofensiva.

Em outras palavras, Footprint é uma série de recursos que dão ao ciberinvasor, seja hacker ou cracker, o poder de extrair mais detalhes sobre a sua meta. Por meio do Footprint, ele tem a capacidade de decifrar a funcionalidade de várias aplicações e serviços, permitindo, dessa forma, o aperfeiçoamento de seu plano de ataque.

Desafio

Realize uma consulta através do Whois, inserindo um domínio de site que você costuma navegar. Depois, insira este mesmo domínio na ferramenta IP Location para descobrir outras características. Apresentar os passos.

https://www.invertexto.com/minha-localizacao-atual

ANEXO:

A distinção entre **hacker** e **cracker** é importante para entender as diferentes intenções e abordagens dentro do mundo da segurança digital.

- Hacker:

- Definição: Originalmente, o termo "hacker" se refere a uma pessoa com habilidades avançadas em informática e programação, que explora sistemas de computador para entender como funcionam e, muitas vezes, melhorar sua segurança.

- Intenção: Hackers geralmente têm intenções éticas e positivas, como identificar e corrigir falhas de segurança, melhorar sistemas ou contribuir para o avanço da tecnologia. Alguns hackers, conhecidos como "white hats", são contratados para testar a segurança de sistemas, enquanto outros, chamados de "grey hats", podem explorar falhas sem permissão, mas sem intenção maliciosa.

- Atividades: Podem incluir pentesting (teste de penetração), desenvolvimento de software de segurança, pesquisa em cibersegurança e participação em comunidades de código aberto.

- Cracker:

- Definição: Um cracker, por outro lado, é uma pessoa que utiliza suas habilidades para invadir sistemas com intenções maliciosas. O termo é frequentemente associado a atividades ilegais, como roubo de dados, sabotagem, ou distribuição de malware.

- **Intenção:** Crackers têm motivações que incluem ganho financeiro, protesto político (hacktivismo), vingança ou simplesmente a intenção de causar danos.
- **Atividades:** Podem incluir roubo de informações pessoais, instalação de ransomware, deface (desfiguração) de sites, e distribuição de software pirata.

Resumindo, enquanto **hackers** podem ser vistos como exploradores éticos e inovadores da tecnologia, **crackers** são associados à exploração maliciosa e ilegal dos sistemas de computador.