EEEP Deputado Roberto Mesquita

Ana Júlia Moreira Costa*
Antonio Isac Moura Rocha*

Footprinting e Coleta de Informações

Segurança da Informação

General Sampaio - CE
2024

RESUMO

A prática de Footprinting, ou Coleta de Informações, é uma fase crucial no ciclo de ataque cibernético, especialmente durante o processo de reconhecimento e preparação para uma invasão. Este artigo explora o conceito de footprinting, suas metodologias e ferramentas associadas, bem como sua aplicação tanto em contextos ofensivos quanto defensivos. A coleta de informações, quando executada de forma ética, pode ser usada para identificar vulnerabilidades em sistemas e redes, auxiliando na melhoria da segurança cibernética. O estudo também discute as implicações legais e éticas envolvidas no uso de técnicas de footprinting e coleta de informações.

Abstract:

The practice of Footprinting, or Information Collection, is a crucial phase in the cyber attack cycle, especially during the process of reconnaissance and preparation for an invasion. This article explores the concept of footing, its associated methodologies and tools, as well as its application in both offensive and defensive contexts. Information collection, when carried out ethically, can be used to identify vulnerabilities in systems and networks, helping to improve cybersecurity. The study also discusses the legal and ethical implications involved in using footprinting and information collection techniques.

PALAVRAS-CHAVES:
Footprinting, Coleta de Informações, Segurança Cibernética, Reconhecimento, Vulnerabilidades, Ética.

1 INTRODUÇÃO

O Footprinting, ou Coleta de Informações, refere-se ao processo de recolher dados sobre um alvo para ajudar na identificação de possíveis vulnerabilidades e pontos de acesso em sistemas e redes. Essa prática é uma das primeiras etapas de um ataque cibernético, mas também é utilizada de forma defensiva por profissionais de segurança para fortalecer a infraestrutura contra ameaças externas. A coleta de informações pode envolver uma variedade de fontes, incluindo dados públicos disponíveis na internet, registros de DNS, redes sociais e outras fontes abertas.

No contexto da Segurança da Informação, o footprinting pode ser dividido em duas categorias principais: footprinting passivo e footprinting ativo. O primeiro se refere a métodos de coleta de informações sem interagir diretamente com os sistemas ou redes alvo, enquanto o segundo envolve ações diretas, como sondagens e testes de penetração, para descobrir vulnerabilidades.

Este artigo tem como objetivo analisar as técnicas de footprinting e coleta de informações, abordando suas aplicações, implicações éticas e legais, e como essas práticas impactam a segurança cibernética.

2 CONCEITO E DEFINIÇÃO DE FOOTPRINTING

Footprinting, em português “pegada”, também conhecida como **reconhecimento**, é a técnica usada para coletar informações sobre os sistemas de computadores e as entidades às quais eles pertencem. Para obter essa informação, um hacker pode usar várias ferramentas e tecnologias. Esta informação é muito útil para um hacker que está tentando quebrar um sistema inteiro.

Quando usado no léxico de segurança do computador, o termo "Footprinting" geralmente se refere a uma das fases de pré-ataque, que são tarefas executadas antes de se fazer o ataque real. Algumas das ferramentas usadas para o Footprinting são Footprinting, em português “pegada”, também conhecida como reconhecimento, é a técnica usada para coletar informações sobre os sistemas de computadores e as entidades às quais eles pertencem. Para obter essa informação, um hacker pode usar várias ferramentas e tecnologias. Esta informação é muito útil para um hacker que está tentando quebrar um sistema inteiro.[1]

Quando usado no léxico de segurança do computador, o termo "Footprinting" geralmente se refere a uma das fases de pré-ataque, que são tarefas executadas antes de se fazer o ataque real. Algumas das ferramentas usadas para o Footprinting são Sam Spade, nslookup, traceroute, Nmap e neotrace.

REFERÊNCIAS:

1. http://searchsecurity.techtarget.com/definition/footprinting
2. http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

3 TIPOS DE FOOTPRINTING

3.1. Footprinting Passivo

O Footprinting passivo envolve a coleta de dados sem interagir diretamente com o alvo. As fontes mais comuns de informações passivas incluem:

Whois: Consulta de informações sobre o domínio de uma organização, como nome, endereço, número de telefone, entre outros dados de registro.
DNS: Consultas ao sistema de nomes de domínio que revelam informações sobre os servidores de nomes, endereços IP e outros registros relacionados ao domínio.
Redes sociais: Análise de perfis públicos e interações nas redes sociais para obter informações sobre os empregados, estrutura organizacional e outros detalhes que possam ser utilizados para ataques direcionados.
Informações públicas: Dados disponíveis publicamente em sites da empresa, relatórios anuais, documentos legais, entre outros.
O uso de footprinting passivo é geralmente mais difícil de ser detectado, pois o atacante não interage diretamente com o sistema alvo.

3.2. Footprinting Ativo

O Footprinting ativo, por outro lado, envolve interação direta com os sistemas da organização, o que pode gerar alertas ou registros nos logs do sistema. Exemplos de técnicas de footprinting ativo incluem:

Ping Sweeping: Técnica utilizada para descobrir quais máquinas em uma rede estão ativas.
Port Scanning: Exploração de portas abertas em sistemas e servidores para identificar pontos de vulnerabilidade.
Banner Grabbing: Extração de informações sobre os serviços e sistemas operacionais a partir dos banners retornados por serviços como HTTP, FTP e SMTP.

Traceroute: Determinação do caminho que os pacotes de dados percorrem até chegar ao destino, permitindo identificar a infraestrutura de rede utilizada pelo alvo.

Embora o footprinting ativo forneça informações mais detalhadas, ele também pode ser facilmente detectado por sistemas de monitoramento e segurança.

2.3. Coleta Ativa de Informações

Uma interação envolve interação direta com o alvo do sistema obtido informações. Alguns deles incluem: Scanner de rede: ferramentas como Nmap podem ser usadas para mapear um recinto ou alvo e identificar dispositivos conectados e seus serviços disponíveis e suas versões, importantes para a identificação de possíveis falhas de segurança. Interrogação DNS: consultando servidores DNS, informações sobre subdomínios, servidores de email, servidores web e outros alvos na infraestrutura podem ser descobertos. Análise de cabeçalho HTTP: examinar cabeçalhos HTTP específicos às respostas do servidor web revela detalhes sobre a versão do servidor, quadros de frameworks e quaisquer outras tecnologias que sejam uma ameaça.

3.3. Identificação de Vulnerabilidade

Com as informações adquiridas, a próxima etapa é analisar os dados e identificar vulnerabilidades e riscos no próprio sistema. Isso pode ser feito por ferramentas de varredura de vulnerabilidades, como o Nessus OpenVAS ou ferramenta de exploração específica. O mapeamento de portas abertas, a identificação de protocolos vulneráveis e as pesquisas de falhas comuns em softwares ou sistemas operacionais podem revelar falhas na segurança.

3.4. Identificando vulnerabilidades

Depois de coletar as informações, o próximo passo é analisar os dados para identificar vulnerabilidades e riscos do sistema. Com ferramentas como Nessus, OpenVAS ou qualquer software específico para exploração, uma verificação de vulnerabilidade pode ser realizada. O mapeamento de portas abertas, a identificação de protocolos vulneráveis e a busca por

falhas conhecidas no software ou no sistema operacional podem esclarecer pontos de contato de segurança fracos.

3.5. Análise/relatório

Uma vez feita a recolha e identificação de potenciais vulnerabilidades, é vital que os dados sejam sistematicamente organizados e analisados. Nesta fase, os profissionais de segurança deverão aplicar patentemente os resultados da recolha e elaborar o relatório técnico. O documento deve abranger: Um resumo das informações coletadas Descrições das vulnerabilidades descobertas Recomendações para mitigar o problema O objetivo deste relatório é servir como uma imagem clara e pragmática das ameaças identificadas e dos possíveis passos para superá-las.

3.6. Ferramentas utilizadas para o Footprinting

Existem muitas ferramentas que podem ser utilizadas para coletar informações no processo de footprinting. Alguns dos mais conhecidos incluem:

Nmap: Ferramenta de scanner de rede e descoberta de hosts.

Shodan: motor de busca que se concentra em encontrar dispositivos e máquinas conectadas à internet, como câmeras de segurança e servidores.

Whois: Pesquisar registros de domínio em relação a informações de localização e infraestrutura.

Google Hacking: quando se torna mais sútil e usa operadores de consulta do Google para encontrar informações detalhadas sobre o alvo.

3.7. Considerações Legais e Ética

Vale ressaltar que, apesar de ser uma ótima técnica de teste de invasão, os aspectos legais e éticos e o footprinting estão implicados. Algumas técnicas usadas para obter informações específicas podem ser classificadas como crime, da mesma forma que um ataque de social

engineering ou hacking. é importante que os profissionais sigam as regras e normas baseadas nela, pois a lei e a ordem também são moralmente éticas e obtêm o consentimento antes de testar redes ou dispositivos seguros.

4 CONCLUSÃO

O Footprinting é uma etapa essencial no ciclo de segurança cibernética, fornecendo informações críticas para identificar vulnerabilidades em sistemas e redes. Ao coletar dados ativos e passivos, você pode mapear a estrutura do alvo para prever falhas que os invasores podem explorar. A eficácia deste trabalho não reside apenas no uso correto das ferramentas, mas também na capacidade de interpretar e correlacionar as informações recebidas. Além disso, o Footprinting deve ser realizadas de forma ética e legal, respeitando as norma s de saúde e segurança. Agir com responsabilidade é importante porque pod e levar a danos legais. No cenário de ameaças cibernéticas em constante evolução, a pegada deve ser vista como um processo contínuo que se adapta às novas tecnologias e aos novos riscos. Feito da maneira certa, não apenas ajuda a proteger seus sistemas, mas também fortalece sua postura geral de segurança, permitindo responder melhor às ameaças.

Referências

1. ANTON, A. A. *Footprinting and Information Gathering Techniques for Ethical Hacking*. Journal of Information Security, 2022.
2. KISS, M. R. *The Role of Footprinting in Cybersecurity: A Comprehensive Guide*. Cybersecurity Research Institute, 2023.
3. SMITH, T. *Tools for Footprinting and Information Gathering*. Journal of Cybersecurity, 2021.
4. Shodan. (2024). *Shodan Search Engine*. https://www.shodan.io