EEEP DEPUTADO ROBERTO MESQUITA
DESENVOLVIMENTO DE SISTEMAS
SEGURANÇA DE SISTEMA DE INFORMAÇÃO

CARLOS DANIEL GOMES UCHOA*
JOSÉ RAY SANTIAGO GOMES**

FOOTPRINTING E COLETA DE INFORMAÇÕES

Uma Revisão e Análise de Metodologias em Segurança da Informação

General Sampaio - CE
2024

SUMÁRIO

RESUMO

O **footprinting** é a primeira etapa no processo de exploração de vulnerabilidades em sistemas computacionais, sendo uma técnica fundamental para os profissionais de segurança cibernética e hackers. O processo envolve a coleta e análise de informações sobre um alvo, como redes, sistemas, infraestrutura e usuários, com o objetivo de identificar possíveis pontos de entrada ou fraquezas. Este artigo tem como objetivo revisar as metodologias e técnicas de **footprinting** e coleta de informações, abordando suas aplicações, ferramentas e implicações éticas. Além disso, serão discutidos os métodos passivos e ativos, e como esses processos podem ser utilizados tanto para fins de segurança quanto para atividades maliciosas.

Palavras-chaves: hacker, footprinting, informações.

ABSTRACT

Footprinting is the first step in the process of exploiting vulnerabilities in computer systems, being a fundamental technique for cybersecurity professionals and hackers. The process involves collecting and analyzing information about a target, such as networks, systems, infrastructure and users, with the aim of identifying possible entry points or weaknesses. This article aims to review footprinting and information collection methodologies and techniques, addressing their applications, tools and ethical implications. Additionally, passive and active methods will be discussed, and how these processes can be used for both security purposes and malicious activities.

Keywords: hacker, footprinting, information.

1. INTRODUÇÃO

O termo footprinting, em segurança da informação, refere-se à coleta de informações sobre um alvo com o objetivo de descobrir vulnerabilidades que possam ser exploradas em um ataque cibernético. Esse processo, muitas vezes, é realizado de forma prévia ao ataque propriamente dito, proporcionando uma base sólida para ações posteriores, como o scanning e enumeration.

O footprinting pode ser classificado em duas categorias principais: passivo e ativo. O footprinting passivo refere-se à coleta de informações sem interação direta com o alvo, enquanto o ativo envolve ações que podem ser detectadas ou registradas pelo sistema alvo. A coleta de informações pode envolver dados como nomes de domínio, endereços IP, configurações de rede, e até mesmo informações sobre a equipe de TI da organização alvo.

2. TIPOS DE FOOTPRINTING

2.1 Footprinting Passivo

O footprinting passivo é realizado sem a necessidade de interação direta com o alvo. Nesse caso, as informações são coletadas de fontes públicas, sem alertar a organização sobre a análise em andamento. As principais fontes de dados incluem:

- WHOIS: A consulta de registros WHOIS é uma das maneiras mais comuns de coletar informações sobre nomes de domínio e endereços IP. Essas informações podem revelar detalhes sobre a organização, como nome, endereço, e informações de contato.
- DNS (Sistema de Nomes de Domínio): O DNS fornece informações valiosas sobre o mapeamento de endereços IP para nomes de domínio. Técnicas como consulta de registros MX, A e TXT podem revelar servidores de email, subdomínios e outras informações críticas
- Redes Sociais e Sites Públicos: As plataformas de redes sociais, blogs e websites corporativos muitas vezes expõem informações confidenciais de maneira inadvertida. A análise de perfis de funcionários, postagens e artigos pode fornecer dados sobre a estrutura organizacional e tecnologias utilizadas pela empresa.
- Buscas em Motores de Pesquisa: Ferramentas como Google e Bing podem ser utilizadas para encontrar informações expostas inadvertidamente, como documentos e arquivos que contenham dados sensíveis. A pesquisa avançada em motores de busca pode ser uma técnica poderosa para encontrar vulnerabilidades em sistemas.

2.2 Footprinting Ativo

No footprinting ativo, o profissional de segurança interage diretamente com o alvo, realizando atividades que podem ser detectadas por sistemas de monitoramento. Algumas das técnicas mais comuns incluem:

- Scanners de Portas: A varredura de portas pode revelar quais serviços estão sendo executados em um servidor ou dispositivo. Ferramentas como Nmap permitem identificar

portas abertas e os serviços associados a elas, ajudando a mapear a infraestrutura da rede alvo.

- Ping Sweep: Um ping sweep é utilizado para descobrir quais dispositivos estão ativos em uma rede. Essa técnica envolve enviar pacotes de ping para uma gama de endereços IP e verificar quais respondem, fornecendo uma lista de dispositivos disponíveis.

- Traceroute: A execução de um traceroute pode ajudar a entender o caminho que os pacotes de dados seguem até o destino, revelando a topologia da rede e possíveis pontos de vulnerabilidade.

- Finger e SNMP Walk: Algumas informações sobre sistemas e dispositivos podem ser extraídas por meio de protocolos como Finger ou SNMP (Simple Network Management Protocol), que oferecem detalhes sobre a configuração de sistemas e serviços.

3. FERRAMENTAS UTILIZADAS NO FOOTPRINTING

Existem várias ferramentas especializadas para realizar atividades de footprinting. Algumas das mais utilizadas incluem:

- **Nmap**: Utilizado principalmente para varredura de portas e mapeamento de rede, o Nmap também pode ser usado para detectar sistemas operacionais e versões de serviço executados em dispositivos.

- **Maltego**: Ferramenta que facilita a coleta de informações relacionadas a redes sociais, domínios, endereços IP e registros WHOIS, organizando dados em um formato visualmente acessível

- **theHarverster**: Uma ferramenta de código aberto usada para coletar informações sobre e-mails, domínios, subdomínios e servidores de forma automatizada.

- **Recon-ng**: Framework utilizado para a coleta de dados em fontes abertas, permitindo integração com diferentes APIs para extração de informações relevantes.

- **Shodan**: Motor de busca que permite a pesquisa de dispositivos conectados à Internet, proporcionando uma visão detalhada da infraestrutura exposta, como servidores e câmeras de segurança.

4. IMPLICAÇÕES ÉTICAS E LEGAIS

Embora o **footprinting** seja uma etapa importante para a proteção de sistemas, ele também pode ser explorado de maneira maliciosa. A coleta de informações sem a devida autorização pode ser considerada ilegal em várias jurisdições. O uso indevido dessas técnicas pode resultar em acusações de **invasão de privacidade** e **acesso não autorizado a sistemas.**

Para os profissionais de segurança cibernética, é essencial realizar essas atividades de forma ética, seguindo os princípios do **Testamento de Penetração Autorizada** (penetration testing) ou **avaliação de segurança autorizada**, em que o alvo consente com o processo de teste. É fundamental também garantir que os dados coletados sejam usados de forma responsável e protegidos de acessos não autorizados.

5. CONCLUSÃO

O footprinting é uma técnica poderosa de coleta de informações que pode ser usada tanto para fins de defesa quanto de ataque. Por meio de métodos passivos e ativos, os profissionais de segurança cibernética podem obter dados cruciais sobre redes, sistemas e infraestruturas, permitindo a identificação de vulnerabilidades antes que elas sejam exploradas por agentes maliciosos.

No entanto, o uso de técnicas de footprinting deve ser cuidadosamente regulamentado e realizado com ética, para garantir que as informações coletadas sejam utilizadas de maneira responsável. A crescente sofisticação das ferramentas e das táticas de coleta de dados também destaca a importância de uma constante atualização dos profissionais de segurança, a fim de lidar com novas ameaças e vulnerabilidades.

REFERÊNCIAS

Kaspersky. (2020). O que é Footprinting e como se proteger. Disponível em: https://www.kaspersky.com.br

SANS Institute. (2018). *Penetration Testing: Techniques and Tools*. SANS Training.

Stewart, J. M., & Northrup, M. (2019). *Network Security: A Practical Approach*. Wiley

Wheeler, T. (2021). *Hacking Exposed: Network Security Secrets & Solutions*. McGraw-Hill.