Cibersegurança Ofensiva: Desvendando vulnerabilidades e invasões digitais

WAGNER CAMARGO VAZ

CONHECIMENTOS ESSENCIAIS EM SEGURANÇA OFENSIVA

Introdução à Segurança Ofensiva

Segurança ofensiva é o ramo da cibersegurança que se concentra em testar e explorar sistemas e redes para encontrar vulnerabilidades antes que atacantes mal-intencionados o façam. Isso envolve pensar como um hacker para identificar falhas e ajudar a corrigir esses problemas. Aqui estão os principais conhecimentos que você precisa para se aventurar na segurança ofensiva.

01

RECONHECIMENTO E ENUMERAÇÃO

Reconhecimento é o processo de coletar informações sobre um alvo, como endereços IP, nomes de domínio, servidores e outros detalhes relevantes. A enumeração é uma fase mais avançada onde você identifica recursos específicos e serviços no alvo, como portas abertas, usuários e versões de software.

RECONHECIMENTO E ENUMERAÇÃO: FUNDAMENTOS DA SEGURANÇA OFENSIVA

O que é reconhecimento?

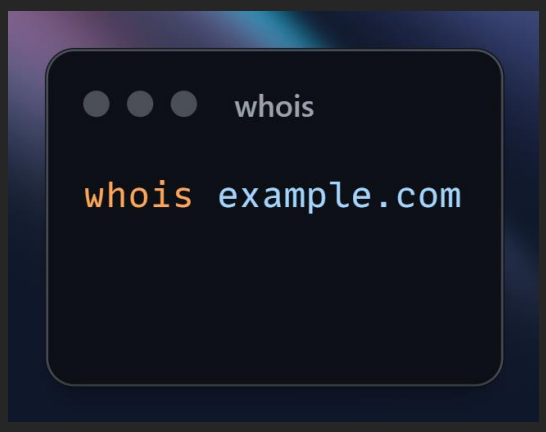
Reconhecimento é a fase inicial de qualquer operação de segurança ofensiva. O objetivo principal é coletar o máximo de informações sobre o alvo. Essas informações podem incluir endereços IP, nomes de domínio, servidores, topologia de rede e até mesmo detalhes de funcionários. Existem duas categorias principais de reconhecimento, o passivo e o ativo:

Reconhecimento Passivo

Envolve a coleta de informações sobre um alvo sem interagir diretamente com ele. Este método é utilizado para evitar a detecção. As fontes de dados para reconhecimento passivo são públicas e acessíveis.

Exemplos:

Pesquisa Whois: Obter informações sobre o registro de um domínio, incluindo dados do registrante e servidores DNS.



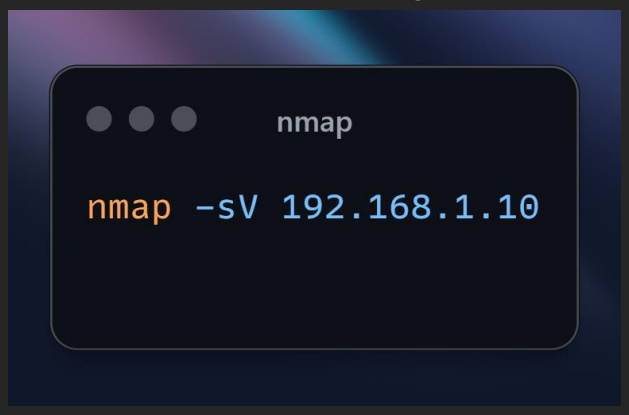
Consulta DNS: Usar ferramentas como dig para obter registros DNS como A, MX, NS, etc.

RECONHECIMENTO E ENUMERAÇÃO: FUNDAMENTOS DA SEGURANÇA OFENSIVA

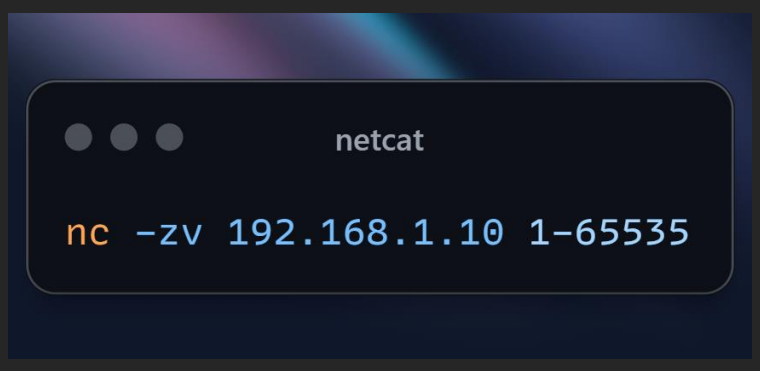
Reconhecimento Ativo

Envolve interações diretas com o sistema alvo. Essas interações podem ser detectadas e monitoradas, mas fornecem informações mais detalhadas e precisas. Durante o reconhecimento ativo, são realizadas varreduras e consultas diretamente na infraestrutura do alvo para mapear sua topologia e identificar possíveis pontos de entrada.

Exemplos: Varredura de Portas com Nmap: Identificar portas abertas e serviços em execução em um host específico.



Netcat: Utilizado para varredura de portas e teste de serviços.



RECONHECIMENTO E ENUMERAÇÃO: FUNDAMENTOS DA SEGURANÇA OFENSIVA

O que é enumeração?

Enumeração é a fase que segue o reconhecimento e envolve a extração de informações mais detalhadas e específicas sobre o alvo. Ao contrário do reconhecimento passivo, a enumeração geralmente envolve interações diretas com o sistema-alvo, o que pode ser detectado. As informações obtidas podem incluir portas abertas, serviços ativos, versões de software, contas de usuário e muito mais.

Técnicas Comuns de Enumeração

Varredura de Portas: Identificação de portas abertas e serviços associados usando ferramentas como Nmap.

Enumerar Serviços: Obtenção de informações detalhadas sobre os serviços em execução, como versões e configurações.

Enumerar Usuários: Identificação de contas de usuário no sistema, especialmente em servidores de e-mail e sistemas operacionais.

SNMP (Simple Network Management Protocol): Usado para obter informações sobre dispositivos de rede.

02

EXPLORAÇAO DE VULNERABILIDADES

Exploração envolve a identificação e uso de falhas em sistemas para ganhar acesso não autorizado. Essa fase pode incluir a utilização de ferramentas automatizadas ou a criação de exploits personalizados.

EXPLORAÇÃO DE VULNERABILIDADES

O que é?

Exploração envolve a identificação e uso de falhas em sistemas para ganhar acesso não autorizado. Essa fase pode incluir a utilização de ferramentas automatizadas ou a criação de exploits personalizados.

Exemplos Reais
Comando: msfconsole
Explicação: Abre o Metasploit Framework, uma ferramenta popular para exploração de vulnerabilidades.

Exemplo de Exploração: Usar o módulo exploit/windows/smb/ms17_010_eternalblue no Metasploit para explorar a vulnerabilidade EternalBlue em sistemas Windows desatualizados.

metasploit eternalblue

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.1.10
exploit
```

EXPLORAÇÃO DE VULNERABILIDADES

Ferramentas

Metasploit Framework: Uma plataforma para desenvolvimento e execução de exploits contra um alvo remoto.

Exploit-DB: Banco de dados de exploits que pode ser pesquisado usando a ferramenta searchsploit.

Burp Suite: Ferramenta de teste de segurança de aplicações web que permite identificar e explorar vulnerabilidades em sites.

03

ENGENHARIA SOCIAL

Engenharia social envolve manipular pessoas para divulgar informações confidenciais. É uma técnica que explora a psicologia humana em vez de vulnerabilidades técnicas.

ENGENHARIA SOCIAL

Engenharia social é uma técnica utilizada por atacantes para manipular indivíduos com o objetivo de obter informações confidenciais ou acesso a sistemas protegidos. Ao invés de explorar falhas técnicas, a engenharia social se aproveita da psicologia humana, utilizando táticas de engano e persuasão para induzir as vítimas a compartilhar dados sensíveis.

Técnica: Phishing
Enviar um e-mail que parece ser de uma fonte confiável, mas contém links maliciosos.
Exemplo de Phishing: Criar uma página de login falsa que se parece com a página oficial de um banco e enviar um e-mail pedindo aos usuários para fazerem login.

Técnica: Pretexting
Criar um cenário falso (pretexto) para obter informações. Por exemplo, fingir ser um funcionário do suporte técnico e solicitar credenciais do usuário.

Técnica: Baiting
Deixar dispositivos infectados, como pen drives, em locais públicos, esperando que alguém os conecte a um computador.

ENGENHARIA SOCIAL

Ferramentas

SET (Social-Engineer Toolkit): Ferramenta que facilita a criação de ataques de engenharia social, como phishing e ataques de clonagem de sites.

Comando: setoolkit
Abre o Social-Engineer Toolkit, onde você pode selecionar diferentes tipos de ataques de engenharia social.

Phishing Frameworks: Plataformas como Gophish permitem criar e gerenciar campanhas de phishing de forma eficaz.

Ferramentas que ajudam a criar, enviar e monitorar e-mails de phishing para testar a resiliência dos usuários contra ataques de engenharia social.

CONCLUSÕES

OBRIGADO POR LER ATÉ AQUI!

Esse Ebook foi gerado por IA e diagramado por humano.
O passo a passo se encontra no meu GitHub.

Esse conteúdo foi gerado com fins didáticos de construção, não foi realizado uma validação cuidadosa humana no conteúdo e pode conter erros gerados por uma IA.

https://github.com/waguiner89