Pós Exploração

Cassiano Peres

DIO Tech Education Analyst

cassiano-dio

peres-cassiano

Objetivo Geral

Neste curso vamos falar da etapa de pós exploração e como se manter conectado ao dispositivo atacado.

Pré-requisitos

Conhecimento prévio em linhas de comando Linux facilita o aprendizado.

Percurso

Etapa 1 Escalonamento de privilégios no Windows

Etapa 2 Extração de dados

Etapa 3 Módulos de pós exploração

Percurso

Etapa 4 Módulos de exploits para persistências

Etapa 1

Escalonamento de privilégios no Windows

Introdução

Pós-exploração refere-se a quaisquer ações tomadas após a abertura de uma *sessão*.

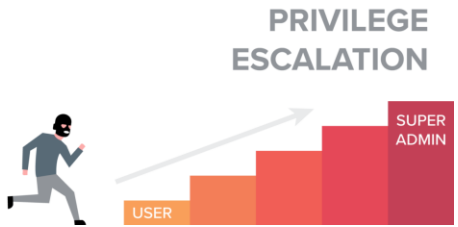
Pós exploração

Uma sessão é um *shell* aberto de uma exploração bem-sucedida ou ataque de força bruta, que por sua vez pode ser um *shell* padrão ou *Meterpreter*.

Pós exploração

Escalonamento de privilégios

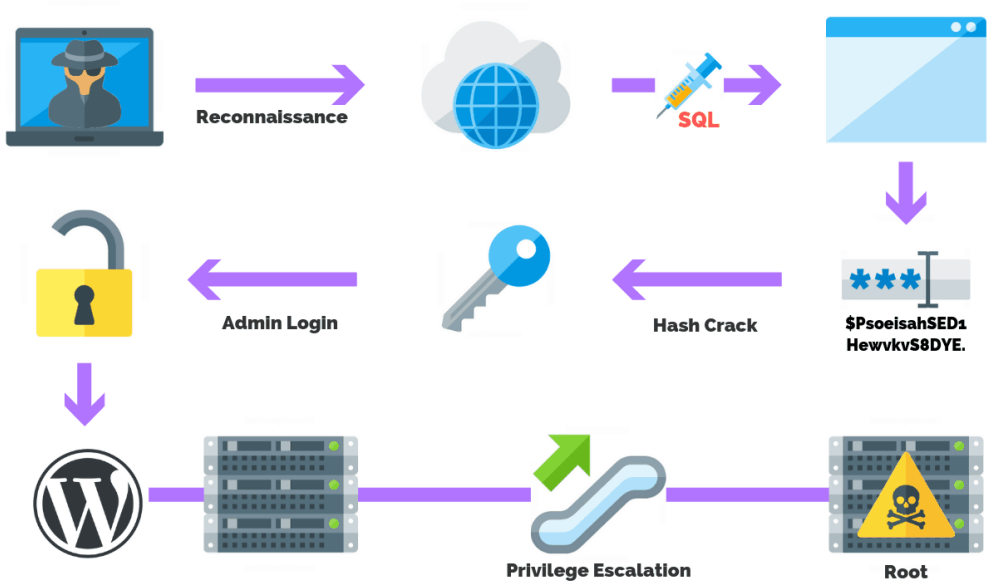
O escalonamento de privilégios também é uma das técnicas mais comuns que os invasores usam para descobrir e exfiltrar dados valiosos e confidenciais.



Escalonamento de privilégios

Para um hacker, o escalonamento de privilégios é a arte de aumentar os privilégios desde o acesso inicial, normalmente um usuário padrão ou conta de aplicativo, até o administrador, root ou até mesmo o acesso total ao sistema.

Escalonamento de privilégios



Prática

Vamos praticar o escalonamento de privilégios em uma VM com Windows.

Etapa 2

Extração de dados com Metasploit

Introdução

Nesta etapa vamos extrair informações do nossa máquina alvo.

Meterpreter

Vamos utilizar o **Meterpreter**, ferramenta disponibilizada no Framework Metasploit.

Prática

Vamos similar um ataque em nossa máquina virtual Windows.

Etapa 3

Módulos de pós exploração no Metasploit

Introdução

Nesta aula vamos explorar outros módulos do Metasploit para a extração de dados.

Tipos de módulos

- Extract credentials;
- Privilege escalation modules;
- Information gathering;
- Spy / Capture

Prática

Vamos extrair dados da VM alvo com os módulos do Metasploit.

Etapa 4

Persistência de sessão com Metasploit

Introdução

Nesta aula vamos aprender a manter uma conexão com a máquina alvo, mesmo após a reinicialização.

Persistência de sessão

O Metasploit tem um script chamado *persistence* que pode nos permitir configurar um Meterpreter (ouvinte) persistente no sistema da vítima.

Módulos de persistência

Vamos utilizar os módulos de persistência do Metasploit e Meterpreter.

Prática

Vamos iniciar e manter uma sessão em uma VM alvo.

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

SCAN ME