

Man in the middle

Cassiano Peres

DIO Tech Education Analyst

 cassiano-dio

 peres-cassiano

Objetivo Geral

Neste curso vamos falar de ataques do tipo *Man in the middle*, onde o atacante se posiciona entre as partes envolvidas na conexão, capturando e manipulando informações.

Pré-requisitos

Conhecimento prévio do conteúdo visto até aqui.

Percurso

Etapa 1

O que é um ataque do tipo *Man in the Middle*?

Etapa 2

Capturando tráfego da rede

Etapa 3

Manipulando a rede

Etapa 1

O que é um ataque do tipo
Man in the Middle?

Introdução

Um ataque *Man in the Middle* é um tipo de ataque de espionagem, em que os invasores interrompem uma conversa ou transferência de dados existente.

Man in the Middle

Depois de se inserirem no “meio” da transferência, os atacantes fingem ser ambos participantes legítimos.

Man in the Middle

- Interceptação de informações e dados;
- Envio de links maliciosos ou outras informações;
- Camuflado.

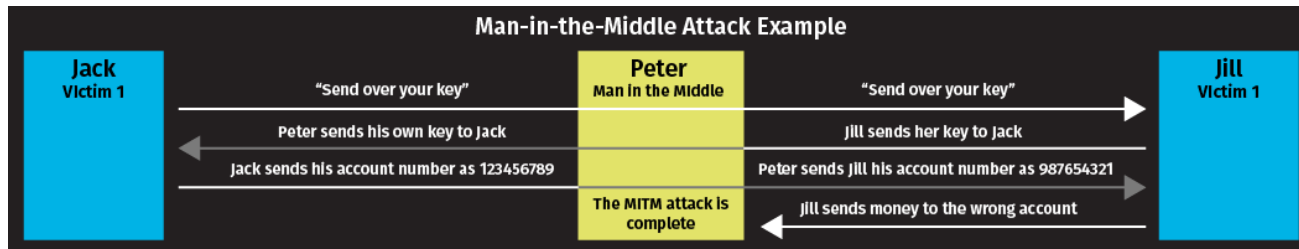
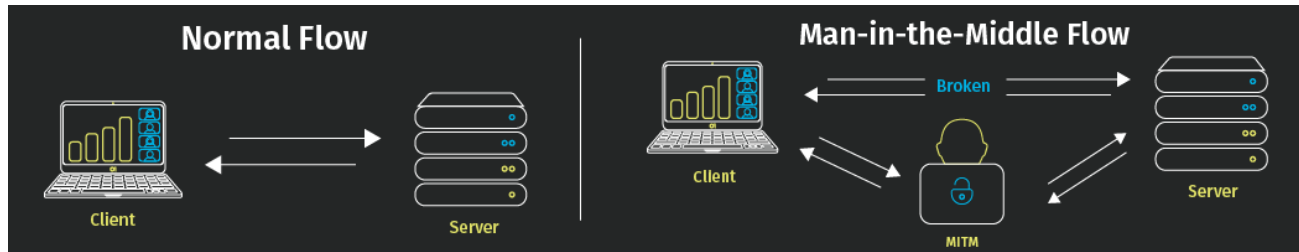
Conceitos chaves

- Tipo de sequestro de sessão;
- Invasores se inserem como **retransmissores** ou **proxies** em uma conexão;
- Exploração em tempo real do tráfego;

Exemplos de ataques

- Intercepção de dados;
- Acesso de senhas e roubo de fundos.

Exemplos de ataques



Ferramentas

- WireShark.
- Ettercap.
- Cain e Abel.
- Bettercap.
- Máquinas virtuais.

Conclusão

Man in the middle é um dos tipos de ataques mais críticos, dado o seu alto potencial de danos.

Etapa 2

Capturando dados da rede

Introdução

Nesta etapa vamos utilizar o Wireshark para capturar dados de uma sessão.

Wireshark

O Wireshark é um analisador de protocolo de rede ou um aplicativo que captura pacotes de uma conexão de rede.

Pacote é o nome dado a uma unidade discreta de dados em uma rede Ethernet típica.



Wireshark

Open-source software



Captures packets



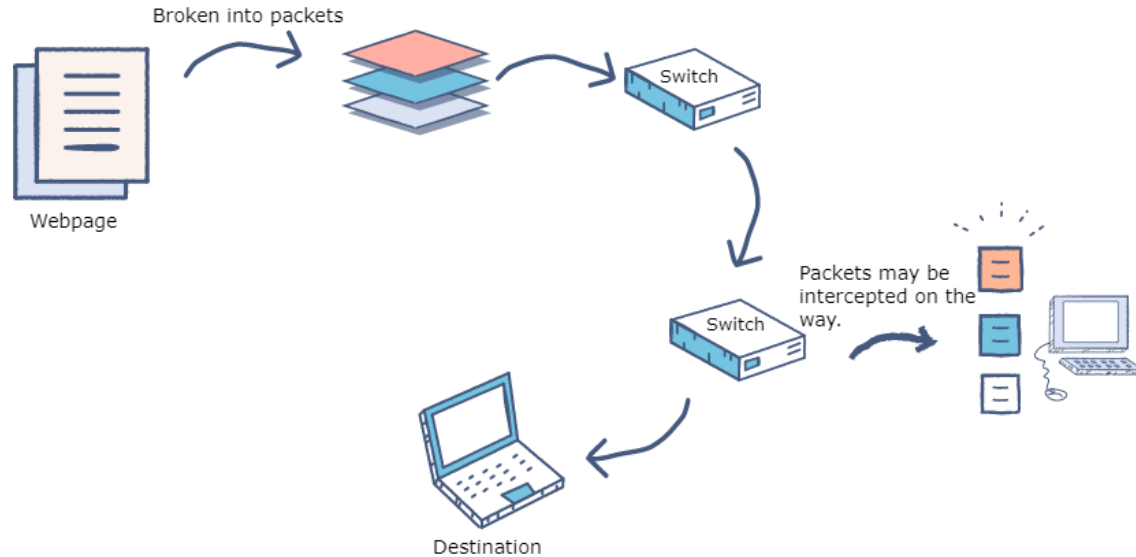
Reveals packet contents

Request in:	
Time:	
Flags:	
Queries:	

Wireshark

O Wireshark é um sniffer de rede, ou seja, é uma aplicação que lê pacotes de dados que atravessam a rede dentro da camada TCP/IP (Transmission Control Protocol/Internet Protocol)

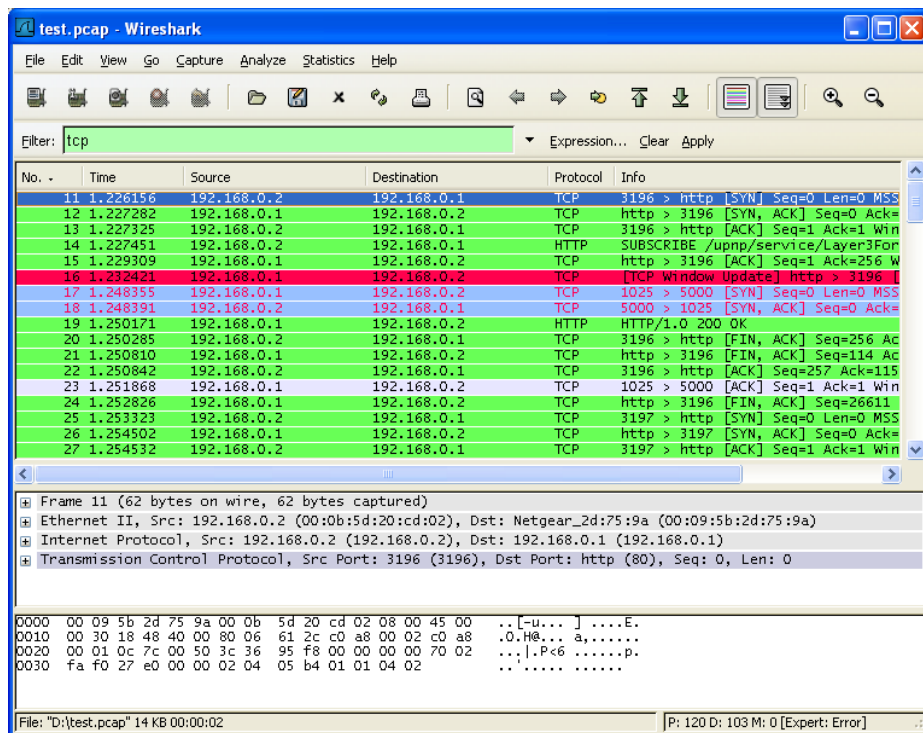
Wireshark



Wireshark

- Captura de pacotes: o Wireshark ouve uma conexão de rede em tempo real e captura fluxos inteiros de tráfego;
- Filtragem: O Wireshark é capaz de fatiar e filtrar os dados usando filtros;
- Visualização: Permite a visualização do conteúdo dos pacotes capturados.

Wireshark



Prática

Vamos utilizar o Wireshark para simular a captura de pacotes em nossa rede.

Etapa 3

Manipulando a rede

Introdução

Vamos continuar explorando ataques do tipo *Man in the Middle*, agora utilizando recursos da ferramenta Ettercap.

Ettercap

Ettercap é um conjunto abrangente para ataques Man in the Middle.



Ettercap

Possui sniffing de conexões ao vivo, filtragem de conteúdo em tempo real e muitos outros recursos.

Suporta dissecção ativa e passiva de muitos protocolos e inclui muitos recursos para análise de rede e host.

Modos de operação

- **Baseado em IP:** os pacotes são filtrados com base na origem e destino IP;
- **MAC:** os pacotes são filtrados com base no endereço MAC, útil para sniffing conexões através de um gateway;

Modos de operação

- **ARP:** utiliza o envenenamento ARP para sniffar em uma LAN entre dois hosts (full-duplex).
- **PublicARP:** usa o envenenamento ARP para sniffar em uma LAN de um host vítima para todos os outros (half-duplex).

Prática

Vamos utilizar o Ettercap para realizar operações do tipo Man in the Middle.

Dúvidas?

- > Fórum/Artigos
- > Comunidade Online (Discord)

