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.

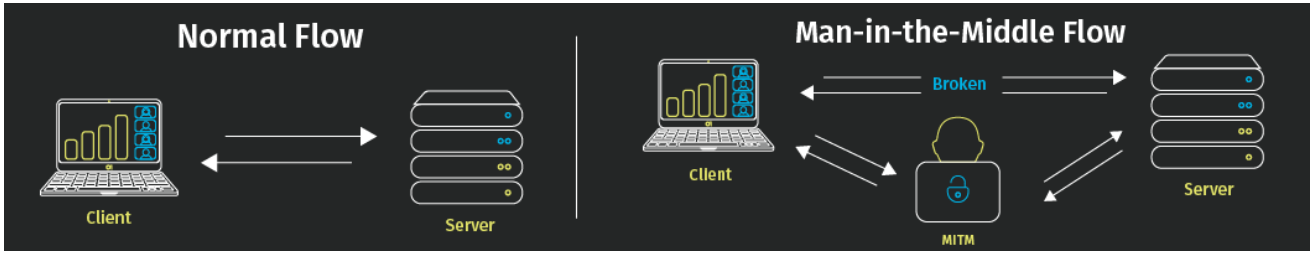
Conceitos chaves

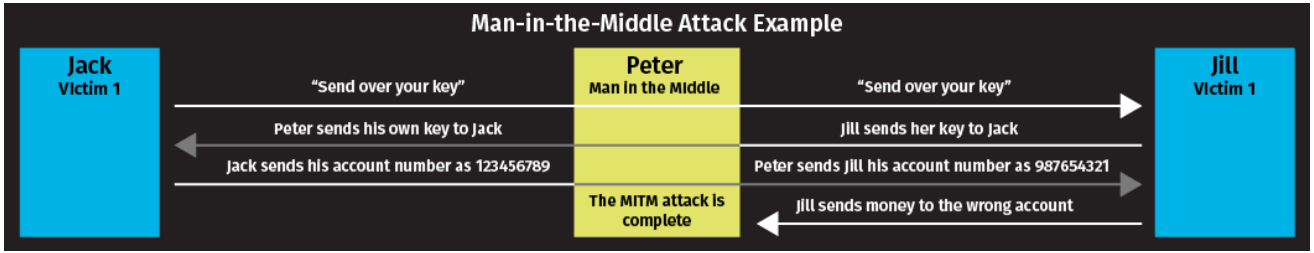
- Tipo de sequestro de sessão;
- Invasores se inserem como **retransmissores** ou **proxies** em uma conexão;
- Exploração em tempo real do tráfego;

Exemplos de ataques

- Interceptação 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

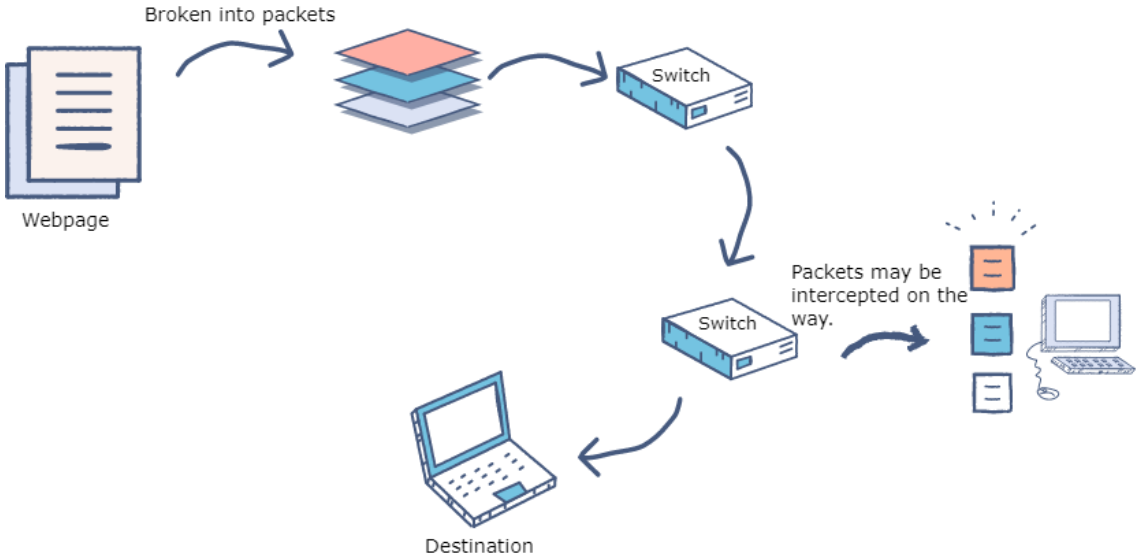
Reveals packet contents

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)

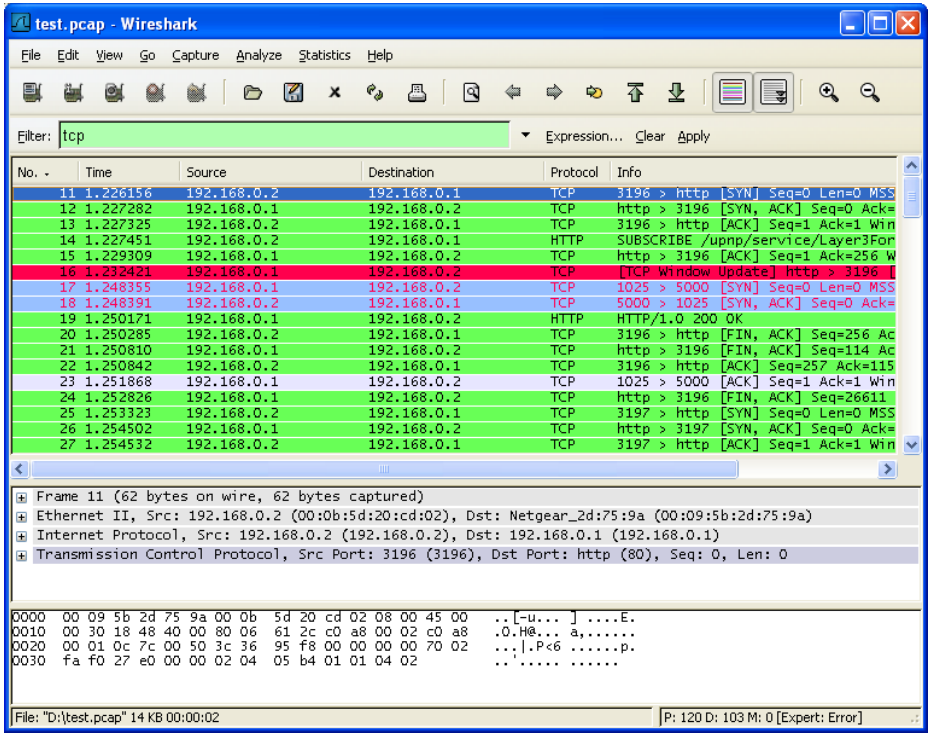
Wireshark


Broken into packets
Webpage
Switch
Switch
Packets may be intercepted on the way.
Destination

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


test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: tcp
Expression... Clear Apply
No. Time Source Destination Protocol Info
11 1.226156 192.168.0.2 192.168.0.1 TCP 3196 > http [SYN] Seq=0 Len=0 MSS
12 1.227282 192.168.0.1 192.168.0.2 TCP http > 3196 [SYN, ACK] Seq=0 Ack=
13 1.227325 192.168.0.2 192.168.0.1 TCP 3196 > http [ACK] Seq=1 Ack=1 Win
14 1.227451 192.168.0.2 192.168.0.1 HTTP SUBSCRIBE /upnp/service/Layer3For
15 1.229309 192.168.0.1 192.168.0.2 TCP http > 3196 [ACK] Seq=1 Ack=256 W
16 1.232421 192.168.0.1 192.168.0.2 TCP [TCP Window Update] http > 3196 [
17 1.248355 192.168.0.1 192.168.0.2 TCP 1025 > 5000 [SYN] Seq=0 Len=0 MSS
18 1.248391 192.168.0.2 192.168.0.1 TCP 5000 > 1025 [SYN, ACK] Seq=0 Ack=
19 1.250171 192.168.0.1 192.168.0.2 HTTP HTTP/1.0 200 OK
20 1.250285 192.168.0.2 192.168.0.1 TCP 3196 > http [FIN, ACK] Seq=256 Ac
21 1.250810 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=114 Ac
22 1.250842 192.168.0.2 192.168.0.1 TCP 3196 > http [ACK] Seq=257 Ack=115
23 1.251868 192.168.0.1 192.168.0.2 TCP 1025 > 5000 [ACK] Seq=1 Ack=1 Win
24 1.252826 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=26611
25 1.253323 192.168.0.2 192.168.0.1 TCP 3197 > http [SYN] Seq=0 Len=0 MSS
26 1.254502 192.168.0.1 192.168.0.2 TCP http > 3197 [SYN, ACK] Seq=0 Ack=
27 1.254532 192.168.0.2 192.168.0.1 TCP 3197 > http [ACK] Seq=1 Ack=1 Win
Frame 11 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[-u...] ....E.
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@... a,......
0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 ...|.P<6 ......p.
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 ..'..... ......
File: "D:\test.pcap" 14 KB 00:00:02
P: 120 D: 103 M: 0 [Expert: Error]

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)