RELATÓRIO MAN IN THE MIDDLE

Objetivo:

O objetivo ético de um ataque Man in the Middle (MITM) em uma rede WPA2 é avaliar a segurança das comunicações internas, verificando se os dados transmitidos entre dispositivos estão adequadamente protegidos contra interceptação. Esse tipo de teste permite identificar se há falhas na criptografia, autenticação ou configuração que possam expor informações sensíveis a invasores. O foco é garantir que os dados trocados dentro da rede estejam resguardados contra espionagem ou manipulação, propondo soluções que reforcem a integridade e confidencialidade das comunicações.

OBS: *ESTE ATAQUE É APENAS PARA UM ENTENDIMENTO SUPERFICIAL DO FUNCIONAMENTO DO MITM, POIS ENVOLVE APENAS A ANÁLISE DE PACOTES, NÃO ENVOLVENDO A MANIPULAÇÃO E REDIRECIONAMENTO DE PACOTES A TERCEIROS.*

Autor: *Enzo Arrue Juan Fuso*
Faculdade: *Fatec São Caetano do Sul*
Curso: *Segurança da Informação*

Introdução

O ataque "Man in the Middle" (MITM) é uma técnica em que o invasor intercepta e potencialmente modifica as comunicações entre duas partes, sem que elas percebam. No contexto de uma rede WPA2, esse tipo de ataque tem como objetivo avaliar se as informações trocadas entre cliente e servidor estão protegidas contra interceptação. A análise desse tipo de vulnerabilidade permite identificar falhas de criptografia ou de configuração que possam comprometer a segurança dos dados em trânsito.

Este relatório detalha as etapas de um teste ético em uma LAN controlada, utilizando máquinas virtuais (VMs) configuradas para expor as fragilidades da comunicação, e propõe soluções para reforçar a integridade e confidencialidade das comunicações.

Softwares/Ferramentas Utilizadas:

VirtualBox (Servidor A e Servidor B), Wireshark (Captura de pacotes), Python (cliente/servidor)

Metodologia

Primeiro configurar as VMs colocando “rede interna” em todas

Configurar IP de cada VM para Rede Interna **(cliente, servidor e atacante)** IPv6 em IPv4.

Comandos se usarmos “Rede Interna”:
ip addr (verifica o estado do ip)
sudo ip addr flush dev enp0s3
sudo ip addr add <IP do cliente/servidor/atacante>/24 dev enp0s3
sudo ip link set dev enp0s3
ip addr show

(exemplos de IPs)
192.168.1.10/24 - cliente

192.168.1.20/24 - servidor
192.168.1.30/24 - atacante

Após isso, utilizar o comando ping das outras VMs, testar a conectividade e analisar se estão na mesma rede interna; por exemplo: Na **VmAtacante** -> ping 192.168.1.20 // ping 192.168.1.30

Em seguida, pegar o código python **cliente.py e servidor.py**

Realizar primeiro para o servidor:
1- sudo apt install python3
2- sudo nano server.py
3- copiar e colar o código abaixo

```
import socket

HOST = "IP_SERVIDOR"
PORT = 50000  #Recomendado usar portas acima da 1023 (portas não privilegiadas)

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.bind((HOST, PORT))
    s.listen()
    conn, addr = s.accept()
    with conn:
        print(f"Connected by {addr}")
        while True:
            data = conn.recv(1024)
            if not data:
                break
            conn.sendall(data)
```

Realizar em seguida na máquina cliente:
1- sudo apt install python3
2- sudo nano cliente.py
3- copiar e colar o código abaixo

```
import socket

HOST = "IP_SERVIDOR"
PORT = 50000  # Usa a mesma porta

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.connect((HOST, PORT))
```

```
    s.sendall(b"Hello, world")
    data = s.recv(1024)

print(f"Received {data!r}")
```

Ambos scripts devem ter a mesma Porta (qualquer uma acima de 1023) e **ambos** scripts devem conter o IP do servidor; como exemplo: 192.168.1.20 (servidor)

Após isso, ir exatamente no diretório dos arquivos **.py** e executar **PRIMEIRO** o código do servidor e depois o .**py** do cliente no terminal do Ubuntu.

Exemplo: **python3 <Nome_do_arquivo>.py** para executar

Se tudo tiver dado certo deverá aparecer no servidor uma mensagem como **“Escutando <IP do cliente>” “Recebido” “<Mensagem recebida>”** e no cliente **“<A mensagem enviada>”**

Assim que for verificado que o cliente e servidor estão se comunicando corretamente,
ir para a **VMAtacante** e seguir os seguintes passos:

1. ping **<IP servidor>** e ping **<IP cliente>**
2. sudo Wireshark (se já estiver instalado na VM)
3. Abrir o Wireshark e esperar uma lista de tráfego abrir
4. Entrar na “**enp0s3**” (se tiver com uma miniatura de gráfico)

Agora, **REFAZER** a ação de executar o código python no servidor e depois no cliente, enquanto o Wireshark analisa o tráfego.

Vai se abrir diversos protocolos de transmissão de dados no Wireshark, usar o filtro para ir direto ao ponto usando algo como: **“tcp.port”, “port 50000”**

Depois, clicar em cada linha do filtro para ver se encontra o **“data” (carga útil, a informação enviada decodificada)**

Assim que encontrado o data no quadrante esquerdo abaixo dos protocolos, clicar com botão direito em cima do data e ir em “**Follow**” e depois “**TCP**” e aparecerá a informação de forma clara e direta.

OBS: O atacante pode escolher se prefere habilitar/desabilitar o redirecionamento de pacotes, 1 para habilitado e 0 para desabilitado.
“echo 1 > /proc/sys/net/ipv4/ip_forward”

OBS: No Wireshark quando analisamos um pacote e clicamos nele, os primeiros 6 conjuntos de dígitos são destinados a Origem, os próximos 6 conjuntos de dígitos

para o Destino e o os 2 conjuntos de dígitos seguintes informa o tipo do conteúdo **(IPv4 ou IPv6).**

Recomendações

Criptografia de Dados: *Implementar protocolos de criptografia mais robustos, como TLS, para garantir a confidencialidade das informações trocadas entre cliente e servidor.*

Autenticação Forte: *Implementar mecanismos de autenticação robusta entre as máquinas da rede interna, garantindo que apenas dispositivos confiáveis tenham permissão para comunicar.*

Monitoramento de Tráfego: *Monitorar o tráfego de rede em busca de comportamentos anômalos e detectar rapidamente tentativas de ataques do tipo MITM.*

Links Complementares:

Wireshark Documentation (Captura e Análise de Pacotes) - https://www.wireshark.org/docs/

Python Socket Programming (Documentação Oficial) - https://docs.python.org/3/library/socket.html

Configuração de Redes no VirtualBox - https://www.virtualbox.org/manual/ch06.html

Man in the Middle Attack Aircrack-ng - https://www.aircrack-ng.org/doku.php?id=man_in_the_middle