MAN IN THE MIDDLE

LUCAS GUIMARÃES MENDES

CYBER CORVUS
UFU

INTRODUÇÃO

- Obtenção de informações
  - Dados bancários
  - Logins e senhas de e-mails
  - Dados sensíveis de usuários ou empresas
- Este ataque explora vulnerabilidades como:
  - Redes abertas ou sem devida proteção
  - Utilização de protocolos de comunicação sem camada de segurança
  - Pacote de dados sem criptografia

DEFINIÇÃO

- **Formalmente:**

  Ataques Man In The Middle (MITM) permitem que cibercriminosos interceptem, enviem e recebam dados que chegam e saem do seu dispositivo sem serem detectados até que a transação esteja completa

- **Informalmente:**

  Um ataque MITM é um nome genérico para qualquer ataque virtual em que alguém fica entre você e o que você está fazendo: entre você e sua transação bancária online por exemplo

SIGLAS IMPORTANTES

- IP – Internet Protocol
- ARP - Address Resolution Protocol
- DNS – Domain Name System
- MAC - Media Access Control
- HTTP - Hypertext Transfer Protocol
- HTTPS - Hyper Text Transfer Protocol Secure
- SSL - Secure Sockets Layer
- CBC - Cipher Block Chaining

CONTEXTO DE UTILIZAÇÃO

- Normalmente usa-se o ataque MITM após uma tentativa frustrada de inserir vírus na máquina do usuário
- Os alvos mais comuns de ataques MITM são:
  - Sites de compras online
  - Sites de serviços bancários
  - Sites que exigem login e senha
  - Redes Wi-fi

FUNCIONAMENTO

- **Etapa 1: Interceptação**
  - Interceptar o tráfego de internet antes que ele chegue ao destino
    - IP Spoofing
    - ARP Spoofing
    - DNS Spoofing
    - Sniffer de Rede

FUNCIONAMENTO

IP Spoofing

- Os dados transmitidos pela internet são divididos em pacotes, e cada pacote possui um cabeçalho contendo informações sobre ele, incluindo os endereços IP’s de origem e destino

- O atacante falsifica o endereço IP de origem dos pacotes a serem enviados para a vítima, assim ele passa a ser uma fonte confiável para estabelecer a comunicação com o usuário ou servidor

- Também é usado para ataques Ddos
  - Tem por objetivo sobrecarregar os servidores com pacotes de dados

FUNCIONAMENTO

ARP Spoofing

- Também chamado de envenenamento de cache ARP
- Geralmente utilizados em redes locais
- Quando um pacote é enviado de um host para outro, o endereço MAC deve ser indicado no cabeçalho, que é um identificador fixo e exclusivo atribuído a cada placa de rede
- Para que o pacote seja aceito é verificado se o MAC especificado faz referência ao endereço IP do destinatário
- O ataque tem como objetivo associar o MAC do atacante ao endereço IP de um host de destino

FUNCIONAMENTO

DNS Spoofing

- Também chamado de envenenamento de cache DNS
- Os servidores DNS permitem estabelecer nomes para os endereços IP. Desta forma, não é necessário que o usuário precise lembrar dos endereços IP de cada site que pretende visitar
- O ataque consiste em alterar os endereços IP dos servidores DNS da vítima para apontar para servidores maliciosos criados pelo atacante

FUNCIONAMENTO

Sniffer de Rede

- Esse software é usado com frequência para monitorar e analisar o tráfego de rede para detectar problemas e manter um fluxo eficiente
- Também pode ser utilizado para obter dados não permitidos, já que todo o tráfego na rede passa por ele
- Pode ser usado para roubar dados, espionar o tráfego na rede e coletar informações do usuário

FUNCIONAMENTO

- **Etapa 2: Descriptografia**
  - Assim que os dados são capturados é necessário decifrá-los
    - Falsificação de HTTPS
    - SSL Beast
    - Sequestro de SSL
    - SSL stripping

FUNCIONAMENTO

Falsificação de HTTPS

- O hacker instala um certificado de segurança raiz falsificado para que seu navegador ache que é um certificado confiável
- Como o navegador confia nele, ele fornece a chave de criptografia necessária para decifrar os dados enviados

SSL BEAST

- BEAST - Browser Exploit Against SSL/TLS
- Aproveita os pontos fracos do Cipher Block Chaining (CBC) para explorar o protocolo Secure Sockets Layer (SSL), e assim obter os dados descriptografados

FUNCIONAMENTO

Sequestro de SSL

- Quando você se conecta a um site, seu navegador se conecta primeiro à versão HTTP (não segura) do site e depois redireciona para a versão HTTPS (segura) do site e o novo servidor seguro fornece ao seu navegador um certificado de segurança
- O ataque acontece justamente antes de você se conectar à versão segura do site, obtendo assim, dados desprotegidos

SSL stripping

- Consiste em rebaixar um site de HTTPS (seguro) para HTTP (não seguro)
- Pode-se utilizar um servidor proxy ou algumas das técnicas de falsificação (spoofing) vistas anteriormente

FERRAMENTAS

- Algumas ferramentas que podem ser utilizadas:
  - WireShark
  - Ettercap
  - Cain e Abel (Windows)
  - Bettercap
  - Máquinas Virtuais

COMO IDENTIFICAR E SE PROTEGER

IDENTIFICAÇÃO

- Algumas dicas podem indicar que você está sendo vítima de um ataque MITM:
  - Atrasos súbitos e longos no carregamento de página, sem motivo aparente.
  - URLs trocando de HTTPS para HTTP.
  - Verificar a tabela ARP.

PROTEÇÃO

- Uma forma de se proteger é utilizar VPN e um bom antivírus.
- Em casos de ataques do tipo SSL a solução é chamada de HSTS (HTTP Strict Transport Security), uma política de segurança que força navegadores e sites a se conectar por meio de conexões HTTPS, a todo custo.

BIBLIOGRAFIA

- https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462, acessado em 04 de novembro de 2019;
- https://www.avg.com/pt/signal/man-in-the-middle-attack, acessado em 04 de novembro de 2019;
- https://www.binarionet.com.br/blog/o-que-e-ip-spoofing-e-como-se-proteger-dele, acessado em 05 de novembro de 2019;

OBRIGADO!

- Lucas Guimarães Mendes
- lucasgm200@gmail.com