TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 11. Session Hijacking

Módulo 12. Evading IDS, Firewalls, and Honeypots

Módulo 13. Hacking Web Servers

Módulo 14. Hacking Web Applications

Módulo 15. SQL Injection

Conceitos de Session Hijacking:

Session Hijacking refere-se à exploração de uma sessão válida onde um atacante assume uma sessão entre dois computadores. O atacante rouba um ID de sessão válido que é utilizado para entrar no sistema e extrair os dados. TCP session hijacking significa tomar o controle de uma sessão TCP trocada entre dois computadores.

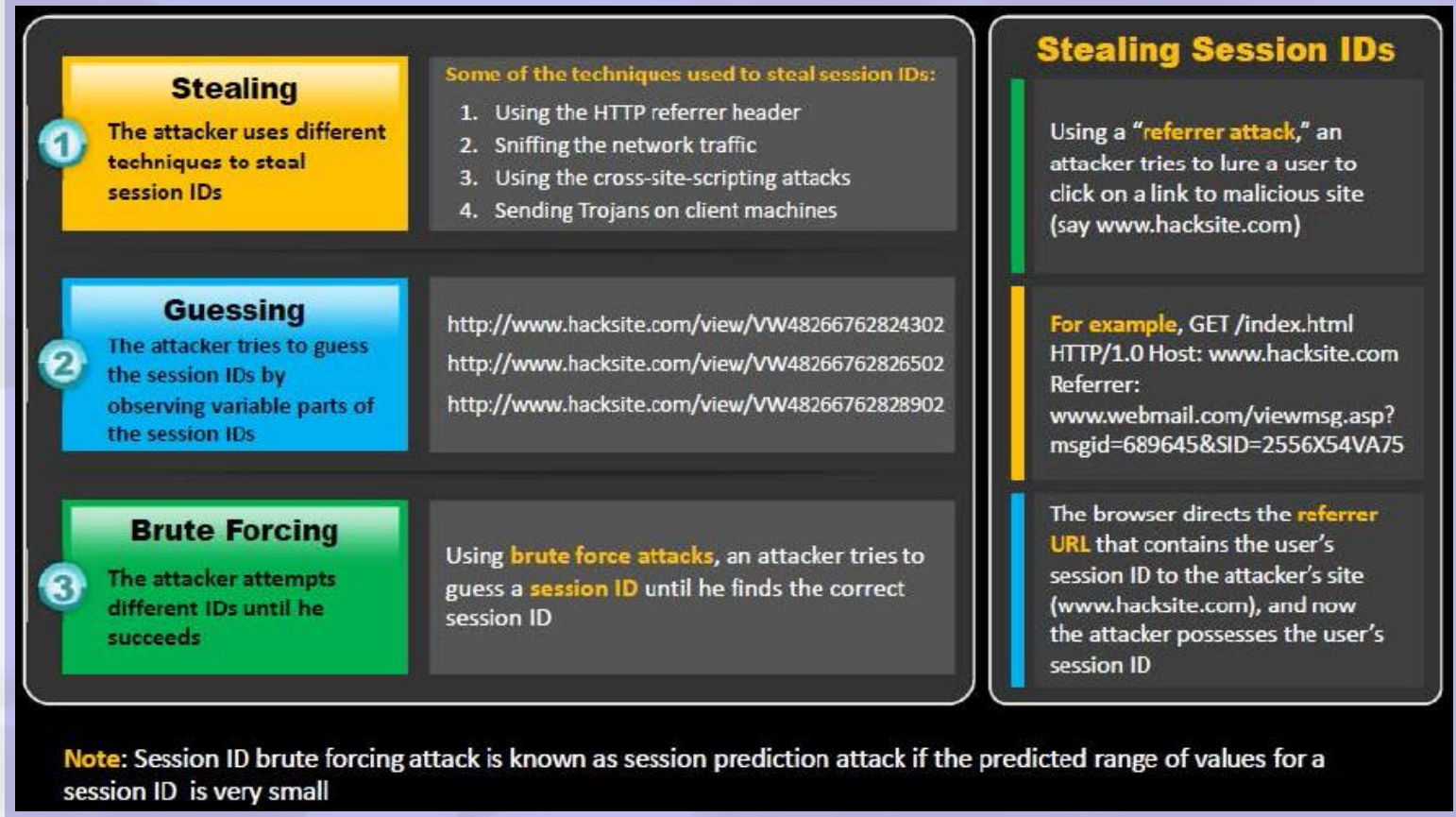
- Falta de bloqueio de conta para ID's de sessão inválidos
- Algoritmo de geração de ID de sessão fraco ou ID'S de sessão pequena
- Tratamento inseguro de IDs de sessão
- Tempo de expiração de sessão indefinido
- A maioria dos computadores que utilizam TCP/IP são vulneráveis
- A maioria das contramedidas não funcionam a menos que você utilize criptografia

CEHv12 (ANSI)

11.Session Hijacking

Session Hijacking

1. Roubando: O atacante utiliza técnicas diferentes para roubar ID's de sessão
2. Adivinhação: O atacante tenta adivinhar as ID's de sessão observando partes das ID's de sessão.
3. Força Bruta: O atacante tenta diferentes ID's de sessão até ter sucesso.



O **ataque de força bruta em ID's de sessão** é conhecido como **ataque de previsão de sessão** se o intervalo previsto de valores para um ID de sessão for muito pequeno.

Session Hijacking

Ataque de spoofing

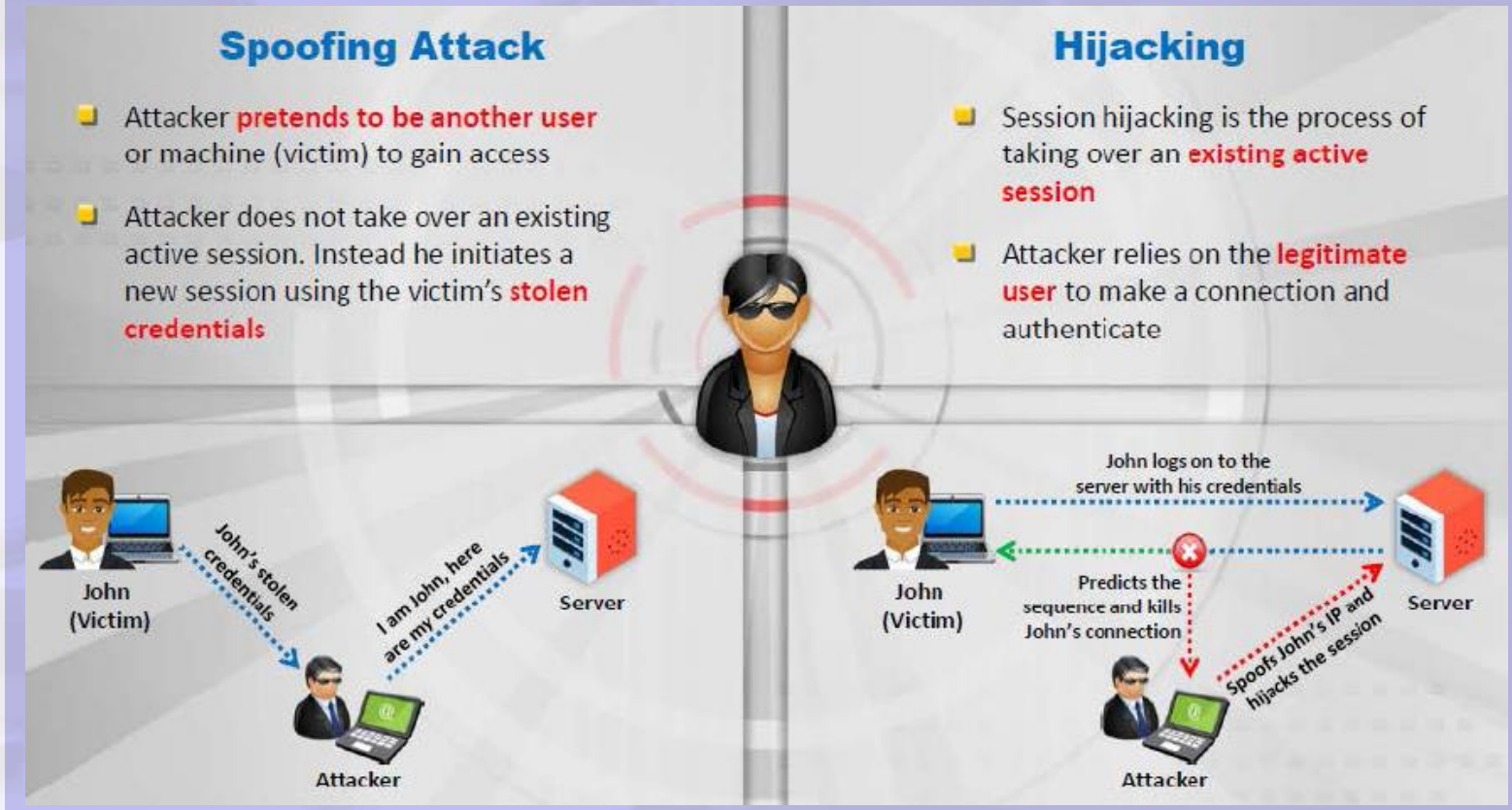
O atacante finge ser outro usuário ou máquina (vítima) para obter acesso.

O atacante não assume uma sessão ativa existente. Em vez disso ele inicia uma nova sessão utilizando as credenciais roubadas da vítima.

Hijacking/Sequestro

o sequestro de sessão é o processo de assumir uma sessão ativa existente.

O invasor depende do usuário legítimo para fazer uma conexão e autenticação.



Processo de Session Hijacking

- **Command Injection/ Injeção de C+omando**

Injetar pacotes no servidor de destino/alvo.

- **Previsão de ID de sessão**

Assumir a sessão.

- **Dessincronização de sessão**

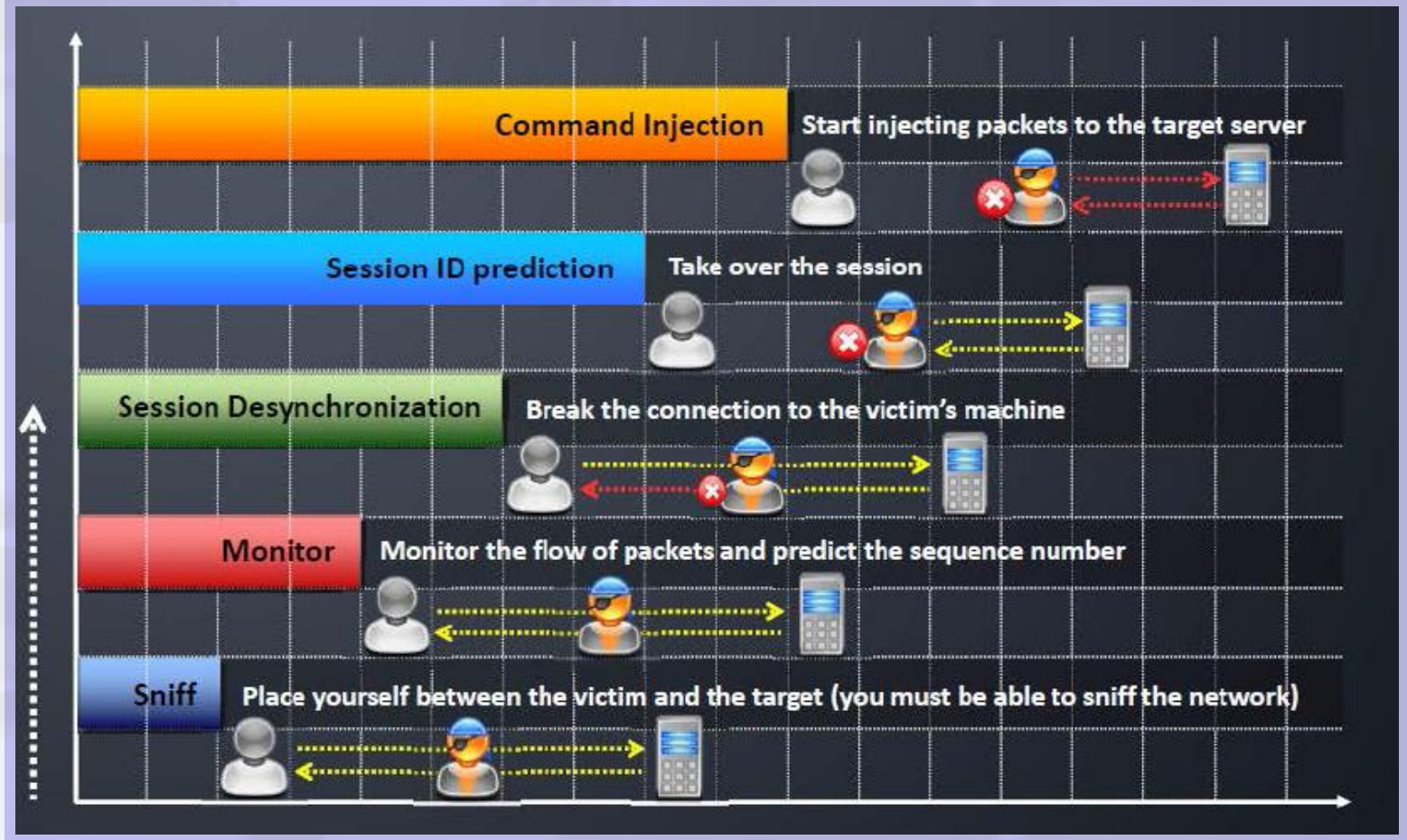
Interromper a conexão com a sessão da vítima.

- **Monitor**

Monitorar o fluxo de pacotes e prever o número de sequência.

- **Sniff**

Colocar-se entre a vítima e o alvo (precisa estar hábil em realizar o sniff na rede).



Tipos de Session Hijacking

- Session Hijacking pode ser ativo ou passivo, dependendo do grau de envolvimento do atacante. A diferença essencial entre um hijack ativo e passivo é que, enquanto um hijack ativo assume uma sessão existente, um sequestro passiva monitora uma sessão em curso.

Ataque passivo

Utiliza sniffers na rede, permitindo que atacantes obtenham informações como IDs de usuário e senhas. O atacante mais tarde pode utilizar esta informação para fazer logon como um usuário válido e assumir privilégios. Password sniffing é o ataque mais simples que pode ser realizado quando se obtém acesso a uma rede.

Ataque ativo

É o ataque MITM. Para que este tipo de ataque tenha sucesso, o número de sequência deve ser adivinhado antes de o alvo responder ao servidor. Atualmente, a previsão de números de sequência não é mais válida para realizar um ataque bem sucedido porque os fornecedores do sistema operacional utilizam valores aleatórios para o número de sequência inicial.

Session Hijacking no modelo OSI

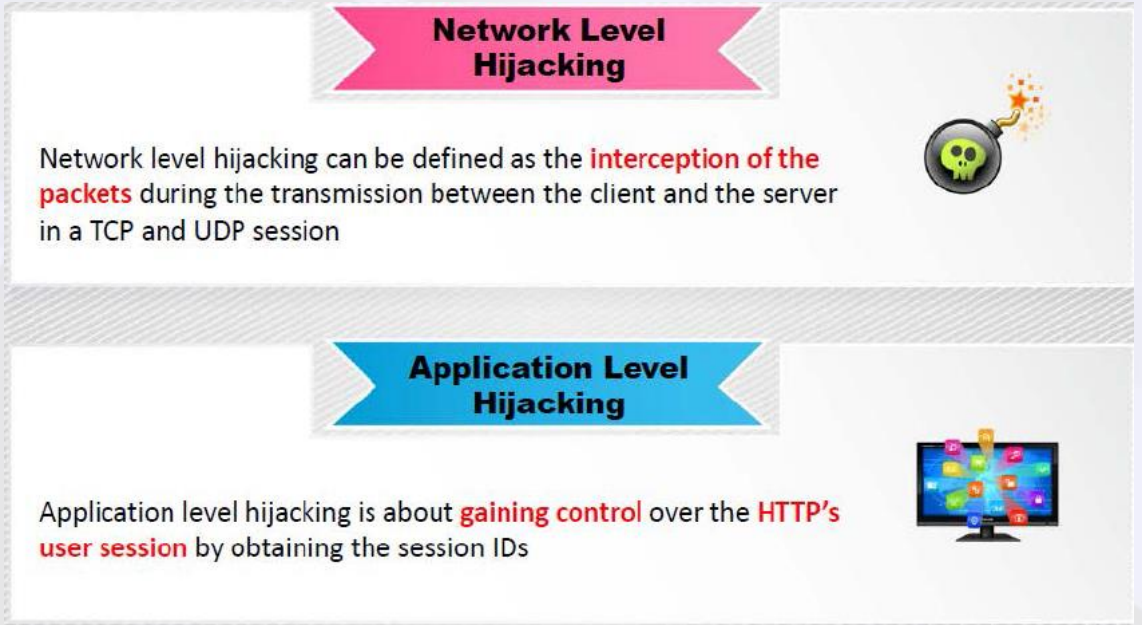
Session Hijacking ao nível de aplicação

Sessões HTTP podem ser sequestradas por obtenção das respectivas IDs de sessão. Várias maneiras em que o sequestro de sessão no nível de aplicação pode ser realizado para comprometer o token de sessão:

- Token de sessão previsível
- Man-in-the-middle
- Ataques do lado do cliente (XSS, trojans, etc.)
- Man-in-the-browser
- Session sniffing

Session Hijacking ao nível de rede

Inicialmente o atacante fareja o tráfego HTTP entre a vítima e o servidor web e analisa os dados capturados e determina a identificação da sessão. Em seguida, o atacante falsifica a si mesmo como a vítima e envia o ID da sessão para o servidor web antes da vítima. Assim, um atacante tem o controle sobre uma sessão existente.

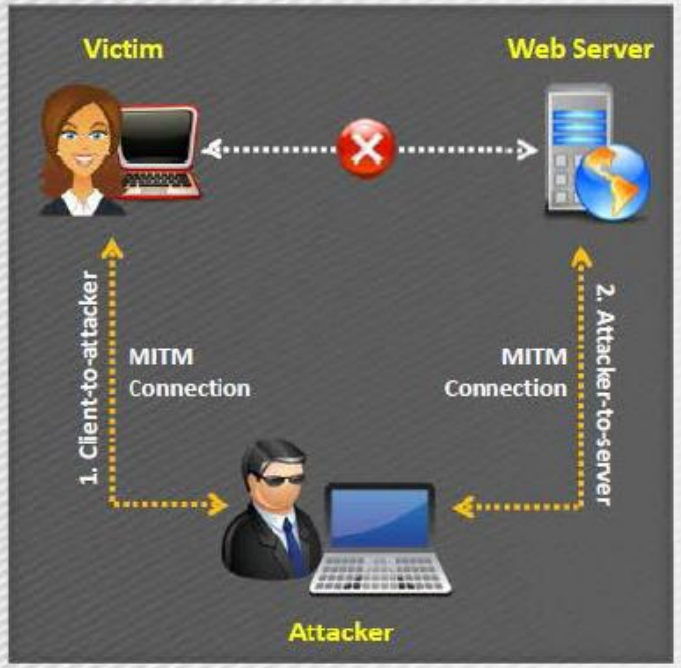


Tokens de Sessão Previsíveis

Ataque de Man-in-the-Middle

O ataque man-in-the-middle é utilizado para invadir uma conexão existente entre os sistemas e interceptar mensagens que estão sendo trocadas.

The man-in-the-middle attack is used to **intrude into an existing connection** between systems and to intercept messages being exchanged



Attackers use different techniques and **split the TCP connection** into two connections

- Client-to-attacker connection
- Attacker-to-server connection

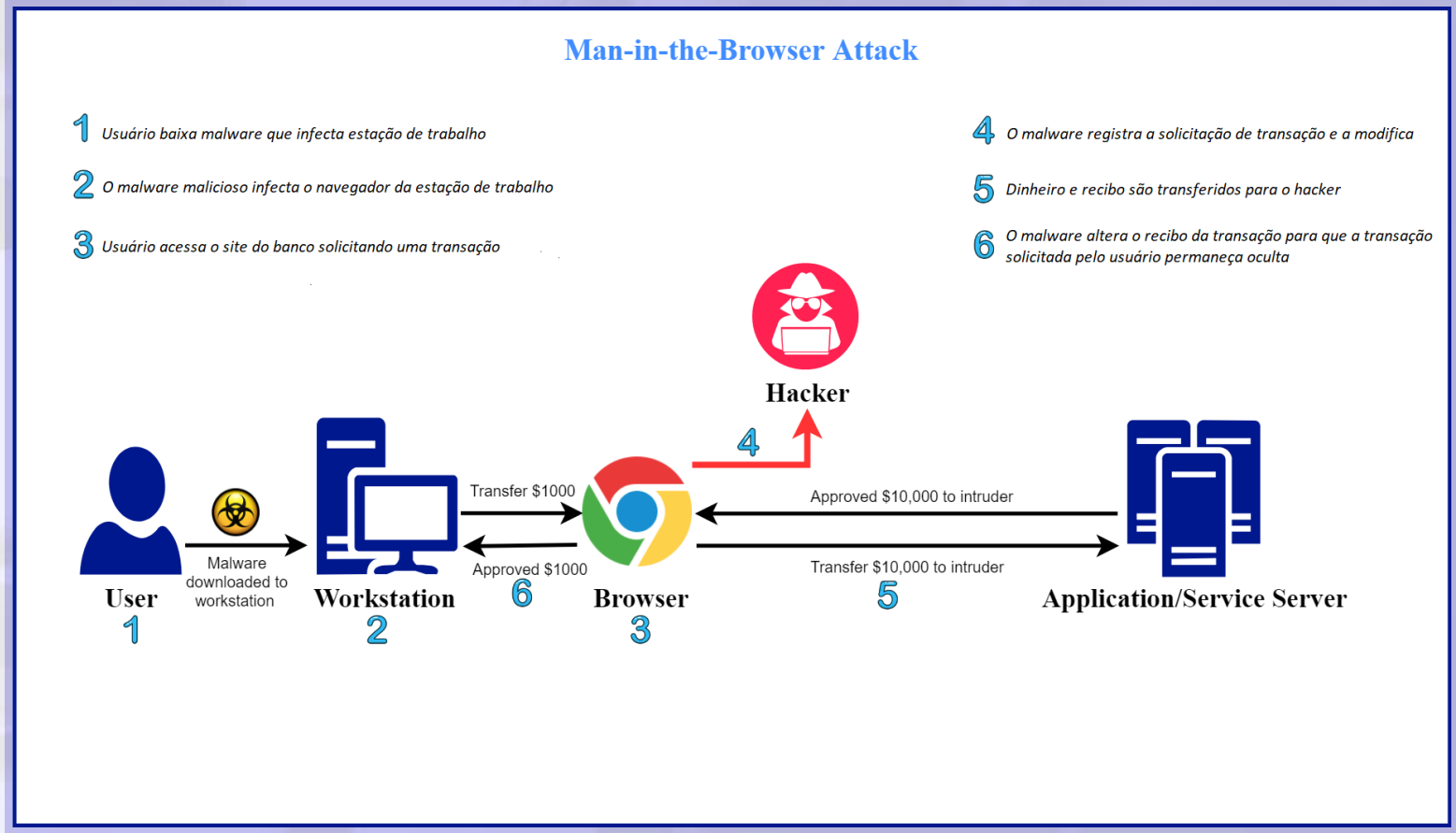
After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the **intercepted communication**

In the case of an **http transaction**, the TCP connection between the client and the server becomes the target

Ataque de Man-in-the-Browser

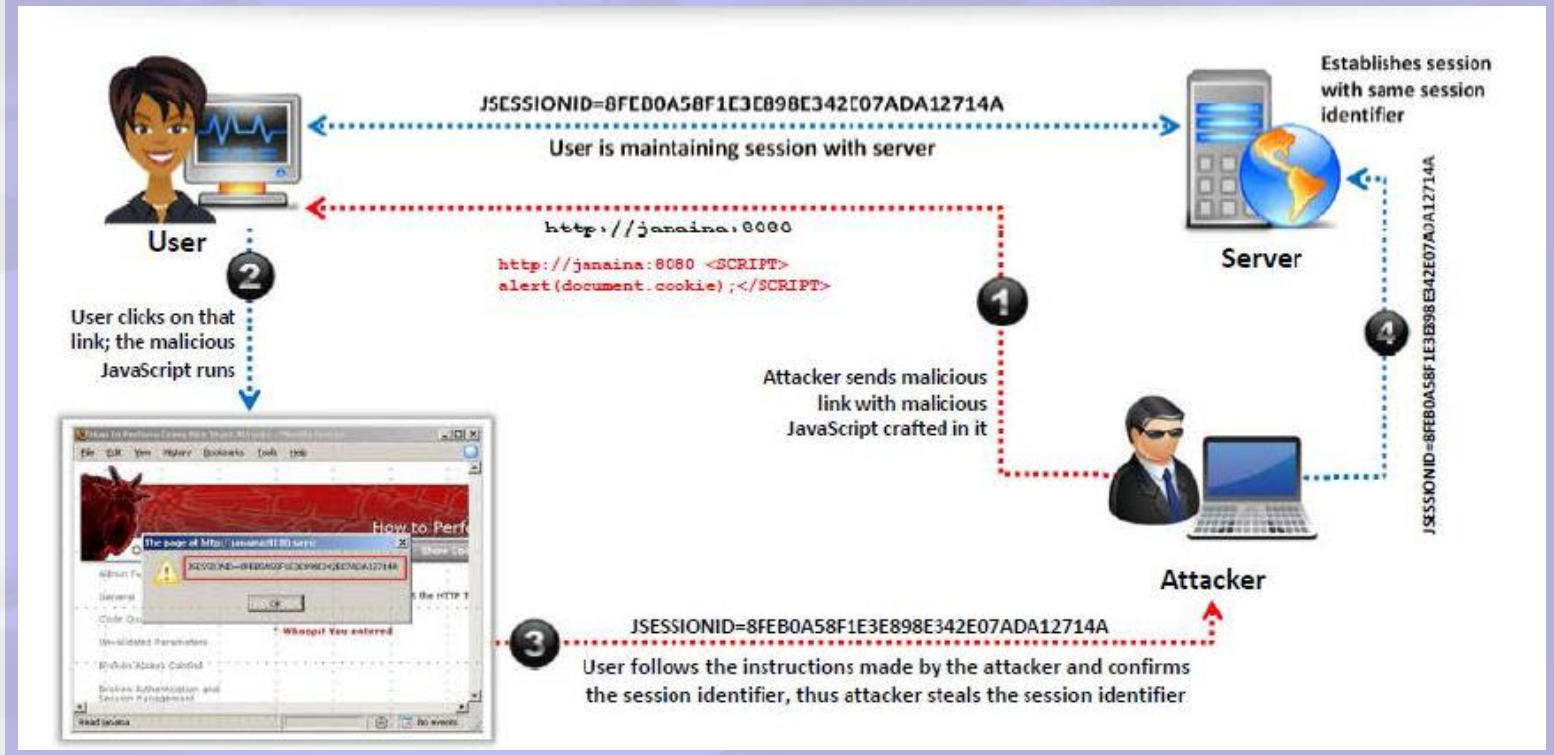
Um ataque man-in-the-browser é semelhante ao de um ataque man-in-the-middle. A diferença entre as duas técnicas é que o ataque man-in-the-browser usa um cavalo de Tróia para interceptar e manipular as chamadas entre o navegador e os seus mecanismos de segurança ou bibliotecas.

Este ataque utiliza um trojan já instalado no sistema para agir entre o navegador e os seus mecanismos de segurança. Este ataque é capaz de modificar e farejar as transações.



Ataque de Cross-site Script

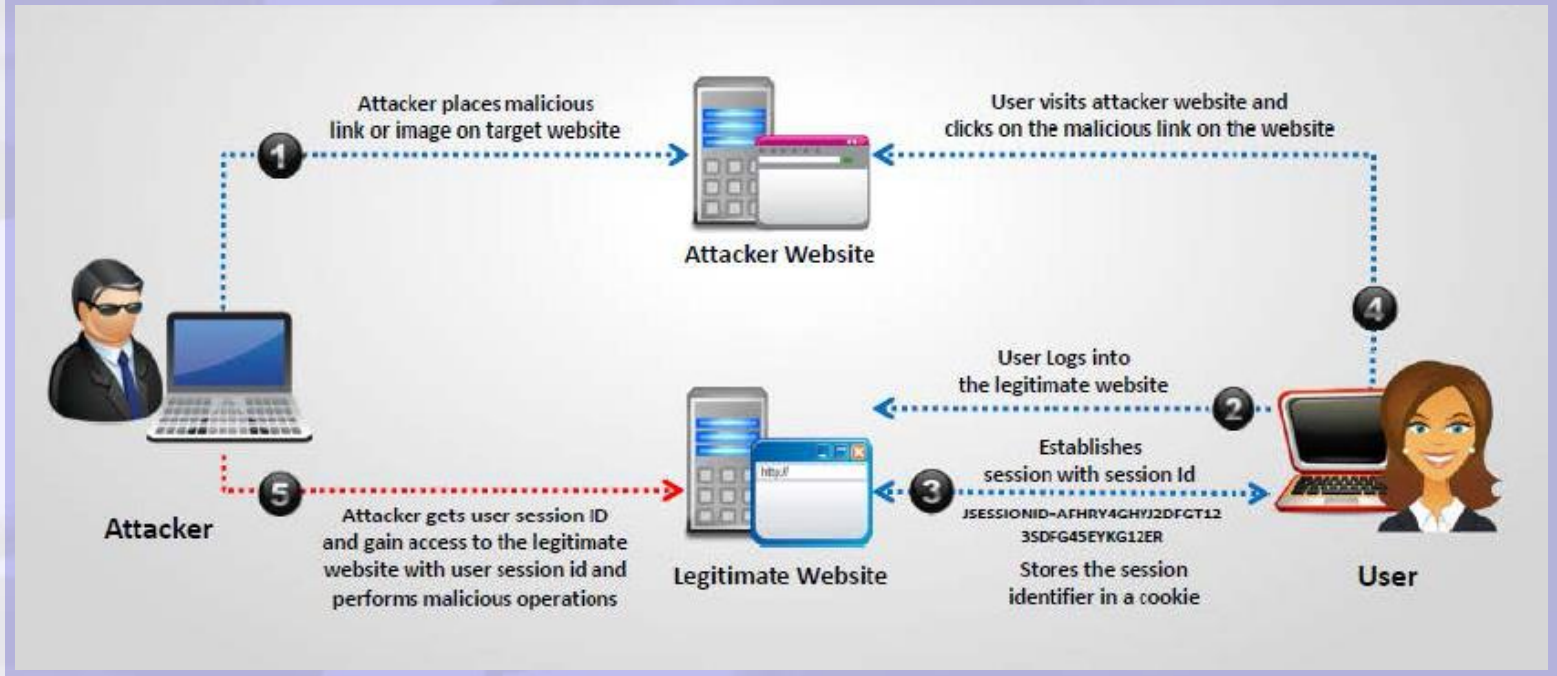
Esta vulnerabilidade geralmente é encontrada em aplicações web, onde há um âmbito de aplicação da injeção de script do lado do cliente para as páginas da web. Esta vulnerabilidade pode ser utilizada para contornar os controles de acesso. O atacante injeta o script malicioso do lado do cliente nas páginas da web e envia para a vítima para executar o ataque de cross-site script.



CSRF

Cross-Site Request Forgery (CSRF) é um ataque que força um usuário final a executar ações indesejadas em uma aplicação web em que está autenticado. Ataques CSRF visam especificamente os pedidos de mudança de estado, não o roubo de dados, uma vez que o atacante não tem nenhuma maneira de ver a resposta ao pedido forjado.

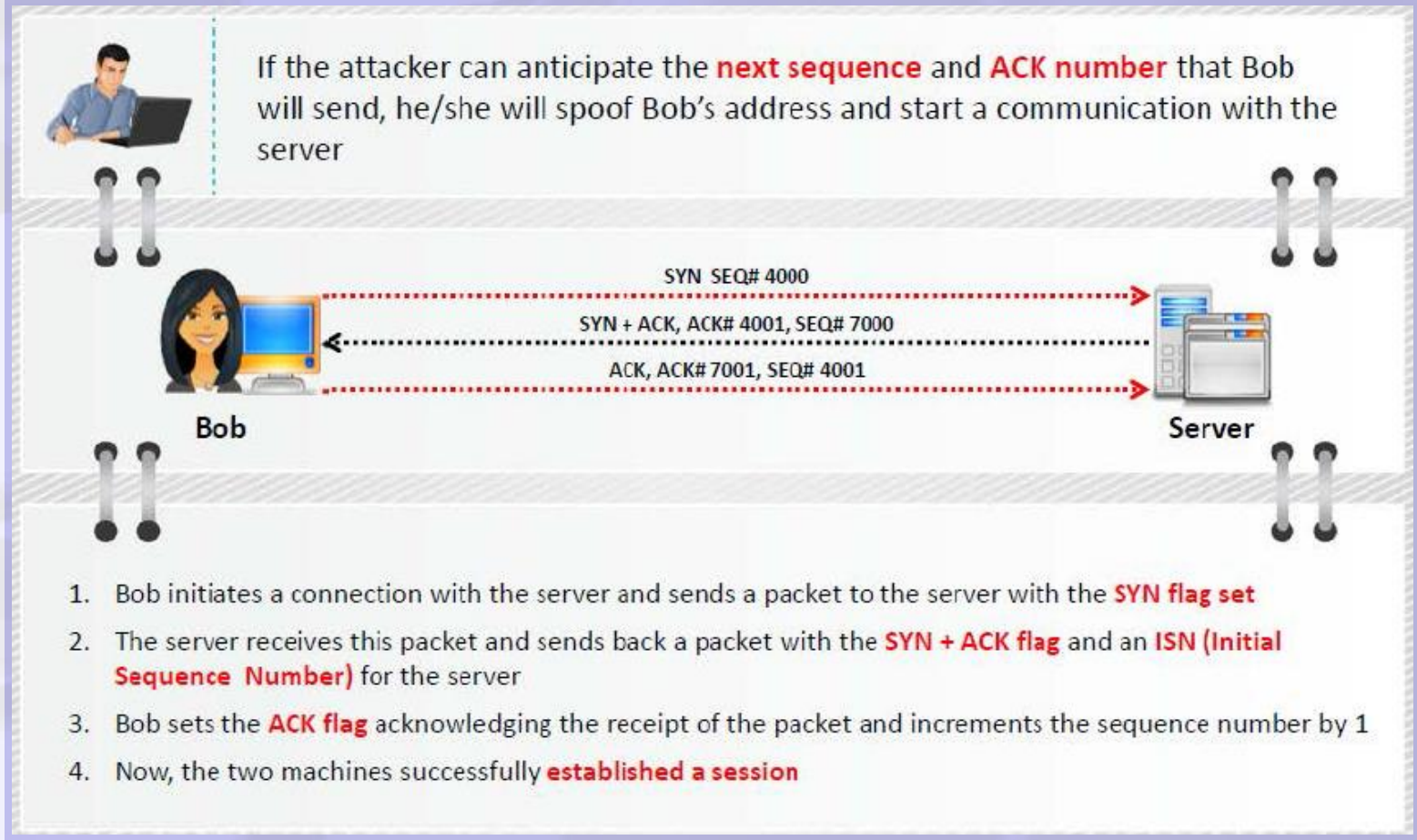
Com uma pequena ajuda da engenharia social (como o envio de um link por e-mail ou chat), um atacante pode enganar os usuários de uma aplicação web para executarem ações de escolha do atacante.



Three-way Handshake

Quando duas partes estabelecem uma conexão utilizando TCP, elas executam um aperto de mão de três vias. Um aperto de mão de três vias inicia a conexão e troca de todos os parâmetros necessários para as duas partes se comunicarem. O TCP utiliza um handshake de três vias para estabelecer uma nova conexão.

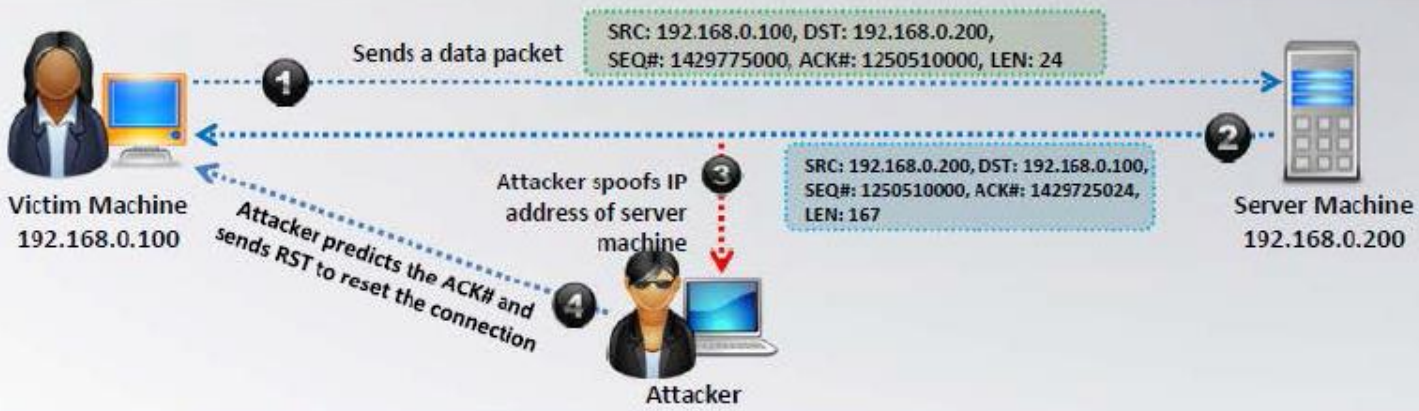
Inicialmente, a conexão no lado do cliente é no estado fechado e no lado do servidor no estado de escuta. O cliente inicia a conexão, enviando o número de sequência inicial (ISN) e definindo o flag SYN. Agora, o estado do cliente está no estado SYN-SENT.



RST Hijacking

RST hijacking é uma forma de sequestro de TCP/IP onde um pacote reset (RST) é injetado. Neste ataque, o atacante primeiro fareja a conexão entre a origem e a vítima para pegar a informação de estabelecimento da conexão tais como endereços IP da origem e da vítima, números de sequência, etc.
Agora, o atacante envia um pacote RST com um endereço de origem falso e o número de reconhecimento da conexão real e, em seguida, envia para a vítima.

- RST hijacking involves injecting an **authentic-looking reset (RST) packet** using spoofed source address and predicting the acknowledgment number
- The hacker can reset the victim's connection if it uses an **accurate acknowledgment number**
- The victim believes that the source actually sent the **reset packet** and **resets the connection**
- RST Hijacking can be carried out using a **packet crafting tool** such as Colasoft's Packet Builder and TCP/IP analysis tool such as tcpdump



Conceitos de Session Hijacking:

Session Hijacking refere-se à exploração de uma sessão válida onde um atacante assume uma sessão entre dois computadores. O atacante rouba um ID de sessão válido que é utilizado para entrar no sistema e extrair os dados. TCP session hijacking significa tomar o controle de uma sessão TCP trocada entre dois computadores.

- Falta de bloqueio de conta para ID's de sessão inválidos
- Algoritmo de geração de ID de sessão fraco ou ID'S de sessão pequena
- Tratamento inseguro de IDs de sessão
- Tempo de expiração de sessão indefinido
- A maioria dos computadores que utilizam TCP/IP são vulneráveis
- A maioria das contramedidas não funcionam a menos que você utilize criptografia

CEHv12 (ANSI)

11.Session Hijacking

zaproxy - WEB Vulnerability Scanner

- XSS
- CSRF
- Proxy
- snifer

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.