Ataques

AULA TEÓRICA 4 08/03/2023SM

Sumário

Ataques:

- Força bruta & Dicionário;
- Ataque DoS;
- Man-in-the-middle;
- Spoofing; e
- outros

Métodos de Ataques

Um dos objectivos do controlo de acesso é prevenir acessos não autorizados aos objectos, ie, ao sistema e aos dados;

Para além de controlar o acesso, a segurança procura precaver alterações e exposições não autorizadas de informação, bem como fornecer disponibilidade consistente.

Ataque

- **Ataque** é um acto que aproveita uma vulnerabilidade para comprometer um sistema controlado.
- É executado por um **agente de ameaça** que danifica ou rouba uma informação da organização ou activo físico.
- **Vunerabilidade** é uma fraqueza identificada num sistema controlado, onde não existem controlos ou estes já não tenham efeito.

Métodos de Ataques

Entidades maliciosas costumam se concentrar em violar o perímetro de um sistema de segurança para obter acesso aos dados, alterar ou destruir dados e inibir o acesso válido para dados e recursos;

Para tal, existem métodos de ataque extremamente complexos que exigem um conhecimento detalhado dos sistemas vítimas e técnicas de programação;

Por outro lado, há outros muito simples de executar que basta um endereço IP e a capacidade de manipular algumas ferramentas ou scripts.

Métodos de Ataques

Embora existam muitos tipos de ataques, eles podem ser agrupados em um conjunto de classificações ou categorias.

1. Ataques de dicionário e força bruta;
2. Ataques de negação de Serviços (DoS);
3. Malware: vírus, worms, Trojans, spyware, e muito mais;
4. Man-in-the-middle (Interceptação);
5. Sniffers;
6. Spamming;
7. Spoofing (Personificação);

Métodos de Ataques

Ataques de estágio único – **brute-force/dictionary, spoofing, malware e ataques de negação de serviço** – são os mais comuns, porque eles são os mais fáceis de montar contra um alvo e exigem apenas acesso básico à Internet;

Os outros ataques são mais complexos e envolvem uma componente de intrusão para impulsionar um ataque dentro do perímetro da rede.

Métodos de Ataques

Ataques de força-bruta

Um ataque de força-bruta é a tentativa de descobrir as palavras-chave das contas de utilizadores por sistematicamente tentar todas as possibilidades de combinações de letras, números e símbolos;

"… existem programas automatizados que conseguem fazer um ataque do tipo **wordlist** (dicionário) e/ou **força bruta**, esses programas são simples em questão de interface, porém são muito potentes e dependendo do tipo de senha e tamanho, pode ser que eles consigam quebra-la em no máximo **1 hora"**.

Métodos de Ataques

Ataques dicionário

Trata-se de uma tentativa de descobrir palavras-chave por apresentar cada possível palavra-chave em uma lista pré-definida de palavras-chave comuns ou esperadas;

Os ataques de password empregam um método criptográfico específico conhecido como ataque de aniversário, também chamado de *reverse hash matching.*

Métodos de Ataques

Contra-medidas de ataques de password:

Controlar o acesso físico ao sistema;

Controlar o acesso electrónico aos ficheiros de palavras-chave;

Criar uma política de palavras-chave fortes;

Empregar autenticação multi-facto;

Métodos de Ataques

Interrupção (*Denial of Service*) – ataques que impedem o sistema de processar ou responder ao tráfico legítimo ou solicitações de recursos e objectos;

Existem diversos tipos de ataques de inundação DoS tais como:

1. Inundar uma vítima particular com um fluxo contínuo de pacotes;
2. Interrupção distribuída de serviço (DDoS) – resulta na inundação de uma vítima por pacotes provenientes de várias fontes;
3. DoS Reflexivo Distribuído (DRDoS) – tira o proveito da operação normal de DNS e actualizações de protocolos de roteamento.

Interrupção

Métodos de Ataques

Contra-medidas de interrupção:

1. Identificar e desligar o dispositivo atacante;
2. Bloquear pacotes dos sistemas comprometidos;

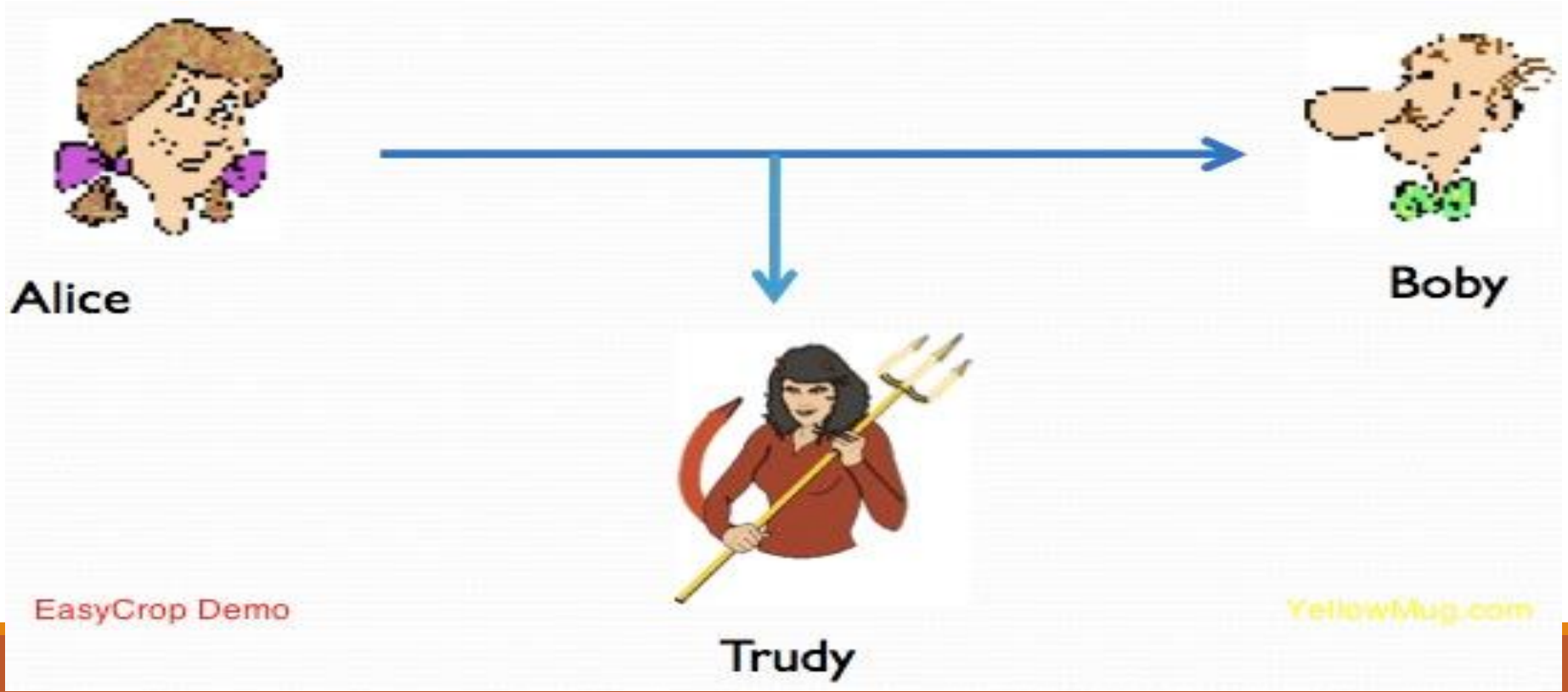
Ataques

Interceptação (*man in the middle*) – ocorre quando um utilizador malicioso ganha posição entre as extremidades de comunicação em progresso;

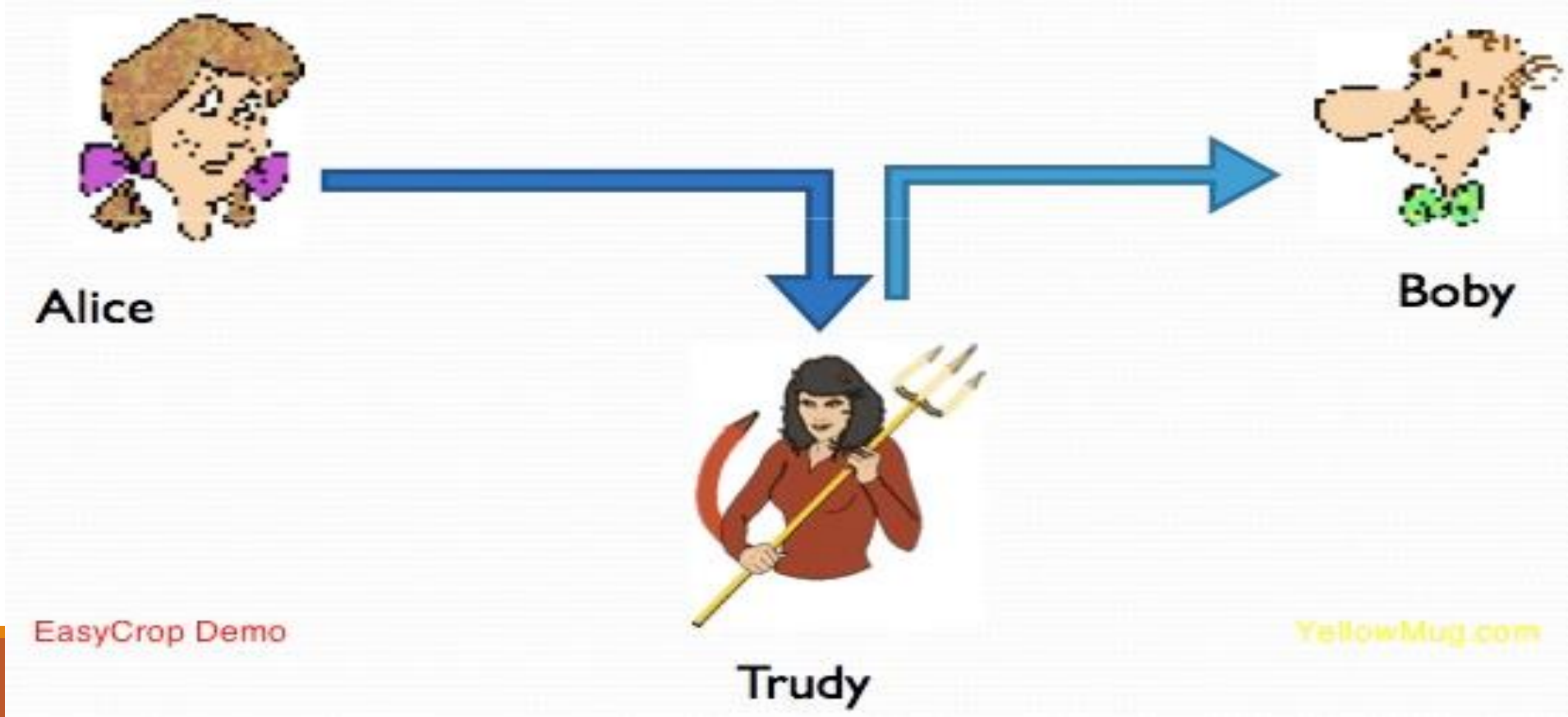
Existem dois tipos:

1. *Sniffing* – envolvendo copiar ou espiar o tráfico entre duas partes;
2. *Eavesdropping* – o atacante age como receptor de dados enviados pelo cliente e emissor de dados enviados para o servidor emissor.

Intercepção/Sniffing



Modificação/Eavesdropping



Ataques

Contra-medidas de Intercepção:

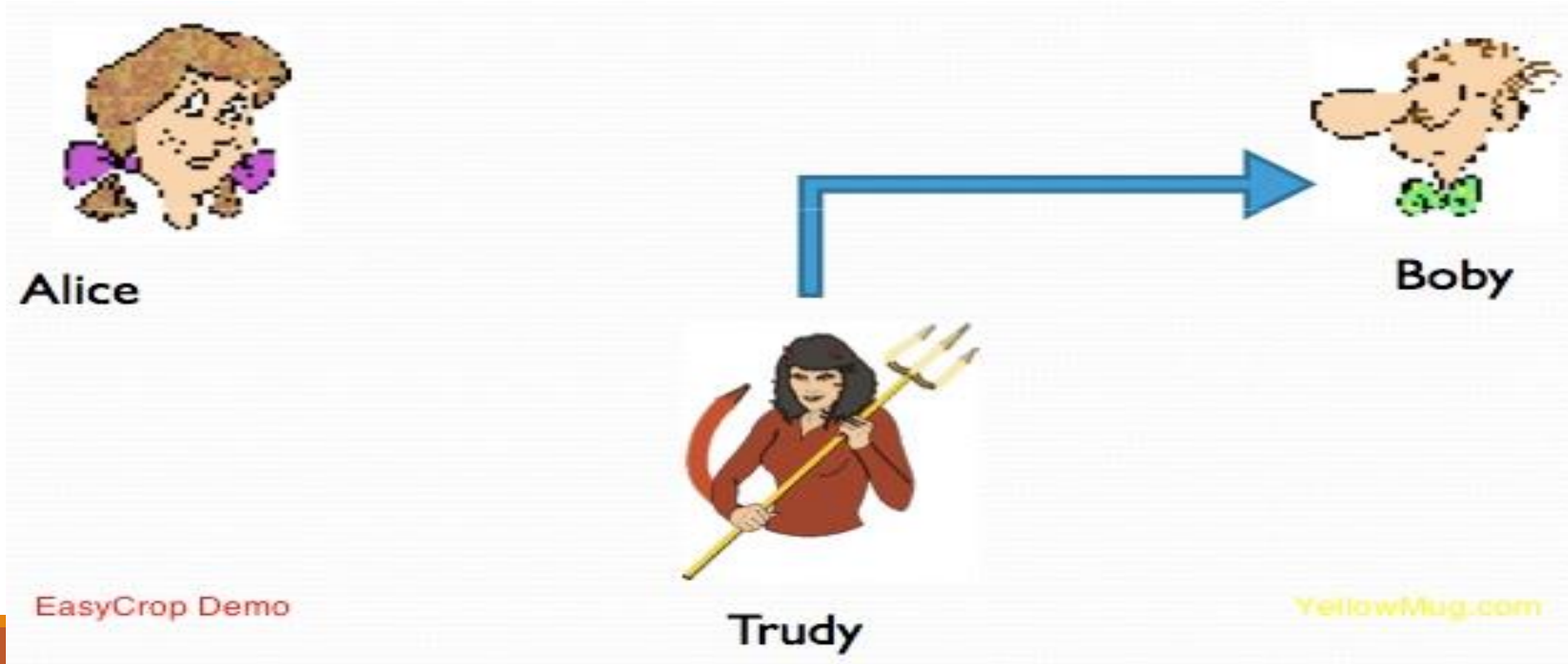
1. Requer melhoramento no estabelecimento de sessão, identificação, e autenticação de processos;
2. Os SDI(IDS) não podem normalmente detectar este tipo de ataque, mas podem detectar actividades anormais ocorrendo sobre links de comunicação “segurados”.

Ataques

Personificação ou fabricação (*spoofing*) – considera-se personificação a entidade que acede à informação ou transmite mensagem se passando por uma entidade autorizada – violação da autenticidade;

Ocorre quando: (1) um intruso utiliza o ID do usuário e palavra-chave roubados para ganhar o acesso, (2) o atacante altera o endereço da fonte em um pacote malicioso ou, (3) um atacante assume a identidade de um cliente para enganar o servidor de modo que este transmita dados controlados.

Personificação



Ataques

Contra-medidas de Personificação ou fabricação:

1. Habilitar a verificação da fonte/destino nos roteadores;
2. Empregar um Sistema de Detenção de Intrusão para detectar e bloquear ataques

TPC

Ataques:

- SYN Flood;
- Smurf;
- **Ping-of-Death, Stream, Teardrop and Land;**
- Spamming;
- Crackers e Hackers;
- Engenharia Social;
- Cryptojacking;