Segurança da Informação

ATAQUES VII

Professor: Jósis Alves

Técnicas de Ataques

❑ Exploits

Códigos criados para explorar vulnerabilidades que ainda não se tornaram conhecidas ou não possuem correção pelo fabricante.

Sistema Operacional, aplicações e aplicativos.

Ex: Servidor Web, Adobe Acrobat Reader, Windows XP, etc.

- **Defesa**

Manter sistemas operacionais, aplicações e aplicativos atualizados.

❑ Ataque *Zero day*

Um ataque de exploit de dia zero ocorre no mesmo dia em que um ponto fraco for descoberto no software.

Nesse momento, ele é explorado antes que uma correção seja disponibilizada pelo seu criador.

Um vetor de ataque (ferramenta e/ou método de exploração) contra a qual não existe correção conhecida (patches, service packs, hotfixies, recomendações técnicas)

1) Ano: 2018 Banca: FAURGS Órgão: BANRISUL Prova: FAURGS - 2018 - BANRISUL - Segurança da Tecnologia da Informação

No contexto de segurança de dados, qual das alternativas abaixo melhor define um Zero-Day?

A) É uma falha de software cuja correção ainda não foi disponibilizada pelos seus mantenedores.
B) É um ataque, realizado em uma determinada data, coordenado por computadores infectados.
C) É um ataque que redireciona um usuário para um website falso.
D) É um dispositivo de segurança que monitora atividades de rede em tempo real.
E) É uma vulnerabilidade de segurança associada ao protocolo Network Time Protocol (NTP).

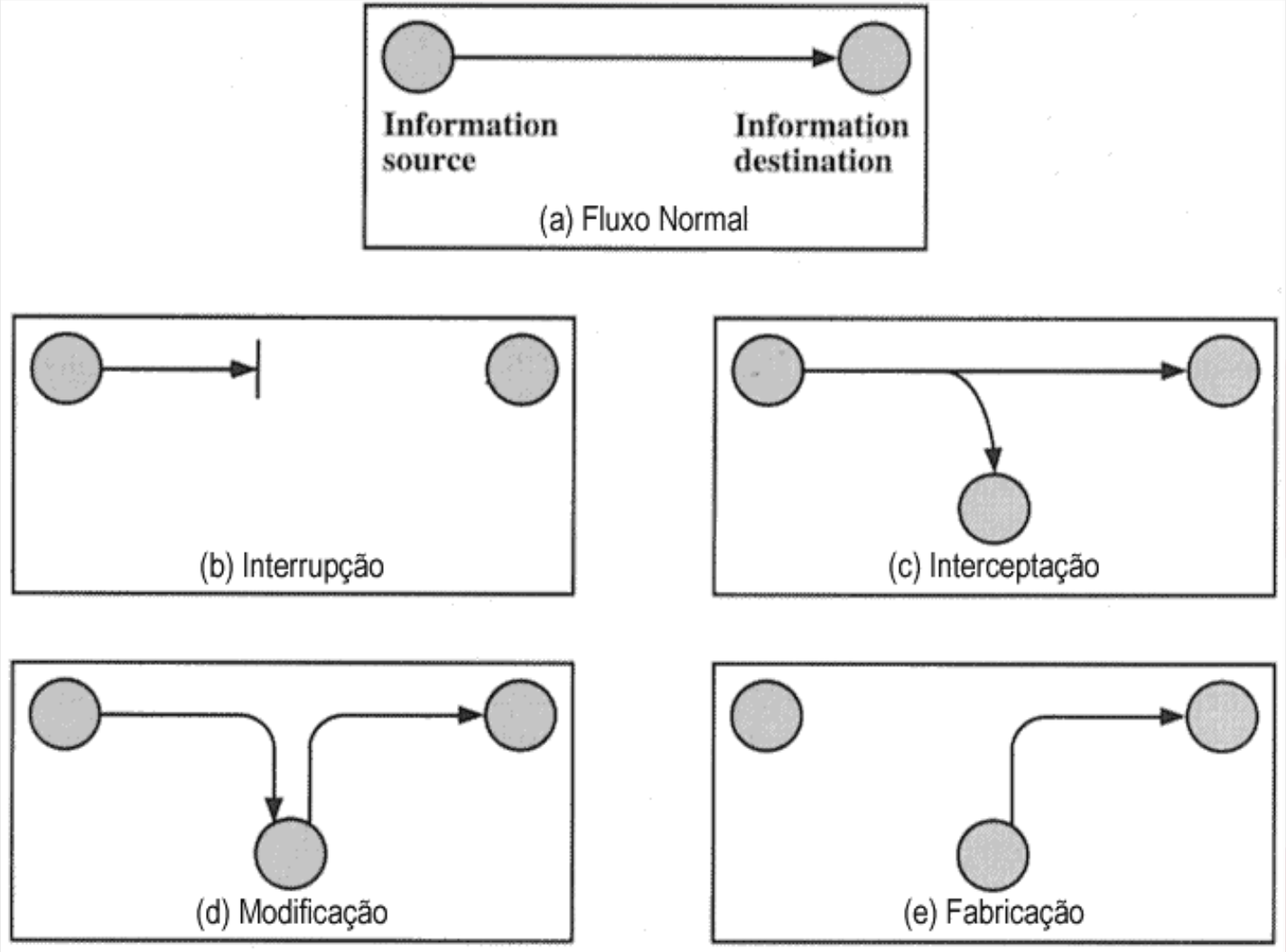
2) Ano: 2018 Banca: CESPE / CEBRASPE Órgão: ABIN Prova: CESPE - 2018 - ABIN - Oficial de Inteligência - Área 4

Acerca das ameaças persistentes avançadas (APT), vulnerabilidades zero day e engenharia social, julgue o item a seguir.

Um exploit elaborado para um ataque direcionado e com base em uma vulnerabilidade zero day permanece efetivo até que a vulnerabilidade seja publicamente revelada e a correção de software seja produzida, distribuída e aplicada.

( ) certo ( ) errado

❑ Ataques


Information source
Information destination
(a) Fluxo Normal
(b) Interrupção
(c) Interceptação
(d) Modificação
(e) Fabricação

❑ Tipos de Ataques

- **Ativos**: Modificação, criação ou interrupção de um fluxo de dados.

Sendo subdivididos:

  - ✓ Repetição
  - ✓ Personificação (disfarce)
  - ✓ Modificação (mensagem)
  - ✓ Negação de Serviço

- **Passivos**: Monitoramento de transmissões, bisbilhotar.

  - ✓ Revelação de conteúdo
  - ✓ Análise de tráfego

3) Ano: 2017 Banca: FCC Órgão: TST Prova: FCC - 2017 - TST - Analista Judiciário – Suporte em Tecnologia da Informação

No contexto da segurança de redes de computadores existem basicamente dois tipos de ataques, o passivo e o ativo. Dentre os ataques do tipo passivo, inclui-se

A) Injeção SQL.
B) Man in the middle.
C) Ataque Smurf.
D) DNS spoofing.
E) Varredura de portas.

4) Ano: 2019 Banca: IF-SP Órgão: IF-SP Prova: IF-SP - 2019 - IF-SP - Informática

Tanto nas recomendações X.800 da ITU-T, quanto na RFC 2828, os ataques à segurança são classificados como ataques passivos e ataques ativos. Um ataque passivo tenta descobrir ou utilizar informações do sistema, mas não afeta seus recursos. Um ataque ativo tenta alterar os recursos do sistema ou afetar sua operação.

4) Ano: 2019 Banca: IF-SP Órgão: IF-SP Prova: IF-SP - 2019 - IF-SP - Informática

Com base na informação, assinale a alternativa correta.

A) A análise de tráfego é um tipo de ataque ativo, e além de alterar os dados, é muito difícil de detectar, sendo a prevenção a melhor defesa.

B) Um ataque de disfarce envolve a captura passiva de uma unidade de dados e sua subsequente reprodução para produzir um efeito não autorizado.

C) A modificação de mensagens é um exemplo de ataque ativo, pois significa que mensagens foram adiadas, reordenadas ou alteradas.

D) Um ataque ativo de repetição impede ou inibe o uso ou gerenciamento normal das instalações de comunicação.

GABARITO
1 - A
2 - certo
3 - E
4 - C