UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

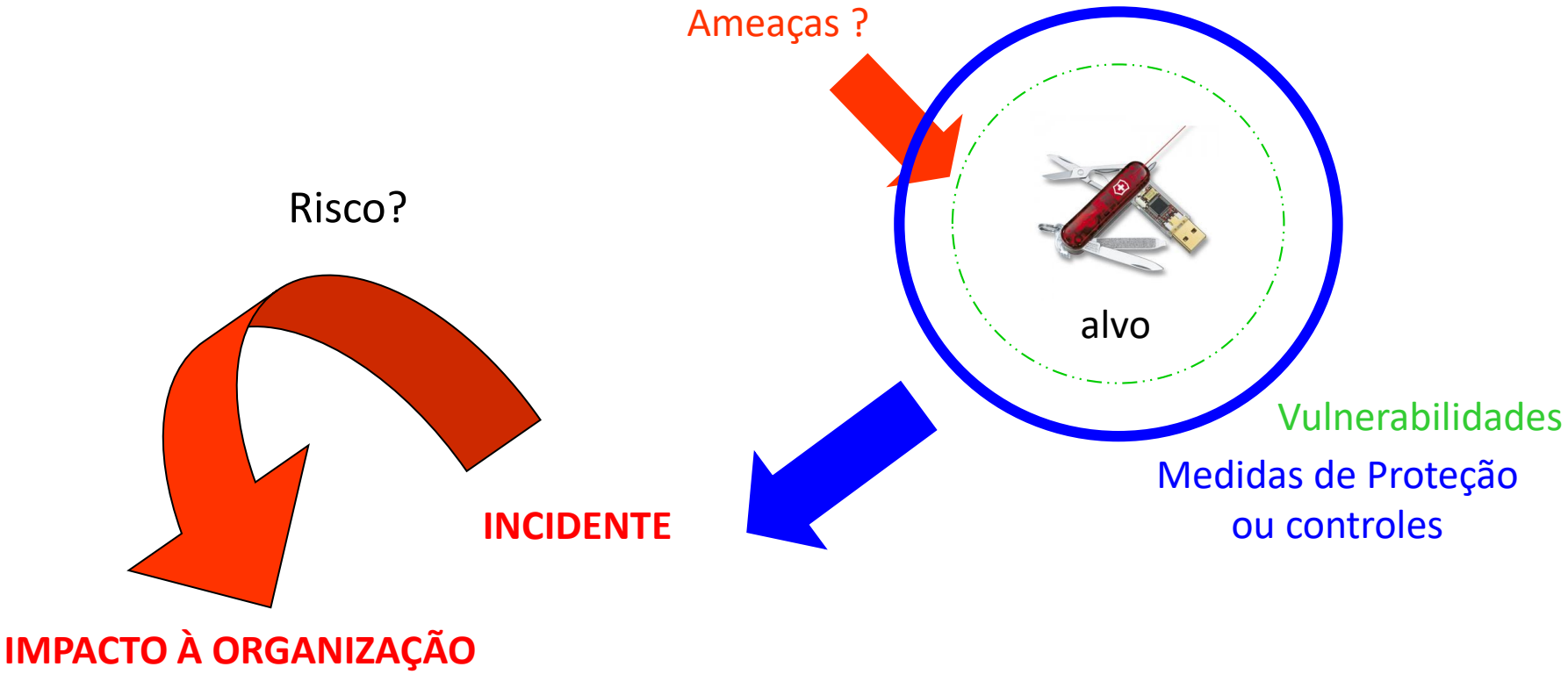
Segurança da Informação
Aula 3 – Ameaças, Risco e Ataques.

Prof. Dr. Eng. Fred Sauer

fsauer@gmail.com

http://www.fredsauer.com.br

Unidade 2: Ameaças, Vulnerabilidades e Ataques



$$\text{Risco} = \frac{V \times A \times I}{M}$$

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

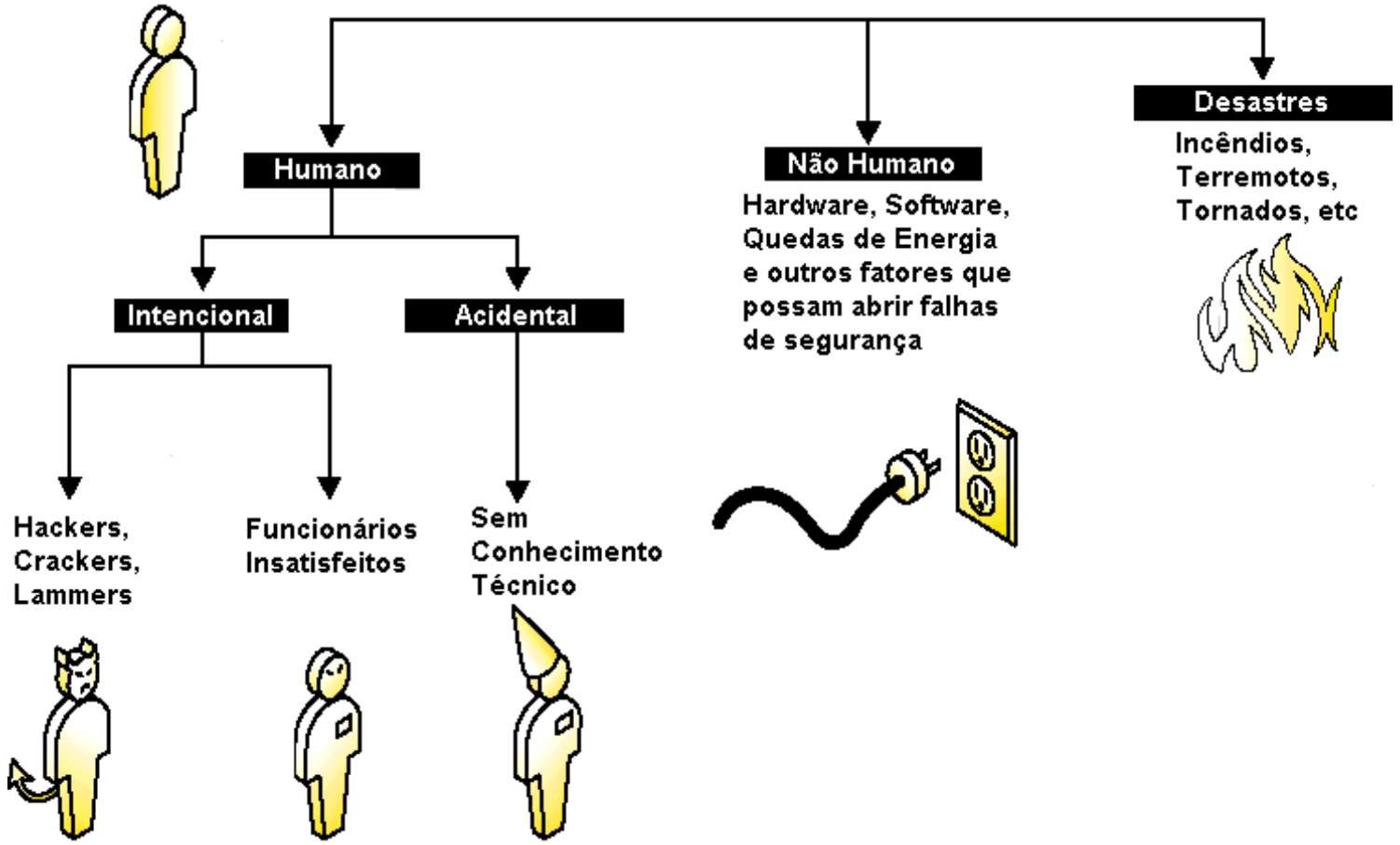
Conceitos

- **Ameaça:** elemento ativo, que busca vulnerabilidades para explorar, causando impactos à corporação
- **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
- **Impacto:** é o efeito da exploração de uma vulnerabilidade por uma ameaça.
- **Controle, Contramedida ou Medida de Proteção:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;
  - São exemplos: firewall, IDS, IPS, antivírus, etc.

- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

  - Classificação:
    - Tipo:
      - Física; e
      - Lógica.
    - Agente:
      - Humano;
        - » Intencional; e
        - » Acidental.
      - Não Humano;
      - Desastre;

Unidade 2: Ameaças, Vulnerabilidades e Ataques



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Exemplos de Ameaças

- Ataques: ações realizadas contra um sistema de informações com intenção de obter, tornar indisponível e danificar informações;
- Backdoor: brechas intencionais, não documentadas, em programas legítimos, que permitem o acesso ao sistema por parte de seus criadores ou mantenedores;
- Hackers: usuários avançados, que possuem um exímio conhecimento em informática;
- Crackers: usuários que quebram sistemas de segurança de acesso a servidores. Os crackers também burlam os sistemas anticópia e antipirataria de alguns programas (criam “cracks”);

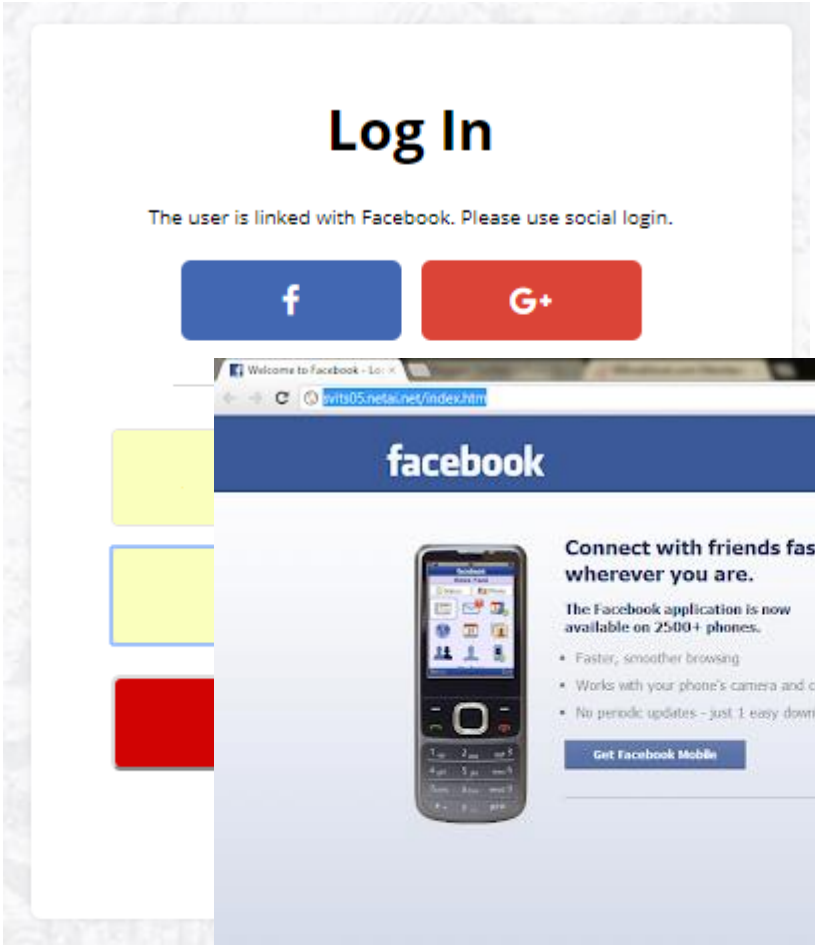
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

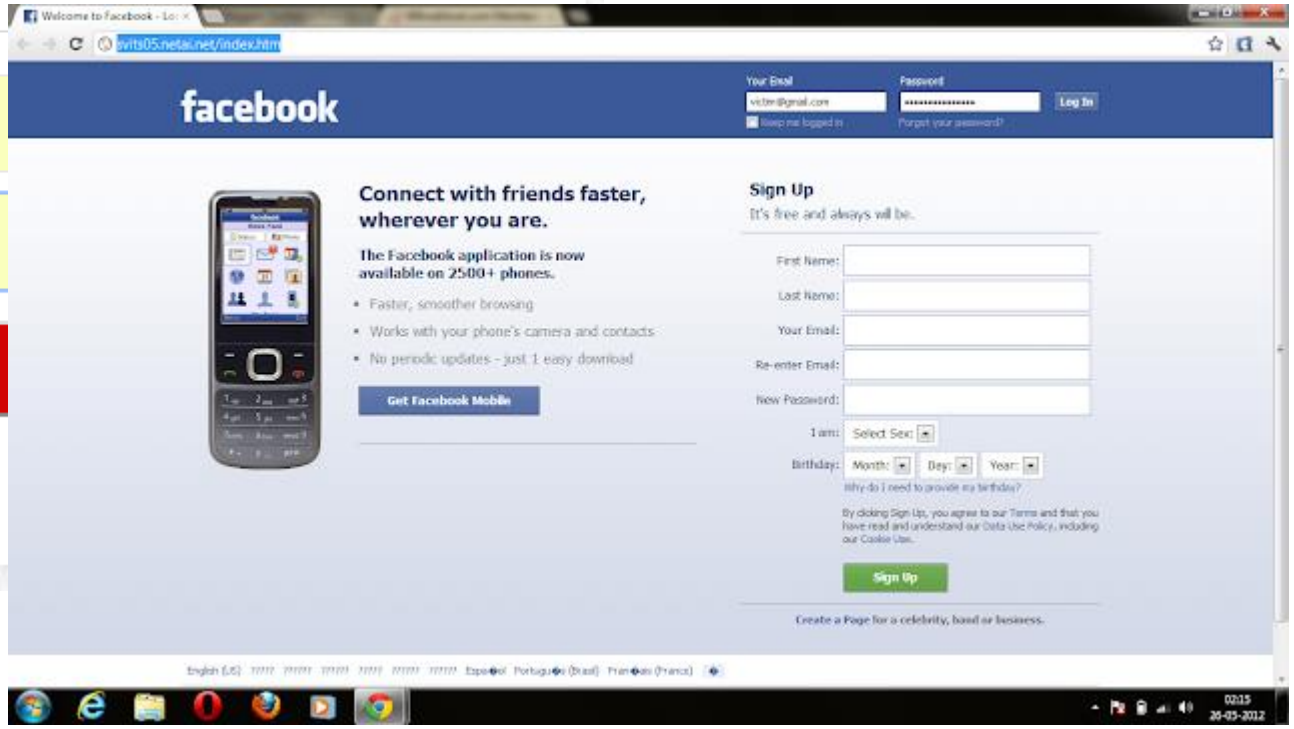
Exemplos de Ameaças

- SPAM: envio em massa de mensagens de e-mail não autorizadas pelos destinatários.
- SCAM (Golpe): uma série de técnicas para enganar os usuários de sistemas de informação no intuito de enviar-lhe um programa maléfico ou simplesmente obter seus dados (*Phishing Scam*).

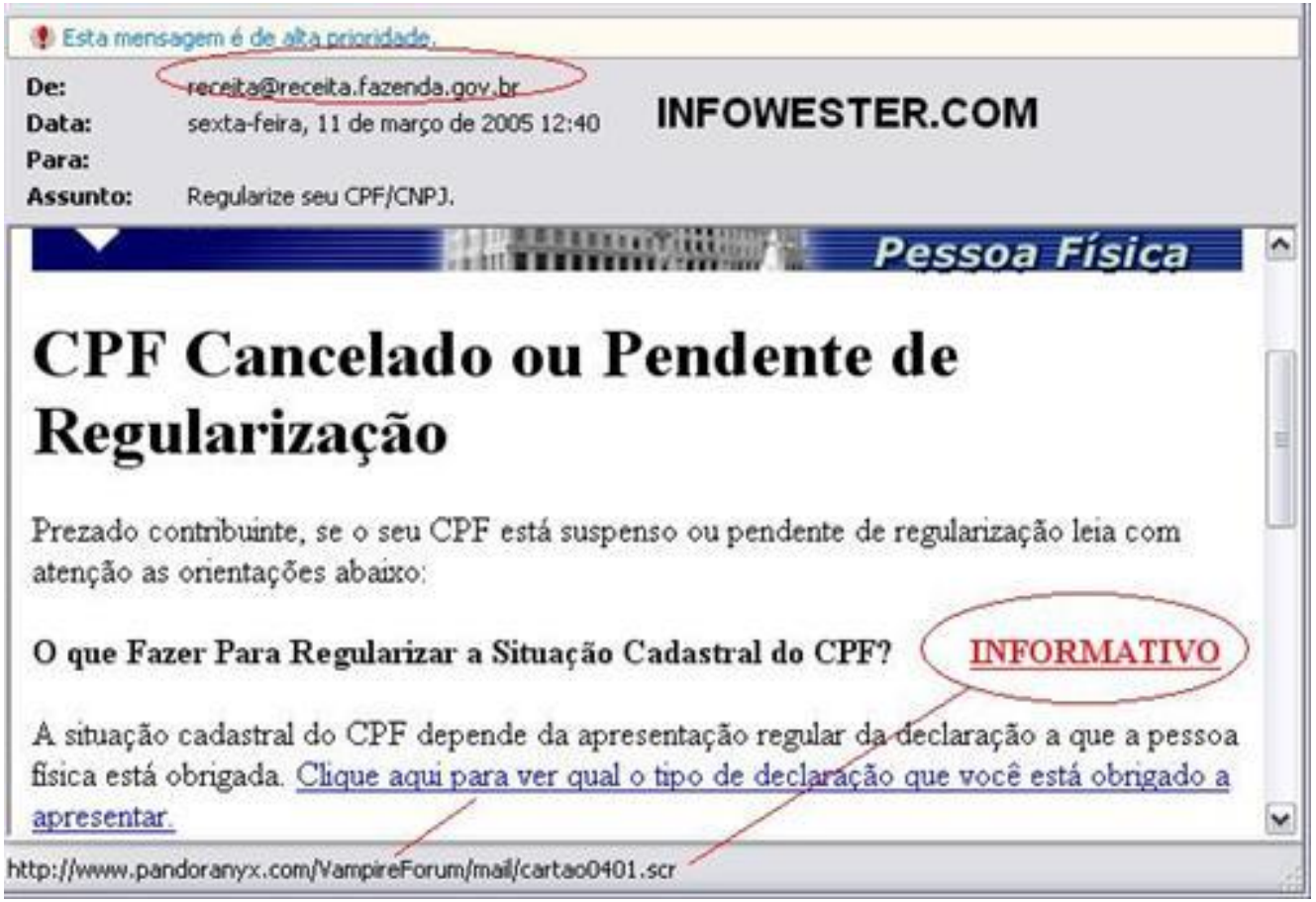
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Exemplo de SCAM (phishing scam)





Exemplo de SCAM



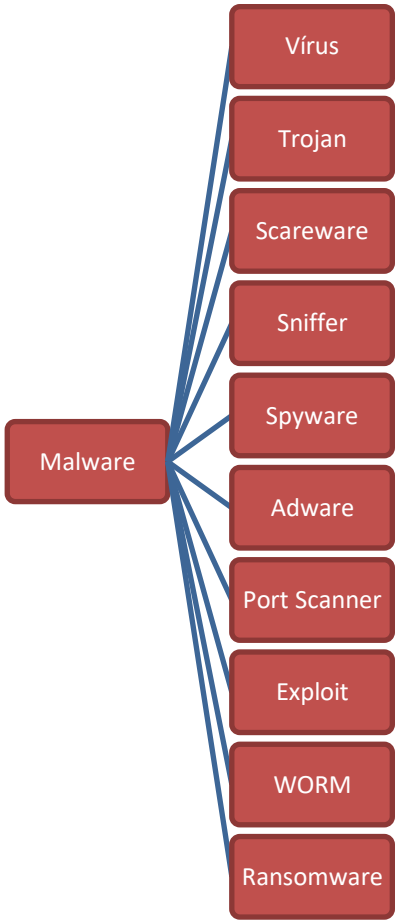
➢SCAM: Características comuns das mensagens

- A maioria das vezes é não-direcionado
  - Remetente que você desconhece.
  - Serviços que você não usa.
- Pouco caso com a inteligência do leitor
  - Links inoperantes.
  - Informações pessoais, mas não identifica o destinatário *(ex. um extrato de dívida, mas não traz o nome do devedor)*.
  - Link para domínio claramente falso (ex: receita.fazenda.com).
- Links para baixar programas
  - A ansiedade faz com que as pessoas ignorem os avisos do navegador, antivírus e acabam executando o programa.
- Pede informações que não devem ser fornecidas
  - Senhas
  - Recadastramento de email, *facebook*, etc.

- ***Engenharia Social:*** É uma técnica que consiste em enganar usuários usando técnicas de persuasão.
  - Através deste recurso valioso, é possível ter acesso a informações importantes para acesso a rede, como senhas de usuários, horários de realização de operações específicas na rede...
  - Explora fraquezas humanas e sociais;
  - Uso de falsa identidade;
  - Explora boa vontade e boa fé das pessoas;
  - Uso de psicologia e de técnicas de intimidação;

Exemplos de Ameaças

- Malware: programas criados com objetivos prejudiciais, comprometendo, assim a segurança dos sistemas de informação;



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Vírus

- Vírus de computador: um programa (ou parte de um programa) que:
  - Necessita de um hospedeiro para existir (um vírus se "anexa" ao conteúdo de um arquivo para viver);
  - Consegue se replicar (copiar) para outros arquivos (hospedeiros), toda vez que é executado;

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

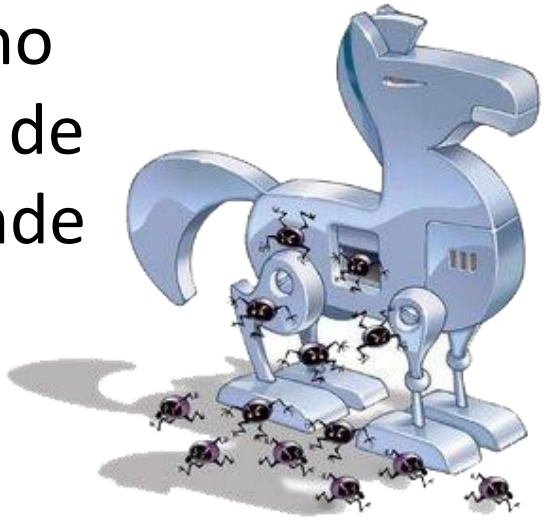
Vírus

- Vírus de Boot: afetam o setor de boot do HD para serem carregados sempre que o Sistema Operacional for carregado.
- Vírus de Macro: afetam os programas da Microsoft que são baseados em VBA (Visual Basic for Applications), como os documentos do Microsoft Office (.DOC e .XLS)
- Vírus de Executável: afetam os arquivos executáveis, como os que têm extensão .EXE e .COM
- Vírus Stealth: escondem-se do Antivírus (por exemplo, como BAD BLOCKS – falhas de disco)
- Vírus Polimórficos: mudam de “assinatura” a cada infecção para dificultar a sua detecção.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Trojan Horse (Cavalo de Tróia)

- Cavalo de Tróia (Trojan Horse):
  - Um programa que apresenta-se como algo inofensivo (um jogo, um cartão de Natal, etc.) e que, na verdade, esconde objetivos maliciosos, como apagar dados, roubar informações e, mais comumente, abrir portas de comunicação para que se possa invadir o computador que o executou.
  - Não se replica ao ser executado.



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Worm

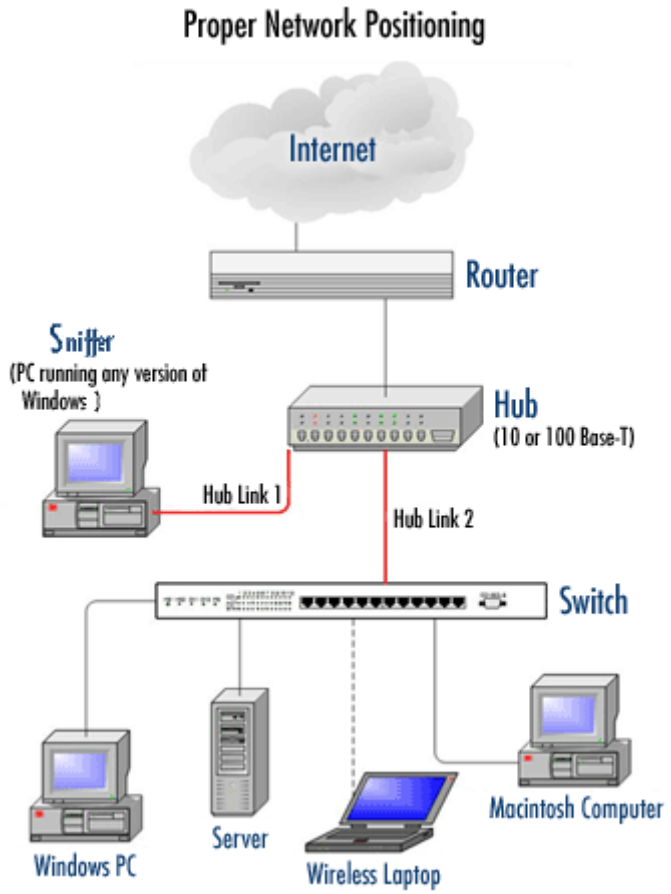
- WORM: um programa que usa falhas na segurança da comunicação através da estrutura das redes para se copiar de computador para computador.
- Um WORM não precisa de hospedeiro, pois ele próprio é o arquivo que se copia. O WORM não precisa ser acionado pelo usuário, pois se utiliza de falhas nos protocolos e serviços da rede para se espalhar;

Scareware

- SCAREWARE
- Utiliza engenharia social para convencer a vítima de que ela está em perigo.
- Em geral, tenta convencer a vítima a comprar/instalar programas (potencialmente maliciosos) ou sem benefício real.

Sniffer

- Sniffer: um programa que é instalado na máquina do atacante e serve para capturar os quadros da rede que chegam àquela máquina, mesmo os que não estão direcionados a ela.
- Sniffers só são 100% efetivos se forem posicionados adequadamente.



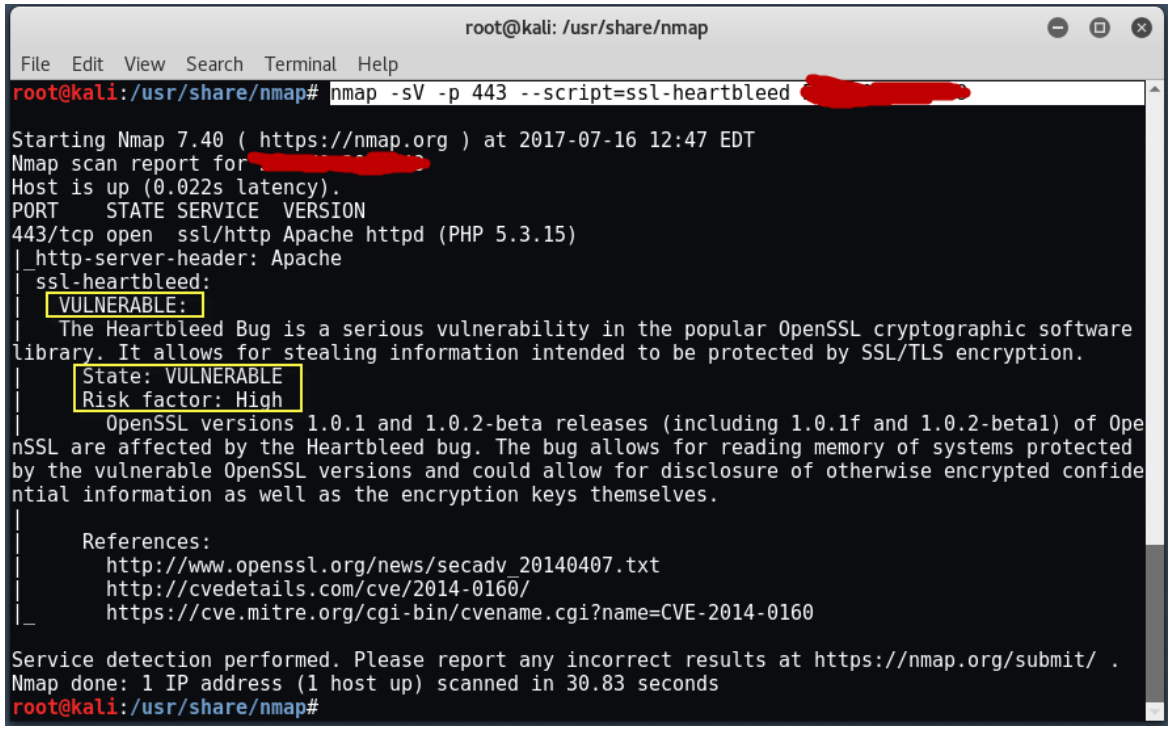
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Spyware e Adware

- **Spyware**: um programa que monitora e registra os "hábitos" de navegação e acesso à Internet do micro infectado.
  - Um spyware pode conter *keyloggers* (capturadores de teclado) e *screenloggers* (capturadores de tela) para "copiar" o que o usuário está fazendo no computador.
- **Adware:** um programa que fica "fazendo anúncios de propaganda" no micro infectado;

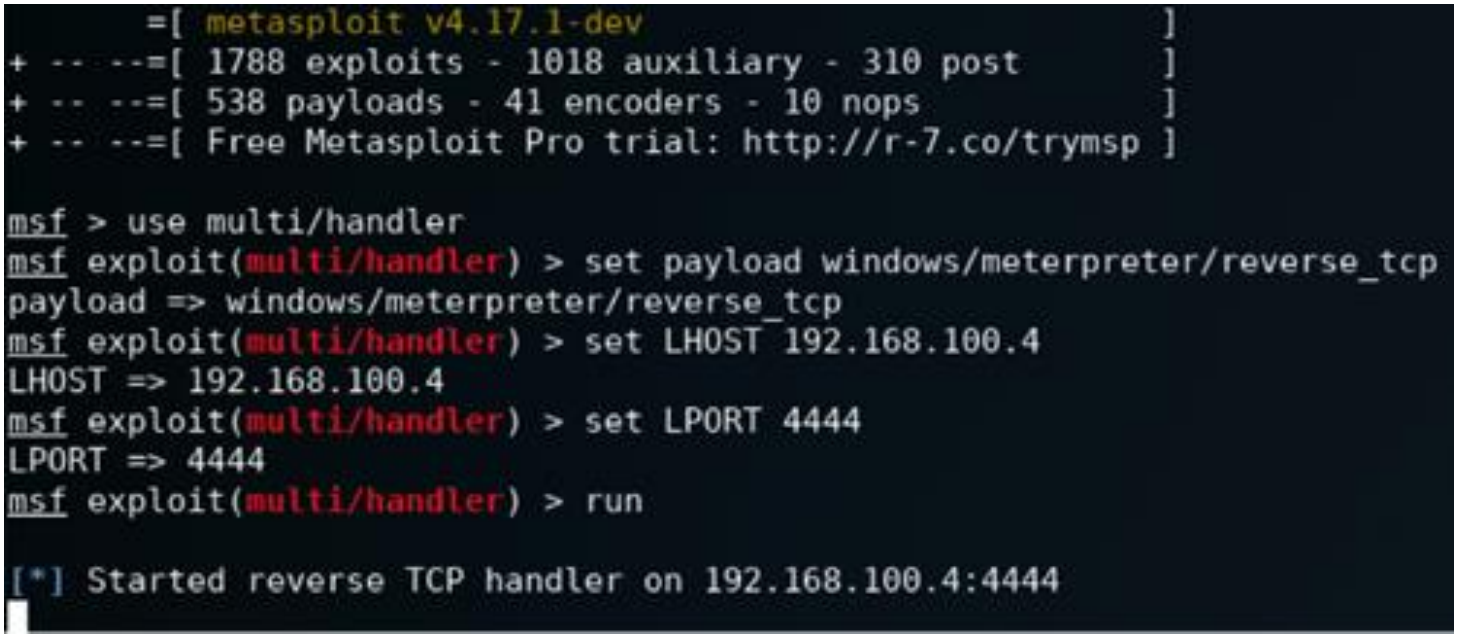
Port Scanner

- **Port Scanner**: um programa que vasculha um computador alvo à procura de portas (serviços) abertas para que, através delas, se possa perpetrar uma invasão àquele micro;



Exploit

- Exploit: um programa construído para tirar vantagem de alguma falha, ou vulnerabilidade **conhecida** em um sistema de informações;



Ransonware

- RANSOMWARE: um programa que restringe acesso a um sistema ou aos dados, tipicamente através de criptografia, e exige o pagamento de um resgate (*ransom)* pela chave.

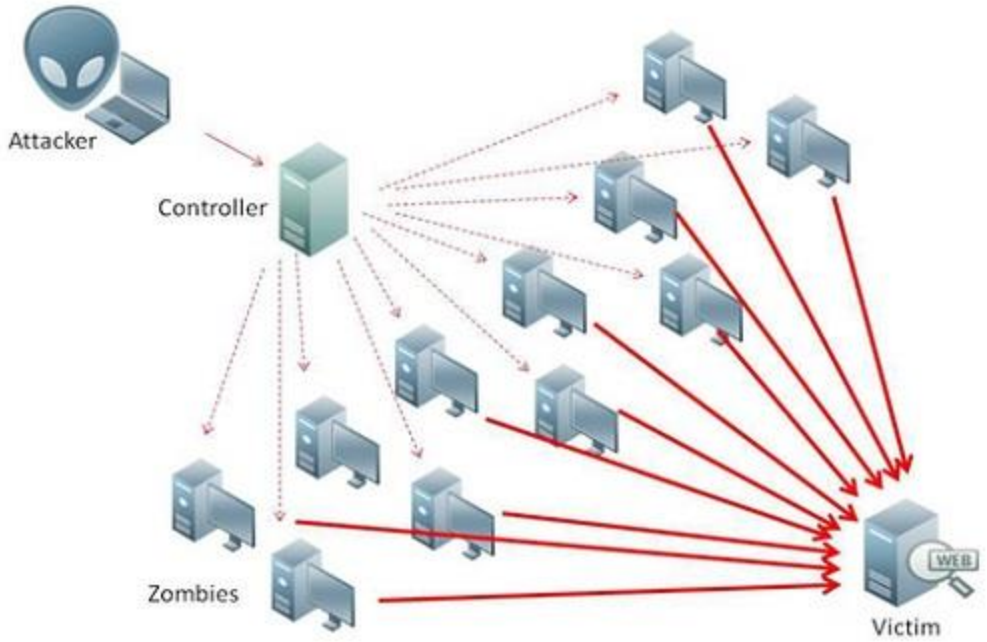
IP Spoofing

- ***IP Spoofing (Disfarce de IP):*** Não é bem uma forma de ataque, mas uma técnica para fazer um atacante não ser detectado.
  - É possível "forjar" o endereço IP de origem de um pacote para evitar represálias dos sistemas atacados.
  - Explora-se, nesse caso, a condição, no protocolo IPv4 que dispensa reconhecer o IP de origem para rotear os pacotes.

DoS (Denial of Service)

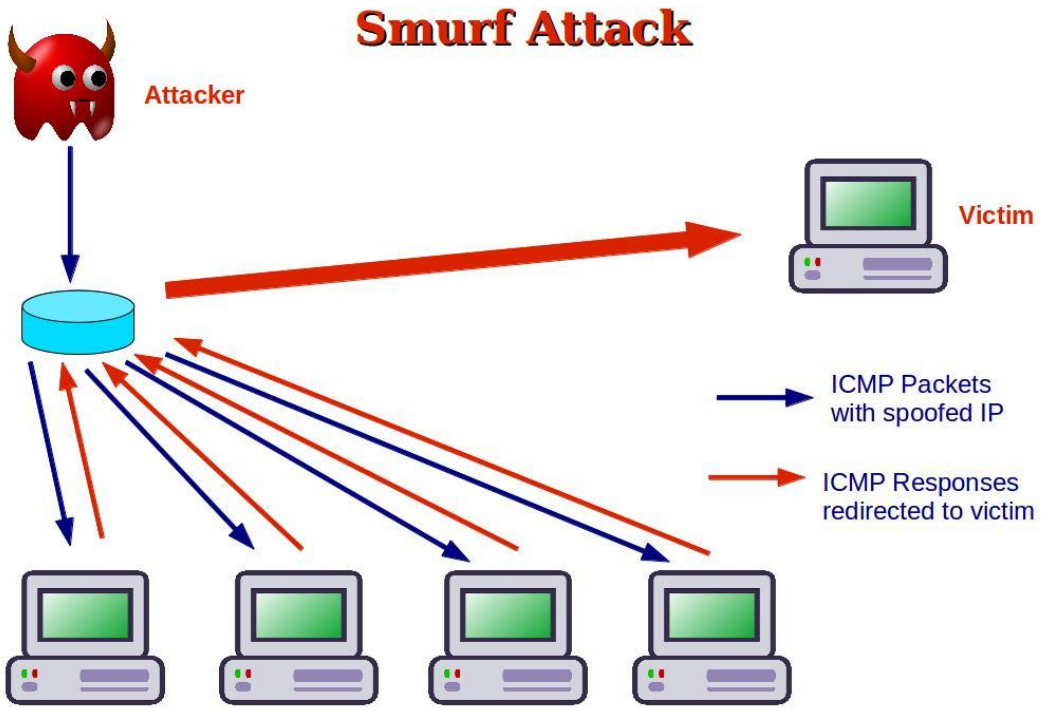
Negação de serviço

- Não é o nome de uma única técnica de ataque, mas de uma série delas.
  - Todo ataque DoS tem como objetivo fazer o computador vítima deixar de responder às requisições verdadeiras, ou seja, atentar contra a **disponibilidade** do sistema.



Alguns Tipos de Ataques

- ***Ataques Smurf:*** Consiste em enviar várias solicitações PING ao endereço de broadcast de rede, colocando, como origem do pacote, um ***spoofing*** (disfarce de IP) p/ o endereço do alvo a ser atacado
- Isso fará todas as estações de rede enviarem pacotes de resposta a esse micro.



Alguns Tipos de Ataques

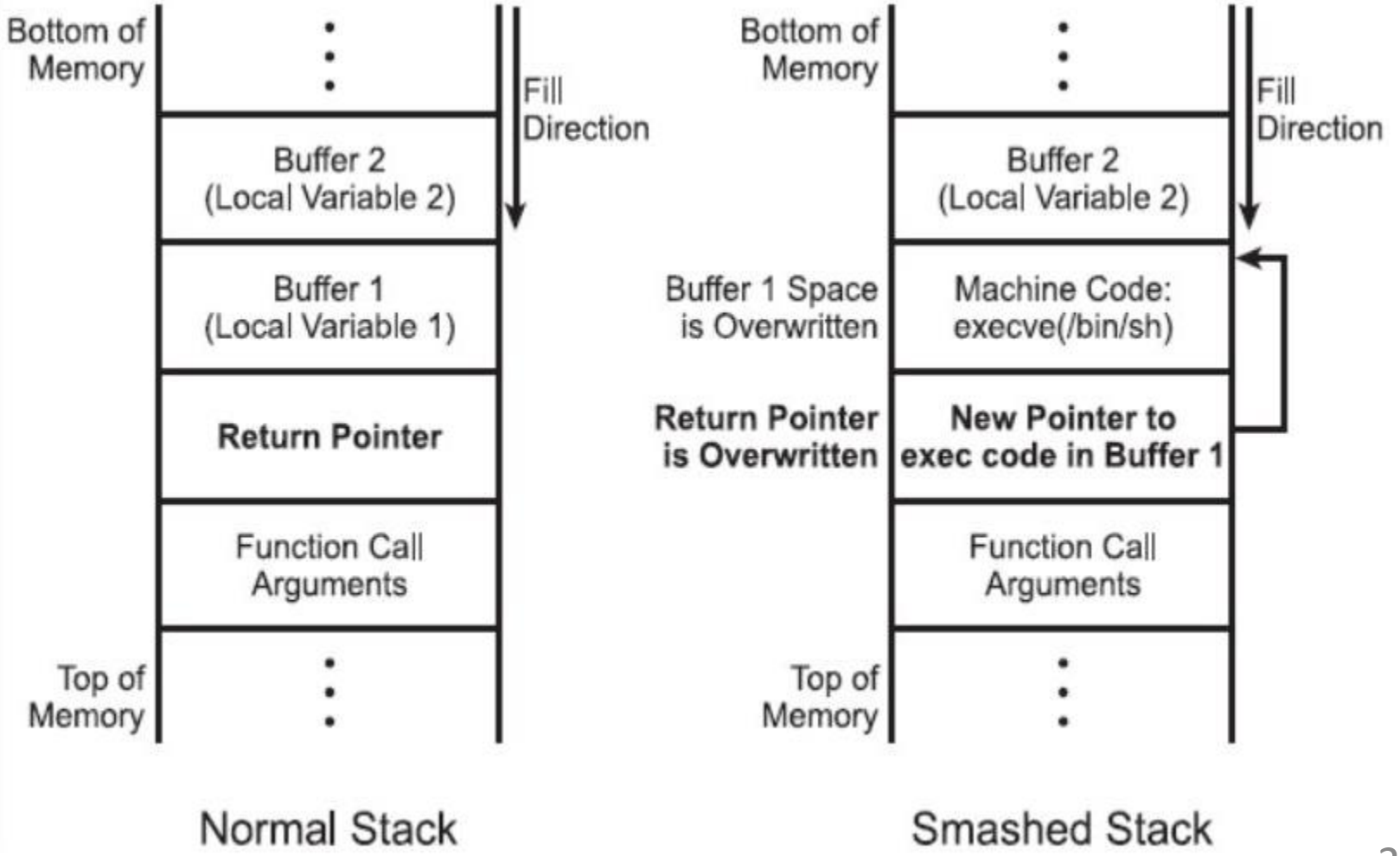
- ***Buffer Overflow (Sobrecarga de Memória):***

  Consiste em oferecer a um servidor uma quantidade de dados que ele não suporta para uma determinada informação.

  - Se houver falhas na forma como o servidor lida com tais excessos, ele poderá “invadir” uma área de memória destinada a outra parte do programa e, com isso, travar.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Buffer Overflow

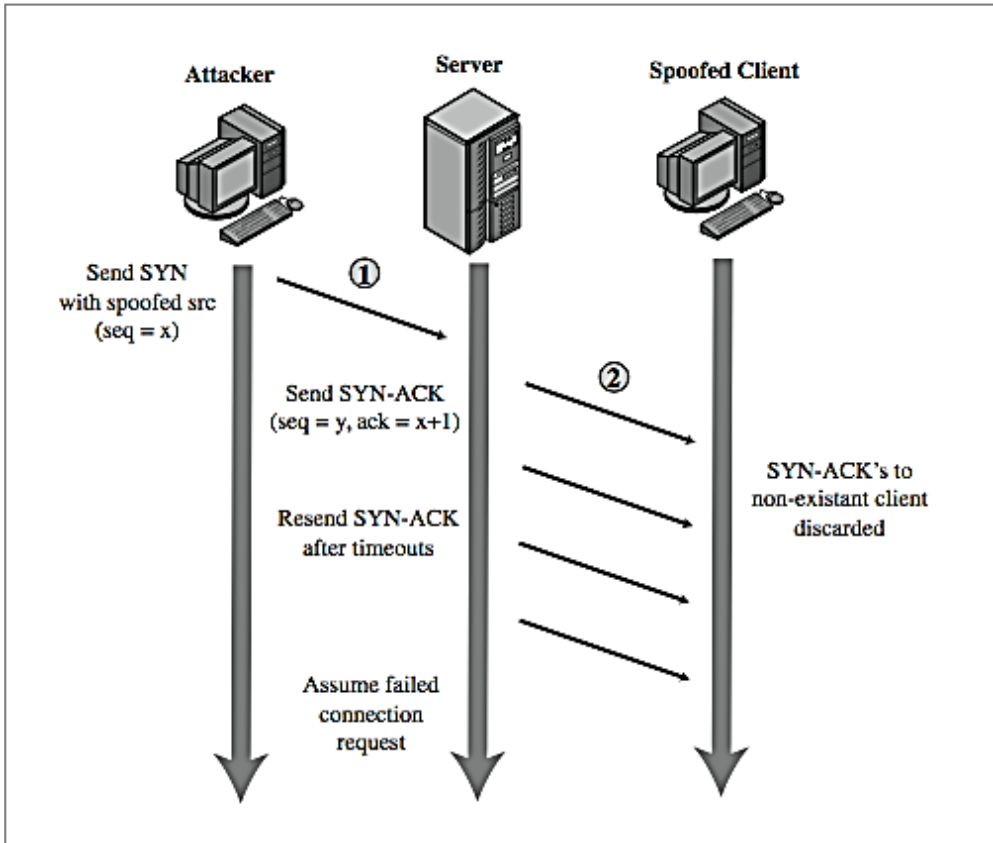


Alguns Tipos de Ataques

- ***SYN Flooding (Inundação SYN):***

  consiste em enviar sucessivos pedidos de conexão TCP (segmentos SYN) e não efetivar a conexão real.

  - O servidor vai ficar tentando responder às requisições SYN, mas não obterá respostas e terá que esperar pelo timeout.
  - Enquanto isso, ficará preso e não aceitará conexões legítimas, feitas por usuários verdadeiros.



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fixação

- Na equação do risco, o elemento passivo é a _____VULNERABILIDADE_____. Sozinho, não oferece perigo, mas se explorada por uma _____AMEAÇA_____, pode causar _____IMPACTOS_____ à organização. Para evitar isso, usamos _____MECANISMOS DE SEGURANÇA_____.
- Um malware que se replica toda vez que seu hospedeiro é executado é um _____VÍRUS_____. Se ele se propaga sem precisar de ação do usuário é um _____WORM_____. Se ele estiver anexado a um programa funcional é um _____TROJAN_____.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fixação

- Um malware para copiar dados sigilosos de um dispositivo é um _____. Se apenas fizer propaganda é um _____. Um artefato que testa os serviços disponíveis em um host é um _____, e um que captura o tráfego que chega até a sua interface é um _____.
- Um _____ explora falhas de proteção de memória, e um malware de _____ compromete a disponibilidade.

SPYWARE
ADWARE
PORT SCANNER
SNIFFER
BUFFER OVERFLOW
DENY OF SERVICE