uniesp
Centro Universitário

SISTEMAS PARA INTERNET

REDES DE COMPUTADORES

PROFª PRISCILLA DE ALMEIDA

REDES DE COMPUTADORES

AULA 09

SEGURANÇA EM REDE BÁSICA

- **Tipos de Ameaças**

Malware, Phishing, Ataques de Força Bruta, Ataques de Negação de Serviço (DoS), Sniffing de Rede, Engenharia Social, etc.

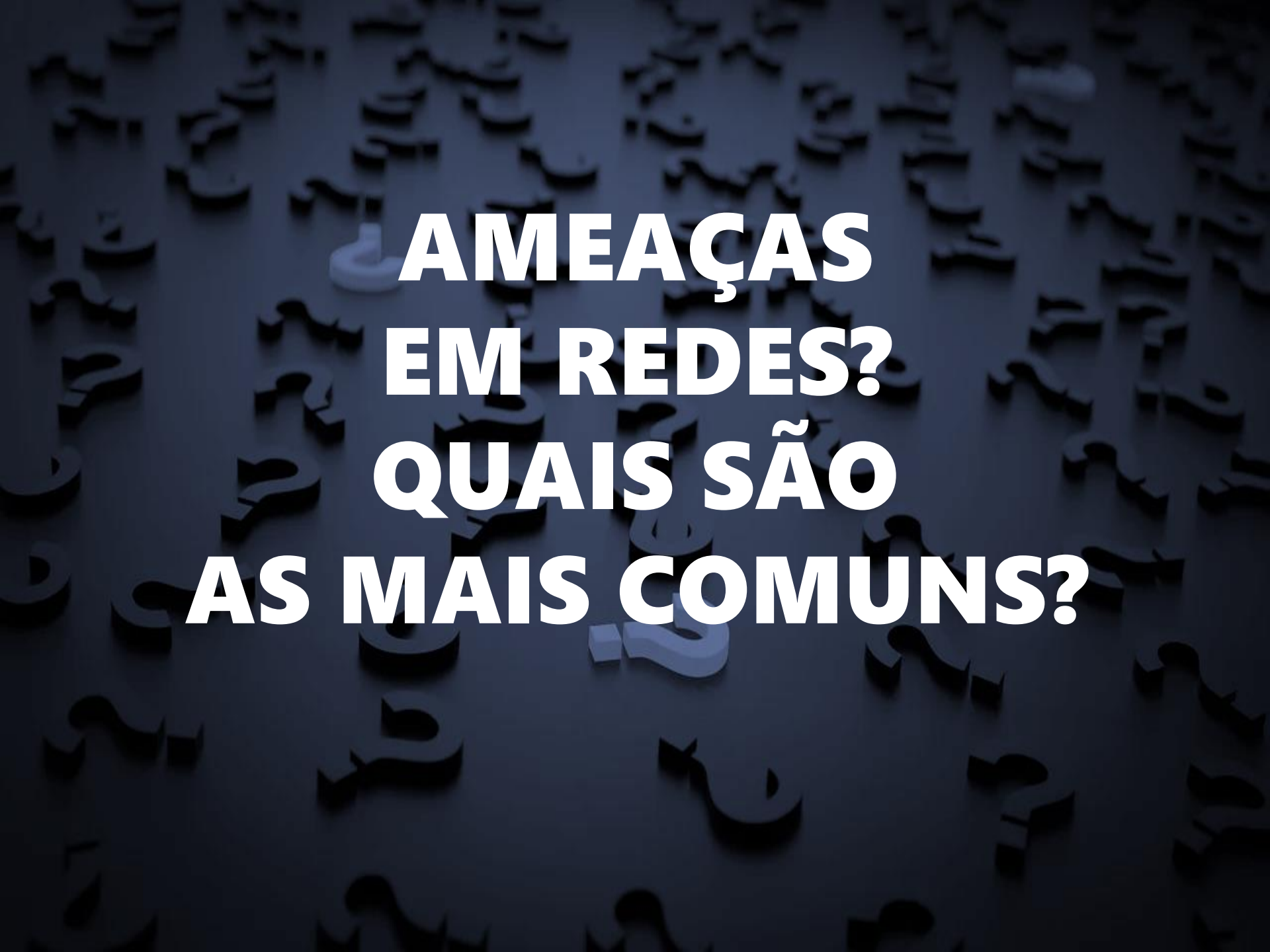
- **Normas e regulamentações**

AULA PASSADA...

Compreensão dos conceitos fundamentais de segurança em rede
Confidencialidade
Integridade
Autenticidade
Disponibilidade
Privacidade
Proteção contra Ameaças
Cumprimento de Normas e Regulamentações
Manutenção da Reputação
Proteção de Recursos Críticos

AULA PASSADA...

Compreensão dos conceitos fundamentais de segurança em rede
Confidencialidade
Integridade
Autenticidade
Disponibilidade
Privacidade
Proteção contra Ameaças
Cumprimento de Normas e Regulamentações
Manutenção da Reputação
Proteção de Recursos Críticos


AMEAÇAS
EM REDES?
QUAIS SÃO
AS MAIS COMUNS?

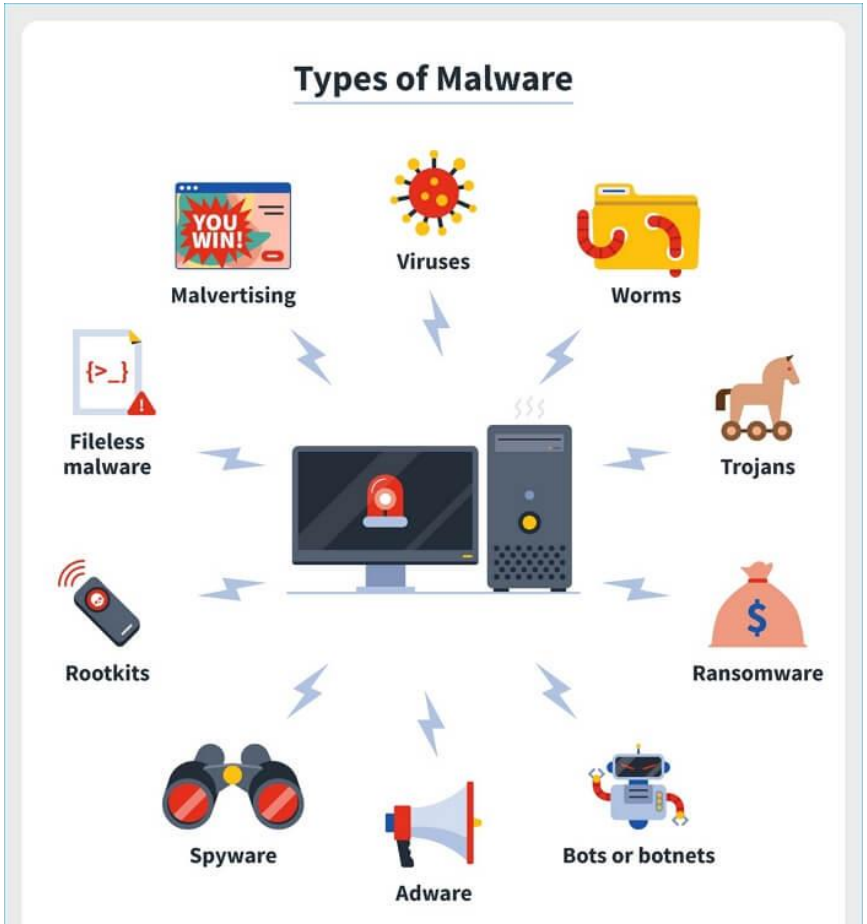
LIDANDO COM AMEAÇAS

LIDANDO COM AMEAÇAS

TIPOS MAIS COMUNS: **Malware | Phishing | Ataques de Força Bruta | Ataques de Negação de Serviço (DoS) | Sniffing de Rede | Engenharia Social**

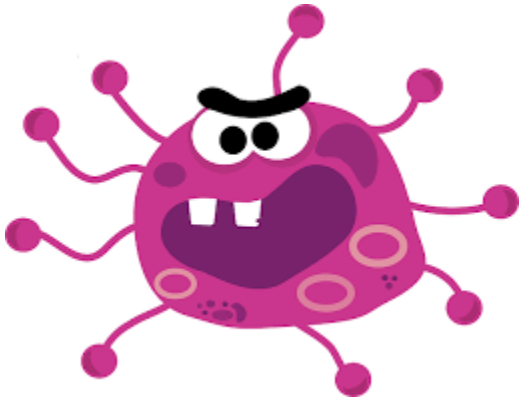
LIDANDO COM AMEAÇAS

Malware refere-se a software malicioso projetado para danificar ou explorar sistemas. Isso inclui vírus, worms, trojans e ransomware.



LIDANDO COM AMEAÇAS

Malware refere-se a software malicioso projetado para **danificar ou explorar sistemas**. Isso inclui **vírus**, **worms**, **trojans** e **ransomware**.



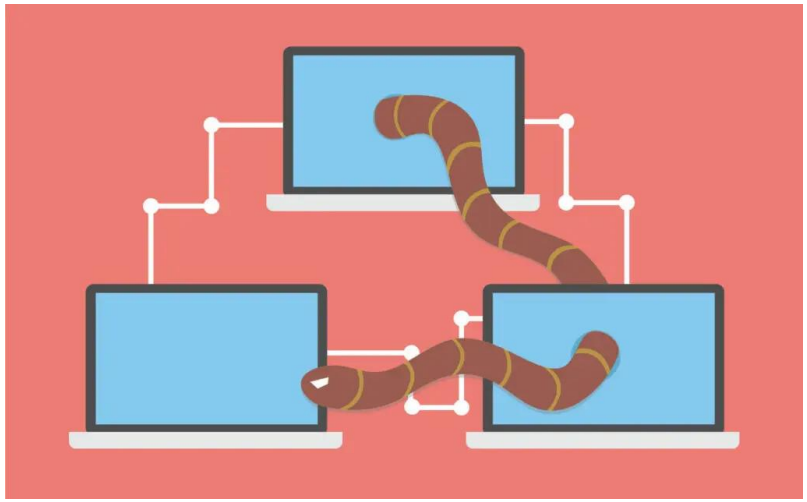
Vírus

Características: Um vírus é um tipo de malware que se anexa a um programa existente ou a um arquivo executável. Ele pode se espalhar quando esse programa ou arquivo é executado. Os vírus frequentemente danificam ou alteram dados, e alguns podem se autoreplicar.

Propagação: Geralmente, os vírus se espalham quando os usuários compartilham arquivos infectados, seja por meio de dispositivos USB, e-mails ou downloads da internet.

LIDANDO COM AMEAÇAS

Malware refere-se a software malicioso projetado para danificar ou explorar sistemas. Isso inclui vírus, worms, trojans e ransomware.



Worms

Características: são malwares que se reproduzem e se espalham automaticamente por redes, muitas vezes explorando vulnerabilidades de segurança. Eles não precisam de um arquivo hospedeiro para se mover, ao contrário dos vírus.

Propagação: podem se espalhar rapidamente pela internet, infectando computadores e dispositivos conectados em rede.

LIDANDO COM AMEAÇAS

Malware refere-se a software malicioso projetado para danificar ou explorar sistemas. Isso inclui vírus, worms, trojans e ransomware.

Trojans

Características: "Cavalos de Troia" são malwares disfarçados de software legítimo. Eles não se replicam sozinhos, mas podem abrir uma porta dos fundos em um sistema, permitindo que atacantes obtenham acesso não autorizado.

Propagação: Trojans geralmente são distribuídos por meio de downloads de software aparentemente legítimos, anexos de e-mail ou links maliciosos.

LIDANDO COM AMEAÇAS

Malware refere-se a software malicioso projetado para danificar ou explorar sistemas. Isso inclui vírus, worms, trojans e ransomware.

Ransomware

Características: é projetado para criptografar os dados em um sistema e, em seguida, exigir um resgate (geralmente em criptomoedas) em troca da chave de descriptografia. Ele pode se espalhar rapidamente e causar danos significativos.

Propagação: Ransomware muitas vezes entra nos sistemas por meio de emails de phishing, sites comprometidos ou exploração de vulnerabilidades.


Ooops, your files have been encrypted!
Payment will be raised on
XX/XX/XXXX
Time Left
00:15:00:59
Your files will be lost on
XX/XX/XXXX
Time Left
00:22:05:00
Contact Us
Check Payment
Decrypt
Copy

LIDANDO COM AMEAÇAS

Phishing é uma técnica em que os atacantes tentam enganar os usuários para revelar informações confidenciais, como senhas, por meio de mensagens fraudulentas. Conscientização do usuário e filtros anti-phishing são cruciais para mitigar essa ameaça.

Exemplo:

Um usuário recebe um e-mail aparentemente legítimo de um serviço bancário, informando que há atividades suspeitas em sua conta. O e-mail inclui um link que direciona o usuário para uma página falsa, semelhante à página de login do banco. Nessa página, o usuário é solicitado a inserir suas credenciais, incluindo nome de usuário e senha, para "verificar" a conta ou resolver o problema...

LIDANDO COM AMEAÇAS

Ataques de Força Bruta envolvem tentativas repetitivas de adivinhar senhas ou chaves de criptografia. Práticas seguras, como o uso de senhas complexas e bloqueio após tentativas falhas, são estratégias eficazes.

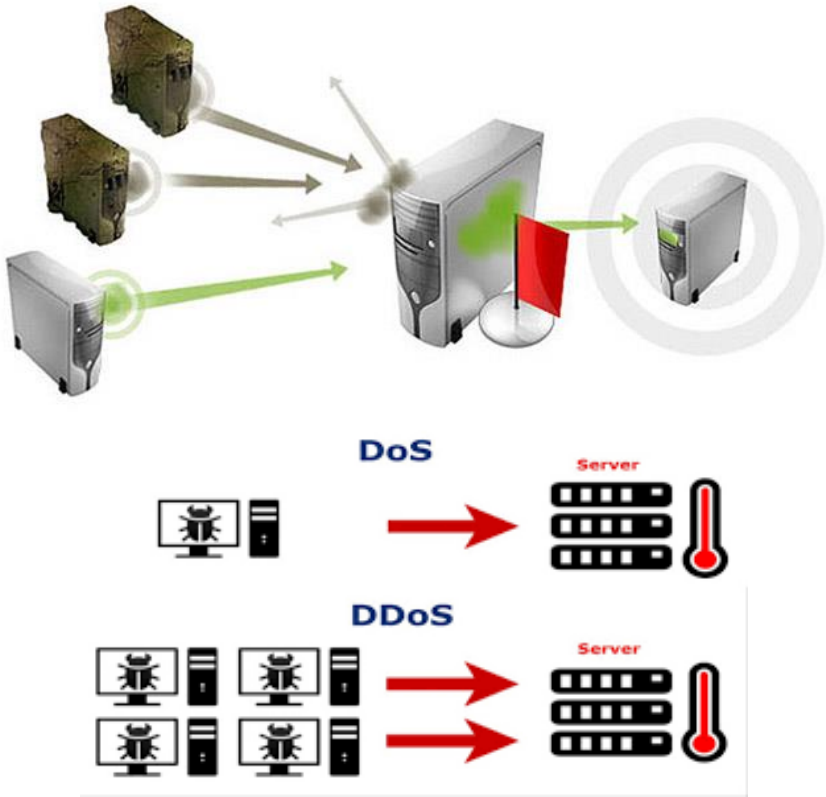
LIDANDO COM AMEAÇAS

```
30 -o hydra-http-post-attack.txt
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-09-08 22:42:23
[DATA] max 10 tasks per 1 server, overall 64 tasks, 74548575 login tries (l:45/p:1656635), ~116482 tries per task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 0
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 007007
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 000007
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 000000
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 00000000
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 0660
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: !root
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 0311
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 0000
[80][http-post-form] host: testphp.vulnweb.com   login: Administrator   password: 0007
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 0
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 000000
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 0000
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 007007
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: !root
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 000007
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 00000000
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 0007
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 0660
[80][http-post-form] host: testphp.vulnweb.com   login: administrator   password: 0311
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 0000
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: !root
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 00000000
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 0311
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 000000
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 000007
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 0007
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 0660
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 007007
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 0
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 007007
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 0000
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 000000
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 000007
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 00000000
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 0007
[80][http-post-form] host: testphp.vulnweb.com   login: security   password: 0311
[80][http-post-form] host: testphp.vulnweb.com   login: superuser   password: 0
[80][http-post-form] host: testphp.vulnweb.com   login: sysadmin   password: !root
[80][http-post-form] host: testphp.vulnweb.com   login: sysadmin   password: 0
[80][http-post-form] host: testphp.vulnweb.com   login: sysadmin   password: 0000
```

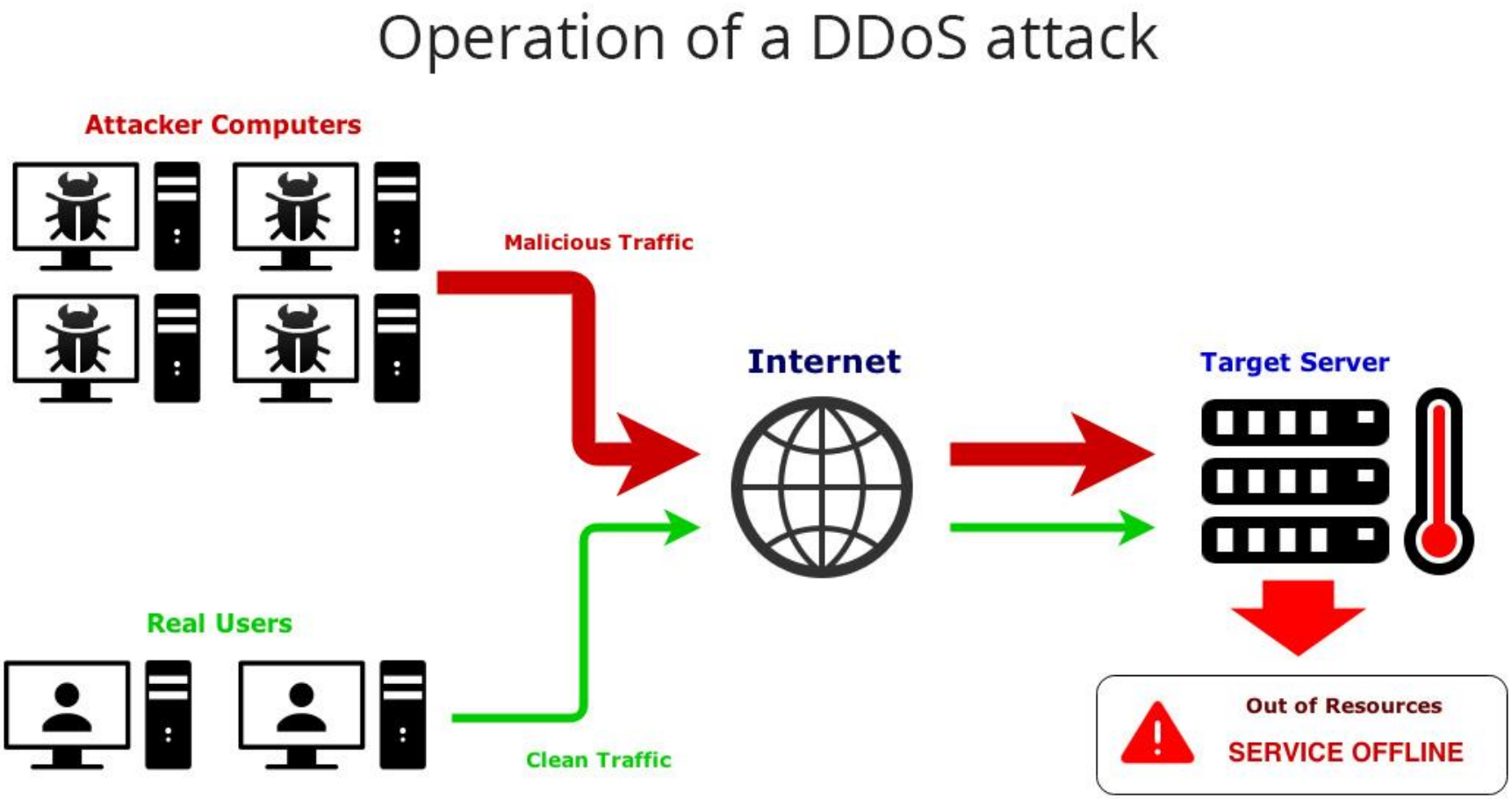
Ataques de Negação de Serviços (DoS)

Ataques DoS buscam sobrecarregar um sistema, tornando-o inacessível. Firewalls, sistemas de detecção de intrusões (IDS) e balanceamento de carga são usados para mitigar esses ataques.



Exemplo:
O atacante utiliza uma rede de computadores comprometidos (botnet) para enviar uma grande quantidade de solicitações HTTP simultâneas ao servidor do site. O servidor fica sobrecarregado ao processar um número excessivo de solicitações, consumindo recursos como largura de banda, capacidade de processamento e memória. Como resultado, o servidor não consegue lidar com solicitações legítimas, tornando o site inacessível para usuários genuínos.

LIDANDO COM AMEAÇAS



LIDANDO COM AMEAÇAS

Sniffing de Rede

envolve a interceptação não autorizada de dados transmitidos pela rede. Criptografia, uso de redes privadas virtuais (VPNs) e monitoramento ativo ajudam a evitar sniffing.

Refere-se à prática de capturar e analisar o tráfego de rede, muitas vezes com o objetivo de interceptar informações sensíveis, como senhas, dados de login ou informações confidenciais transmitidas por uma rede. Essa prática é altamente invasiva e representa uma séria ameaça à segurança da informação.

LIDANDO COM AMEAÇAS

Engenharia Social **é a manipulação psicológica dos usuários para obter informações confidenciais. A conscientização do usuário e a educação são vitais para prevenir ataques baseados em engenharia social.**

Isso envolve explorar a confiança, persuasão ou até mesmo o medo para conseguir que as vítimas realizem ações que beneficiem o atacante.

Spoofing de IP e MAC

Spoofing de IP (Internet Protocol)	Spoofing de MAC (Media Access Control)
Spoofing de IP é uma técnica em que um atacante mascara ou falsifica o endereço IP para fazer parecer que a origem de uma comunicação é diferente da real. Isso pode ser usado para enganar sistemas, encaminhar tráfego de forma maliciosa ou até mesmo realizar ataques mais complexos, como ataques de negação de serviço distribuído (DDoS).	Spoofing de MAC envolve a alteração ou falsificação do endereço MAC de um dispositivo. O endereço MAC é uma identificação única atribuída à placa de rede de um dispositivo.
Exemplo de Spoofing de IP: Um atacante falsifica o cabeçalho IP de um pacote de dados para modificar o endereço de origem. O pacote é enviado à rede de destino, fazendo com que os sistemas acreditem que o tráfego se origina de uma fonte confiável.	Exemplo de Spoofing de MAC: Um atacante modifica o endereço MAC de sua placa de rede para corresponder ao endereço MAC de outro dispositivo na rede. O atacante pode então tentar se passar por esse dispositivo na rede.

LIDANDO COM AMEAÇAS SIMPLES

RESUMO DAS PRINCIPAIS AÇÕES:

- **Malware:** Utilize antivírus e antimalware para proteger contra software malicioso.
- **Phishing:** Esteja atento a e-mails e mensagens suspeitas e evite clicar em links não confiáveis.
- **Ataques de Força Bruta:** Implemente senhas fortes e políticas de bloqueio após várias tentativas de login incorretas.
- **Spoofing de IP e MAC:** Use autenticação forte para evitar falsificação de identidade.
- **Sniffing de Rede:** Use criptografia para proteger dados transmitidos na rede.
- **Ataques de Negação de Serviço (DoS):** Implemente medidas para mitigar ataques DoS, como firewalls e serviços de mitigação de tráfego.

NORMAS E REGULAMENTAÇÕES

NORMAS E REGULAMENTAÇÕES

As normas e regulamentações de segurança em redes variam de acordo com o país e a região. No Brasil e em muitos outros países, existem várias referências e padrões reconhecidos internacionalmente que orientam as práticas de segurança em TI.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Lei Geral de Proteção de Dados

é a legislação brasileira que regula o tratamento de dados pessoais por organizações públicas e privadas. Ela visa garantir a privacidade e a segurança dos dados pessoais.

NORMAS E REGULAMENTAÇÕES

ISO/IEC 27001

Esta é uma norma internacional que estabelece os requisitos para um sistema de gestão de segurança da informação (SGSI). Ela fornece diretrizes abrangentes para implementar, monitorar, manter e melhorar a segurança da informação em uma organização.

NORMAS E REGULAMENTAÇÕES

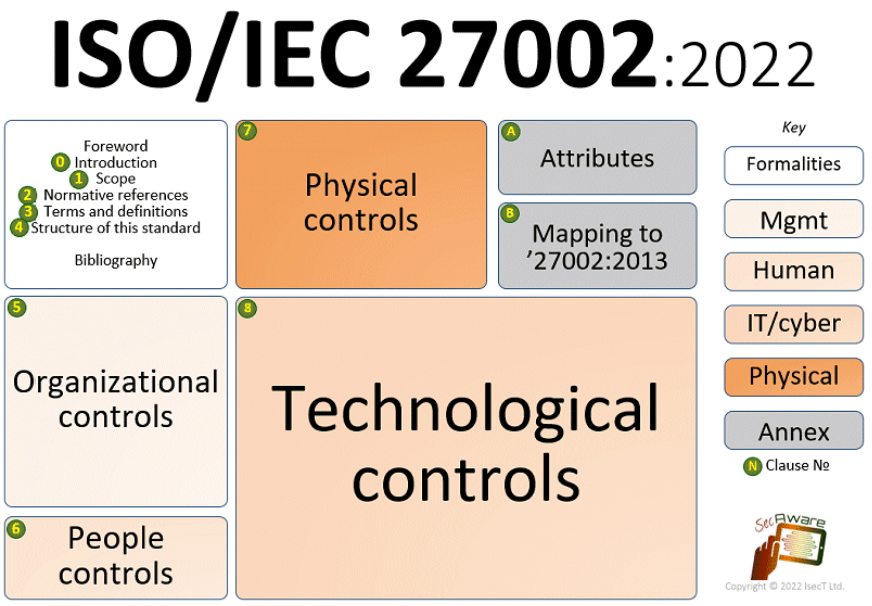
ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

ISO/IEC 27002

Complementando a ISO/IEC 27001, esta norma oferece um conjunto de controles e diretrizes práticas para implementar medidas de segurança em uma organização. Ela fornece um conjunto detalhado de boas práticas de segurança.

Lançada em 2022 pela ABNT:

ISO/IEC 27002: Segurança da Informação, Segurança Cibernética e Proteção da Privacidade — Controles de Segurança da Informações

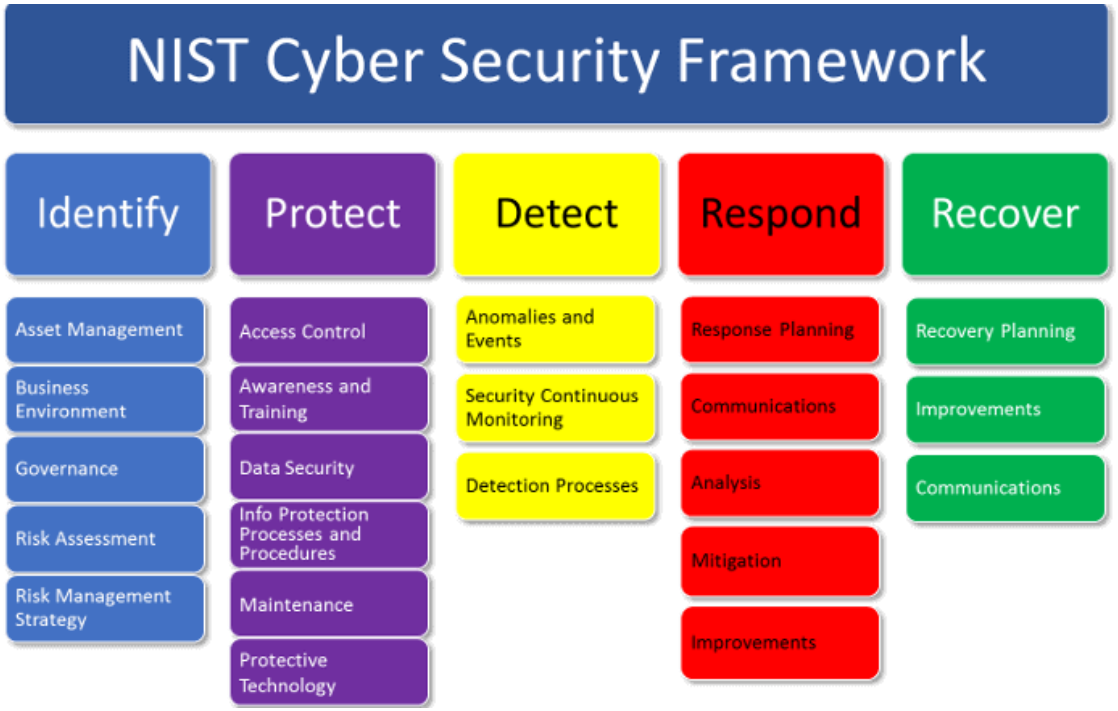


NORMAS E REGULAMENTAÇÕES

NIST
National Institute of Standards and Technology

NIST (National Institute of Standards and Technology):

Nos Estados Unidos, o NIST publica várias diretrizes e padrões de segurança, incluindo o Framework de Cibersegurança do NIST, que oferece orientações sobre como organizações podem fortalecer suas posturas de segurança.



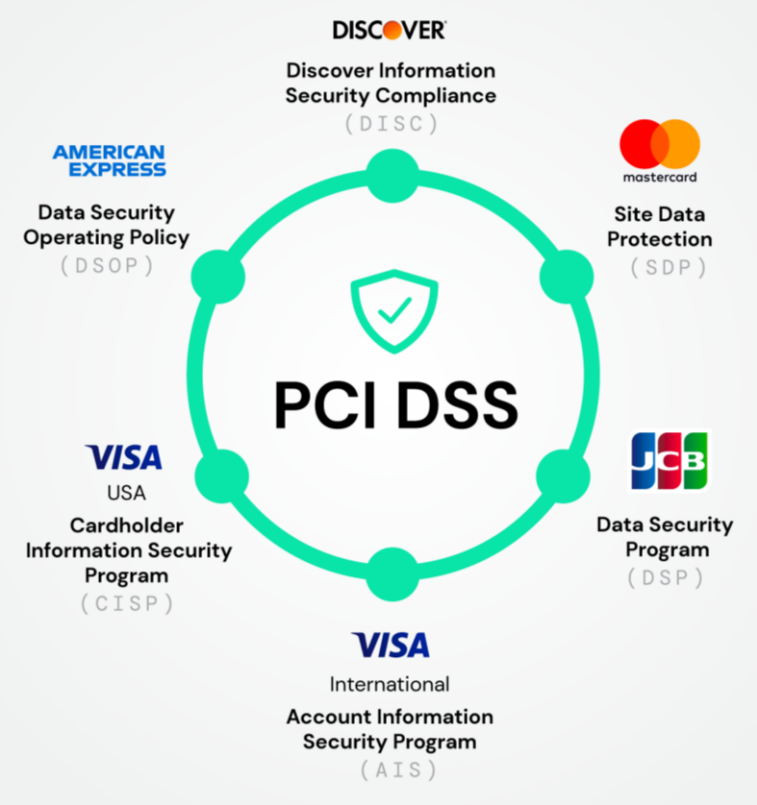
NORMAS E REGULAMENTAÇÕES

GDPR (General Data Protection Regulation) - União Europeia:
Aplicável a organizações que lidam com dados de residentes da União Europeia, o GDPR estabelece requisitos rigorosos para proteger a privacidade e a segurança dos dados pessoais.

NORMAS E REGULAMENTAÇÕES

PCI DSS (Payment Card Industry Data Security Standard):

Esta é um conjunto de normas de segurança de dados que visa proteger informações de cartões de pagamento durante transações.



Estabelecido pelo Conselho de Padrões de Segurança da Indústria de Cartões de Pagamento (PCI SSC), esse padrão é aplicável a qualquer entidade que processe, armazene ou transmita informações de cartões de pagamento, como comerciantes, processadores de pagamento, bancos e provedores de serviços.

... ATIVIDADES