



Olá, Professor!
Peço que realize a **avaliação do conteúdo** com o intuito de manter o nosso material sempre atualizado.

Avalie este
conteúdo! 🚀 ✨



<https://bit.ly/451BDqS>



Segurança cibernética

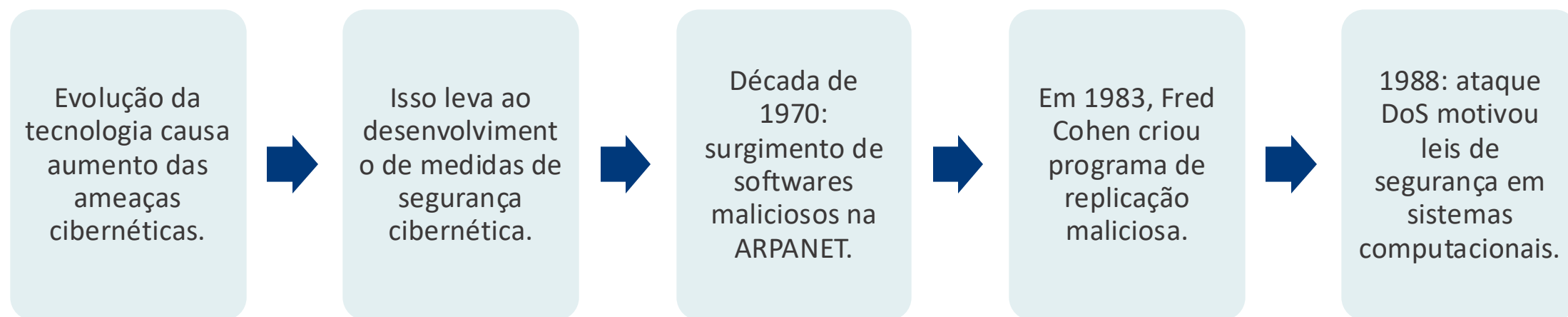


Princípios e conceitos de segurança cibernética



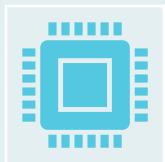
— Histórico da segurança cibernética

Décadas de 1970 e 1980

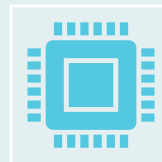


— Histórico da segurança cibernética

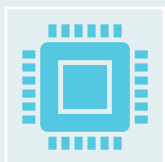
Década de 1990



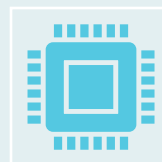
Na década de 1990, a criação da World Wide Web (WWW) estabeleceu a Internet moderna.



A popularização da Internet levou à priorização da segurança em redes e software.



Protocolos iniciais enfatizaram usabilidade, não segurança, resultando em ataques mais frequentes, como o worm Melissa.



A necessidade de soluções abrangentes de cibersegurança se tornou evidente.

— Histórico da segurança cibernética

Anos 2000

No ano 2000, mais de 300 milhões de usuários conectados à Internet.

Aumento da utilização da rede resultou em ataques maiores, como o worm "ILOVEYOU".

Em 2001, a Convenção sobre Crimes Cibernéticos propôs um tratado para entender crimes na Internet, com aval de mais de 60 países.

Em 2002, a União Europeia adotou política de proteção de dados eletrônicos e, em 2003, os EUA criaram sua Divisão Nacional de Segurança Cibernética.

— Histórico da segurança cibernética

Entre 2010 e 2022

- Entre 2010 e 2022, o número de dispositivos eletrônicos cresceu, incluindo automação, Big Data e Inteligência Artificial.
- Aumento da complexidade tecnológica trouxe novos desafios em Segurança Cibernética.
- Incidentes incluíram vazamentos de dados pessoais e ataques de **ransomware e botnets**, como WannaCry e Mirai.



— Histórico da segurança cibernética

Entre 2010 e 2022

Veja como atua cada um desses tipos de malware:



Ransomware

É utilizado por cibercriminosos para criptografia dos dados pessoais do usuário.



Botnet

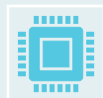
Atua infectando dispositivos para controlá-los remotamente e executa ataques de DDoS.

— Segurança cibernética e da informação

Conceitos



Segurança Cibernética: Medidas para preservar a confidencialidade, integridade e disponibilidade da informação no ciberespaço.



Ciberespaço: Ambiente resultante da interação de pessoas, softwares e serviços na Internet.



Segurança da Informação: Assegura CID (Confidencialidade, Integridade e Disponibilidade) da informação em qualquer meio.

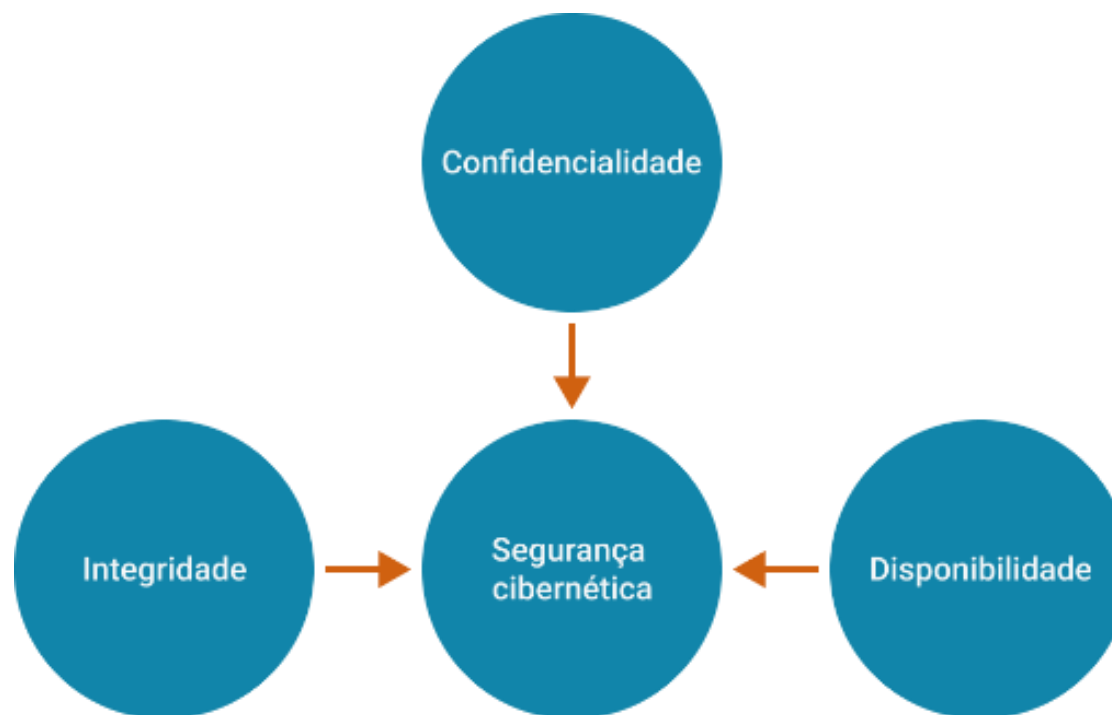


Exemplo de diferença: Informação em carta vs. Informação confidencial armazenada em ativos de TI.

— Segurança cibernética e da informação

Conceitos

Pilares da segurança cibernética:



— Segurança cibernética e da informação

Propriedades adicionais da segurança cibernética

Pilares:

Autenticidade

Não repúdio

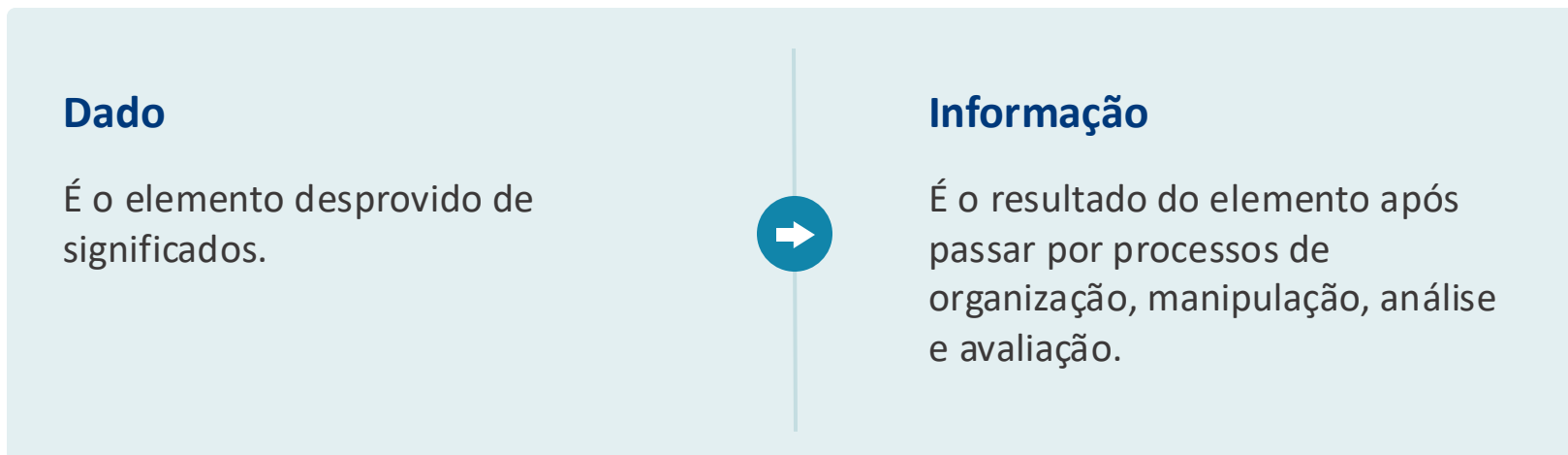
Responsabilidade

Confiabilidade

— Informação e dado

Conceitos

O conceito de **dado** está intrinsecamente associado ao conceito de **informação**:



— Informação e dado

Conceitos



Dados se transformam em informações com significado após organização e análise.



Profissionais de cibersegurança devem identificar onde a informação reside em diferentes ativos e formatos.



Sistema de Informação (SI) reúne, armazena, processa e distribui informações para clientes, funcionários e gestores.



SI pode estar em diversos ativos conectados ao ciberespaço. A proteção de dados é crucial para a segurança das informações de uma organização.

— A classificação da informação

Fatores



Classificação da informação é crucial para a proteção de dados.



Critérios de classificação incluem sensibilidade, valor, requisitos legais e importância.



Informações podem ser classificadas de ultrassecreta a pública.



Classificar informações economiza recursos e ajuda na segurança.

— A classificação da informação

Fatores

A classificação da importância da informação leva em consideração dois princípios:

Presença da informação

Neste caso, a organização já possui a informação.

Ausência da informação

Aqui, se a informação é necessária para a organização, mas não obtida, sua importância é calculada com base no custo de oportunidade.

— O valor da informação

A Importância do Valor

O valor divide-se em 4 tipos:

Valor de uso

Valor de troca

Valor de propriedade

Valor de restrição

— A classificação da informação nos ativos de TI

Procedimentos

Para realizar a classificação do grau de sensibilidade da informação, seguimos estas ações:

Categorizar a informação

Designação de acesso com base em função e relação hierárquica na organização.

Atribuir dono para o ativo de TI

A atribuição de acesso designa um responsável pela autorização de acesso à informação. O detentor não é o dono, mas é responsável pela integridade do ativo de TI.

Etiquetar as informações

Classificação dos ativos de TI com etiquetas ou no conteúdo, dependendo da sensibilidade da informação.

— Gerenciamento de riscos para a proteção de dados

Requisitos

A proteção de dados na segurança cibernética envolve várias medidas. O investimento depende do risco e vulnerabilidade.

Risco

Risco de segurança da informação e cibernética: probabilidade de ameaças explorarem vulnerabilidades, com potencial dano à organização.

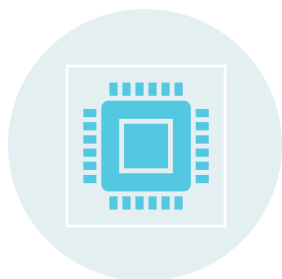


Vulnerabilidade

Risco de segurança pode ser uma fraqueza em um ativo. Sua exploração pela ameaça resulta em um **incidente**.

— Gerenciamento de riscos para a proteção de dados

Requisitos



Gerenciamento de risco é vital para evitar incidentes cibernéticos, com hackers visando redes corporativas.



Eficácia das medidas de segurança deve ser balanceada com custos, considerando o valor dos ativos a proteger.



Riscos podem ser ligados a incertezas financeiras, acidentes naturais, ciberataques, mas podem ser previstos e minimizados com gerenciamento adequado.



O gerenciamento de risco requer avaliação baseada na estratégia de negócios, conformidade legal e objetivos de negócios, considerando o prejuízo financeiro da falta de segurança.

— Análise e avaliação de riscos

Objetivos



Identificação de ativos e seus valores, abrangendo informações, processos e atividades essenciais, além de suporte e infraestrutura.



Determinação de ameaças (intencionais e acidentais) e vulnerabilidades, considerando danos físicos, eventos naturais, falhas técnicas, espionagem, entre outros.



Avaliação da possibilidade das ameaças se concretizarem e impactarem as operações da organização.



Equilíbrio entre o custo do incidente e medidas de segurança, para garantir que os gastos com segurança sejam proporcionais ao valor dos ativos protegidos.

— Tipos de análise do risco

Análise quantitativa

- Análise quantitativa calcula prejuízos financeiros e probabilidade de incidentes.
- Requer identificação de custos de segurança, valor de ativos e considera vulnerabilidades, eficácia das medidas e intervalos prováveis de ameaças.
- Identifica riscos aceitáveis quando medidas de segurança são financeiramente inviáveis.
- Limitações incluem a dificuldade de calcular o valor exato de ativos, especialmente quando seu valor varia com a perda ou indisponibilidade dos dados.



— Tipos de análise do risco

Análise qualitativa

- Análise qualitativa não envolve valores monetários, mas classifica riscos com base na gravidade das ameaças.
- Utiliza experiência, boas práticas e intuição para identificar contramedidas.
- Requer um grupo experiente para propor cenários de ameaças, avaliar perdas potenciais e definir contramedidas.
- Técnicas incluem discussões, pesquisas, questionários e simulações.

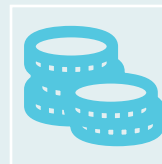


— Valoração dos ativos

Como atribuir valor aos ativos



A valoração de ativos é crucial para segurança da informação e cibernética.



Ativos podem ser valorados quantitativa (em moeda) ou qualitativamente (como insignificante a crítico).



Critérios incluem custo original, custos relacionados a ameaças e impactos na confidencialidade, integridade, disponibilidade e reputação.



Outros critérios podem ser adicionados, considerando o contexto organizacional, e a dependência de processos aumenta o valor do ativo.

— Valoração dos ativos

Como atribuir valor aos ativos

Para facilitar o processo de valoração de ativos dependentes, é importante verificar as seguintes situações:

Valores menores ou iguais

Caso os valores de ativos dependentes, como os dados, sejam menores ou iguais ao valor do ativo em questão, como o computador, o valor do último permanece o mesmo.

Valores maiores

Caso os valores dos ativos dependentes sejam maiores que do ativo em questão, é recomendável que o valor desse último se eleve de acordo com o grau de dependência ou valores dos outros ativos.

— Avaliação do impacto do risco

Critérios para avaliação



A avaliação do impacto do risco é crucial após a valoração dos ativos.



O impacto pode variar de acordo com a maturidade da proteção de dados e o tipo de impacto, seja imediato (operacional) ou futuro (relativo aos negócios).



O impacto imediato pode ser direto (valor financeiro de substituição, custo de aquisição, custo das transações suspensas) e indireto (custo de oportunidade, mau uso de informações, violações regulatórias e éticas).



O mesmo incidente pode causar danos diferentes em organizações diferentes, dependendo de vários fatores, incluindo financeiros e de mercado.

— Avaliação do impacto do risco

Estimativa do impacto financeiro associado a ameaças

Existem fórmulas que auxiliam na determinação de valores monetários, como:

EF (*exposure factor*)

SLE (*single loss expectancy*)

ARO (*annualized rate of occurrence*)

ALE (*annualized loss expectancy*)

— Mitigação do risco

Estratégias

Após avaliar ativos e impacto, elaboramos estratégias de tratamento de risco. Existem três tipos comuns:

1

Prevenção ou anulação do risco.

2

Tolerância ao risco.

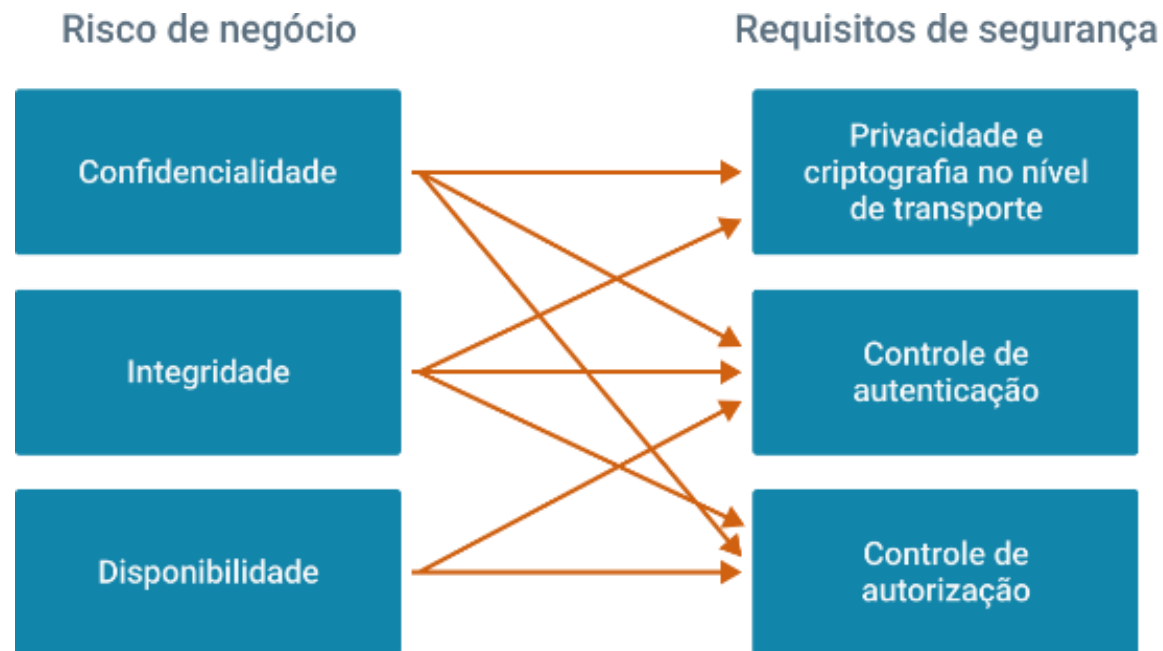
3

Redução ou minimização do risco.

— Mitigação do risco

Estratégias

Cada propriedade da segurança cibernética poderá ser preservada de acordo com os seguintes requisitos:



— Mitigação do risco

Tratamento do risco

Após a triagem dos riscos, a organização planeja medidas de tratamento, que podem incluir:

- Aplicar os devidos controles de segurança para redução dos riscos.
- Aceitar racional e objetivamente os riscos.
- Evitar que o risco se torne incidente.
- Transferir o risco a terceiros, como fornecedores ou seguradoras, caso haja responsabilidade desses entes.
- Implementar controles definidos para lidar com o risco.

— Mitigação do risco

Tratamento do risco

Especificamente em relação à estratégia de redução do risco, deve-se implementá-la de acordo com os seguintes aspectos:

Objetivos da organização

Normas da legislação e eventuais regulamentos nacionais ou internacionais

Restrições e requisitos das operações da organização

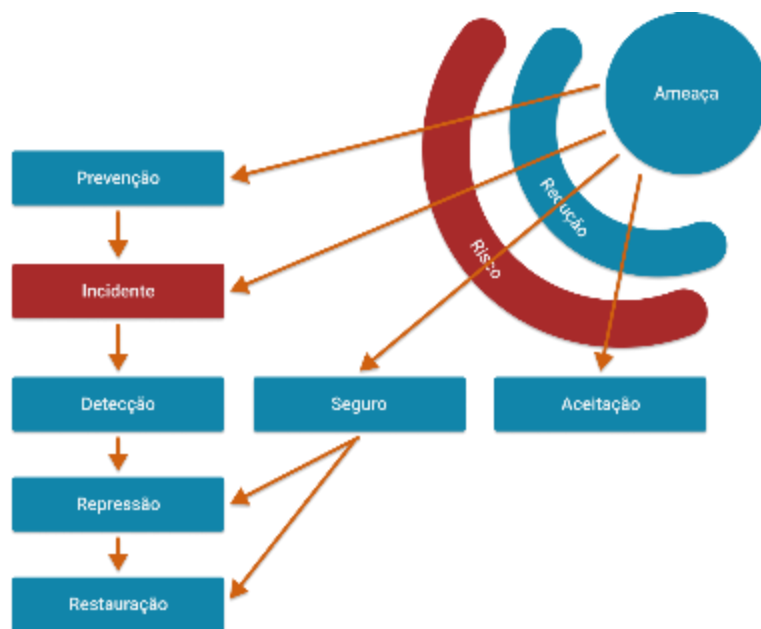
Equilíbrio de investimento entre o custo de mitigar o risco e o dano causado

Custo de adoção e operacionalização da medida de tratamento de risco proporcional às limitações.

— Mitigação do risco

Contramedidas para mitigação do risco

Análise de riscos estruturada propõe contramedidas para minimizar consequências e reduzir chances de incidentes.



Contramedidas de mitigação do risco.

— Conceituação do plano de cibersegurança

Características do plano



O plano de cibersegurança abrange medidas gerais para proteger ativos cibernéticos.



Objetiva minimizar desperdício de recursos e prevenir danos causados por incidentes cibernéticos.



Não há um modelo único, cada organização mapeia riscos de forma única.

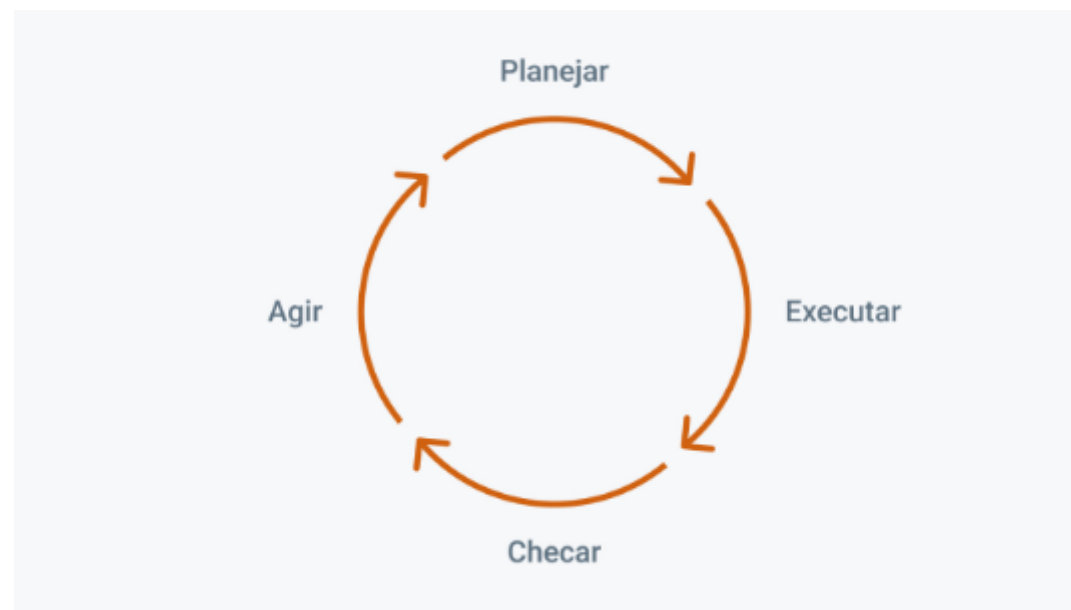


As ações incluem descrever situação atual, estado ideal, identificar oportunidades, avaliar maturidade e comunicação.

— Conceituação do plano de cibersegurança

Características do plano

Modelo **PDCA** (*Plan-Do-Check-Act*):



— Conceituação do plano de cibersegurança

Características do plano

Com o ciclo PDCA, dispomos de uma forma dinâmica e ampla para criarmos, executarmos, monitorarmos e melhorarmos o plano de cibersegurança.



Fases do plano de cibersegurança.

— Estruturação do plano de cibersegurança

Fases do plano

Identificação

- Identificação inclui listar ativos, responsabilidades, missões, importância no setor e governança.
- Priorização de ativos com base em valor e criticidade.
- Estabelecimento de responsabilidades para segurança cibernética.
- Avaliação de impacto, ameaças, vulnerabilidades e riscos a serem tolerados ou mitigados.



— Estruturação do plano de cibersegurança

Fases do plano

Proteção



Checagem de emissão, gerenciamento e revogação de identidades e credenciais.

- Auditoria de dispositivos, usuários e processos.
- Gerenciamento de acesso, integridade de rede e segurança de dados.
- Conscientização, backups, planos de resposta, gerenciamento de vulnerabilidades e logs de auditoria.

— Estruturação do plano de cibersegurança

Fases do plano

Detecção

- Identificar e gerenciar comportamento normal e anômalo.
- Coletar, analisar e alertar sobre eventos.
- Monitorar rede, ambiente e acesso não autorizado.
- Melhorar continuamente a detecção de ameaças.



— Estruturação do plano de cibersegurança

Fases do plano

Resposta



Encadeamento de medidas em plano de resposta cibernética.

- Conscientização do pessoal sobre funções e atividades.
- Comunicação consistente de incidentes.
- Cooperação com parceiros, compartilhamento de informações e aprendizado com incidentes passados.

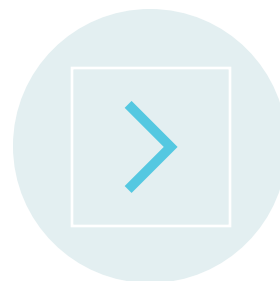
— Estruturação do plano de cibersegurança

Fases do plano

Recuperação



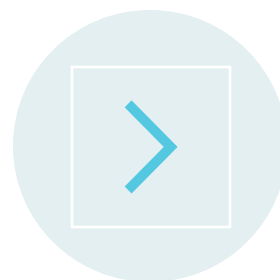
Encadeamento das medidas no plano de recuperação.



Incorporação de lições aprendidas de incidentes anteriores.



Atualização contínua das estratégias de recuperação de ativos.



Gerenciamento de relações públicas para mitigar impactos na reputação e comunicação com todas as partes interessadas.

Análise das vulnerabilidades e dos tipos de ataques

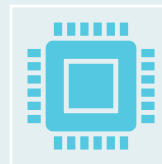


— O que é mapeamento de redes?

Definição



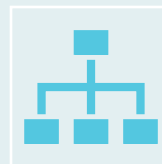
Mapeamento de redes é a identificação de hosts, sistemas operacionais e serviços em uma rede.



Utiliza ferramentas que manipulam pacotes de protocolos como TCP, UDP e ICMP.



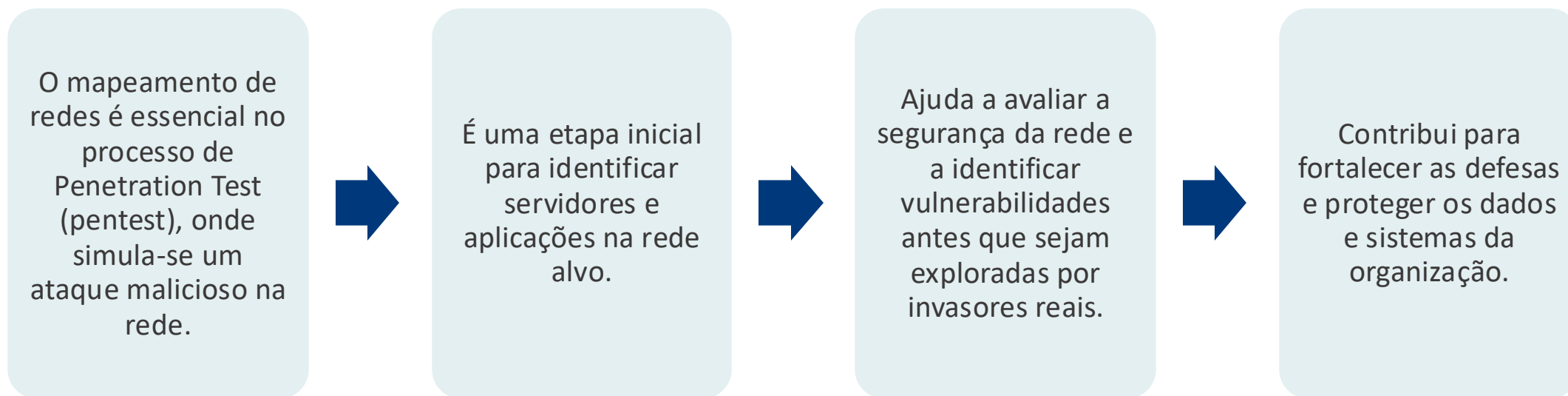
Serve para administradores de rede otimizarem seu ambiente, mas também pode ser explorado por atacantes.



Importante para compreender a estrutura e funcionamento da rede.

— O que é mapeamento de redes?

Aplicações



— O que é mapeamento de redes?

Fases

O mapeamento de redes envolve as seguintes fases:



Host Scan: Identifica servidores, máquinas e dispositivos na rede.



Port Scan: Descobre as portas TCP e UDP abertas nesses servidores.



Service Scan/OS fingerprint: Identifica os serviços e sistema operacional dos servidores.



Varredura de Vulnerabilidades: Pesquisa as vulnerabilidades nos servidores.

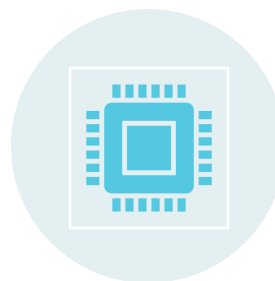
É importante realizar o Host Scan antes de qualquer outra varredura para uma abordagem organizada e eficaz.

— O que é mapeamento de redes?

Hot Scan – ferramenta ping



O "ping" é uma ferramenta comum que usa ICMP para verificar a disponibilidade de uma máquina, gerando ICMP Reply em resposta.



"fping" é uma ferramenta que envia pacotes ICMP para várias máquinas simultaneamente, eficaz para Host Scan.



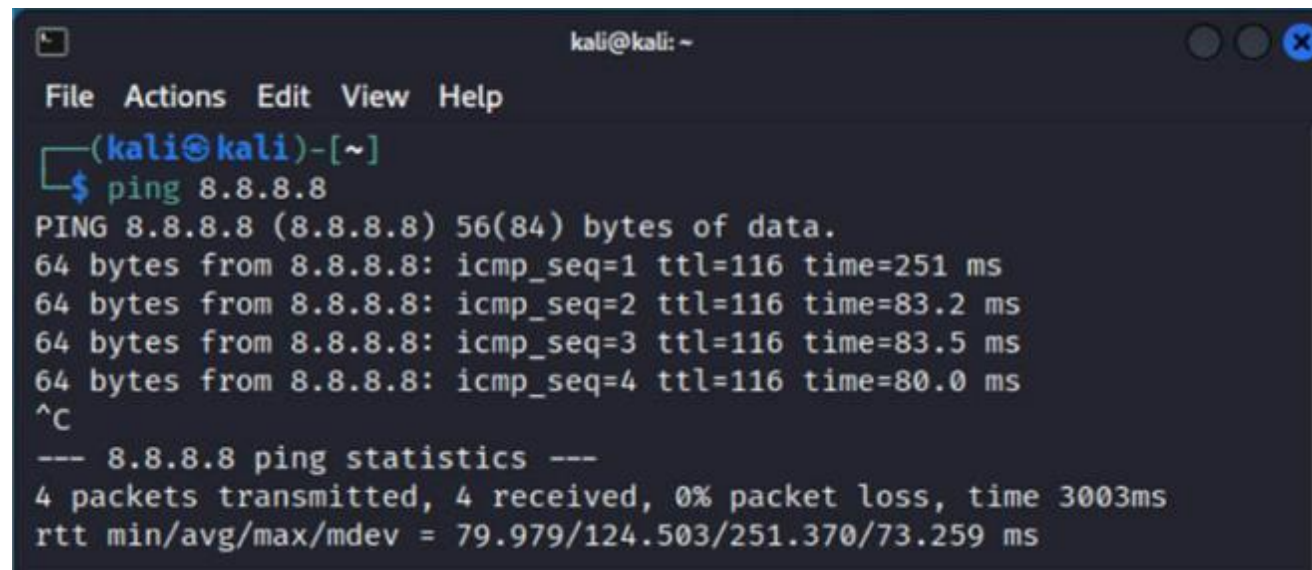
Ambas as ferramentas ajudam a identificar máquinas ativas na rede.



São usadas para verificação de conectividade e descoberta de dispositivos na rede.

— O que é mapeamento de redes?

Hot Scan – ferramenta ping

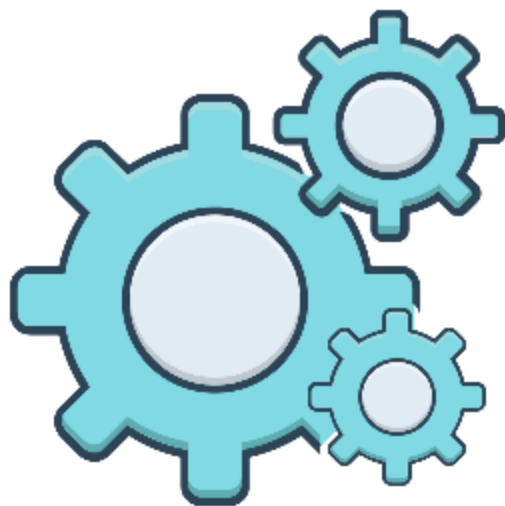


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=251 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=83.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=83.5 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=80.0 ms  
^C  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 79.979/124.503/251.370/73.259 ms
```

Captura de tela da ferramenta de linha comando ping.

— O que é mapeamento de redes?

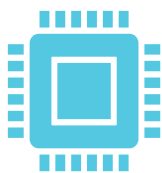
Ferramenta nmap



O Nmap é uma ferramenta poderosa que mapeia redes, identifica portas, serviços e vulnerabilidades, e até mesmo o sistema operacional de hosts remotos.

— O que é mapeamento de redes?

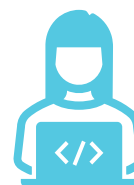
Hot Scan – nmap



O Nmap realiza o Host Scan de forma abrangente, testando diferentes tipos de pacotes ICMP e verificando as portas 443 e 80 do protocolo TCP.



O Nmap, por padrão, começa verificando a disponibilidade do host e, se ativo, realiza uma varredura nas mil portas mais comuns.



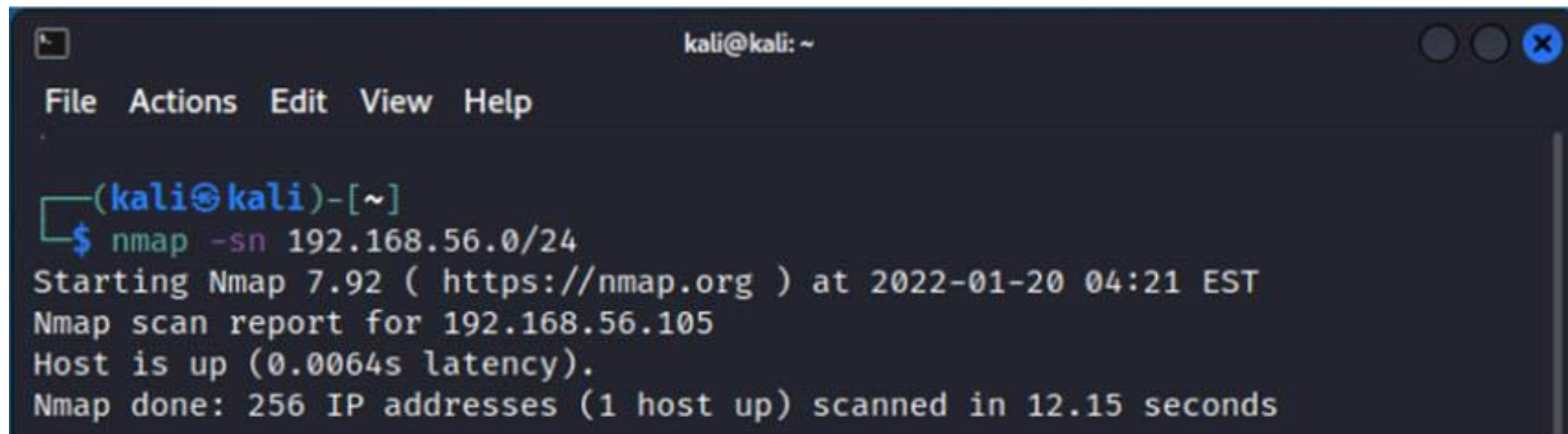
A opção '-sn' é usada para instruir o Nmap a verificar apenas a disponibilidade dos hosts.



O Nmap identifica os hosts ativos na rede e fornece informações detalhadas sobre eles, como o endereço IP 192.168.56.105 na captura de tela.

— O que é mapeamento de redes?

Hot Scan – nmap

A screenshot of a terminal window with a dark background. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a prompt '(kali@kali)-[~]' followed by the command '\$ nmap -sn 192.168.56.0/24'. The output of the command is displayed below: 'Starting Nmap 7.92 (https://nmap.org) at 2022-01-20 04:21 EST', 'Nmap scan report for 192.168.56.105', 'Host is up (0.0064s latency).', and 'Nmap done: 256 IP addresses (1 host up) scanned in 12.15 seconds'.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -sn 192.168.56.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 04:21 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.0064s latency).  
Nmap done: 256 IP addresses (1 host up) scanned in 12.15 seconds
```

Captura de tela de Host Scan com a ferramenta nmap na rede 192.168.56.0/24.

— O que é mapeamento de redes?

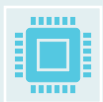
Hot Scan – nmap

A tabela mostra outras possibilidades de como escolher os endereços de ip a serem testados pela ferramenta.

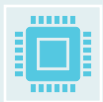
Opção	Explicação
\$ nmap -sn 192.168.56.105	Teste no endereço de ip 192.168.56.105
\$ nmap -sn 192.168.56.0/24	Teste nos endereços de ip de 192.168.56.1 até 192.168.56.255.
\$ nmap -sn 192.168.56.1-100	Teste nos endereços de ip de 192.168.56.1 até 192.168.56.100.
\$ nmap -sn -iL arquivo.txt	Teste nos endereços de ip escritos no arquivo.txt. O arquivo deve possuir um endereço de ip por linha.

— Mapeamento de Portas com nmap

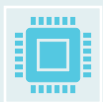
Como funciona um mapeamento de portas?



O mapeamento de portas identifica portas TCP e UDP abertas em servidores.



O nmap é uma ferramenta para realizar Port Scans, como a varredura das mil portas mais comuns.



A saída do nmap exibe números de portas, status 'open' para portas abertas e serviços associados.

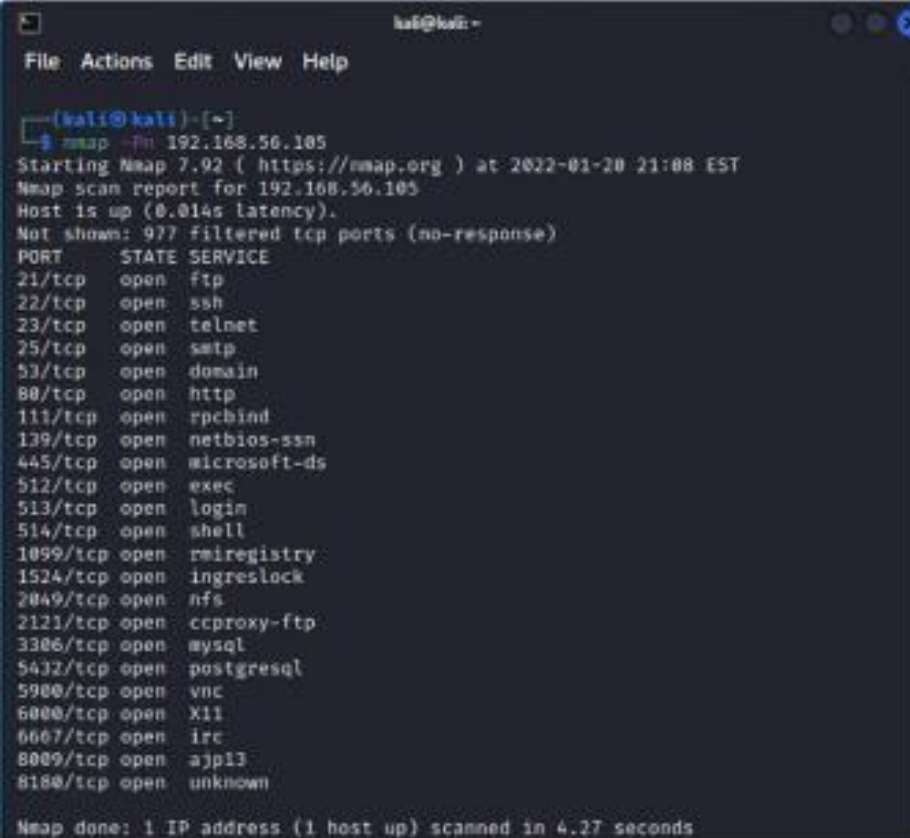


A opção '-Pn' no nmap evita o Host Scan quando a rede já tem máquinas ativas.

— Mapeamento de Portas com nmap

Como funciona um mapeamento de portas?

Captura de tela da saída do Port Scan realizado com a ferramenta nmap.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -Pn 192.168.56.105  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 21:08 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.014s latency).  
Not shown: 977 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8089/tcp  open  ajp13  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 4.27 seconds
```

— Mapeamento de Portas com nmap

Como funciona um mapeamento de portas?

A tabela a seguir mostra outras opções relacionadas ao Port Scan.

Opção	Explicação
\$ nmap -Pn 192.168.56.105 -p 22,80,443	Faz a varredura apenas nas portas 22,80 e 443.
\$ nmap -Pn 192.168.56.105 -p 20-80	Faz a varredura em todas as portas de 20 até 80, inclusive.
\$ nmap -Pn 192.168.56.105 -p-	Faz a varredura em todas as portas TCP, ou seja, da porta 1 até a porta 65535.
\$ nmap -Pn 192.168.56.105 -p T:80,U:53	Faz a varredura na porta 80 TCP e na porta 53 UDP.
\$ nmap -Pn 192.168.56.105 --top-ports=100	Faz a varredura nas 100 portas mais utilizadas no mundo.

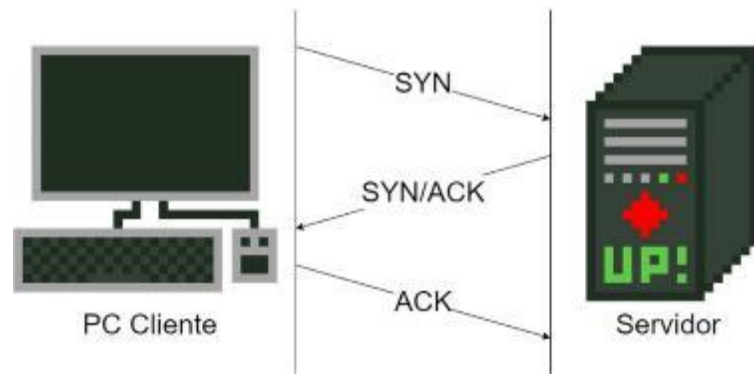
— Mapeamento de Portas com nmap

Port Scan padrão do nmap

- O Port Scan padrão executado pelo nmap depende do usuário que está executando.
- Se for um usuário comum do sistema, será executado o TCP Connect Scan, e se for um usuário privilegiado, como root do Linux ou o Administrador do Windows, será executado o TCP SYN Scan.

— Mapeamento de Portas com nmap

3-Way Handshake



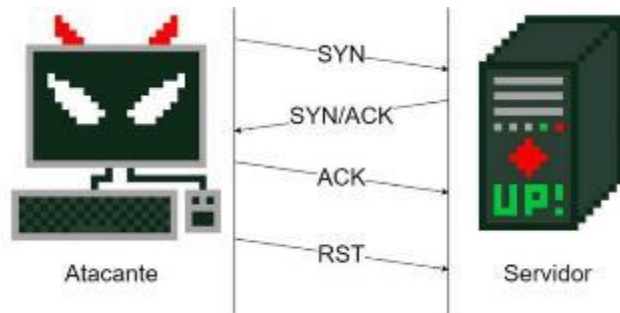
O 3-way handshake é a etapa de estabelecimento de conexão no protocolo TCP.

- Envolve a troca de 3 pacotes: SYN do cliente, SYN/ACK do servidor e ACK do cliente.
- Esse processo garante confiabilidade na conexão TCP, iniciando-a de forma segura.

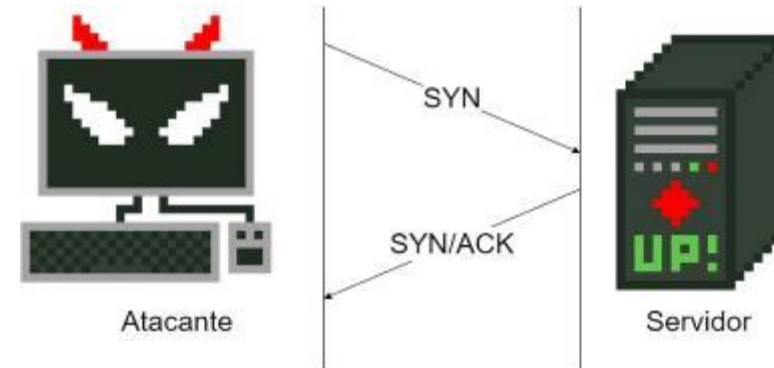
— Mapeamento de Portas com nmap

Port Scan com TCP Connect Scan

TCP Connect Scan: Testa se porta está aberta com 3-Way Handshake; RST confirma status da porta.



Processo de Port Scan com TCP Connect Scan quando a porta do servidor está aberta.

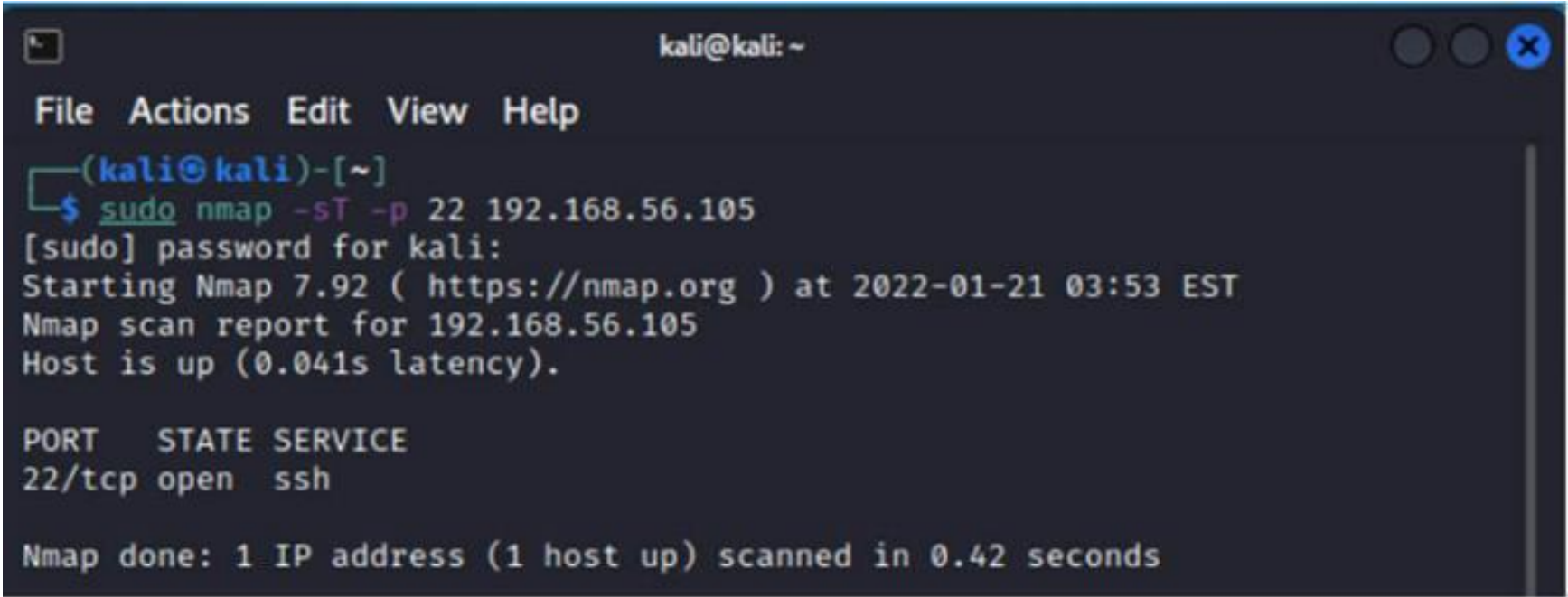


Processo de Port Scan TCP Connect Scan quando a porta do servidor está fechada.

— Mapeamento de Portas com nmap

Port Scan com TCP Connect Scan

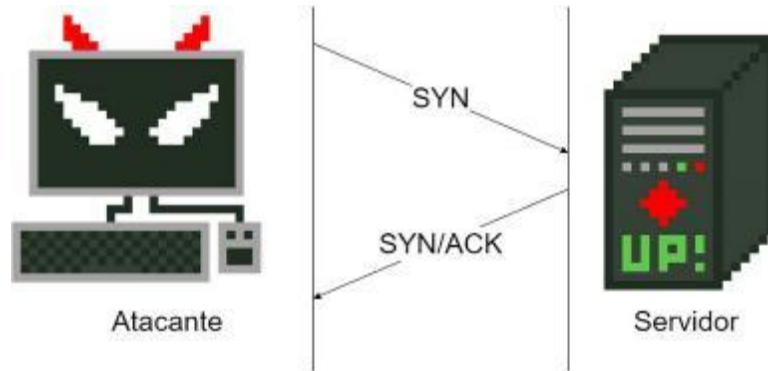
Para forçar o *nmap* a utilizar esse método, deve-se usar a opção '-sT' na linha de comando.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sT -p 22 192.168.56.105  
[sudo] password for kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 03:53 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.041s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

— Mapeamento de Portas com nmap

Port Scan com TCP SYN Scan



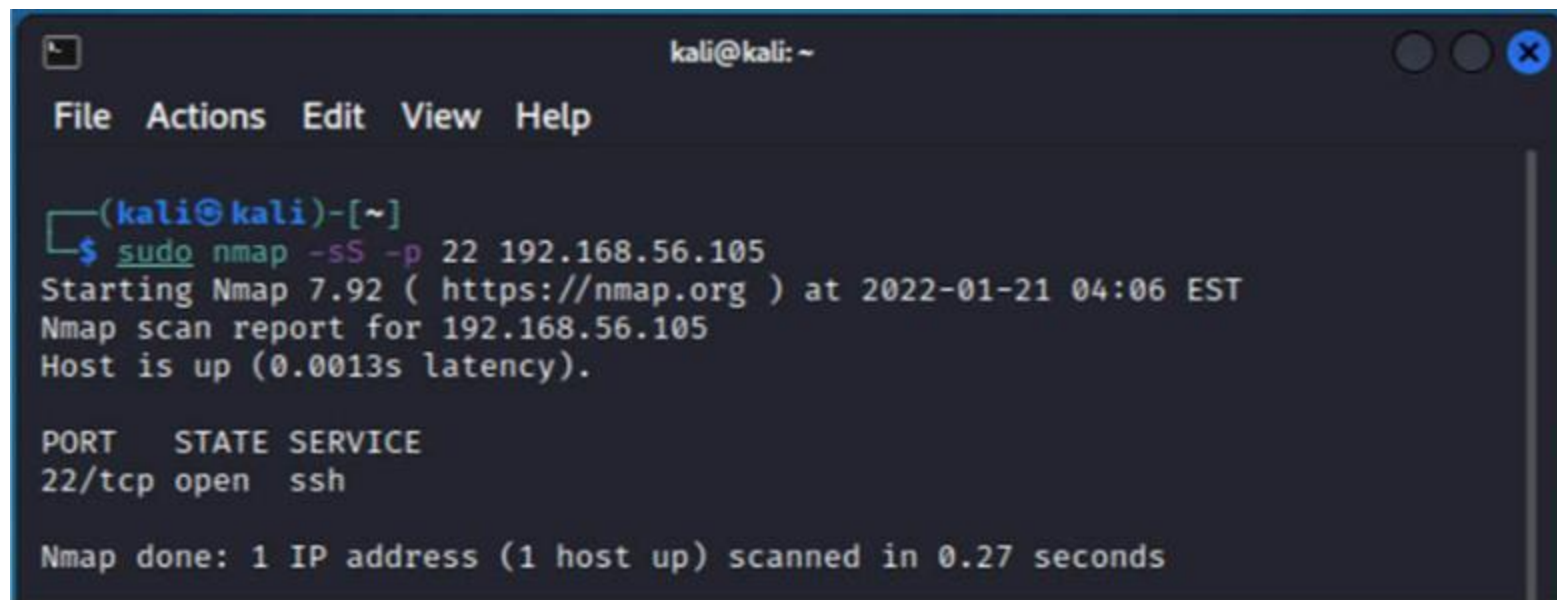
TCP SYN Scan: Envio de pacotes SYN e aguardo de resposta do servidor.

- Resposta SYN/ACK indica porta aberta; resposta RST indica porta fechada.
- Método mais rápido e discreto do que o 3-Way Handshake completo.
- Útil para mapear portas de maneira eficiente e rápida.

— Mapeamento de Portas com nmap

Port Scan com TCP SYN Scan

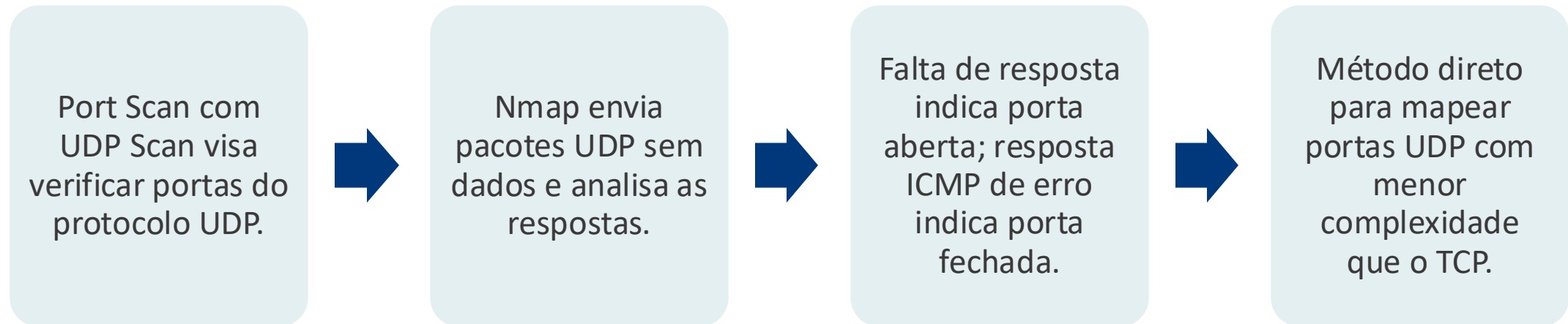
Pode-se usar a opção '-sS' na linha de comando para obrigar o nmap a fazer a varredura com esse método.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sS -p 22 192.168.56.105  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 04:06 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.0013s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

— Mapeamento de Portas com nmap

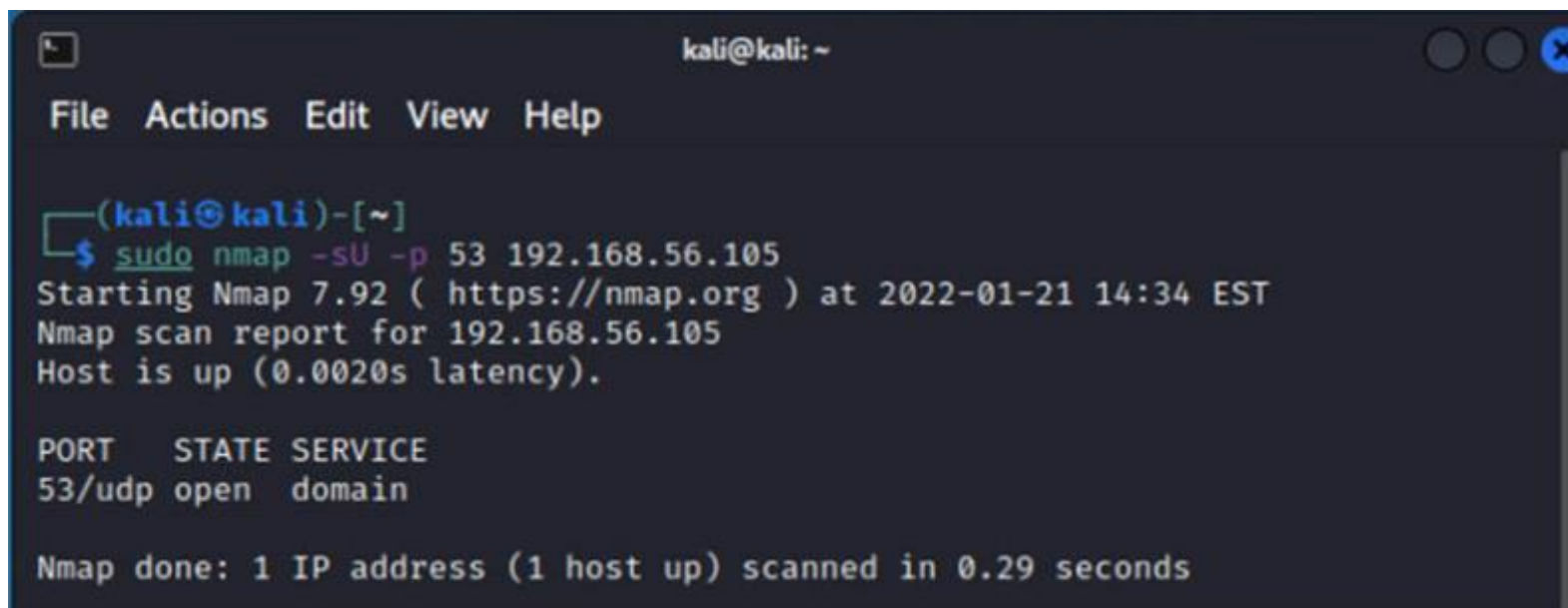
Port Scan com UDP Scan



— Mapeamento de Portas com nmap

Port Scan com UDP Scan

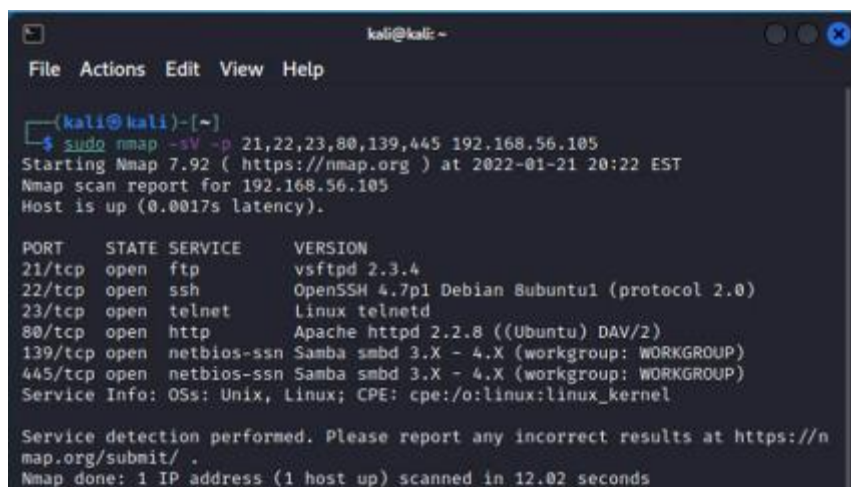
Para executar essa varredura, pode-se utilizar a opção '-sU' na linha de comando.

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The command entered is '\$ sudo nmap -sU -p 53 192.168.56.105'. The output shows 'Starting Nmap 7.92 (https://nmap.org) at 2022-01-21 14:34 EST', 'Nmap scan report for 192.168.56.105', and 'Host is up (0.0020s latency)'. A table follows with columns 'PORT', 'STATE', and 'SERVICE', containing one row: '53/udp open domain'. At the bottom, it says 'Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds'.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sU -p 53 192.168.56.105  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 14:34 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.0020s latency).  
  
PORT      STATE SERVICE  
53/udp    open  domain  
  
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```


— Mapeamento de vulnerabilidades

Service Scan



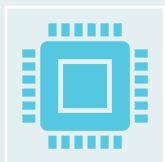
```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo nmap -sV -p 21,22,23,80,139,445 192.168.56.105  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 20:22 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.0017s latency).  
  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 12.02 seconds
```

Service Scan: Identifica serviços e suas versões em portas abertas.

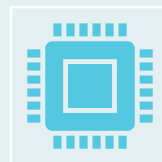
- Usa pacotes para estabelecer conexão e solicitar informações sobre serviços.
- Opção '-sV' no nmap habilita essa varredura detalhada.
- Fornece informações detalhadas sobre os serviços em execução nos hosts.

— Mapeamento de vulnerabilidades

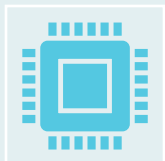
OS Fingerprint



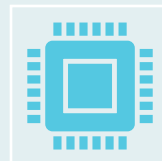
OS Fingerprint: Identifica o sistema operacional do servidor.



Baseia-se em diferenças na implementação de redes e serviços entre sistemas.



Usa informações como o TTL (Time to Live) em pacotes para determinar o sistema.



TTL padrão varia entre sistemas, fornecendo pistas para a identificação.

— Mapeamento de vulnerabilidades

OS Fingerprint

Tabela – TTL de sistemas operacionais no protocolo ICMP.

Sistema Operacional	TTL padrão
FreeBSD 5	64
Windows 10	128
Linux Kernel 2.4	255

— Mapeamento de vulnerabilidades

OS Fingerprint

Para que o nmap tente descobrir qual o sistema operacional de um alvo, pode-se utilizar a opção '-O'.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ sudo nmap -sV -p 21,22,23,80,139,445 -O 192.168.56.105  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 20:42 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge|general purpose|switch  
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450  
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (88%)  
No exact OS matches for host (test conditions non-ideal).  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.03 seconds
```

— Mapeamento de vulnerabilidades

Scripts do nmap

O nmap possui vários scripts com diferentes funções e categorias. Duas categorias importantes para a descoberta de vulnerabilidades são default e vuln.

— Mapeamento de vulnerabilidades

Scripts do nmap

Os *scripts* da categoria default são simples, de rápida execução e dão informações básicas sobre os serviços. Para executá-los, pode-se executar o *nmap* com a opção '*--script "default"*' ou com a opção '*-sC*'.



— Mapeamento de vulnerabilidades

Categoria vuln

Os scripts da categoria vuln buscam, dentro dos serviços selecionados, vulnerabilidades conhecidas e fáceis de identificar, sem explorá-las. Para executar esses scripts, pode-se utilizar a opção '--script "vuln"'.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ nmap --script "vuln" -p 21 192.168.56.105  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 01:32 EST  
Nmap scan report for 192.168.56.105  
Host is up (0.0039s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
ftp-vsftpd-backdoor:  
  VULNERABLE:  
    vsFTPD version 2.3.4 backdoor  
    State: VULNERABLE (Exploitable)  
    IDs:  BID:48539  CVE:CVE-2011-2523  
    vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.  
    Disclosure date: 2011-07-03  
    Exploit results:  
      Shell command: id  
      Results: uid=0(root) gid=0(root)  
    References:  
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523  
      https://www.securityfocus.com/bid/48539  
      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html  
      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_ba  
ckdoor.rb  
  
Nmap done: 1 IP address (1 host up) scanned in 13.78 seconds
```

— Tipos de vulnerabilidades

Definição

Atacantes usam informações de varredura para realizar ataques direcionados.

Vulnerabilidades variam de configurações inadequadas a Buffer Overflow.

Incluem credenciais fracas e vulnerabilidades zero-day.

Ataques podem ser de origem externa ou interna.

— Tipos de vulnerabilidades

Erros em configuração de serviços



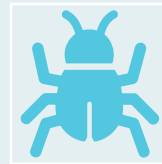
Erros de configuração ocorrem quando serviços são implementados rapidamente e descuidadamente.



Exemplo: credenciais padrão no serviço de FTP, como "anonymous" sem senha.



Isso pode permitir que um atacante acesse informações do sistema facilmente.



Tais erros comprometem a segurança do serviço.

— Tipos de vulnerabilidades

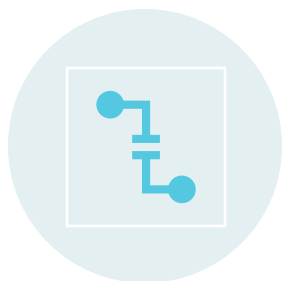
Buffer Overflow

A vulnerabilidade de buffer overflow, ou estouro de buffer, permite que, ao enviar determinados dados para uma aplicação, seja possível a manipulação do comportamento do software responsável por essa aplicação.



— Tipos de vulnerabilidades

Buffer Overflow na função strcpy() em C



Vulnerabilidade em Buffer Overflow: Problema ocorre quando a função `strcpy()` em C não limita a quantidade de caracteres copiados.



Se a string de origem for maior que a de destino, a função pode escrever além dos limites da memória alocada.



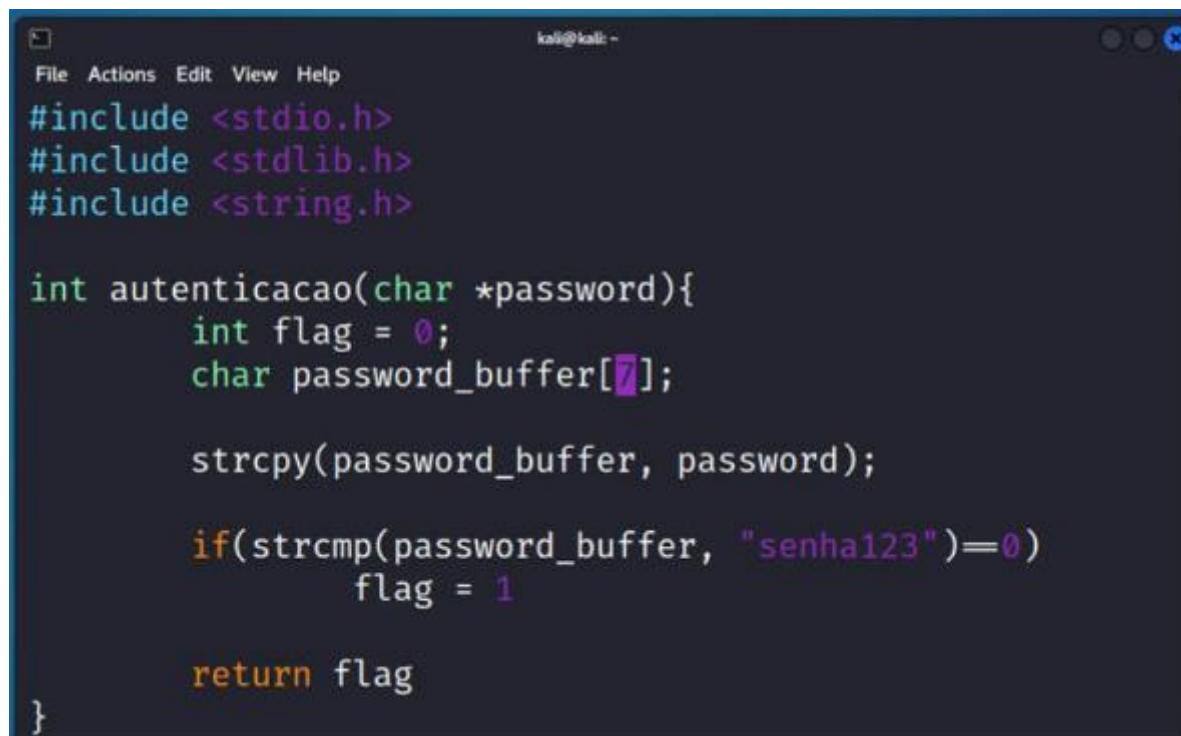
Neste exemplo, a função autenticação usa `strcpy` para copiar a senha para `password_buffer`.



Se um atacante enviar caracteres extras, pode sobrescrever outros dados na memória, como a variável "flag". Isso pode ser explorado para alterar a variável e comprometer a autenticação.

— Tipos de vulnerabilidades

Buffer Overflow na função strcpy() em C



```
kali@kali: -
File Actions Edit View Help
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int autenticacao(char *password){
    int flag = 0;
    char password_buffer[7];

    strcpy(password_buffer, password);

    if(strcmp(password_buffer, "senha123")==0)
        flag = 1

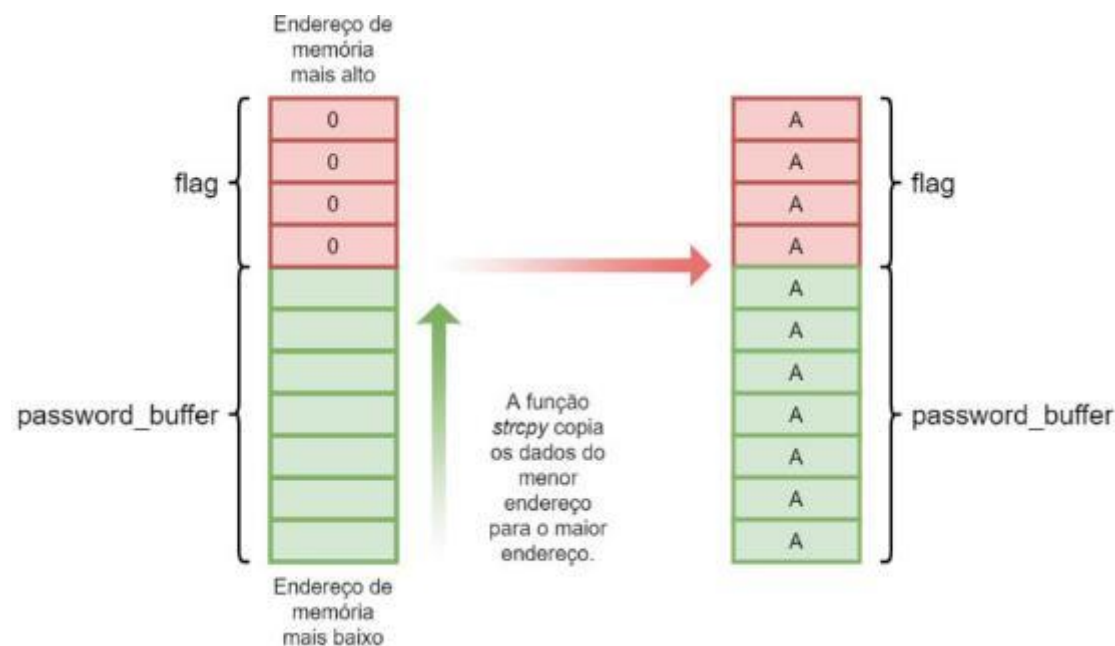
    return flag
}
```

Captura de tela de código vulnerável da função autenticação no software vim.

— Tipos de vulnerabilidades

Buffer Overflow na função strcpy() em C

A imagem a seguir é apenas uma representação de como o ataque funciona, não sendo fiel ao ambiente real.



— Tipos de vulnerabilidades

Credenciais fracas

Senhas fracas são graves problemas de segurança, facilitando ataques.

Atacantes usam ferramentas para testar senhas rapidamente.

Duas abordagens comuns: ataque de bruteforce (tentando todas as combinações possíveis) e dictionary attack (usando listas de palavras-chave comuns).

Complexidade de senha é essencial para melhorar a segurança.

— Tipos de vulnerabilidades

Ataques de dicionário

Ataques de dicionário buscam senhas testando uma lista predefinida de palavras ou combinações.



Usam wordlists, listas de senhas comuns, como "rockyou," que incluem senhas populares, como "iloveyou" e "password."



Atacam alvos com senhas previsíveis, como códigos PIN de 4 dígitos ou senhas óbvias baseadas em datas, como o ano de nascimento.

— Tipos de vulnerabilidades

Vulnerabilidades 0-day ou zero-day

Vulnerabilidades 0-day (ou zero-day) são falhas descobertas por atacantes antes de serem corrigidas pelo desenvolvedor.

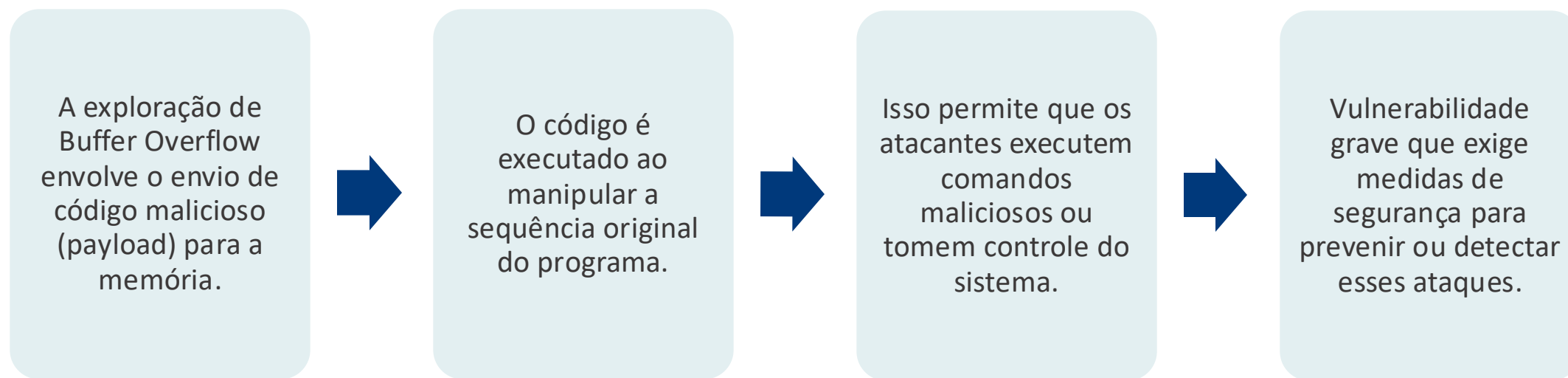
São "0-day" porque o desenvolvedor não teve tempo (0 dias) para criar uma correção.

São altamente perigosas, pois os atacantes podem explorá-las com alta probabilidade de sucesso, uma vez que não há correção disponível.

Representam uma grande ameaça à segurança, exigindo respostas rápidas e soluções alternativas.

— Exploração das vulnerabilidades

Exploração de Buffer Overflow



— Exploração das vulnerabilidades

Os registradores

- Os registradores fazem parte do processador de um computador. Seu tamanho, em computadores de 64 bits é de 8 bytes, ou 64 bits.
- Eles são usados para armazenar informações para execução de cálculos no processador.



— Exploração das vulnerabilidades

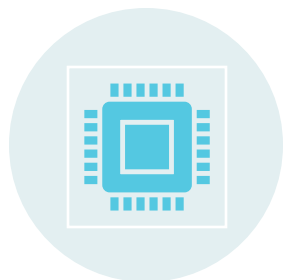
O registrador EIP



- Um dos registradores mais importantes é o EIP (Extended Instruction Pointer, ou ponteiro para instruções estendido).
- Ele é responsável por indicar ao processador qual instrução será executada.

— Exploração das vulnerabilidades

O que são instruções?



Instruções são operações básicas em linguagem de máquina executadas pelo processador.



Um compilador traduz o código de linguagem de programação em sequências de instruções de máquina.



Cada instrução tem um código chamado de opcode específico para cada tipo de processador.



Exemplos de instruções incluem operações como soma, subtração, multiplicação e operações lógicas, como xor e or.

— Exploração das vulnerabilidades

Como alterar o EIP?



No contexto de programação em C, o registro EIP (Instruction Pointer) armazena o endereço da próxima instrução a ser executada.



Quando uma função é chamada, o valor de EIP é alterado para apontar para o código dessa função.



Para retornar à função de chamada, o endereço de EIP é salvo na memória (geralmente na pilha) para posterior restauração.

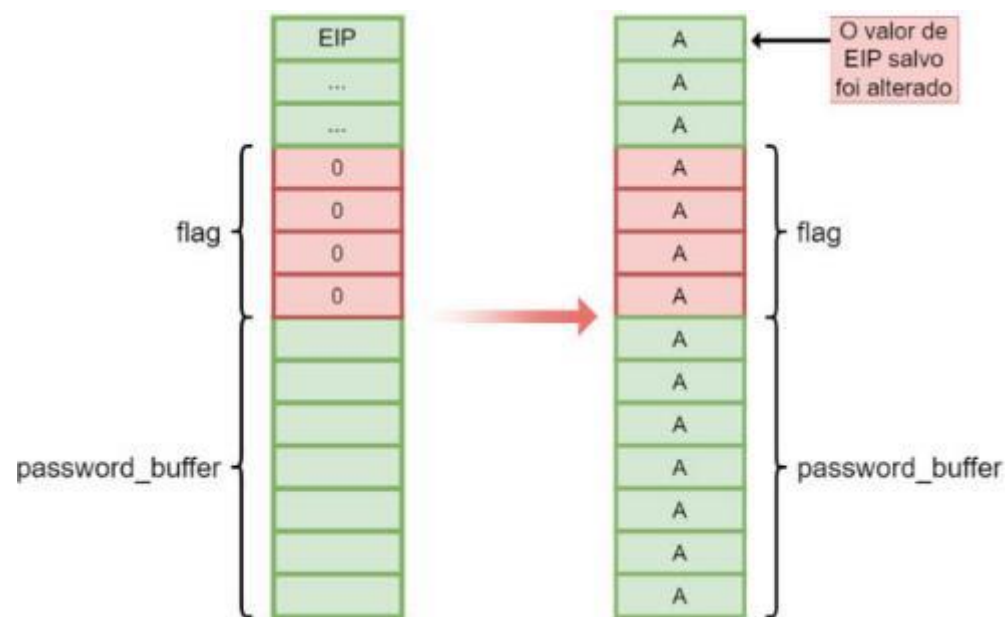


A técnica de buffer overflow permite a modificação do valor de EIP, o que pode levar à execução de código malicioso e à alteração do comportamento normal do programa.

— Exploração das vulnerabilidades

Como alterar o EIP?

Valor de EIP alterado com buffer overflow.



— Exploração das vulnerabilidades

Para onde aponta o novo EIP?



Atacantes alteram valores na memória e enviam código malicioso com o novo valor do EIP.



EIP, que apontava para o endereço de retorno, é redirecionado para código malicioso.



Isso é ilustrado na imagem, onde o EIP é redirecionado para o código do atacante.



Podem criar acesso via Bind Shell ou Reverse Shell.

— Exploração das vulnerabilidades

Bind Shell

A bindshell é um tipo de código enviado através de payload, que abre uma porta em um servidor.



— Exploração das vulnerabilidades

Bind Shell

Com a porta aberta, o atacante se conecta a essa porta e a *bindshell* dá acesso a uma linha de comando no servidor alvo.



— Exploração das vulnerabilidades

Reverse Shell

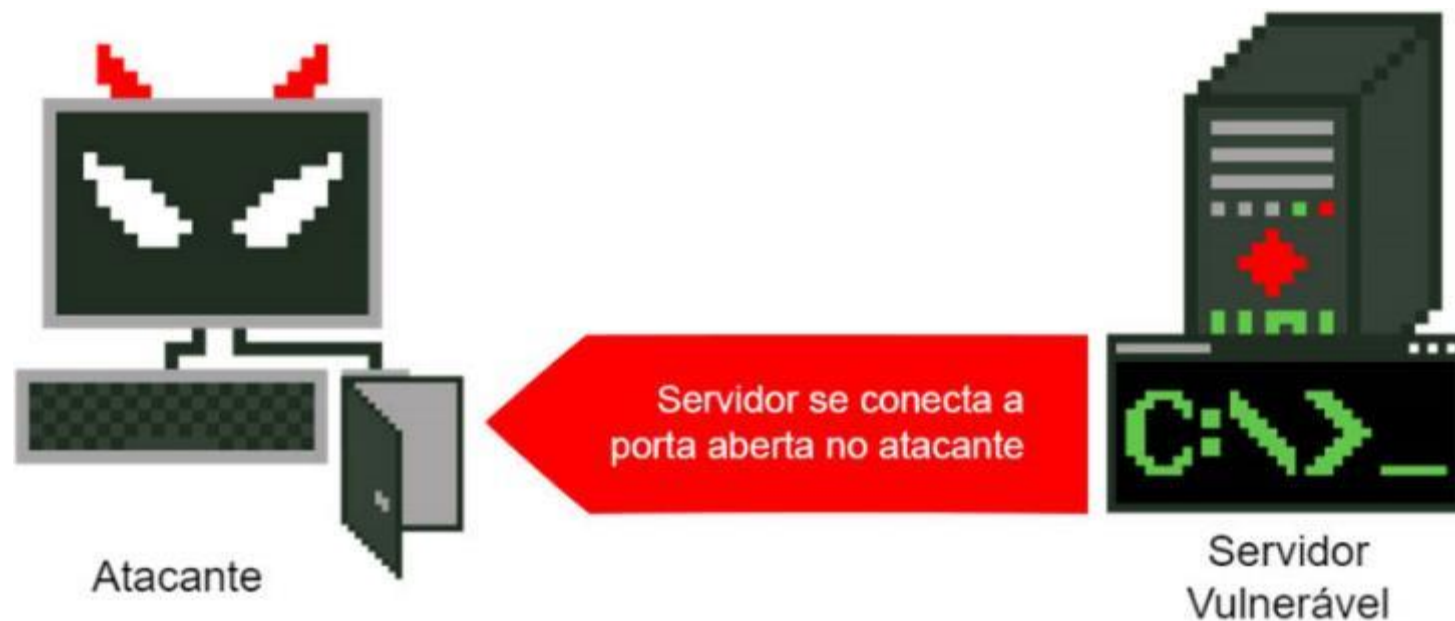
Reverse shell, ou shell reversa, é um código malicioso enviado para o servidor com o objetivo de que ele se conecte ao atacante.



— Exploração das vulnerabilidades

Reverse Shell

Em seguida, o servidor alvo, ao executar a reverse shell, se conecta na porta do atacante e fornece, ao atacante, uma linha de comando.



— Ataques de Negação de Serviço

Como ocorrem os ataques de negação de serviço?



Ataques de negação de serviço exploram vulnerabilidades em protocolos para bloquear acessos legítimos.



Enviam uma enorme quantidade de pacotes para sobrecarregar o sistema-alvo.



Objetivo: impedir o funcionamento normal do serviço ou site.

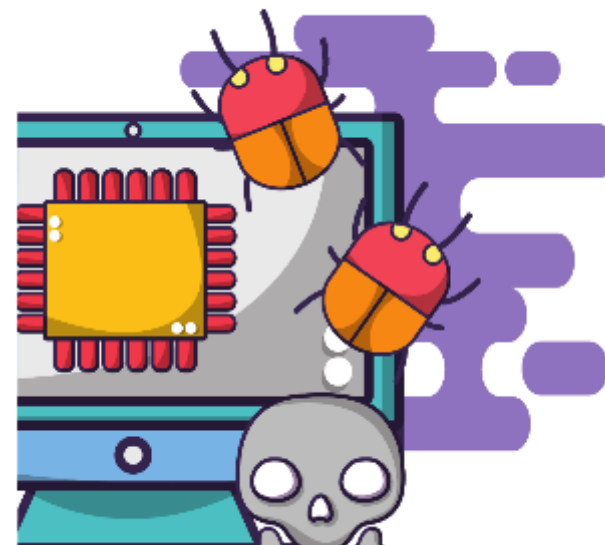


Buscam tornar o recurso inacessível a usuários legítimos.

— Ataques de Negação de Serviço

DoS – Denial of Service

- O DoS (Denial of Service) é a primeira forma dos ataques de negação de serviço.
- O ataque é executado a partir de uma única máquina, explorando vulnerabilidades na rede para tornar determinado sistema inacessível.



— Ataques de Negação de Serviço

DDoS – Distributed Denial of Services



DDoS - A evolução: Devido à proteção contra DoS, surgiram os DDoS (Distributed Denial of Service) que usam várias fontes.



Ataques coordenados: Realizados por botnets, que são dispositivos infectados controlados centralmente pelo atacante.



Amplificação de pacotes: Objetivo é enviar uma grande quantidade de pacotes para sobrecarregar o alvo.



Desafio de segurança: A complexidade desses ataques demanda medidas robustas de proteção

— Ataques de Negação de Serviço

Crescimento de ataques DdoS

Crescimento de Botnets: O número de dispositivos em botnets está aumentando, com 4% dos 500 mil dispositivos de IoT no Brasil pertencendo a uma botnet.



Ataques DDoS Constantes: Ataques DDoS ocorrem diariamente, visando vários alvos, de acordo com o relatório da Threat Intelligence da A10 Networks.



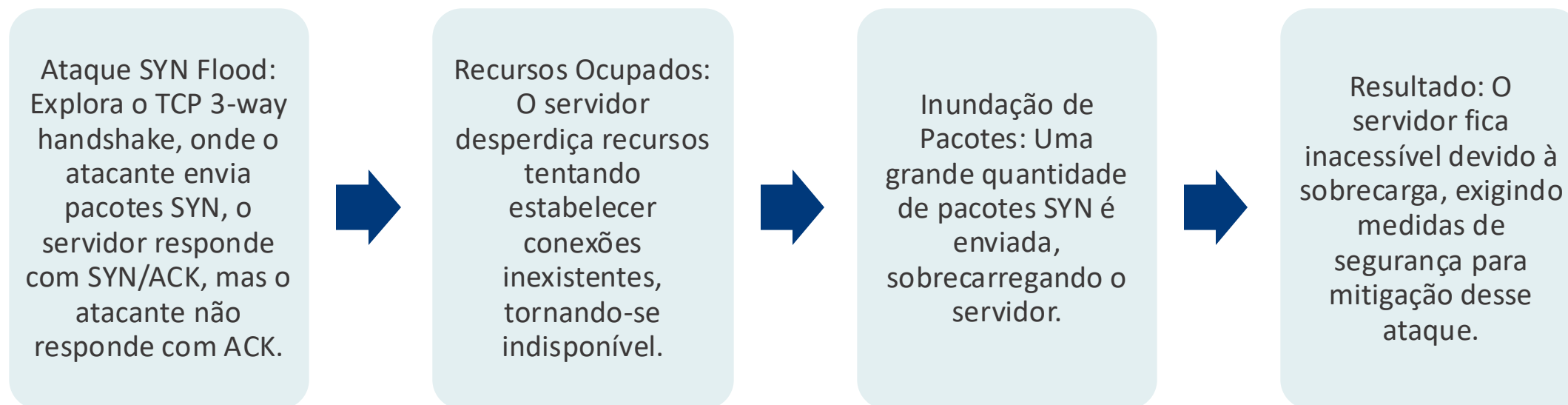
Causas do Crescimento: O crescimento das botnets é impulsionado pelo aumento de dispositivos de IoT e pelas novas vulnerabilidades nesses dispositivos.



Desafio de Segurança: Essa tendência exige medidas robustas de segurança cibernética para proteger contra ameaças em constante evolução.

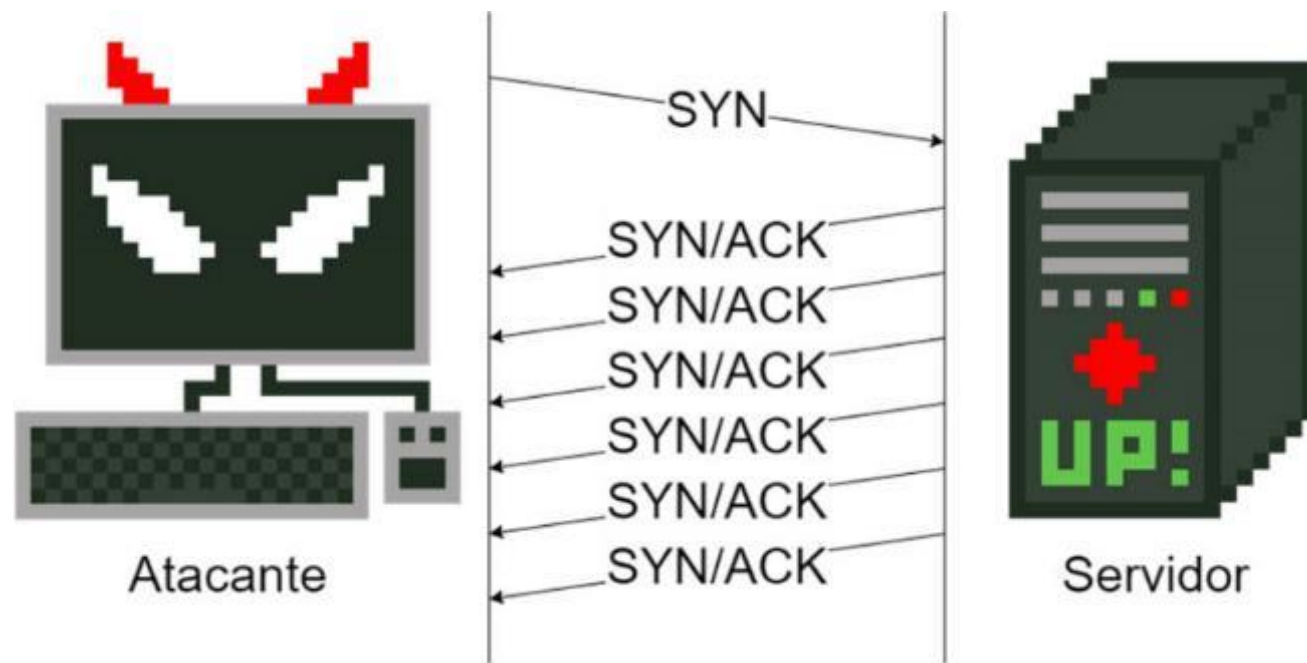
— Ataques de Negação de Serviço

Ataque SYN Flood



— Ataques de Negação de Serviço

Ataque SYN Flood



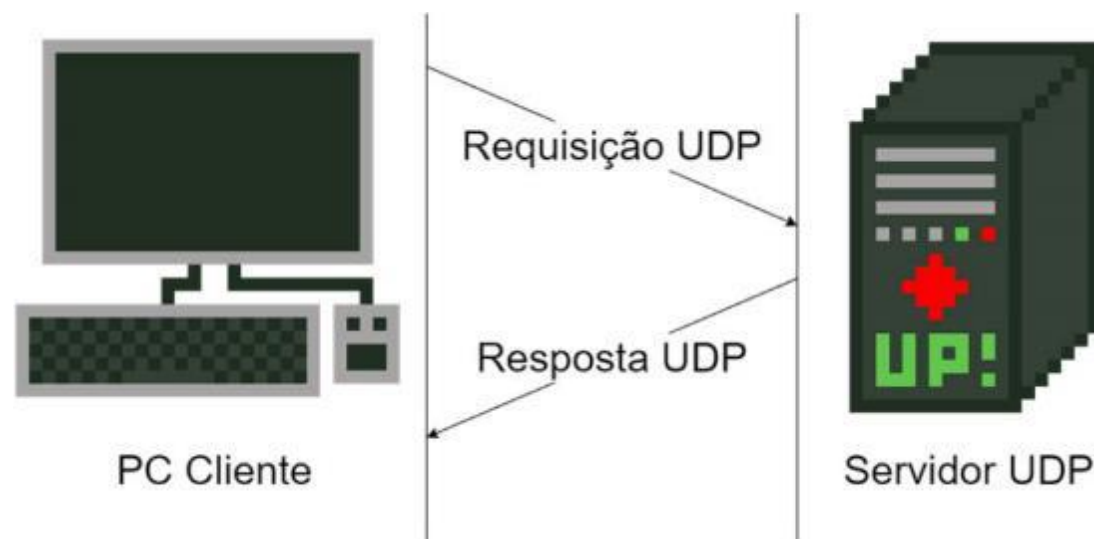
SYN Flood, ou Inundação de SYN.

— Ataques de Negação de Serviço

UDP Reflection

O protocolo UDP (User Datagram Protocol), diferentemente do protocolo TCP, não é orientado a conexão.

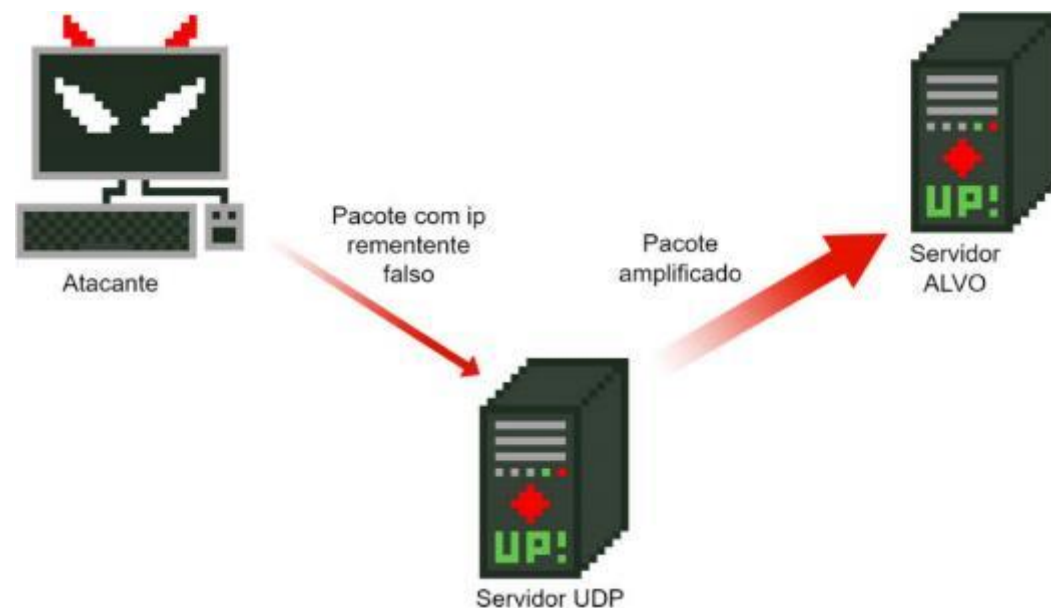
Além disso, não existe a necessidade de nenhum procedimento como o *3-way handshake*.



— Ataques de Negação de Serviço

UDP Reflection

Um ataque de *UDP reflection* pode ser feito enviando pacotes para um servidor que possua algum serviço de *UDP* falsificando o endereço de origem.



— Ataques de Negação de Serviço

Fator de amplificação



Fator de Amplificação: Refere-se à diferença entre a quantidade de dados enviada para o alvo e a quantidade enviada pelo atacante.



UDP Reflection Attack: Exemplifica esse conceito, onde um pacote de 64 bytes ao servidor DNS gera até 3400 bytes de resposta para o alvo.



Protocolo DNS: Em ataques DNS, o fator de amplificação geralmente varia entre 28 e 54, destacando a potencial sobrecarga causada por esse tipo de ataque.

— Engenharia Social

O que é Engenharia Social?

Engenharia Social: Manipulação psicológica para obter informações confidenciais.

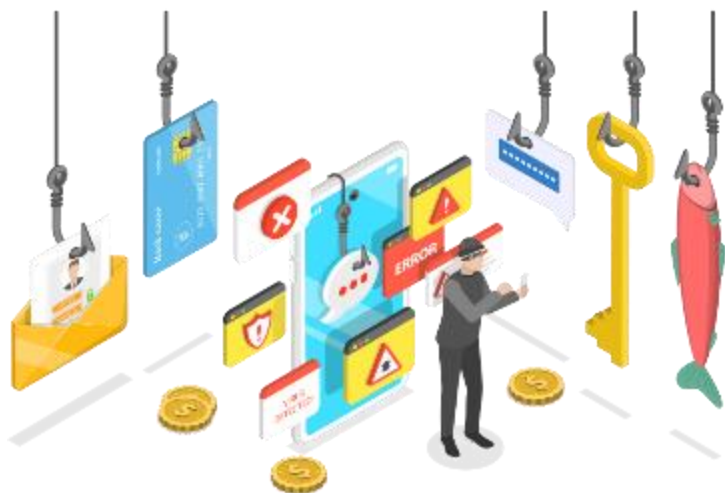
Exploração Emocional: Usa sentimentos como medo, curiosidade e empatia.

Foco no Humano: Ataca o ponto fraco das organizações: as pessoas.

Requer Pesquisa: Entender alvos para eficácia.

— Engenharia Social

Principais abordagens



Principais Abordagens: Ataques de engenharia social envolvem intimidação, persuasão, bajulação e assistência.

- Intimidação: Usando autoridade, explora medo e urgência.
- Persuasão: Lisonja e nomes importantes geram empatia e culpa.
- Bajulação: Constrói relacionamentos a longo prazo para obter confiança e informações.
- Assistência: Fornecer ajuda para obter informações confidenciais.

— Engenharia Social

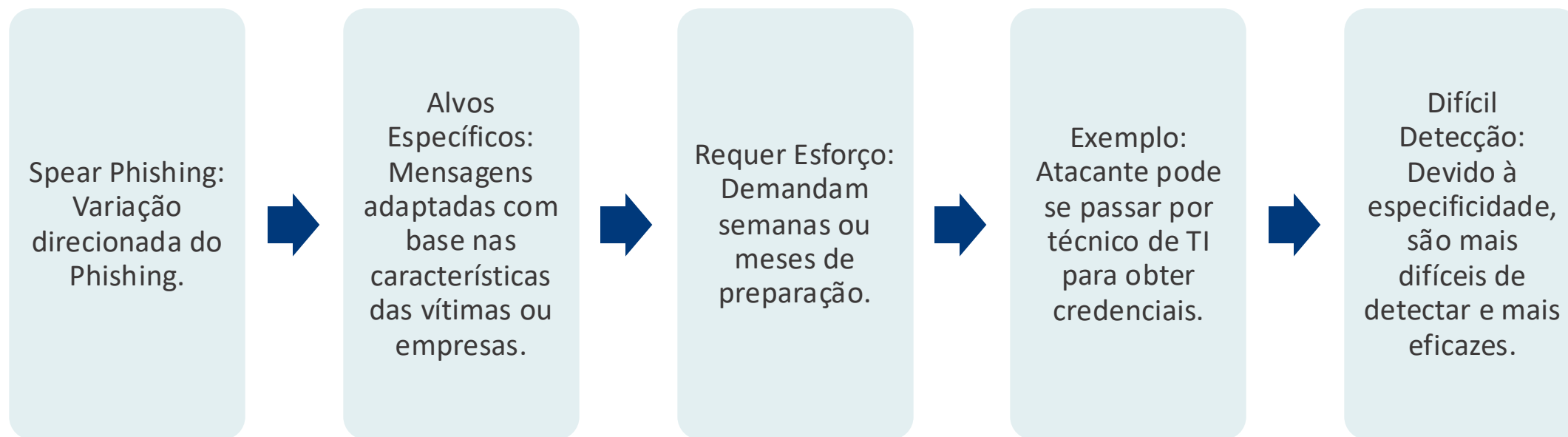
Phishing

- **Phishing:** Técnica popular de engenharia social via e-mail/mensagens, cria urgência, curiosidade ou medo para obter informações ou instalar malware.
- **Ataques Genéricos:** Geralmente, são fáceis de identificar e bloquear por meio de políticas de firewall.



— Engenharia Social

Spear phishing



— O que são malwares?

Definição



Malwares: São softwares maliciosos que exploram vulnerabilidades e causam danos a dispositivos.

- **Diversas Finalidades:** Podem visar desde prejudicar computadores pessoais até atacar grandes empresas.
- **Variedade de Funcionamento:** Cada malware age de maneira distinta, explorando diversas vulnerabilidades e infectando diferentes sistemas.

— O que são malwares?

Técnica de detecção de malwares

Ambas são utilizadas por antivírus para verificar atividade maliciosa em um computador.

Técnica baseada em assinaturas digitais

Busca por comportamentos específicos que são considerados maliciosos.

Técnica baseada em comportamento

A técnica baseada em comportamento, ou anomalia, possui informações sobre o que é considerado como atividade normal.

— O que são malwares?

Tipos de malwares

Worm ou Vírus

Backdoor

Botnet

Downloader

Laucher

**Information -
stealing**

Ransomware

— O que são malwares?

Análise estática básica



Análise de Malware: Técnica para examinar códigos maliciosos e compreender seu comportamento.

- Objetivo: Responder a incidentes, determinar as ações do malware e detectá-lo com precisão.
- Quatro Etapas: Inclui análise estática básica, análise dinâmica básica, análise estática avançada e análise dinâmica avançada.

— Exemplos de ataques de malwares

Stuxnet

Worm famoso por atacar usina via USB, danificando equipamentos sem conexão à Internet.

Wannacry

Ransomware global de 2017, explorando vulnerabilidade EternalBlue, vazada pela NSA via Shadow Brokers.

Mirai Botnet

Worm ataca dispositivos IoT, cria rede controlada por atacante, realiza ataques DDoS notáveis, como à Dyn.

— Como se proteger?

O que fazer em caso de ataque?

Diversas são as possibilidades de enviar *malwares* para alvos. Algumas técnicas são simples e outras são complexas.

**Utilização de
antivírus**

**Download de
softwares piratas**

**Dispositivos USB
encontrados em
lugares públicos**

Vírus total

— O que é Wi-Fi?

Padrão IEEE 802.11

- Wi-Fi e IEEE 802.11: Redes sem fio com padrões estabelecidos pelo IEEE.
- IEEE 802.11: Padronização criada em 1997 para WLANs (Redes Locais sem Fio).
- Evolução dos Padrões: Versões atualizadas ao longo do tempo, a mais recente é "IEEE Std 802.11axTM-2021".



— O que é Wi-Fi?

Conceitos fundamentais



Wi-Fi BSS: Conjunto de estações Wi-Fi, incluindo pelo menos um AP (Ponto de Acesso).



AP (Ponto de Acesso): Central da rede, onde os dispositivos (clientes) se conectam.



BSSID: Identifica exclusivamente cada BSS, geralmente é o endereço MAC do AP.



SSID: Nome amigável da rede Wi-Fi visível durante a busca por redes.

— O que é Wi-Fi?

Faixas de frequência e canais

- **Faixas de Frequência:** Wi-Fi opera nas faixas ISM (Industrial, Scientific, and Medical). São usadas duas principais faixas: 2,4 GHz e 5 GHz.
- **Canais:** Canais dividem as faixas em bandas menores. A faixa de 2,4 GHz tem 14 canais de 22 MHz cada, variando de 2.401 MHz a 2.495 MHz.



— Segurança em Wi-Fi

Redes Wi-Fi OPEN

Redes Wi-Fi WEP

**Criptografia
simétrica**

**Criptografia do WI-
FI WEP**

Wi-Fi WEP OPEN

Wi-Fi WEP SKA

WPA

**Criptografia do
WPA**

**Autenticação do
WPA**

WPA-PSK

WPA-EAP

Wi-fi WPA 2

— Ataques a redes sem fio

Tipos de ataques a redes sem fio

O framework
aircrack-ng

Placas Wi-Fi em
modo monitor

Monitoramento de
redes sem fio

Monitoramento de
uma rede
específica

Ataques a rede
WPA/WPA2

Negação de serviço
em redes
WPA/WPA2

Quebra de senha

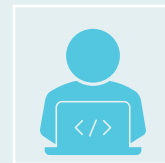
Vulnerabilidades comuns da OWASP



— Visão geral da estrutura de uma aplicação web moderna



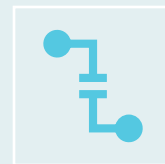
Evolução das Aplicações Web:
Antigamente, baseadas em HTML,
JavaScript e CSS, menos responsivas.



Ajax: Introdução do Ajax (JavaScript
e XML) para tornar aplicações mais
responsivas e interativas.



JavaScript no Navegador: JavaScript
executado no navegador para ações
do usuário.



WebServices: Uso comum de
protocolo HTTP para disponibilizar
serviços web, dividindo aplicações
em componentes comunicantes.

— Visão geral da estrutura de uma aplicação web moderna

WebServices são serviços (ou funcionalidades) disponibilizados que utilizam tecnologias similares às das aplicações web. As **duas** mais usadas para disponibilizar WebServices são:

Simple Object Access Protocol (SOAP)

Protocolo de comunicação.

Representational State Transfer (REST)

Conjunto de princípios para transmissão de dados.

— Visão geral da estrutura de uma aplicação web moderna

Mudanças na Arquitetura de Aplicações Web: Evolução para APIs REST, uso de JSON/XML, JavaScript no navegador e frameworks SPA.

Componentes Típicos de uma Aplicação Web Moderna: API REST, JSON/XML, JavaScript, Frameworks SPA, autenticação, servidores web, bancos de dados e armazenamento de dados do lado do cliente.

Características do REST: Independência de tecnologia do cliente, sem estado (stateless) e suporte para cache, mapeando ações HTTP para recursos do servidor.

Uso de Comandos HTTP: REST utiliza comandos HTTP como GET, POST, PUT, e outros além de GET e POST.

— Visão geral da estrutura de uma aplicação web moderna

Você pode verificar que, nos protocolo HTTP e nos padrões XML e JSON, ocorre as seguintes situações:

HTTP

Por meio de comandos simples já existentes no protocolo HTTP, como PUT, DELETE, GET E POST, é possível realizar um conjunto de operações em um endpoint com uma API REST.

XML e JSON

á o XML e JSON são padrões para representar os dados utilizados, por exemplo, pelas APIs REST (não se limitando apenas a elas).

— Visão geral da estrutura de uma aplicação web moderna

SPA (Single Page Application): Não limitado a uma única página. Carrega todos recursos na primeira requisição e carrega novos conteúdos via JavaScript, sem recarregar a página. Diferente das abordagens tradicionais. Usa várias tecnologias e frameworks.



— Injeção

Injeção de SQL

- **Injeção de Código:** Explora falhas de processamento de dados inválidos, permitindo a introdução de código em programas vulneráveis.
- **Injeção de SQL:** Testada na máquina virtual OWASP BWA para demonstrar a exploração de vulnerabilidades SQL em aplicações.

— Injeção

Injeção de SQL

Desafio "Login #1 Basic Login": Testes com pares de login/senha revelam vulnerabilidade de injeção de SQL.



Desafio "Login #2 JavaScript Validation": Restrição de caracteres especiais na senha dificulta a injeção de SQL.



Soluções Possíveis: Uso de ferramentas como Burp Suite para interceptar e modificar requisições, contornando validações de JavaScript.

— Injeção

Injeção de comando

Injeção de Comando em DVWA:

Exemplo de injeção de comando em outra aplicação vulnerável, a "Damn Vulnerable Web Application" (DVWA).

Desafio "Command Execution":

Campo permite a entrada de um IP para executar o comando PING no servidor.

Exemplo de Injeção de Comando:

Inserção de comando "8.8.8.8; cat /etc/debian_version" resulta na execução remota de comandos no servidor e exibe "squeeze/sid".

— Quebra de controle de acessos

- **Controle de Acesso em Aplicações Web:** Restringir acesso a seções ou páginas com base nas necessidades dos usuários.
- **Exemplo de Loja Virtual:** Apenas administradores precisam acessar a área de administração para cadastrar produtos, definir preços, e promoções. Visitantes ou clientes não precisam disso.



— Quebra de controle de acessos

Exemplos de controle de acesso quebrado

Acesso a um painel de controle/administrativo de hospedagem.

Acesso a um servidor via FTP/SFTP/SSH.

Acesso ao painel administrativo de um site.

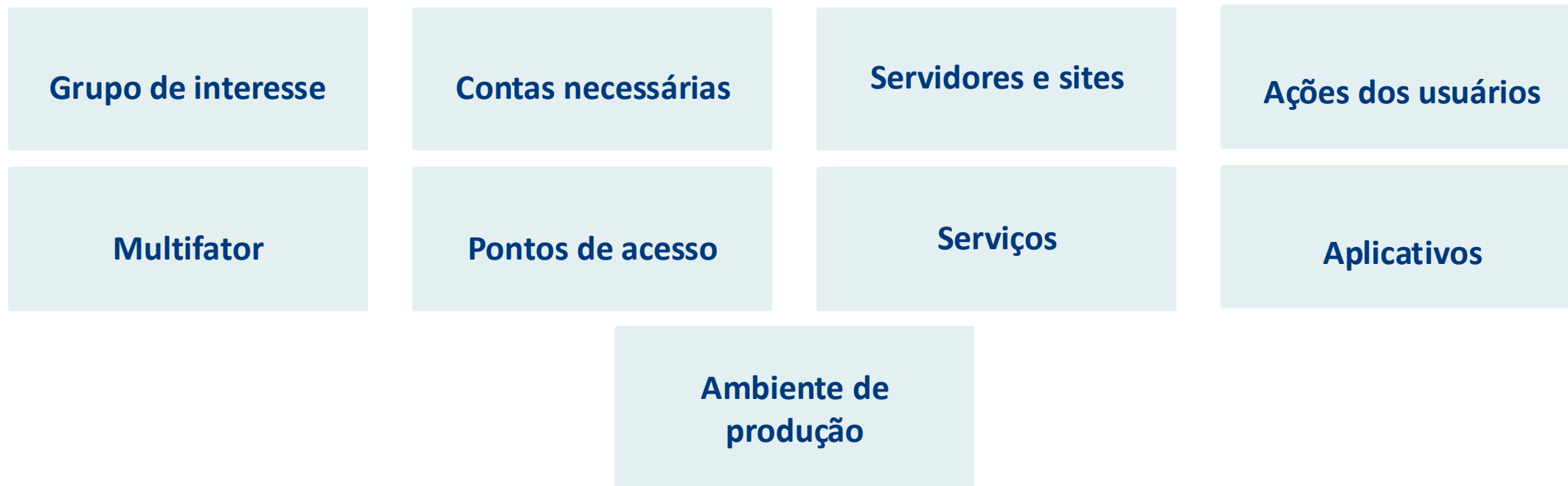
Acesso a outros aplicativos em seu servidor.

Acesso a um banco de dados.

— Quebra de controle de acessos

Mitigando os riscos

Pode-se reduzir os riscos com algumas medidas.



— Falhas criptográficas

- **Falhas Criptográficas:** Ocorrem quando dados confidenciais ficam acessíveis devido à falta de criptografia, configurações inadequadas ou vulnerabilidades em sistemas e aplicações.
- **Dados Confidenciais:** Incluem informações pessoais, bancárias e credenciais de login.
- **Importância da Proteção:** Crucial para garantir a privacidade dos usuários, considerando a legislação como a Lei Geral de Proteção de Dados no Brasil.



— Falhas criptográficas

Pode-se classificar os dados em **dois tipos**:

Dados armazenados

Todos os dados que não se movem na rede estão em repouso.

Dados em trânsito

São dados transmitidos através de uma rede.

— Falhas criptográficas

Exemplo de aplicação de criptografia às senhas



- **Criptografia de Senhas:** Senhas são armazenadas como hashes unidirecionais, tornando difícil reverter para a senha original.
- **Exemplo:** A senha "q2e5t7u9" pode ser convertida em "79183ceb1c094d34e19e73a427bd524c" usando um algoritmo de hash como o md5.

— Projeto inseguro

Projeto Inseguro:
Riscos de segurança originados de falhas no projeto e arquitetura, independentemente da qualidade da implementação.

Exemplos: Ausência de limites para entradas, uso de funções inseguras (como extração de arquivos sem controle), privilégios excessivos.

Solução Personalizada: Não há uma solução única, cada caso requer abordagem adaptada.

Importância: Define o grau de segurança necessário no projeto e na arquitetura.

— Projeto inseguro

Algumas formas de se prevenir o projeto inseguro:

Ciclo de vida de desenvolvimento seguro

Biblioteca de padrões ou componentes seguros

Métodos específicos

Controles de segurança

Verificações de front-end e back-end

Resistência dos fluxos críticos ao modelo de ameaça

Consumo de recursos

— Configurações de segurança incorretas

Configurações podem causar diversos problemas em um sistema:

Falhas não corrigidas

Configurações padrão

Páginas não utilizadas

Arquivos e diretórios
desprotegidos

Serviços desnecessários

— Configurações de segurança incorretas

Observando a vulnerabilidade

O OWASP apresenta alguns cenários possíveis:

Cenário 1

O servidor de aplicativos vem com aplicativos de exemplo que não são removidos do servidor de produção, podendo ter falhas de segurança conhecidas que os invasores usam para comprometer o servidor.

Cenário 2

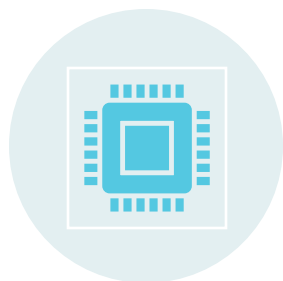
A listagem do diretório não está desabilitada no servidor. Um invasor descobre que pode simplesmente listar diretórios, que encontram e baixam as classes Java compiladas.

Cenário 3

A configuração do servidor de aplicativos permite mensagens de erro detalhadas a serem devolvidas aos usuários.

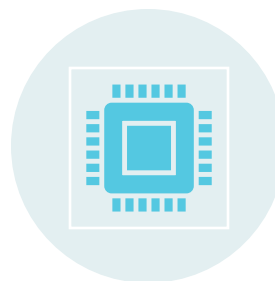
— Configurações de segurança incorretas

Realizando varredura de vulnerabilidades

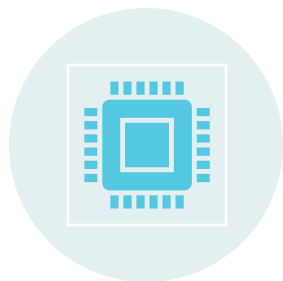


Varredura de Vulnerabilidades:

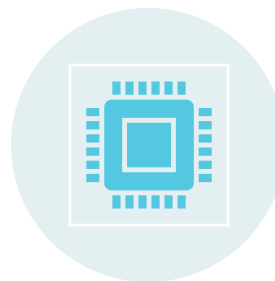
Utilize ferramentas open-source como Nessus, OpenVAS, nmap e Nikto.



Exemplo com Nikto: Facilmente instalado no Ubuntu com apt. Pode detectar software desatualizado e diretórios de aplicações conhecidas.



Importância: Identifica vulnerabilidades no sistema, incluindo versões desatualizadas de software e falhas de configuração.



Ação Necessária: Atualize software desatualizado e restrinja o acesso a diretórios sensíveis.

— Configurações de segurança incorretas

Como evitar configurações incorretas

Seguem algumas sugestões para evitar ou mitigar problemas de configurações incorretas:

Configuração de ambientes de desenvolvimento, controle de qualidade e produção.

Instalação mínima.

Processo de revisão e atualização.

Processo automatizado de verificação.

— Componentes vulneráveis e desatualizados



Dependências das aplicações modernas: Negligenciar atualizações no back-end e front-end resulta em riscos de segurança.



Exemplo do WordPress: Em 2019, 56% dos CMS estavam desatualizados, muitos usando WordPress com plugins desenvolvidos de forma insegura.



Problemas Comuns: Falta de atualização pelos administradores e ausência de práticas seguras de desenvolvimento.



Importância da Atualização: Falha em atualizar aumenta a probabilidade de vulnerabilidades conhecidas persistirem na aplicação.

— Componentes vulneráveis e desatualizados

Aplicações vulneráveis

De acordo com as diretrizes OWASP, os aplicativos vulneráveis estão desatualizados nos seguintes casos:

Versões de todos os componentes.

Software vulnerável, sem suporte ou desatualizado.

Plataforma, as estruturas e as dependências subjacentes.

Configurações do componentes.

— Componentes vulneráveis e desatualizados

Prevenção

Remover todas as dependências desnecessárias.

Obter componentes apenas de fontes oficiais.

Não usar componentes que não tenham manutenção ativa.

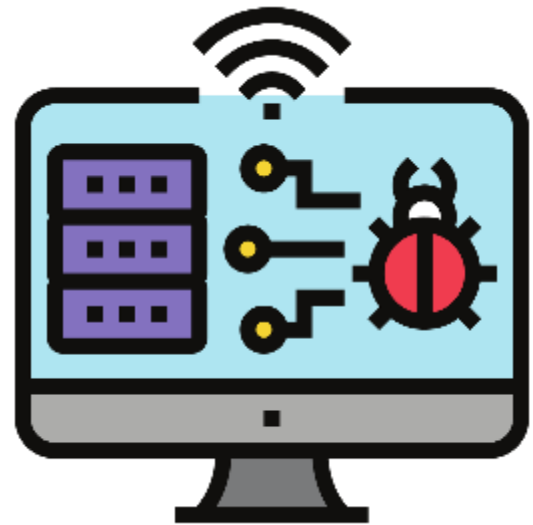
Usar patching virtual com a ajuda de um firewall de aplicativo de site.

Ter um inventário de todos os seus componentes do lado do cliente e do lado do servidor.

Monitorar fontes, como, (CVE) e (NVD), para obter informações sobre as vulnerabilidades nos componentes.

— Falhas de identificação e autenticação

- **Falhas de Autenticação:** Quando invasores comprometem senhas, chaves ou tokens para assumir identidades.
- **Problemas Lógicos:** Erros na lógica de autenticação, permitindo ataques de força bruta.



— Falhas de identificação e autenticação

Dois cenários típicos em que existe a vulnerabilidade de quebra de autenticação:

Cenário 1

Utilização de força bruta com o emprego de listas de senhas conhecidas.

Cenário 2

A maioria dos ataques de autenticação ocorre devido ao uso contínuo de senhas como único fator de autenticação.

— Falhas de identificação e autenticação

Os três tipos mais comuns de fatores são:

Algo que você sabe

Como uma senha ou um PIN memorizado.

Algo que você tem

Como um smartphone.

Algo que você é

Como uma impressão digital.

— Falhas de identificação e autenticação

Conclusão

A Vulnerabilidade pode ser evitada seguindo alguns conselhos:

Autenticação multifator

Implemente a autenticação multifator para evitar ataques automatizados.

Credencial padrão

Não cadastre nenhuma credencial padrão.

Verificação de senha fraca

Implemente verificações de senha fraca.

Rotação de senha

Avalie a complexidade e as políticas de rotação da senha.

Login malsucedidas

Limite ou atrase cada vez mais as tentativas de login malsucedidas.

Ataques de enumeração de contas

Garanta que os caminhos de registro, recuperação de credencial e API sejam protegidos.

— Falhas de integridade de dados e software

- **Falhas de Integridade de Dados:** Se dados críticos não são verificados, invasores podem adulterá-los, incluindo códigos maliciosos.
- **Atualizações de Software:** Atualizações automáticas podem ser vulneráveis a ataques de MitM, comprometendo a integridade do aplicativo.



— Falhas de integridade de dados e software

Desserialização insegura



Desserialização insegura envolve converter dados serializados de volta em objetos, o que pode ser explorado por invasores se não for tratado com segurança.



Serialização converte objetos em dados, permitindo armazená-los ou transmiti-los.



A desserialização inadequada pode levar a vulnerabilidades se os dados serializados forem manipulados.



É importante validar e filtrar dados durante a desserialização para prevenir ataques.

— Falhas de integridade de dados e software

Desserialização insegura

Como funciona o ataque



O ataque de desserialização insegura envolve acessar e editar objetos serializados para explorar vulnerabilidades.



Pode ser feito diretamente no arquivo serializado ou ao modificar os dados durante o processo de desserialização.



Exemplo: um invasor altera um cookie com dados de perfil, tornando-se administrador após a desserialização.

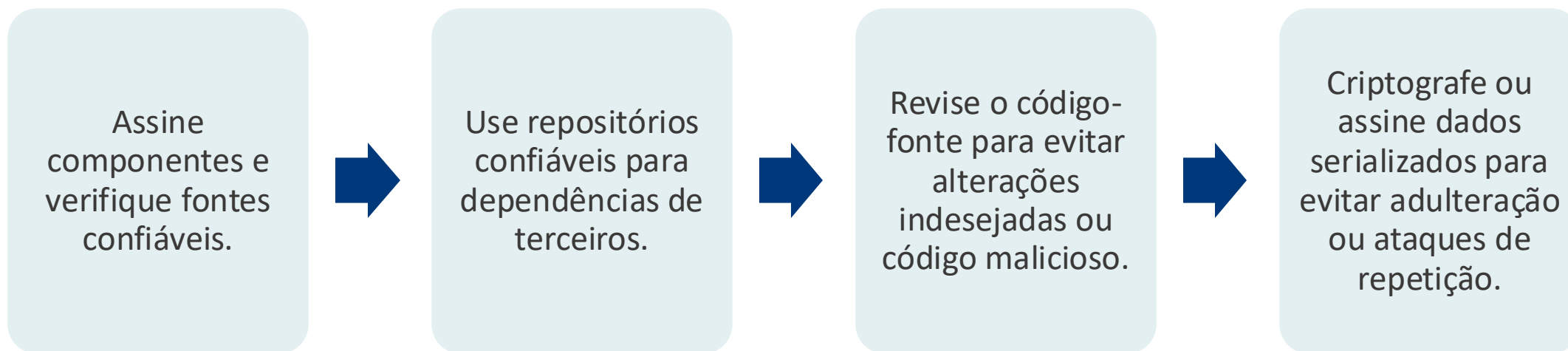


O sucesso depende da falta de validação adequada no código da aplicação.

— Falhas de integridade de dados e software

Desserialização insegura

Prevenção



— Falha de registro e monitoração de segurança



Falta de registro e monitoração é um problema sistêmico que afeta todas as camadas da arquitetura de sistemas.

- Proteger todo o ecossistema do site é crucial para evitar invasões e garantir a segurança.
- A segurança absoluta é impossível, mas a monitoração constante permite ação imediata em caso de intrusão.
- Eventos não registrados e sistemas não monitorados representam sérios riscos à segurança.

— Falha de registro e monitoração de segurança

Não ter um processo eficiente de registro de eventos e monitoramento pode aumentar os danos de comprometimento de um site. O registro de ambos pode ser separado em três partes:

Coleta de registros

Gerenciamento de log

Monitoramento/ análise
de log

— Falsificação de requisição do lado do servidor

Visão geral

O SSRF é um ataque que induz um usuário autenticado a realizar ações indesejadas em um aplicativo web.

Isso pode ser feito por meio de e-mails com links maliciosos que redirecionam a vítima para funções autenticadas.

Um ataque SSRF bem-sucedido pode comprometer a segurança do aplicativo web, especialmente se a vítima for uma conta administrativa.

Contramedidas e hardening



— O que são as ferramentas?

- As ferramentas de segurança e a criptografia são recursos essenciais na mitigação de incidentes de segurança.
- O uso desses recursos depende de planejamento e conhecimento do universo de vulnerabilidades que o ambiente possui, de modo a escolher a solução certa para cada problema.



— Criptografia



Desde a antiguidade, a criptografia tem sido usada para proteger informações sensíveis.



A criptografia é essencial para garantir a confidencialidade dos dados.



Integrar a segurança desde o início no desenvolvimento de aplicações é fundamental.



A criptografia se divide em criptografia simétrica e assimétrica, cada uma com seus usos específicos.

— Criptografia

Criptografia simétrica



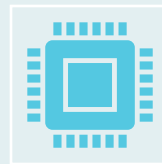
Criptografia simétrica utiliza uma única chave compartilhada para comunicação privada.



A famosa cifra de César exemplifica o uso de criptografia simétrica.



Existem dois tipos de algoritmos simétricos: cifras de bloco e cifras de fluxo.



O AES (Advanced Encryption Standard) é um exemplo de algoritmo simétrico amplamente adotado devido a suas características, como chaves de 128 bits e alta eficiência.

— Criptografia

Criptografia assimétrica



Criptografia assimétrica utiliza duas chaves, uma pública e uma privada, para segurança e autenticidade.

- Garante confidencialidade com a chave pública do destinatário.
- Usa uma infraestrutura de chaves públicas (PKI) para autenticar chaves públicas.
- Combina criptografia simétrica para eficiência com criptografia assimétrica para segurança e integridade.

— Criptografia

Algoritmos de autenticação e integridade



Criptografia assimétrica é lenta; para autenticidade e integridade, funções hash criptográficas são usadas.



Funções hash geram um hash fixo a partir da mensagem e são rápidas.



São unidirecionais, impossibilitando reverter o cálculo para obter a mensagem original.



A probabilidade de alterar a mensagem e obter o mesmo hash é extremamente baixa devido ao "efeito cascata".

— Criptografia

Ferramentas de segurança

- Ferramentas de segurança se dividem em segurança do sistema e aplicações AAA.
- Segurança do sistema protege contra vulnerabilidades em aplicações e sistema operacional.
- Mecanismos de rede operam nas interfaces, permitindo ou bloqueando pacotes de acordo com regras.
- Essas medidas evitam ações maliciosas que possam comprometer o sistema.

— Criptografia

Ferramentas de segurança

Firewall

Filtros de pacotes

Gateways de circuito

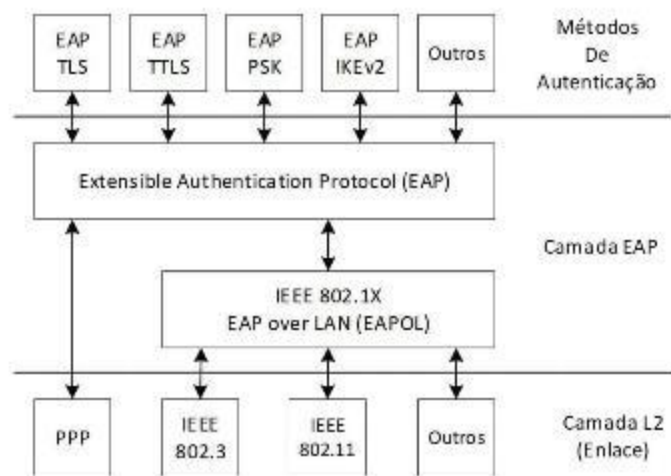
Relay (Gateway) de
aplicação

Detecção de Intrusos

Virtual Private Network
(VPN)

— Criptografia

Aplicações de AAA



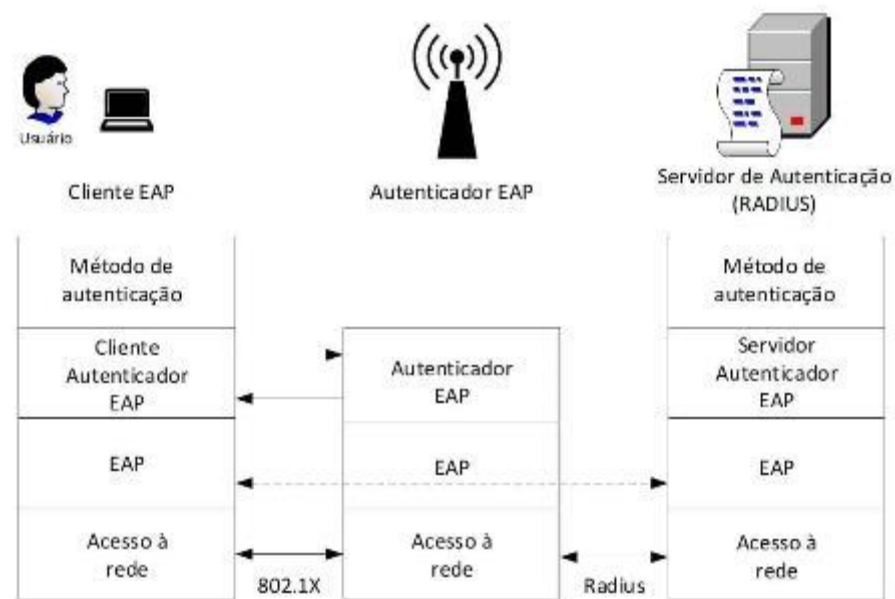
O controle de acesso é crucial na segurança da informação para evitar excesso de direitos.

- O padrão IEEE 802.1X é uma solução AAA que exige autorização explícita com base em políticas após a autenticação do usuário via EAP.
- Registra as atividades do usuário (accounting) para controle e monitoramento da rede.

— Criptografia

Aplicações de AAA

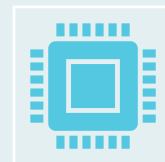
O EAP é um **protocolo de negociação e controle da autenticação**. É versátil quanto aos algoritmos usados e ao enlace, suportando redes cabeadas e sem fio.



— Protocolo IP – Internet Protocol



O protocolo IP (Internet Protocol) visa encaminhar pacotes para seu destino usando o princípio de "melhor esforço", sem criptografia ou autenticação.



A segurança na camada de rede pode ser alcançada com o uso do IPSEC, um conjunto de protocolos para IPv4 e parte do IPv6.

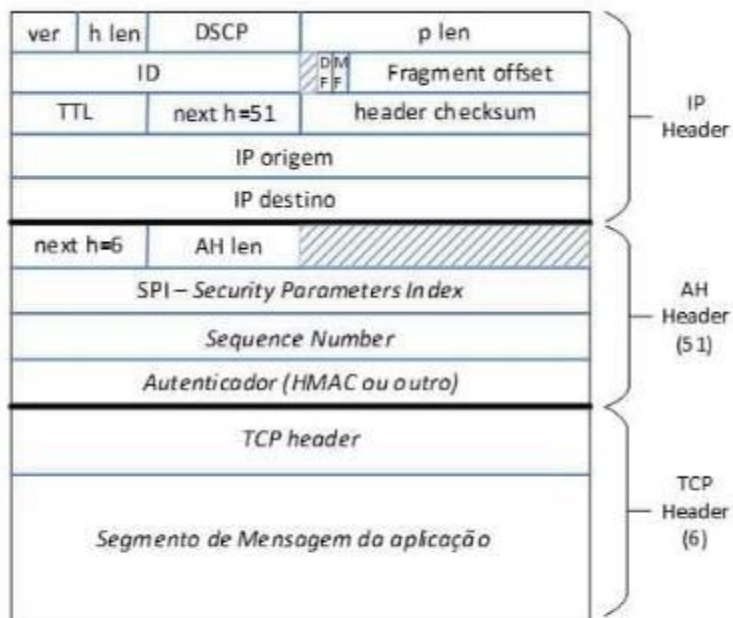


O IPSEC inclui o Authentication Header (AH) para autenticar o cabeçalho IP, o cabeçalho TCP e os dados da aplicação.

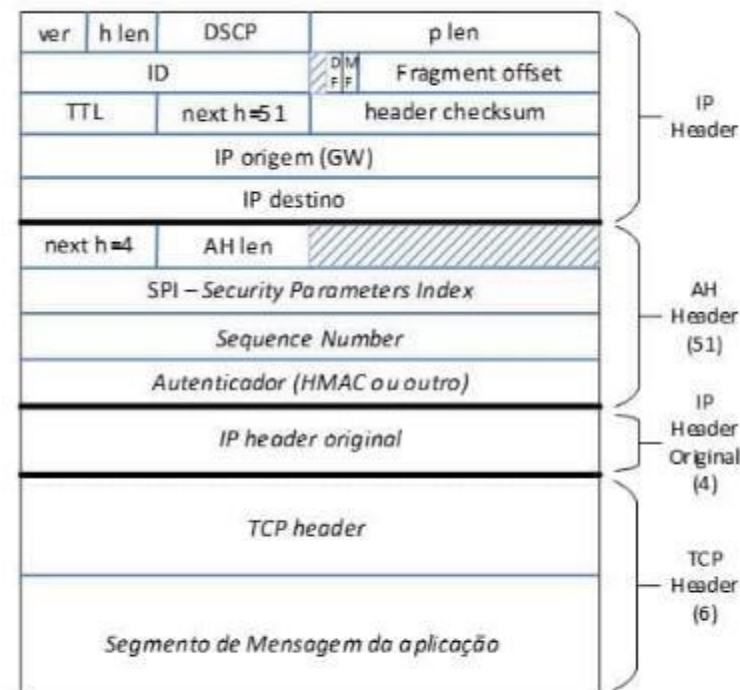


Ele também oferece o Encapsulating Security Payload (ESP) para criptografar pacotes e fornecer autenticação.

— Protocolo IP – Internet Protocol



AH em modo TRANSPORTE

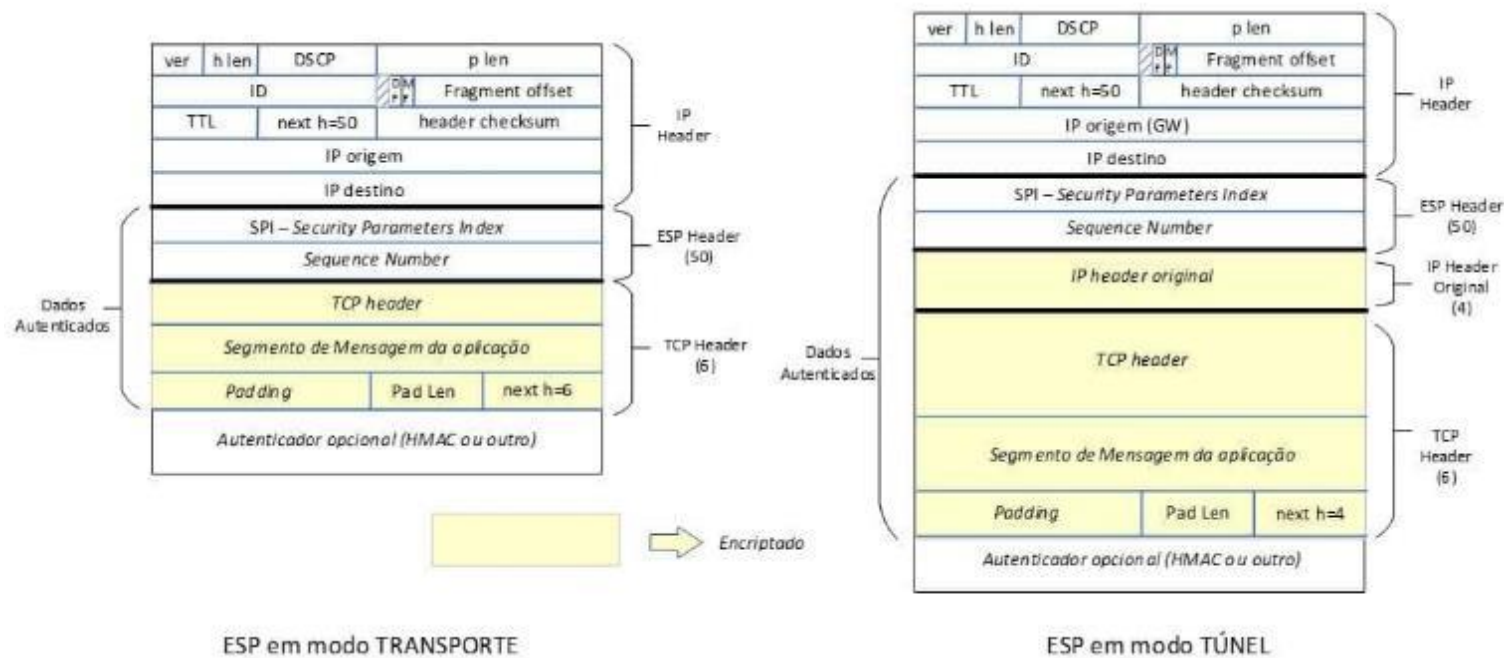


AH em modo TÚNEL

Cabeçalho AH.

— Protocolo IP – Internet Protocol

O cabeçalho ESP é usado quando se deseja a confidencialidade. A imagem a seguir ilustra o ESP.



— Protocolo TCP - Transmission Control Protocol



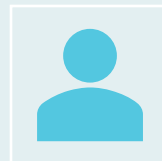
O TCP (Transmission Control Protocol) é responsável por garantir a confiabilidade na comunicação entre hosts em uma rede IP não confiável.



Não possui implementações de segurança, e as identidades dos pontos de conexão (sockets) não são verificadas.



O TCP estabelece conexões com um processo de "handshake" e utiliza numerações sequenciais de segmentos para identificar perdas e manter a ordem.



Não há autenticação dos usuários envolvidos no TCP.

— Protocolo TCP - Transmission Control Protocol

TCP Hijacking

Sequestro de sessão TCP: nesse tipo de ataque uma ameaça “entra” no meio de uma comunicação TCP com intenções maliciosas.

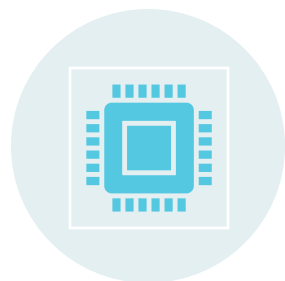
Técnicas conhecidas (GOODRICH, 2013) são a previsão de sequência TCP e o sequestro de sessão:

Previsão de Sequência TCP

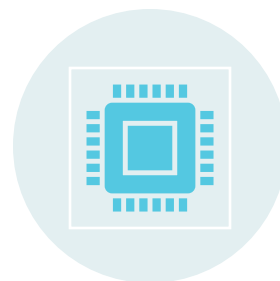
Sequestro de sessão

— Protocolo TCP - Transmission Control Protocol

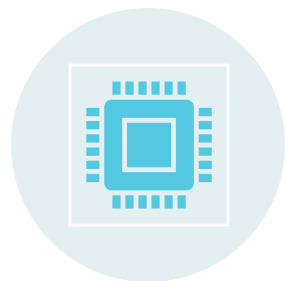
Negação de serviço TCP



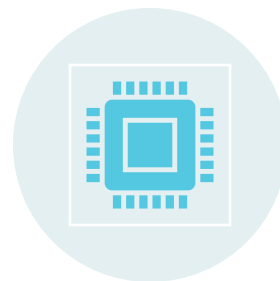
Ataques de negação de serviço (DoS) no TCP sobrecarregam servidores.



Ataque de inundação de SYN
envia muitas solicitações de conexão SYN para sobrecarregar o servidor.



Ataque otimista ACK TCP
aumenta a carga no servidor com ACKs para janelas não completamente recebidas.



IDS e limites de parametrização são usados para mitigar esses ataques.

— Protocolo UDP – User Datagram Protocol

O UDP é um protocolo simples para serviços de requisições e respostas curtas.

Mesmo sem alocar recursos como o TCP, pode ser usado em ataques de negação, especialmente com ataques reflexivos.

Alguns comandos em aplicações UDP provocam respostas grandes, criando o efeito amplificador.

A detecção e combate a esses ataques exigem IDS e políticas restritivas para provedores de serviços baseados em UDP.

— Domain Name System (DNS)



O DNS é uma estrutura global que permite a resolução de nomes de domínio em endereços IP de forma rápida e eficiente.



Ele utiliza caches para armazenar resoluções de domínio, reduzindo o tráfego e melhorando a velocidade.



Devido à alta dependência do DNS, a segurança é uma prioridade.



Um ataque comum ao DNS é o "pharming" e "phishing".

— Domain Name System (DNS)

Pharming e Phishing

Pharming é uma variação do phishing que visa obter informações sensíveis através de um site clonado.



O ataque de pharming envolve a introdução de uma resolução falsa no cache DNS.



Isso é feito por meio de um envenenamento do cache DNS, onde um atacante envia respostas falsas antes das legítimas.

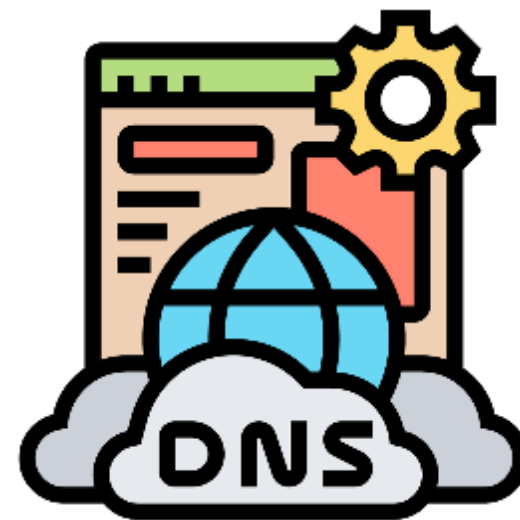


Vulnerabilidades no DNS, como falta de autenticação de números de 16 bits e consultas para subdomínios inexistentes, destacam a necessidade do DNSSEC para maior segurança.

— Domain Name System (DNS)

DNSSEC

- DNSSEC é uma extensão do DNS que utiliza assinaturas digitais em todas as respostas, reforçando a segurança.
- Requer o uso de certificados digitais por servidores DNS e a adoção global, um desafio para a cibersegurança.



— Protocolo HTTP – Hypertext Transfer Protocol



O protocolo HTTP foi originalmente desenvolvido para transportar páginas web em texto claro.

- A segurança foi posteriormente abordada com o uso do SSL/TLS, criando o HTTPS.
- O SSL/TLS oferece confidencialidade, integridade e autenticação nas comunicações entre clientes e servidores web.

— Segurança em sistemas operacionais

- Sistemas operacionais são extensos com milhões de linhas de código, frequentemente com vulnerabilidades descobertas após o lançamento.
- Ações de segurança são essenciais para proteger sistemas, abordando a segurança no Microsoft Windows e distribuições Linux.



— Segurança em ambiente windows

A Microsoft recomenda ações de segurança no Windows, incluindo:

- Proteção contra malware com Windows Defender.
- Certificação de serviços seguros.
- Encriptação de dados sensíveis.
- Políticas de segurança, firewall revisado, permissões controladas, senhas fortes e logins de usuário com direitos limitados.

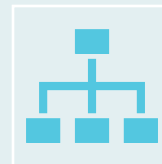


— Segurança em ambiente windows

Arquivo de registro



O Windows armazena informações em arquivos de registro, o que pode ser explorado por aplicativos maliciosos.



Evite logins genéricos de administrador; use "executar como administrador" quando necessário.



Crie grupos com privilégios diferenciados para usuários.



Monitore o consumo de recursos para identificar atividades maliciosas.

— Segurança em ambiente windows

Aplicações importantes para o gerenciamento da segurança em ambiente Windows

Aplicações importantes para o gerenciamento da segurança:

Netstat

Windows event viewer

Política de segurança local

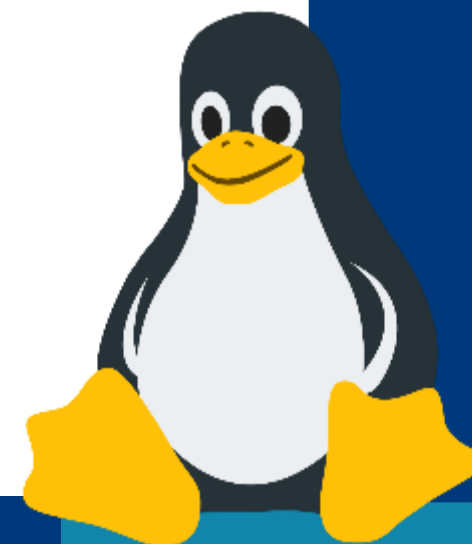
Windows defender

Windows Firewall

— Segurança em ambiente windows

Segurança em ambiente linux

- O Linux é um sistema operacional open source usado principalmente para servidores e segurança.
- No Linux, quase tudo é gerenciado por arquivos, o que pode representar um risco de segurança.
- Acesso a arquivos de configuração e permissões são críticos para a segurança do ambiente Linux.

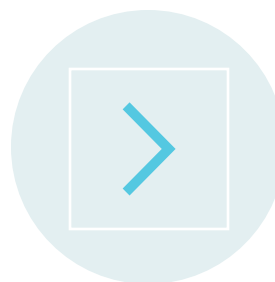


— Segurança em ambiente windows

Melhores práticas para o hardening de um ambiente Linux



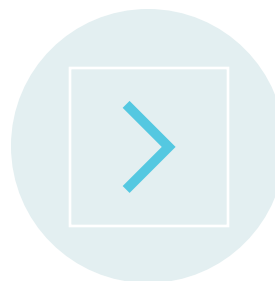
Gerenciar cuidadosamente as credenciais e papéis dos usuários.



Controlar o acesso remoto usando ferramentas como o SSSD.



Minimizar pacotes e desativar serviços não essenciais.



Manter o sistema e os pacotes atualizados, implementar MFA e revisar logs regularmente.

— Segurança em ambiente windows

Melhores práticas para o hardening de um ambiente Linux

Alguns dos logs mais importantes incluem:

`/var/log/message`

`/var/log/auth.log`

`/var/log/secure`

`/var/log/boot.log`

`/var/log/dmesg`

`/var/log/cron`

— Segurança em redes sem fio (802.11)

Como os protocolos da internet foram concebidos para operação cabeada, a adoção de canais de rádio para tráfego de dados trouxe desafios como (GOODRICH, 2013):

Espionagem de tráfego

Sequestro de sessão

Negação de serviço

**Personificação do Access
Point (AP)**

Intrusão

Verificação de identidade

— Segurança em redes sem fio (802.11)

Existem quadros 802.11 com finalidades específicas de interesse para a segurança:

Quadro de autenticação

Usado para a identificação de um cliente ao AP. Também usado para a resposta do AP ao usuário.

Quadro de associação

Caso a identificação tenha sido bem-sucedida, o usuário envia esse quadro para que o AP insira essa estação no seu mecanismo de controle de acesso ao meio físico.

Quadro de beacon

Quadro de “anúncio” da existência de uma rede.

— Segurança em redes sem fio (802.11)

Wired Equivalent Privacy (WEP)

Esse primeiro mecanismo apresentou problemas graves e atualmente não é recomendado. O WEP disponibiliza dois modelos de associação:

Sistema aberto

O cliente usa as informações de um quadro de beacon, como o SSID, canal e taxa de operação etc. para se associar sem a necessidade de chaves.

Chave compartilhada

Nesse modelo, cliente e AP precisam ter uma chave previamente compartilhada.

— Segurança em redes sem fio (802.11)

WPA

A Wi-Fi Alliance propunha o WPA, com ações bem objetivas para solucionar os problemas do WEP:

**Problemas com o IV
(initialization vector)**

CRC

Chaves estáticas

— Segurança em redes sem fio (802.11)

Modelos de autenticação WPA



WPA oferece diversos modelos de autenticação, incluindo login-senha, certificados e métodos EAP.



O cliente envia credenciais ao ponto de acesso (AP) que encaminha para o servidor de autenticação.



O servidor gera uma Master Session Key (MSK) para derivar chaves, dependendo da configuração.



A comunicação entre cliente e servidor ocorre via EAPoL, garantindo flexibilidade na segurança Wi-Fi.

— Segurança em redes sem fio (802.11)

WPA2

O WPA2, baseado no IEEE 802.11i, trouxe melhorias, incluindo:

- Compatibilidade com WEP (chaves de 40 ou 104 bits).
- TKIP para confidencialidade e integridade com chaves temporárias.
- CCMP para criptografia com AES e integridade com CMAC.
- Utiliza chaves criptográficas temporárias para segurança aprimorada.



— Segurança em redes sem fio (802.11)

IEEE 802.11w

O IEEE 802.11w aborda a proteção dos quadros de gerenciamento e controle, prevenindo ataques de negação de serviço, especialmente na injeção de quadros de desautenticação.



— Segurança em redes sem fio (802.11)

WPA3

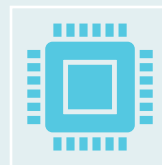


- WPA3 é uma evolução do Wi-Fi com maior segurança.
- Protege os quadros de gerenciamento e utiliza um método de autenticação robusto chamado SAE para criar chaves mais resistentes a ataques.

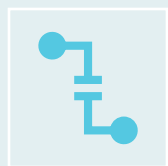
— Segurança de dispositivos internet of things (IOT)



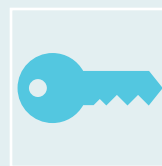
A rápida expansão de dispositivos IoT gera desafios de segurança devido a recursos limitados e vulnerabilidades.



Muitos dispositivos não atualizam firmware, têm autenticação fraca e comunicação não criptografada.

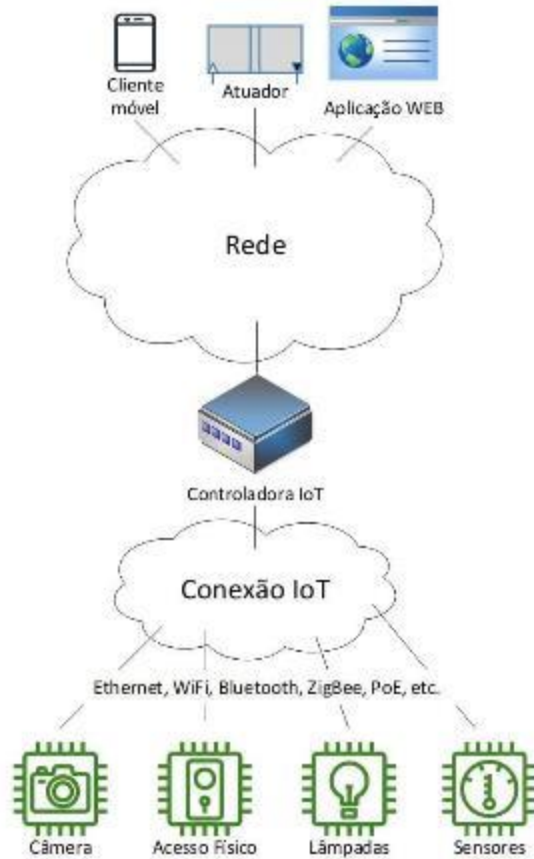


Integrar segurança a dispositivos IoT requer equilíbrio entre proteção e requisitos como baixo consumo de energia.



Soluções avançadas, como controladoras com autenticação e criptografia, podem afetar a interoperabilidade e a simplicidade necessárias para dispositivos IoT.

— Segurança de dispositivos internet of things (IOT)



Cenário de conectividade com IoT

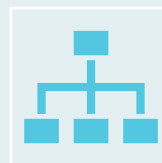
Respostas à incidentes e recuperação (disaster recovery)



— Conceitos básicos de evento e incidente



Evento: Qualquer ocorrência observável em um sistema de informação, como criação de arquivo.



Incidente: Evento que resulta em consequências negativas para a organização ou sistema, como um sistema crítico indisponível.



A resposta a incidentes é essencial para reduzir danos e custos de recuperação.



Deve ser uma prática organizada e metodológica para tratar incidentes de segurança.

— Plano de resposta a incidentes e CSIRT

Organizações devem ter um plano de resposta a incidentes para lidar com problemas eficientemente. Isso é feito observando os seguintes passos:

Identifique e priorize
ativos

Identifique os riscos
potenciais

Estabeleça procedimentos

Configure uma equipe de
resposta

Treinamento

— Fases de uma metodologia de resposta a incidentes

Preparação



Preparação envolve definir políticas e planos para incidentes de segurança.



Inclui estabelecer uma equipe de resposta a incidentes e treiná-los.



Garanta que as políticas e planos sejam aprovados pela gerência.



Verifique se a equipe CSIRT está bem preparada com treinamento e simulações.

— Fases de uma metodologia de resposta a incidentes

Preparação

Os itens que compõem o checklist desta etapa:



Todos foram treinados com base nas políticas de segurança?



As políticas de segurança e o plano de resposta a incidentes foram aprovados pela gerência apropriada?



A CSIRT conhece suas funções e as notificações necessárias para fazê-lo?



Todos os membros da CSIRT participaram de simulações?

— Fases de uma metodologia de resposta a incidentes

Detecção e análise

Fase de detecção visa identificar desvios e determinar se são incidentes.



Usar registros, alertas IDS e firewall para detecção.



Comparar com métricas pré-estabelecidas para confirmar incidentes.



Notificar CSIRT e estabelecer canais de comunicação.



Nomear um analista forense para avaliar e coletar evidências.



Documentar todos os aspectos do processo de detecção e escopo.

— Fases de uma metodologia de resposta a incidentes

Detecção e análise

Itens que compõem o checklist dessa etapa:

**Quando o evento
aconteceu?**

Como foi detectado?

Quem o descobriu?

**Alguma outra área foi
impactada?**

**Qual é o escopo do
comprometimento?**

**Isso afeta as operações
em qual nível?**

**A fonte (vetor de entrada)
do evento foi descoberta?**

— Fases de uma metodologia de resposta a incidentes

Contenção

Esta fase foca na limitação de perdas e prevenção de mais danos. Ela inclui várias subetapas, e cada uma delas é vital para a mitigação completa e a preservação adequada das evidências.

Contenção de curto prazo

Limita o dano assim que possível, bem como isola um único ativo ou um determinado segmento de rede.

Backup do sistema

Cria uma imagem duplicada do sistema afetado (snapshot) antes de qualquer outra ação, para garantir a preservação das evidências.

Contenção de longo prazo

Deixa o sistema afetado temporariamente desativado para reparo, de forma que os processos de negócio suportados por ele possam ser retomados por meio do restante do processo de resposta de incidente.

— Fases de uma metodologia de resposta a incidentes

Contenção

Itens que compõem o checklist desta etapa:



O que foi feito para conter o incidente em curto prazo?



O que foi feito para conter o incidente em longo prazo?



Algun malware descoberto foi colocado em quarentena do resto do ambiente?



Que tipo de backups existem?



Todas as credenciais comprometidas foram revisadas quanto à legitimidade e reforçadas?

— Fases de uma metodologia de resposta a incidentes

Erradicação

Nesta fase de erradicação de incidentes:

- Restaure os sistemas afetados para o estado operacional desejado.
- Implemente controles adicionais para evitar recorrências.
- Atualize a documentação de incidentes.
- Registre custos e horas de trabalho para avaliar o impacto geral do incidente.



— Fases de uma metodologia de resposta a incidentes

Erradicação

Itens que compõem o checklist desta etapa:

Os artefatos do invasor foram removidos com segurança?

O sistema foi “hardenizado”, sanitizado e as atualizações de segurança foram aplicadas?

O sistema pode ser refeito?

— Fases de uma metodologia de resposta a incidentes

Recuperação

Na fase de reintegração dos sistemas afetados:

- Reintroduza sistemas no ambiente de produção com testes e monitoramento cautelosos.
- Defina o tempo para restauração das operações, em consenso com a CSIRT e a área de negócio afetada.
- Especifique as ferramentas de teste e medidas para garantir a funcionalidade dos sistemas.
- Estabeleça o tempo de monitoramento pós-restauração para detecção de desvios.



— Fases de uma metodologia de resposta a incidentes

Recuperação

Itens que compõem o checklist desta etapa:

- Quando os sistemas podem retornar à produção?
- Os sistemas foram corrigidos e testados?
- O sistema pode ser restaurado a partir de um backup confiável (íntegro)?
- Por quanto tempo os sistemas afetados serão monitorados e o que será monitorado durante esse tempo?
- Quais ferramentas garantirão que incidentes semelhantes não ocorram novamente?

— Fases de uma metodologia de resposta a incidentes

Recuperação

Algumas questões a serem respondidas nesta etapa:

Quais mudanças precisam ser feitas?

Como o treinamento dos colaboradores e da CSIRT deve ser melhorado?

Qual vulnerabilidade foi explorada?

Quais garantias devem ser empregadas para que incidentes semelhantes não ocorram novamente?

— Processo de gestão de vulnerabilidades

- Identificação contínua de falhas e fraquezas nos ativos.
- Atividades contínuas para compreender e gerenciar vulnerabilidades, exigindo tempo e recursos.
- Correção de vulnerabilidades é uma etapa crítica para evitar incidentes.
- Objetivo: reduzir o risco associado às vulnerabilidades a níveis aceitáveis.



— Processo de gestão de vulnerabilidades

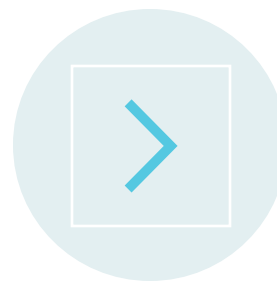
As principais etapas do processo de gestão de vulnerabilidades são:



— Processo de gestão de vulnerabilidades



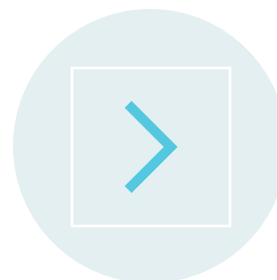
A etapa de classificação de risco contextualiza as vulnerabilidades encontradas com a relevância para o negócio.



As ferramentas de varredura usam padrões como CVE e CVSS para referenciar e classificar vulnerabilidades.



O CVE (Common Vulnerabilities and Exposures) fornece uma identificação única para cada vulnerabilidade.



O CVSS (Common Vulnerability Scoring System) classifica a severidade das vulnerabilidades.

— Processo de gestão de vulnerabilidades

CVE – Common Vulnerabilities and Exposures



Programa global da MITRE para identificar, definir e catalogar vulnerabilidades de segurança.



Atribui um número único no formato CVE-AAAA-NNNNN a cada vulnerabilidade.



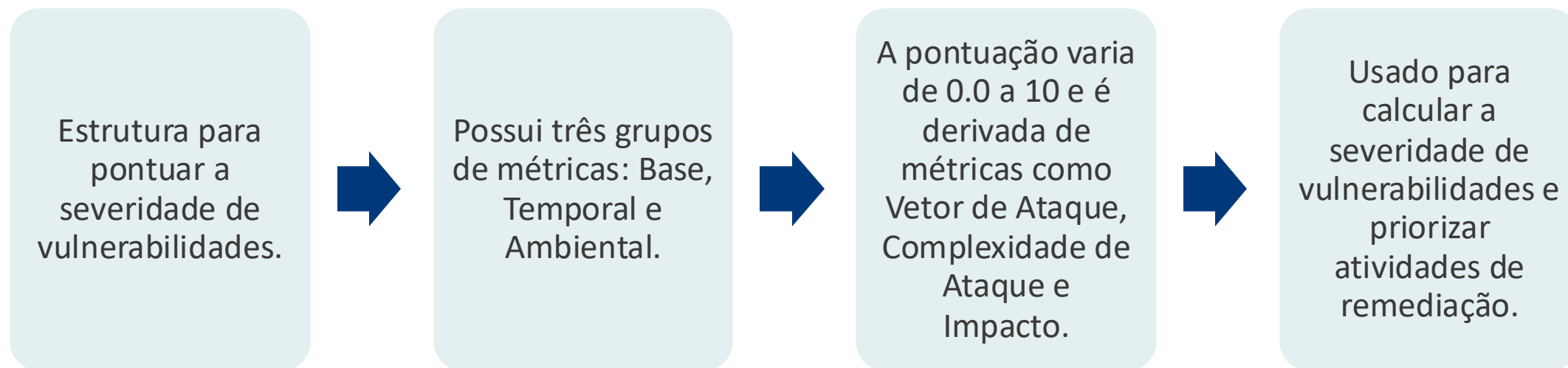
Usado por profissionais de TI e segurança para garantir a comunicação consistente e coordenação na resolução de vulnerabilidades.



Cada registro CVE inclui descrição, severidade, referências, histórico e data de publicação.

— Processo de gestão de vulnerabilidades

CVSS – Common Vulnerability Scoring System



— Processo de gestão de vulnerabilidades

Classificações de severidade das vulnerabilidades

- As classificações de severidade do CVSS (Common Vulnerability Scoring System) variam de Baixa (0.0 a 3.9) a Crítica (9.0 a 10.0).
- Por exemplo, a CVE-2016-0051 é classificada como Alta com um score de 7.9, indicando uma vulnerabilidade significativa.



— Processo de gestão de vulnerabilidades

Gerenciamento de patches



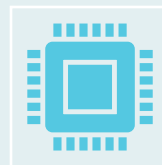
Norma ISO/IEC 27002:2013 recomenda testar controles em ambiente de homologação antes da produção.



É importante obter informações sobre vulnerabilidades e avaliar riscos.



Empresas têm muitos ativos e vulnerabilidades, necessitando gerenciamento de patches.



Patches são correções de vulnerabilidades em produtos de software e hardware.

— Processo de gestão de vulnerabilidades

Gerenciamento de patches

Patches podem ser classificados como:

Patch de correção

Hotfix

Rollup

Pacote de serviços (Service Pack)

— Processo de gestão de vulnerabilidades

Gerenciamento de patches

Como boas práticas para um processo de gerenciamento de patches, temos os seguintes passos:

**Identifique os
ativos**

Classifique

**Crie ambientes
agregados**

Monitore

Crie backup

Deploy

Continuidade

Documente

— Processo de gestão de vulnerabilidades

Gerenciamento de patches



Use uma ferramenta SCAP para verificar ativos semanalmente.



Realize verificações autenticadas com agentes locais ou scanners remotos com privilégios elevados.



Empregue uma conta dedicada para verificações autenticadas.



Automatize atualizações de sistemas e software de terceiros e verifique a correção de falhas periodicamente.

— Conceito de computação forense

Computação forense envolve a coleta e análise de evidências digitais após incidentes de segurança.

O Código de Processo Penal exige exames de corpo de delito; na computação forense, é o processo de coleta e análise de dados.

Combina Ciência da Computação e Criminalística para buscar materialidade e autoria de incidentes digitais.

Objetivo: identificar todos os agentes envolvidos em ações legais.

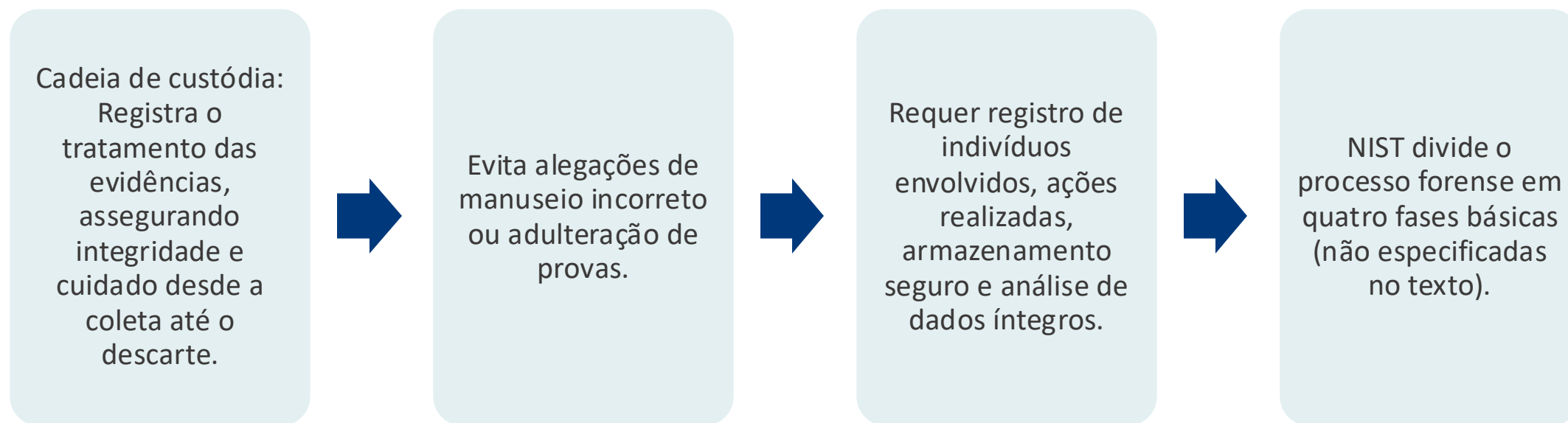
— O processo forense

- Local de crime: Espaço onde um delito ocorreu, com evidências para esclarecer dinâmica, autoria e materialidade.
- Local de crime informático: Local com ativos computacionais relacionados a um incidente investigado.
- Processo investigatório: Segue etapas padrão, incluindo ordem de volatilidade e cadeia de custódia, como em outras investigações.



— O processo forense

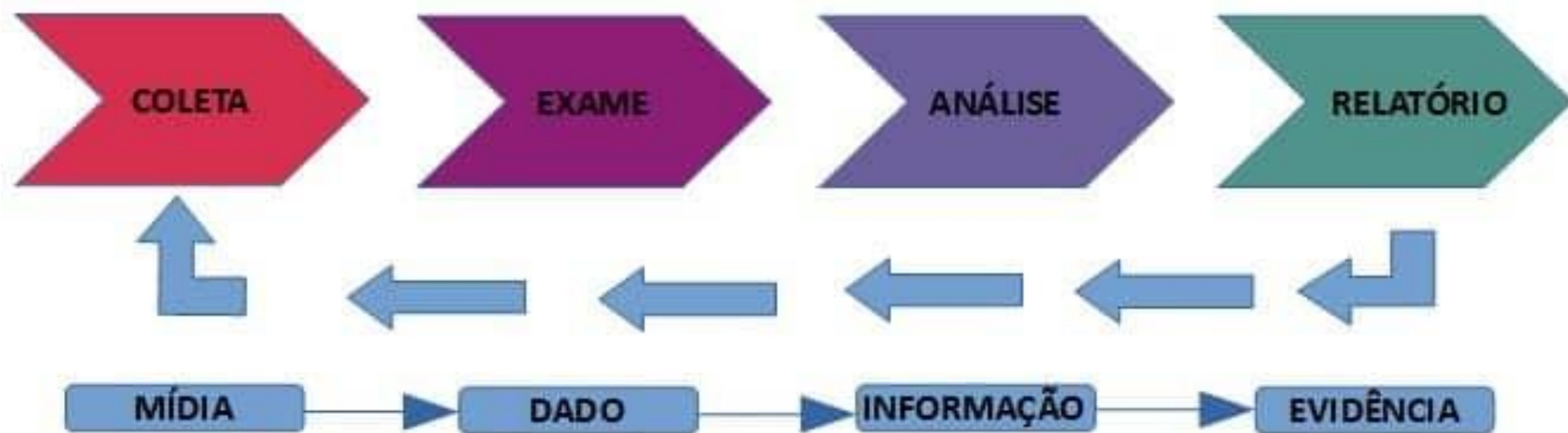
Cadeia de custódia



— O processo forense

Cadeia de custódia

O processo forense é dividido em quatro fases básicas:



— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados não voláteis

Garantir integridade da coleta é crucial para preservar o estado original dos dados.,

Aspectos comuns em file systems: arquivos deletados, slack space e espaço livre.

Arquivos deletados não são apagados, apenas seus ponteiros são marcados como excluídos.

Análise forense é realizada em uma cópia fiel da fonte de dados, garantindo preservação do material.

— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados não voláteis

As principais formas de cópia de dados são:

Backup lógico

Um backup lógico copia os diretórios e arquivos de um volume lógico.

Imagem

Também conhecida como imagem de disco, a imagem gera uma cópia bit a bit da mídia original, incluindo slack space e espaço livre.

— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados não voláteis

MAC Times



Metadados que registram eventos de modificação (modified), acesso (accessed) e criação (created) de arquivos.



Análise forense envolve a extração e análise de milhares de arquivos, exigindo discernimento para identificar os relevantes.

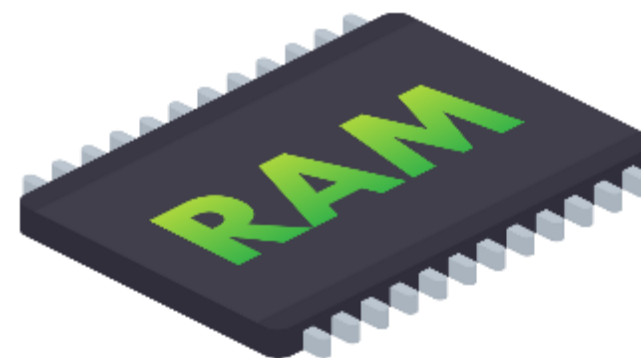


Tipos de arquivos comuns têm extensões como .JPG, .MP3, mas extensões podem ser alteradas, sendo necessário considerar o file header para identificação.

— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados voláteis

- Dados voláteis são perdidos quando a energia é cortada, como memória RAM, arquivos de swap e hibernação.
- No Windows, exemplos de arquivos voláteis incluem pagefile.sys, hiberfil.sys e swapfile.sys.



— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados voláteis

Algumas informações que podem ser obtidas através da coleta de dados da memória RAM são:

Configuração de rede

Conexões de rede

Processos em execução

Arquivos abertos

Sessões de login

Registros de hora

— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados voláteis

Arquivos de configuração

Arquivos de configuração particularmente interessantes são:

Tarefas agendadas

Arquivos de senha

Usuários e grupos

— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados voláteis

Arquivos de log

Arquivos de log interessantes são:

Event Logs

Audit Logs

Application Logs

— Aspectos, técnicas e ferramentas forenses

Coleta e análise de dados voláteis

Outros sistemas e aplicativos:

Command History

Recently Accessed Files

Application Files

Dump Files

Recently Accessed Files

Temporary Files

— Conceitos, métricas e estratégias de continuidade



Desastres são ações não planejadas que afetam negativamente os ativos críticos, causando perdas e crises.



Recuperação de desastres envolve reparar, reconstruir e substituir sistemas e pessoal após um desastre.



Gestão de continuidade busca identificar ameaças e seus impactos, garantindo a sobrevivência da organização.



Baseia-se na análise de riscos e de impacto no negócio.

— Conceitos, métricas e estratégias de continuidade

Análise de riscos

O gerenciamento de riscos é um processo cíclico que inclui quatro fases:

Avaliar

Analisar

Responder

Mitigar

— Conceitos, métricas e estratégias de continuidade

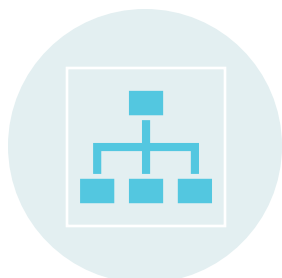
Análise de impacto no negócio



Análise de Impacto no Negócio (AIN) avalia os efeitos de interrupções em operações críticas.



Identifica e quantifica os riscos, chances de ocorrência e danos organizacionais.



Abrange todas as fases do negócio para tratar riscos em funções essenciais e sistemas críticos.



Exemplo: Avaliar custos e impactos de um ataque de ransomware que corrompe backups e indisponibiliza um sistema por cinco dias.

— Conceitos, métricas e estratégias de continuidade

Análise de impacto no negócio

Funções e sistemas críticos

Criticidade	Comprometimento
Muito Alta (5)	Poderá afetar toda a organização e as perdas serão catastróficas.
Alta (4)	Poderá afetar um ou mais negócios da organização e as perdas serão graves.
Média (3)	Poderá afetar parte dos negócios da organização e as perdas serão consideráveis.
Baixa (2)	Poderá afetar uma parte pequena e localizada da organização e as perdas serão baixas.
Muito Baixa (1)	Poderá afetar uma parte muito pequena e localizada da organização e as perdas serão mínimas.

- A importância é classificada qualitativa e quantitativamente, considerando o impacto na operação.
- **Exemplo:** o sistema de refrigeração de um centro de dados é mais crítico que o dos escritórios, devido ao risco de falhas catastróficas.
- Importância relativa é determinada para comparação e priorização.

— Conceitos, métricas e estratégias de continuidade

Análise de impacto no negócio

Funções e sistemas críticos

As métricas comuns que devem estar contidas na BIA incluem:

Tempo de inatividade máximo tolerável (MTD – Maximum Tolerable Downtime)

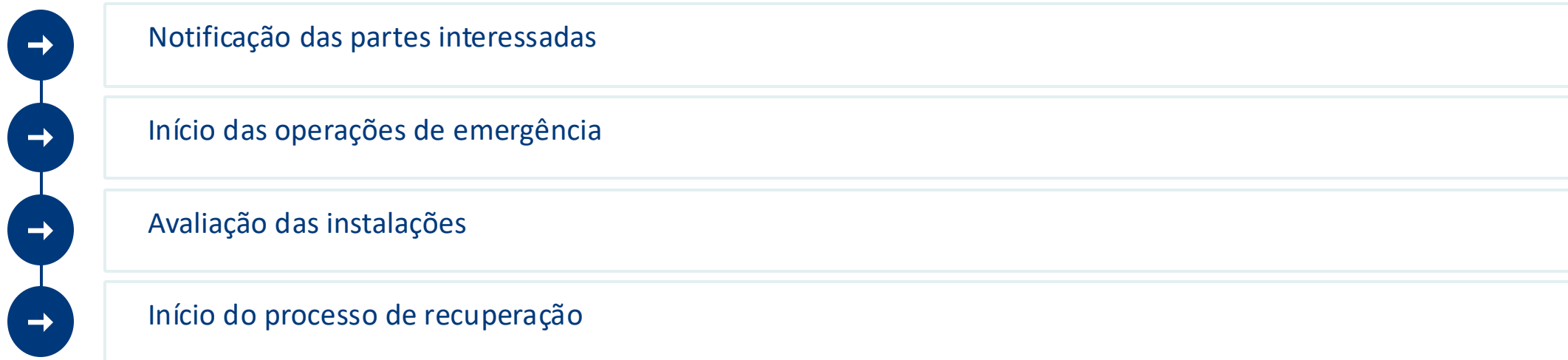
Objetivo do ponto de recuperação (RPO – Recovery Point Objective)

Objetivo do tempo de recuperação (RTO – Recovery Time Objective)

Tempo médio para reparar/substituir (MTTR – Mean Time to Repair)

— Ações a serem tomadas na ocorrência de um desastre

O processo de recuperação de desastres inclui diversas fases e viabiliza o retorno da operação do negócio. Em essência, o passo a passo da recuperação segue o seguinte roteiro:



— Ações a serem tomadas na ocorrência de um desastre

Locais de recuperação

Hot site

É uma rede alternativa totalmente configurada, que pode ficar on-line rapidamente após um desastre.

Warm site

É um local inativo ou que executa funções não críticas em condições normais de operação.

Cold site

É um local alternativo predeterminado, onde um ambiente de operações pode ser reconstruído após um desastre.

— Ações a serem tomadas na ocorrência de um desastre

Tipos de backup

Backup completo

Backup diferencial

Backup incremental

— Principais diretrizes a respeito dos processos de continuidade e recuperação de desastres

