

# Módulo 3 - Aulas 3 e 4

## Módulo 3: Técnicas utilizadas na identificação de ameaças

### Aula 3: Estratégias de resiliência

#### Objetivos

- ☒ Assimilar o conceito de resiliência em segurança da informação.
- ☒ Compreender sua importância para a continuidade dos negócios.
- ☒ Entender e aplicar algumas das estratégias práticas de resiliência.

#### Conceitos

- ☒ Resiliência de site de operações, diversidade, defesa em profundidade.
- ☒ Gerenciamento de configuração e ativos, controle de mudanças.
- ☒ Estratégias de disrupção e de engano (honeypots, honeynets, honeyfiles).

#### Introdução

Bem-vindos à aula sobre estratégias de resiliência em segurança da informação! Hoje, discutiremos as complexidades e desafios enfrentados pelas organizações, explorando estratégias essenciais para garantir a continuidade dos negócios e a segurança de dados. O objetivo central desta aula é capacitar os estudantes, futuros profissionais de segurança da informação, a compreenderem e aplicarem estratégias de resiliência.

A informação é um ativo valioso, e as organizações enfrentam uma série de desafios que vão desde a sua gestão eficaz até a resposta rápida a mudanças e incidentes. A resiliência em segurança da informação emerge como um importante pilar para enfrentar esses desafios, permitindo que as organizações se recuperem de eventos adversos e continuem operando com confiança.

À medida que avançamos, veremos como estratégias como o gerenciamento de ativos, controle de mudanças e resiliência de site de operações não são apenas teorias, mas abordagens práticas e fundamentais para garantir a segurança dos dados em organizações de todos os tamanhos e setores.

## **Gestão de configuração e mudança**

### **Gerenciamento de configuração**

O gerenciamento de configuração é uma prática em segurança da informação que se concentra na identificação, controle e manutenção de configurações de sistemas e software em uma infraestrutura. Envolve o estabelecimento de políticas, processos e ferramentas para gerenciar mudanças nas configurações, garantindo a integridade e segurança dos ativos de informação.

Os controles de resposta e recuperação referem-se a todo o conjunto de políticas, procedimentos e recursos criados para resposta e recuperação a incidentes e desastres. Esses controles são essenciais para a segurança cibernética, mas tornam-se cada vez mais difíceis de fornecer em grande escala. A resposta e a recuperação eficazes dependem muito de quão bem organizados estão os sistemas de TI no âmbito do site. Sem políticas organizacionais eficazes para administrar o gerenciamento de mudanças e configurações, a resposta e a recuperação são muito mais difíceis. O gerenciamento de configuração garante que cada componente da infraestrutura de TIC esteja em um estado confiável que não divirja de suas propriedades documentadas. O controle e o gerenciamento de alterações reduzem o risco de que alterações nesses componentes possam causar interrupção do serviço. O ITIL (Information Technology Infrastructure Library) é um guia de boas práticas e processos para entrega de serviços de TI bastante utilizado, mundialmente falando. No ITIL, o gerenciamento de configuração é implementado usando os seguintes elementos:

1. **Ativos de Serviço:** São coisas, processos ou pessoas que contribuem para a entrega de um serviço de TI.
2. **Item de Configuração (IC):** É um ativo que requer procedimentos de gerenciamento específicos para ser usado na entrega do serviço. Cada IC deve ser identificado por algum tipo de rótulo, de preferência usando uma convenção de nomenclatura padrão. CIs são definidos por seus atributos e relacionamentos, que são armazenados em um banco de dados de gerenciamento de configuração (CMDB).
3. **Configuração da Linha de Base:** É o modelo de configurações para o qual um dispositivo, instância de VM ou outro IC foi configurado e que deve continuar a operar. Você também pode registrar linhas de base de desempenho, como o rendimento alcançado por um servidor, para comparação com os níveis monitorados.
4. **Sistema de Gerenciamento de Configuração (CMS):** São as ferramentas e o banco de dados que coletam, armazenam, gerenciam, atualizam e apresentam informações sobre ICs e seus relacionamentos. Uma pequena rede pode capturar essas informações em planilhas e diagramas; existem aplicativos dedicados para CMS corporativo.
5. **Diagramas:** São a melhor maneira de capturar os relacionamentos complexos entre os elementos da rede. Os diagramas podem ser usados para mostrar como os ICs estão envolvidos nos fluxos de trabalho de negócios, topologias de rede lógica (IP) e física e layouts de rack de rede. Lembre-se, não basta simplesmente criar o diagrama, é preciso também mantê-lo atualizado.



Banco de Dados de Configuração.

## Gerenciamento de Ativos

O Gerenciamento de Ativos de TI (Tecnologia da Informação) refere-se a um conjunto de práticas e processos que visam identificar, monitorar, manter e proteger os ativos digitais de uma organização. Esses ativos podem incluir hardware, software, dados, redes e outros componentes relacionados à infraestrutura de tecnologia. Um processo de gerenciamento de ativos rastreia todos os sistemas críticos, componentes, dispositivos e outros objetos de valor da organização em um inventário. Também envolve a coleta e análise de informações sobre estes ativos para que seja possível embasar alterações ou de outra forma trabalhar com ativos para atingir os objetivos de negócio da organização.

Existem muitos pacotes de software e soluções de hardware associadas disponíveis para rastreamento e gerenciamento de ativos. Um banco de dados de

gerenciamento de ativos pode ser configurado para armazenar tanta informação quanto for considerado necessário, através de dados típicos como tipo, modelo, número de série, ID do ativo, localização, usuário(s), valor e informações de serviço. Os principais aspectos do Gerenciamento de Ativos envolvem:

1. **Identificação de Ativos:** O processo começa pela identificação completa e precisa de todos os ativos de TI em uma organização. Isso inclui servidores, computadores, dispositivos de rede, software instalado, dados armazenados e outros elementos relacionados à infraestrutura de TI.
2. **Classificação e Categorização:** Após a identificação, os ativos são classificados e categorizados com base em critérios específicos, como importância operacional, criticidade para o negócio, riscos associados e outros parâmetros relevantes.
3. **Monitoramento Contínuo:** O gerenciamento de ativos envolve a implementação de ferramentas e práticas para monitorar continuamente o estado e o desempenho dos ativos. Isso pode incluir o rastreamento de alterações nas configurações, a detecção de vulnerabilidades de segurança e a avaliação do uso e da eficiência dos recursos.
4. **Proteção e Segurança:** O gerenciamento de ativos também abrange estratégias para proteger os ativos de TI contra ameaças de segurança. Isso envolve a implementação de políticas de segurança, criptografia de dados, controle de acesso e outras medidas destinadas a garantir a integridade, confidencialidade e disponibilidade dos ativos.
5. **Manutenção e Atualização:** Os ativos de TI precisam ser regularmente mantidos e atualizados para garantir seu desempenho otimizado e a conformidade com os requisitos de segurança. Isso inclui a aplicação de patches de segurança, atualizações de software e manutenção preventiva de hardware.
6. **Descarte Adequado:** O fim do ciclo de vida de um ativo também faz parte do gerenciamento de ativos. Isso envolve o descarte adequado de hardware obsoleto, a desativação segura de contas de usuários e a garantia de que dados confidenciais sejam adequadamente removidos antes da eliminação de ativos.



Gerenciamento de Ativos.

### Controle de Mudança e Gerenciamento de Mudança

- **Controle de Mudança:** Um processo de controle de mudanças pode ser usado para solicitar e aprovar mudanças de forma planejada e controlada. As solicitações de mudança geralmente são geradas quando algo precisa ser corrigido, quando algo muda ou quando há espaço para melhorias em um processo ou sistema atualmente em funcionamento. A necessidade de mudança é frequentemente descrita como reativa, onde a mudança é imposta à organização, ou como proativa, quando a necessidade de mudança é iniciada internamente. As alterações também podem ser categorizadas de acordo com o seu impacto potencial e nível de risco (grande, significativo, menor ou normal, por exemplo). Em um processo formal de gerenciamento de mudanças, a necessidade ou os motivos da mudança e o procedimento para implementá-la são registrados em um documento de solicitação de mudança (RFC – Request for Change) e submetidos para aprovação.



A RFC será então apreciada no nível apropriado e as partes interessadas afetadas serão notificadas. Pode ser o supervisor ou gerente de departamento se a mudança for normal ou pequena. Mudanças importantes ou significativas podem ser gerenciadas como um projeto separado e exigir aprovação por meio de um conselho consultivo de mudanças (CAB). Elementos Comuns de uma RFC:

1. **Descrição da Mudança:** Detalhes claros e precisos sobre a natureza da mudança proposta, incluindo o que está sendo alterado, removido, ou adicionado.
  2. **Justificativa:** Uma explicação que fundamenta a necessidade da mudança. Isso pode incluir benefícios esperados, correção de problemas existentes, atendimento a requisitos regulatórios, entre outros.
  3. **Impacto da Mudança:** Uma análise dos possíveis impactos da mudança, tanto positivos quanto negativos. Isso pode abranger áreas como operações, segurança, desempenho e custos.
  4. **Plano de Implementação:** Um plano detalhado que descreve como a mudança será implementada, incluindo cronogramas, recursos necessários, testes a serem realizados e procedimentos de reversão (rollback) caso seja necessário desfazer a mudança.
  5. **Aprovação:** Um processo formal para a revisão e aprovação da RFC. Isso geralmente envolve uma equipe de gestão, um comitê de mudanças ou outras partes interessadas relevantes.
  6. **Documentação Pós-Implementação:** Após a implementação da mudança, a RFC pode ser atualizada para incluir informações pós-implementação, como resultados, lições aprendidas e qualquer ajuste adicional necessário.
- **Gerenciamento de Mudanças:** A implementação das mudanças deve ser cuidadosamente planejada levando em consideração como a mudança afetará os componentes dependentes. Para mudanças mais significativas ou importantes, as organizações devem tentar acompanhar a mudança primeiro. Cada mudança deve ser acompanhada por um plano de reversão (ou remediação), para que as mudanças possam ser agendadas com cautela, se houver probabilidade de causar tempo de inatividade do sistema, ou outro impacto negativo no fluxo de trabalho das unidades de negócios que dependem do sistema de TI que está sendo modificado. A maioria das redes possui um período de janela de manutenção programada para tempo de inatividade autorizado. Quando a mudança for implementada, o seu impacto deverá ser

avaliado e o processo revisado e documentado para identificar quaisquer resultados que possam ajudar futuros projetos de gestão de mudanças.

O gerenciamento de mudanças envolve uma série de processos destinados a planejar, avaliar, aprovar, implementar e validar mudanças em um ambiente organizacional. Os processos típicos de gerenciamento de mudanças podem variar dependendo do modelo específico de gerenciamento de serviços de TI adotado, como ITIL (Information Technology Infrastructure Library). Esses processos formam uma estrutura para garantir que as mudanças ocorram de maneira controlada, minimizando riscos e impactos adversos no ambiente operacional. Sua adoção promove a resiliência e a adaptabilidade de uma organização diante das mudanças necessárias em seus sistemas e serviços de TI. Abaixo estão os processos comuns associados ao gerenciamento de mudanças:

1. **Identificação e Registro de Mudanças:** Este processo envolve a identificação proativa de mudanças necessárias no ambiente de TI. Isso pode resultar de vários inputs, como melhorias identificadas, incidentes, ou requisitos de negócios. Suas atividades principais incluem: registro inicial da mudança, atribuição de um identificador único (número de RFC - Request for Change) e documentação da descrição, justificativa e impactos iniciais.
2. **Avaliação e Análise de Mudanças:** Este processo visa avaliar as mudanças propostas quanto à sua viabilidade, impacto e riscos associados. Suas atividades principais incluem: análise de impacto, avaliação de riscos, revisão de custos e benefícios e definição de uma estratégia de implementação.
3. **Aprovação de Mudanças:** Processo no qual as mudanças propostas são submetidas a uma revisão e aprovação formal antes de serem implementadas. As principais atividades incluem: apresentação da RFC para um comitê de mudanças ou gestores, revisão e avaliação da proposta, tomada de decisão sobre a aprovação.
4. **Planejamento de Mudanças:** Este processo envolve a elaboração de um plano detalhado para implementar a mudança, considerando cronogramas, recursos necessários e procedimentos de reversão. As principais atividades são: desenvolvimento de um plano de implementação, estabelecimento de cronogramas e marcos, atribuição de responsabilidades.
5. **Implementação de Mudanças:** A mudança é implementada conforme o plano desenvolvido, com monitoramento constante para garantir uma transição suave. As atividades principais incluem: execução do plano de implementação,



monitoramento em tempo real, aplicação de procedimentos de reversão, se necessário.

6. **Avaliação Pós-Implementação:** Este processo envolve a avaliação dos resultados da mudança após a implementação, incluindo revisão de desempenho, feedback do usuário e identificação de lições aprendidas. As atividades principais são: coleta de dados pós-implementação, comparação dos resultados com os objetivos, documentação de lições aprendidas.



Gerenciamento de Mudança.

## Resiliência em Instalações de TI

### Resiliência de Site de Operações

A resiliência de um site de operações refere-se à capacidade desse site de manter a continuidade operacional, mesmo diante de eventos adversos, falhas ou desastres. Existem diferentes abordagens para criar resiliência em um site de operações, classificadas geralmente como: Hot, Warm e Cold. Cada uma dessas categorias define o nível de preparação e prontidão para a restauração de serviços após uma interrupção. As redes empresariais geralmente fornecem resiliência no nível local. Um local alternativo de processamento ou recuperação é um local que pode fornecer o mesmo nível de serviço (ou similar). Um site de processamento alternativo pode estar sempre disponível e em uso, enquanto um site de recuperação pode levar mais tempo para ser configurado ou ser usado apenas em caso de emergência. A escolha entre hot, warm ou cold depende dos requisitos de negócios, do orçamento disponível e da tolerância ao tempo de inatividade. Cada abordagem oferece um equilíbrio diferente entre custo e tempo de recuperação.

As operações são projetadas para fazer failover no novo site até que o site anterior possa ser colocado online novamente. Failover é uma técnica que garante que um componente, dispositivo, aplicativo ou site redundante possa assumir de forma rápida e eficiente a funcionalidade de um ativo que falhou. Por exemplo, os balanceadores de carga fornecem failover caso um ou mais servidores ou sites atrás do balanceador de carga estejam inativos ou estejam sendo levados para um servidor ou site de processamento alternativo. Assim, servidores redundantes no conjunto de balanceadores garantem que não haja interrupção, por mínima que seja, do serviço. A seguir apresentaremos as diferentes abordagens e suas características para criação de resiliência de site:

1. **Site de Operações Hot:** Um site "hot" é totalmente funcional e pronto para entrar em operação imediatamente em caso de falha no site principal. A infraestrutura, todos os sistemas e dados necessários estão ativos e em funcionamento. Um hot site geralmente envolve a duplicação exata de todos os sistemas, aplicativos e dados do site principal para o site de contingência. Isso é alcançado por meio de tecnologias de replicação em tempo real. Em caso de falha no site principal, a transição para o hot site é praticamente instantânea, minimizando o tempo de inatividade. Suas características incluem:
  - Hardware e software totalmente configurados.
  - Dados sincronizados em tempo real entre o site principal e o site de contingência.
  -

- Rápido tempo de recuperação, praticamente sem tempo de inatividade percebido.
2. **Site de Operações Warm:** Um site "warm" é parcialmente funcional e requer algum tempo para ser totalmente operacional. Normalmente, parte da infraestrutura e dos dados já está configurada, mas algumas atividades manuais podem ser necessárias para ativar completamente o site. Um warm site pode envolver a configuração de parte da infraestrutura antes do incidente, mas pode exigir intervenção manual para estar completamente operacional. Dados podem ser sincronizados regularmente, mas atrasos podem ocorrer, dependendo da frequência das atualizações. Entre suas características estão:
- Parte da infraestrutura está pré-configurada.
  - Dados podem não estar totalmente sincronizados, mas são atualizados regularmente.
  - Tempo de recuperação mais rápido do que um site "cold", mas mais lento do que um site "hot".
3. **Site de Operações Cold:** Um site "cold" é basicamente uma instalação vazia que pode ser configurada quando necessário. Não há infraestrutura operacional nem dados em tempo real. Um cold site requer configuração manual extensiva. Isso pode envolver a instalação de hardware, software e a restauração de dados. Geralmente, é mais econômico do que as opções hot e warm, mas o tempo de recuperação é significativamente mais longo. Suas características incluem:
- Nenhum hardware ou software configurado.
  - Dados podem estar desatualizados ou não disponíveis.
  - Maior tempo de recuperação, pois requer configuração manual e restauração de dados.



Resiliência de Site de Operações.

## Defesa em Profundidade e Diversidade

A combinação de diversidade e defesa em profundidade cria uma resiliência robusta em um site de operações. A diversidade protege contra falhas específicas, enquanto a defesa em profundidade oferece uma estratégia multifacetada para proteger contra uma ampla variedade de ameaças e desafios de segurança. Essas abordagens trabalham em conjunto para fortalecer a postura de segurança e resiliência de um site.

1. **Defesa em Profundidade:** A segurança em camadas é normalmente vista como uma melhoria da resiliência da segurança cibernética porque fornece defesa profunda. A ideia é que, para comprometer totalmente um sistema, o invasor deve passar por vários controles de segurança, proporcionando diversidade de controle. Estas camadas reduzem a superfície potencial de ataque e tornam muito mais provável que um ataque seja dissuadido ou evitado, ou pelo menos detectado e depois evitado por intervenção manual.

A defesa em profundidade é uma estratégia que envolve a implementação de camadas múltiplas de segurança para proteger sistemas e dados. Em resiliência de site, isso significa que não se baseia em uma única linha de defesa, mas em várias

camadas que precisam ser atravessadas antes que um ataque ou falha possa causar danos significativos. Essa abordagem proativa minimiza a probabilidade de sucesso de um ataque e reduz os impactos quando uma falha ocorre. Os níveis de implementação podem ser:

- **Camadas de Segurança:** Implementação de controles de segurança em várias camadas, incluindo firewall, antivírus, sistemas de detecção de intrusões, controle de acesso e criptografia, entre outros.
  - **Monitoramento Contínuo:** Monitoramento constante das operações do site para identificar atividades suspeitas ou falhas em tempo real. Isso permite uma resposta rápida a incidentes.
  - **Atualizações e Patches Regulares:** Manutenção proativa dos sistemas, aplicando regularmente atualizações de segurança e correções de software para corrigir vulnerabilidades conhecidas.
  - **Treinamento e Conscientização:** Investimento em programas de treinamento para a equipe, garantindo que todos os membros compreendam e sigam as práticas de segurança. Isso reduz a probabilidade de erros humanos que podem levar a falhas.
2. **Diversidade:** Aliado à defesa em profundidade está o conceito de segurança através (ou com) diversidade. A diversidade tecnológica refere-se a ambientes que são uma mistura de sistemas operacionais, aplicativos, linguagens de codificação, soluções de virtualização e assim por diante. A diversidade de controle significa que os níveis de controle devem combinar diferentes classes de controles técnicos e administrativos com a gama de controles que previnem, detectam, corrigem e dissuadem. No contexto de resiliência de site, refere-se à prática de incorporar elementos variados e distintos no design e operação de sistemas para mitigar riscos e aumentar a robustez. Essa estratégia busca reduzir a vulnerabilidade do site a falhas únicas, seja por falhas de hardware, software, ou mesmo eventos externos, como desastres naturais. A diversidade pode ser aplicada em vários níveis, incluindo:
- **Diversidade de Hardware e Software:** Utilização de diferentes tipos de hardware e software para executar funções críticas. Isso evita que uma única falha em um tipo específico de hardware ou software cause uma interrupção generalizada.
  - **Diversidade de Fornecedores:** Adoção de soluções de diferentes fornecedores para garantir que a dependência de um único provedor seja reduzida. Isso pode



ser aplicado a hardware, software, serviços em nuvem e outros componentes críticos.

- **Diversidade Geográfica:** Distribuição de recursos e operações em locais geográficos distintos. Isso ajuda a mitigar riscos relacionados a eventos regionais, como desastres naturais, que podem afetar negativamente um local, mas não necessariamente outro.

## Estratégias de Defesa Ativa

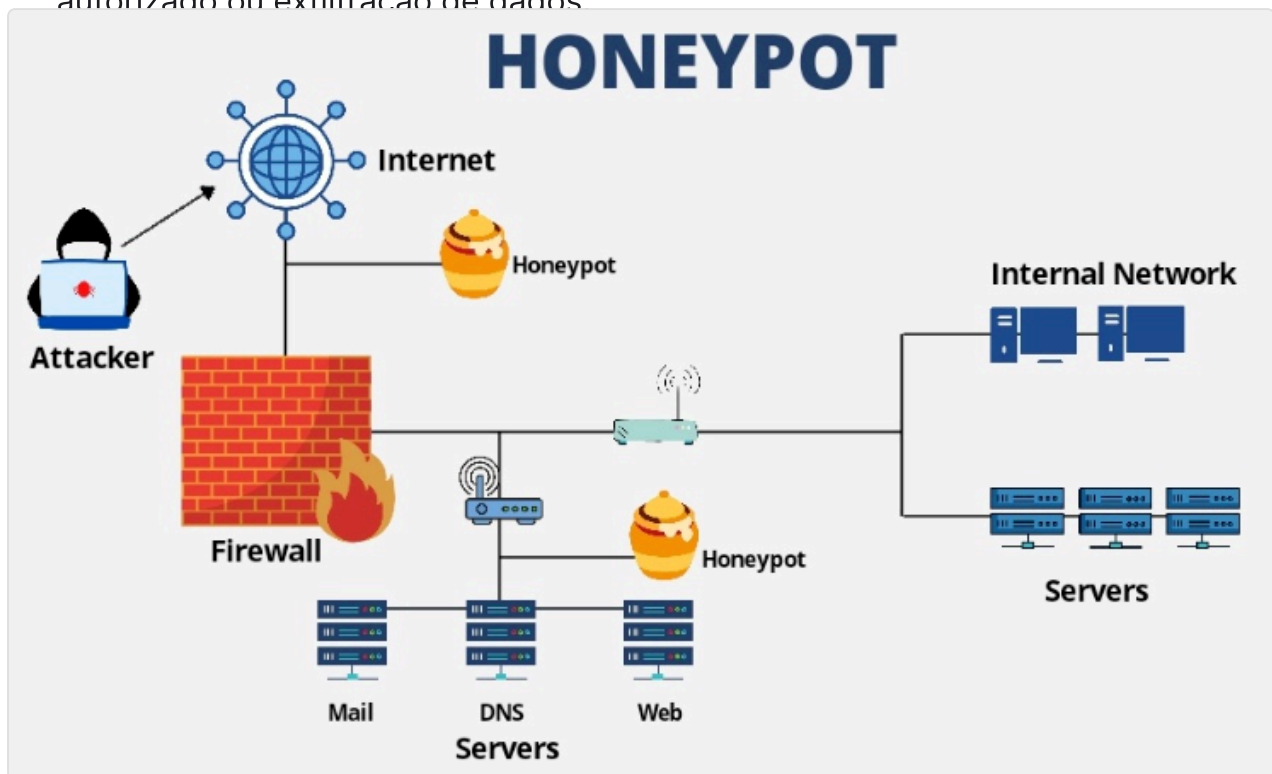
### Estratégias de Engano

A defesa ativa significa um envolvimento com o adversário, mas isto pode ser interpretado de diversas maneiras diferentes. Um tipo de defesa ativa envolve a utilização de recursos chamariz para atuar como isca. É muito mais fácil detectar invasões quando um invasor interage com um recurso chamariz, porque você pode controlar com precisão o tráfego de linha de base e o comportamento normal de uma forma que é mais difícil de fazer para ativos de produção. Veremos a seguir as seguintes estratégias de engano:

1. **Honeypot:** Um honeypot é um recurso de segurança projetado para ser alvo de ataques, desviando a atenção de sistemas reais. Existem dois tipos principais: honeypots de baixa interação, que emulam serviços sem expor vulnerabilidades reais, e honeypots de alta interação, que simulam sistemas operacionais completos e serviços reais. Ao atrair atacantes para um ambiente falso, os honeypots permitem que as organizações estudem táticas, técnicas e procedimentos (TTPs) de potenciais adversários. Isso facilita a detecção precoce e a resposta a ameaças reais.
2. **Honeynet:** Uma honeynet é uma rede de honeypots interconectados. Essa abordagem amplia as capacidades do honeypot, permitindo a observação de atividades coordenadas em uma escala maior. Honeynets proporcionam uma visão mais abrangente das estratégias de ataque, pois simulam uma rede real. Elas são particularmente eficazes para a detecção de ataques coordenados e campanhas maliciosas mais amplas.
3. **Honeyfile:** Um honeyfile é um arquivo fictício projetado para atrair atividades maliciosas. Pode ser usado para detectar tentativas de acesso não autorizado a informações específicas. Ao monitorar e analisar atividades em torno do



honeypot, as organizações podem identificar tentativas de acesso não autorizado ou exfiltração de dados.



Honeypot.

## Estratégia de Disrupção

A estratégia de interrupção, como parte das estratégias de defesa ativa, busca ativamente interromper ou perturbar as atividades maliciosas de um atacante para minimizar os danos e proteger os ativos da organização. Essa abordagem visa tornar mais difícil para os atacantes alcançar seus objetivos, desencorajando ou limitando seu progresso. A interrupção pode ser aplicada em diferentes níveis, desde a camada de rede até a aplicação, e pode envolver a introdução de obstáculos, restrições ou respostas automáticas. Os principais componentes da estratégia de interrupção incluem:

- **Interrupção na Camada de Rede:** Identificação e bloqueio proativo de tráfego malicioso por meio de firewalls, sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS). Implementação de filtros de pacotes para bloquear endereços IP, portas ou padrões de tráfego associados a atividades maliciosas.
- **Interrupção na Camada de Sistema:** Suspensão ou restrição temporária de contas de usuário suspeitas ou comprometidas para impedir o acesso não

autorizado. Identificação e encerramento de processos ou serviços maliciosos em execução no sistema.

- **Interrupção na Camada de Aplicação:** Implementação de soluções para mitigar ataques de negação de serviço distribuído (DDoS), como redirecionamento de tráfego ou filtragem de pacotes. Desativação temporária de funcionalidades ou serviços críticos que possam ser alvo de exploração até que uma solução mais abrangente seja implementada.
- **Resposta Automatizada:** Desenvolvimento e implementação de scripts ou sistemas automatizados para responder rapidamente a eventos de segurança, como bloqueio automático de endereços IP ou isolamento de sistemas comprometidos.
- **Isolamento de Segmentos de Rede:** Isolamento de segmentos de rede suspeitos ou comprometidos para evitar a propagação lateral de um ataque. Desconexão temporária de serviços ou servidores para evitar que o ataque se propague para outros sistemas.

## Conclusão

Parabéns por ter finalizado a aula de Estratégias de Resiliência! Nesta aula exploramos elementos fundamentais para fortalecer a capacidade de uma organização de se adaptar, recuperar e prosperar diante de desafios, falhas ou ataques. As estratégias abordadas, desde o gerenciamento de configuração até as estratégias de defesa ativa, fornecem um conjunto robusto de ferramentas para promover a resiliência em ambientes de TI.

O Gerenciamento de Configuração destaca a importância do controle e documentação eficientes, enquanto o Gerenciamento de Ativos destaca a necessidade de identificar, monitorar e proteger ativos críticos. O Controle de Mudança e Gerenciamento de Mudança emerge como uma peça crucial para orientar transições suaves, mitigando riscos associados a mudanças operacionais.

A resiliência de site de operações, com abordagens Hot, Warm ou Cold, destaca a necessidade de preparação para lidar com situações de contingência. A diversidade e defesa em profundidade emergem como estratégias valiosas, garantindo que as organizações estejam protegidas contra uma variedade de ameaças.

As estratégias de defesa ativa, como honeypots, honeynets, honeyfiles e estratégias de interrupção, demonstram a importância de uma postura proativa na identificação e enfrentamento de ameaças. Essas estratégias não apenas fortalecem as defesas, mas também fornecem valiosa inteligência sobre os métodos empregados pelos adversários.

Em última análise, a resiliência não é apenas sobre evitar falhas, mas sobre como uma organização se adapta, aprende e se recupera diante de desafios. Ao implementar essas estratégias, as organizações podem não apenas resistir a eventos adversos, mas também prosperar em ambientes dinâmicos e potencialmente hostis. Ao cultivar uma cultura de resiliência, as organizações podem enfrentar os desafios do mundo digital com confiança e determinação.

## Aula 4: Análise de Tráfego TCP/IP

### Objetivos

- ☒ Entender os conceitos e utilidades de ferramentas de detecção de redes.
- ☒ Assimilar o potencial da avaliação da segurança no contexto das redes TCP/IP.
- ☒ Compreender conceito e utilidade de outras ferramentas como Wireshark.

### Conceitos

- ☒ Ferramentas de detecção de rede no ambiente TCP/IP como Nmap.
- ☒ Ipconfig, ifconfig, ping, arp, route, traceroute, tracert, Netstat e nslookup.
- ☒ Análise de pacotes com foco em Wireshark.

### Introdução

Bem-vindos à aula sobre Análise de Tráfego TCP/IP. Hoje abordaremos o tema da segurança organizacional, explorando ferramentas de detecção de rede no

contexto TCP/IP. No cenário atual, entender e proteger as redes torna-se imperativo e é exatamente isso que iremos tratar nas próximas horas.

A análise de tráfego é como um raio-x para as redes, permitindo-nos compreender e avaliar sua saúde e segurança. Ao longo desta aula, examinaremos ferramentas essenciais, como Ipconfig, ifconfig, ping, arp, route, traceroute, tracert, pathping, Ip Scanners, Service Discovery com Nmap, Netstat e nslookup. Cada uma delas desvendará camadas do tecido complexo que compõe as redes de comunicação.

Além disso, exploraremos outras ferramentas de reconhecimento e varredura, ampliando nosso conhecimento para enfrentar desafios específicos na segurança cibernética. Nesta mesma linha veremos a análise de pacotes com Wireshark, entendendo como essa ferramenta nos permite observar e compreender o fluxo de dados em um nível granular. Ao final desta aula, teremos um entendimento das ferramentas essenciais de detecção de rede e seremos capazes de aplicar esse conhecimento na prática.

## **Avaliação da Segurança Organizacional**

A avaliação de segurança refere-se a processos e ferramentas que avaliam a superfície de ataque. Com o conhecimento das táticas e capacidades do adversário, você pode avaliar se os pontos na superfície de ataque são vetores de ataque potencialmente vulneráveis. O resultado da avaliação são recomendações para implantar, aprimorar ou reconfigurar controles de segurança para mitigar o risco de vulnerabilidades serem exploradas por agentes de ameaças.

### **Ferramentas de detecção de rede**

O reconhecimento é um tipo de atividade de avaliação que mapeia a superfície de ataque potencial, identificando os nós e conexões que compõem a rede.

Periodicamente, você precisará executar varreduras usando ferramentas de descoberta de topologia por meio de linha de comando e interface gráfica de usuário (GUI). Você precisará identificar as configurações do host usando ferramentas de fingerprint (método para identificar um dispositivo empregando uma combinação de atributos fornecidos pela configuração do dispositivo e de que forma será usado) e, capturar e analisar o tráfego de rede. Você também deve

entender como as ferramentas podem ser usadas para operar conexões backdoor com um host e para exfiltrar dados.

O processo de mapeamento da superfície de ataque é conhecido como reconhecimento e descoberta de rede. As técnicas de reconhecimento podem ser usadas por agentes de ameaças, mas também por profissionais de segurança para sondar e testar seus próprios sistemas de segurança, como parte de uma avaliação de segurança e monitoramento contínuo. Dessa maneira, a descoberta de topologia (ou "footprinting") significa verificar hosts, intervalos de IP e rotas entre redes para mapear a estrutura da rede de destino. A descoberta de topologia também pode ser usada para construir um banco de dados de ativos e para identificar hosts não autorizados (detecção de sistema não autorizado) ou erros de configuração de rede. Tarefas básicas de descoberta de topologia podem ser realizadas usando as ferramentas de linha de comando integradas ao Windows e ao Linux. As ferramentas a seguir relatam a configuração IP e testam a conectividade no segmento ou sub-rede da rede local.

1. **ipconfig:** Mostra a configuração atribuída às interfaces de rede no Windows, incluindo o endereço de hardware ou controle de acesso à mídia (MAC), endereços IPv4 e IPv6, gateway padrão e se o endereço é estático ou atribuído por DHCP. Se o endereço for atribuído por DHCP, a saída também mostrará o endereço do DHCP servidor que forneceu a concessão.
2. **ifconfig:** Mostra a configuração atribuída às interfaces de rede no Linux.
3. **ping:** Investiga um host em um determinado endereço IP ou nome de host usando o Internet Control Message Protocol (ICMP). Você pode usar o ping com um script simples para realizar uma varredura de todos os endereços IP em uma sub-rede.
4. **arp:** Exibe o cache do protocolo de resolução de endereço (ARP) da máquina local. O cache ARP mostra o endereço MAC da interface associada a cada endereço IP com o qual o host local se comunicou recentemente. Isso pode ser útil se você estiver investigando uma suspeita de ataque de falsificação. Por exemplo, um sinal de ataque man-in-the-middle é quando o endereço MAC do IP do gateway padrão listado no cache não é o endereço MAC do roteador legítimo.



# Scan Network for IP Addresses

```

>arp -a
Interface: 192.168.1.41 --- 0x18
Internet Address      Physical Address      Type
192.168.1.1           b8-46-fc-7c-b8-50     dynamic
192.168.1.25          00-1b-a9-58-04-4e     dynamic
192.168.1.33          00-18-f3-23-50-d6     dynamic
192.168.1.36          0c-8f-ff-4c-92-c6     dynamic
192.168.1.37          60-30-d4-76-b8-c8     dynamic
192.168.1.40          b4-99-ba-de-66-90     dynamic
192.168.1.200         4c-9e-ff-c0-67-bc     dynamic
224.0.0.22           01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.0.2.2            01-00-5e-00-02-02     static
239.0.2.30           01-00-5e-00-02-1e     static
239.0.2.129          01-00-5e-00-02-81     static
239.0.2.153          01-00-5e-00-02-99     static
239.0.5.185          01-00-5e-00-05-b9     static
239.255.255.250      01-00-5e-7f-ff-fa     static

```

Comando arp.

## Configuração de rotas

As ferramentas a seguir podem ser usadas para testar a configuração de roteamento e a conectividade com hosts e redes remotas:

1. **route:** Visualize e configure a tabela de roteamento local do host. A maioria dos sistemas finais usa uma rota padrão para encaminhar todo o tráfego para redes remotas através de um roteador gateway. Se o host não for um roteador, entradas adicionais na tabela de roteamento poderão ser suspeitas.
2. **tracert:** Usa testes ICMP para relatar o tempo de ida e volta (RTT) para saltos entre o host local e um host em uma rede remota. tracert é a versão Windows da ferramenta.
3. **tracert:** Realiza descoberta de rotas a partir de um host Linux. traceroute usa testes UDP em vez de ICMP, por padrão.
4. **pathping:** Fornece estatísticas de latência e perda de pacotes ao longo de uma rota durante um período de medição mais longo. O pathping é uma ferramenta do MS-Windows; o equivalente no Linux é mtr. Num contexto de segurança, a alta latência no gateway padrão em comparação com uma linha de base pode indicar um ataque man-in-the-middle. A alta latência em outros saltos pode ser um sinal de negação ou serviço, ou apenas indicar congestionamento na rede.



```

tabela de roteamento de n1-LinuxRouter1 antes da configuração
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf#
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.0.248 0.0.0.0 255.255.255.252 U 0 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth3

configuração de roteamento estático (adição manual de rotas)
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf#
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf# route add -net 192.168.8.0/24 gateway 192.168.0.250
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf# route add -net 192.168.9.0/24 gateway 192.168.0.250
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf#

tabela de roteamento de n1-LinuxRouter1 depois da configuração
root@n1-LinuxRouter1:/tmp/pycore.52850/n1-LinuxRouter1.conf# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.0.248 0.0.0.0 255.255.255.252 U 0 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth3
192.168.8.0 192.168.0.250 255.255.255.0 UG 0 0 0 eth0
192.168.9.0 192.168.0.250 255.255.255.0 UG 0 0 0 eth0

```

Comando route.

## Scanners IP e Nmap

A varredura de uma rede usando ferramentas como ping consome tempo, não é confiável e não retorna resultados detalhados. A maior parte da descoberta de topologia é realizada usando uma ferramenta de scanner IP dedicada. Um scanner IP realiza a descoberta de hosts e identifica como os hosts estão conectados em uma rede. Para auditoria, existem suítes corporativas, como os produtos System Center da Microsoft. Esses conjuntos podem receber credenciais para realizar varreduras autorizadas e obter informações detalhadas do host por meio de protocolos de gerenciamento, como o Simple Network Management Protocol (SNMP).

O Nmap Security Scanner (nmap.org) é um dos scanners IP de código aberto mais populares. O Nmap pode usar diversos métodos de descoberta de host, alguns dos quais podem operar furtivamente e servir para derrotar mecanismos de segurança, como firewalls e detecção de intrusões. A ferramenta é um software de código aberto com pacotes para a maioria das versões do Windows, Linux e macOS. Pode ser operado com linha de comando ou via GUI (Zenmap).


## Descoberta de serviço e Nmap

Tendo identificado hosts IP ativos na rede e obtido uma ideia da topologia da rede, o próximo passo no reconhecimento da rede é descobrir quais sistemas

operacionais estão em uso, quais serviços de rede cada host está executando e, se possível, qual software aplicativo está sustentando esses serviços. Este processo é descrito como descoberta de serviço. A descoberta de serviços também pode ser usada defensivamente, para investigar possíveis sistemas não autorizados e identificar a presença de portas de serviços de rede não autorizadas.

- **Descoberta com Nmap:** Quando o Nmap conclui uma varredura de descoberta de host, ele reportará o estado de cada porta varrida para cada endereço IP no escopo. Neste ponto, você pode executar verificações adicionais de descoberta de serviço em um ou mais endereços IP ativos. Algumas das principais opções para verificações de descoberta de serviço são:
  1. **TCP SYN (-sS):** Esta é uma técnica rápida também conhecida como varredura semiaberta, pois o host de varredura solicita uma conexão sem reconhecê-la. A resposta do alvo ao pacote SYN da varredura identifica o estado da porta.
  2. **Varreduras UDP (-sU):** Verifica portas UDP. Como estes não usam ACKs, o Nmap precisa esperar por uma resposta ou tempo limite para determinar o estado da porta, portanto a varredura UDP pode demorar muito. Uma varredura UDP pode ser combinada com uma varredura TCP.
  3. **Intervalo de portas (-p):** Por padrão, o Nmap verifica 1.000 portas comumente usadas, conforme listado em seu arquivo de configuração. Use o argumento -p para especificar um intervalo de portas.
- **netstat e nslookup:** Tarefas básicas de descoberta de serviços também podem ser executadas usando ferramentas integradas aos sistemas operacionais Windows e Linux:
  1. **netstat:** Mostra o estado das portas TCP/UDP na máquina local. O mesmo comando é usado no Windows e no Linux, embora com sintaxe de opções diferentes. Você pode usar o netstat para verificar configurações incorretas de serviço (talvez um host esteja executando um servidor web ou FTP que um usuário instalou sem autorização). Você também poderá identificar conexões remotas suspeitas com serviços no host local ou do host para endereços IP remotos. Se você estiver tentando identificar malware, a saída mais útil do netstat é mostrar qual processo está escutando em quais portas.
  2. **nslookup/dig:** Consulta registros de nomes para um determinado domínio usando um DNS específico resolvido no Windows (nslookup) ou Linux (dig). Um invasor pode testar uma rede para descobrir se o serviço DNS está

configurado incorretamente. Um DNS mal configurado pode permitir uma transferência de zona, o que dará ao invasor os registros completos de cada host no domínio, revelando muito sobre a forma como a rede está configurada.



```
kali@kali:~$ nmap -p445 --script smb-vuln-ms17-010 192.168.171.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-08 11:46 EDT
Nmap scan report for 192.168.171.129
Host is up (0.0012s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
  smb-vuln-ms17-010:
    VULNERABLE:
      Remote Code Execution (SMBv1) (ms17-010)
      State: VULNERABLE
      IDs: CVE:CVE-2017-0143
      Risk factor: HIGH
      A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

  Disclosure date: 2017-03-17
  References:
    https://technet.microsoft.com/en-us/library/2017-03-17-010.aspx
    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
kali@kali:~$
```

Descoberta com Nmap.

## Análise de pacotes e Wireshark

Um analisador de protocolo (ou analisador de pacotes) funciona em conjunto com um sniffer para realizar análises de tráfego. Você pode analisar uma captura ao vivo ou abrir um arquivo de captura salva (.pcap). Os analisadores de protocolo podem decodificar um quadro capturado para revelar seu conteúdo em um formato legível. Você pode optar por visualizar um resumo do quadro ou escolher uma visualização mais detalhada que forneça informações sobre a camada OSI, protocolo, função e dados.

Wireshark (wireshark.org) é um utilitário gráfico de captura e análise de pacotes de código aberto, com pacotes de instalação para a maioria dos sistemas operacionais. Tendo escolhido a interface para escutar, a saída é exibida em uma visualização de três painéis. O painel da lista de pacotes mostra um resumo de rolagem dos quadros. O painel de detalhes do pacote mostra campos expansíveis no quadro atualmente selecionado na lista de pacotes. O painel de bytes de pacote mostra os dados brutos do quadro em hexadecimal e ASCII. O Wireshark é capaz

de analisar (interpretar) os cabeçalhos e payloads de centenas de protocolos de rede.

Severity	Summary	Group	Protocol	Count
Error	Malformed Packet (Exception occurred)	Malformed	HTTP	13
Error	Malformed Packet (Exception occurred)	Malformed	JFIF (JPEG) ...	2
Warning	Illegal characters found in header name	Protocol	HTTP	1636
Note	ACK to a TCP keep-alive segment	Sequence	TCP	23
Note	TCP keep-alive segment	Sequence	TCP	23
Note	Duplicate ACK (#1)	Sequence	TCP	1
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Chat	Connection finish (FIN)	Sequence	TCP	12
Chat	GET /download.html HTTP/1.1\r\n	Sequence	HTTP	40
Chat	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	12
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	12
Comment	Packet comments listed below.	Comment	Frame	1

Caça a Ameaças com Wireshark.

## Conclusão

Ao encerrarmos esta aula sobre Análise de Tráfego TCP/IP, é gratificante refletir um pouco sobre os conhecimentos adquiridos começando pela importância da segurança organizacional em um cenário digital em constante evolução. Ao longo da aula, buscamos compreender o papel vital de ferramentas como Ipconfig, ifconfig, Ping, Arp, Route, Traceroute, Tracert, Pathping, Ip Scanners, Service Discovery com Nmap, Netstat e Nslookup para reconhecimento e varredura de redes. Cada uma dessas ferramentas se revelou uma peça-chave no quebra-cabeça da análise de tráfego. Aprofundamos nosso entendimento na análise de pacotes, destacando o poderoso Wireshark como uma ferramenta que permite observar e compreender o fluxo de dados em um nível granular.

É importante ressaltar que o conhecimento adquirido hoje não é apenas teórico; buscamos proporcionar uma experiência prática. Através dos exercícios práticos, esperamos que tenham conseguido aplicar essas ferramentas e conceitos de forma significativa. Que esta aula tenha sido uma ponte para um entendimento mais profundo e para um futuro mais seguro no mundo das redes TCP/IP.

Agradecemos pela participação e parabenizamos por mais uma etapa vencida. Bom trabalho e sucesso em suas futuras explorações digitais!