Atividade Pratica 1

Tema:

- ***”Dê outros exemplos, no mínimo 5 (cinco), de aplicações dos conteúdos de base que serão***

estudados na UC Sistemas Computacionais e Segurança – SCS, explicando cada um

Deles”

Conteúdos :

Segurança da Informação

Exemplo:

- **Malware**: Programas maliciosos como vírus, trojans e worms, que visam comprometer a segurança de sistemas.
- **Phishing**: Ataques que usam comunicações fraudulentas (geralmente via e-mail) para enganar usuários e coletar informações confidenciais, como senhas e dados financeiros.
- **Ransomware**: Tipo de malware que criptografa dados e exige pagamento para restaurar o acesso.

- **Ataques de Engenharia Social**: Manipulação psicológica que explora a confiança de usuários para obter informações confidenciais.

Ferramentas:

- **Criptografia**: Codifica dados para protegê-los contra acessos indevidos.
- **Firewalls**: Dispositivos que monitoram e controlam o tráfego de rede com base em regras de segurança predefinidas.

Práticas:

- **Política de Senhas Fortes**: Uso de senhas longas e complexas, com mudanças periódicas.
- **Atualizações Regulares**: Aplicação de patches de segurança para corrigir vulnerabilidades conhecidas.
- **Backups Frequentes**: Garantir que dados importantes tenham cópias de segurança para evitar perda permanente em caso de incidentes.

Explicação: Segurança da Informação é o conjunto de estratégias e práticas destinadas a proteger as informações de uma organização ou indivíduo contra acessos não autorizados, alterações, destruições ou interrupções. O objetivo central é garantir que os dados estejam disponíveis, íntegros e confidenciais, sem que pessoas não autorizadas

possam manipulá-los, A Segurança da Informação é crucial para a proteção dos ativos digitais e da reputação de empresas

VPN (Virtual Private Network)

Exemplo:

Benefícios:

1. **Privacidade e Anonimato**: Com a VPN, o endereço IP do usuário é ocultado, dificultando o rastreamento de suas atividades online.
2. **Segurança**: VPNs protegem os dados enviados e recebidos, especialmente ao usar redes Wi-Fi públicas, evitando interceptações.
3. **Acesso a Conteúdos Bloqueados**: VPNs permitem que o usuário acesse sites e serviços restritos a determinadas regiões, contornando censuras geográficas.
4. **Proteção contra Espionagem**: Governos, empresas ou criminosos não conseguem acessar os dados, pois a VPN cria uma camada extra de criptografia.

Tipos de VPN:

- **VPN de Acesso Remoto**: Conecta usuários individuais a uma rede privada. Muito usado por empresas para permitir que funcionários acessem recursos corporativos remotamente.

- **VPN de Site a Site**: Conecta redes de diferentes locais, permitindo que duas redes corporativas distantes se comuniquem de maneira segura.

Limitações:

- **Velocidade Reduzida**: Como os dados precisam passar por um servidor intermediário, a conexão pode ser mais lenta.
- **Custos**: VPNs de alta qualidade muitas vezes exigem uma assinatura paga para garantir servidores confiáveis e rápidos.

Explicação: Quando você utiliza uma VPN, todo o tráfego de internet do seu dispositivo passa primeiro por um servidor intermediário, que mascara o seu endereço IP real e o substitui por outro, normalmente localizado em uma região diferente. Essa conexão é criptografada, o que impede que terceiros, como hackers, provedores de internet ou governos, monitorem ou interceptem seus dados.

DLP (Data Loss Prevention)

Exemplo: **Funcionalidades:**

. Monitoramento de Dados: DLP monitora e inspeciona dados em trânsito, em repouso e em uso, identificando informações sensíveis, como números de cartão de crédito, segredos comerciais ou dados pessoais.

. Prevenção de Vazamento: Detecta e impede tentativas de enviar ou copiar dados confidenciais para fora da organização, como por e-mails, dispositivos USB ou uploads não autorizados.

. Classificação de Dados: Ajuda a classificar e marcar dados com base em sua sensibilidade, facilitando a aplicação de políticas de segurança.

. Criptografia: Automatiza a criptografia de dados sensíveis para garantir sua proteção caso sejam transferidos ou acessados de maneira indevida.

Benefícios do DLP:

- **Conformidade**: Ajuda a garantir que a organização esteja em conformidade com regulamentações como a LGPD, GDPR e HIPAA, que exigem proteção rigorosa de dados pessoais e sensíveis.
- **Redução de Riscos**: Minimiza os riscos de vazamento acidental de dados através de funcionários ou terceiros.

- **Proteção de Propriedade Intelectual**: Garante que informações críticas e exclusivas da empresa não sejam compartilhadas de forma indevida.

Benefícios do DLP:

- **Conformidade**: Ajuda a garantir que a organização esteja em conformidade com regulamentações como a LGPD, GDPR e HIPAA, que exigem proteção rigorosa de dados pessoais e sensíveis.
- **Redução de Riscos**: Minimiza os riscos de vazamento acidental de dados através de funcionários ou terceiros.
- **Proteção de Propriedade Intelectual**: Garante que informações críticas e exclusivas da empresa não sejam compartilhadas de forma indevida.

Explicação: um conjunto de ferramentas e processos projetados para proteger informações sensíveis contra acessos não autorizados, vazamentos ou perda. O objetivo principal do DLP é garantir que dados confidenciais, como informações financeiras, pessoais ou proprietárias, permaneçam dentro de uma organização e não sejam expostos acidentalmente ou intencionalmente.

Firewall:

Exemplo: Tipos de Firewalls:

Firewall de Filtro de Pacotes:

- Avalia cada pacote de dados individualmente com base em critérios como endereço IP, porta e protocolo.
- Rápido e eficiente, mas pode ser vulnerável a ataques mais sofisticados.

Firewall de Inspeção com Estado:

- Monitora o estado das conexões de rede e toma decisões de filtragem com base no contexto de uma conexão (estado da sessão).
- Mais seguro que o filtro de pacotes, pois analisa pacotes dentro do contexto de uma sessão.

Firewall Proxy:

- Atua como intermediário entre os usuários e a internet, bloqueando conexões diretas.
- Além de filtrar pacotes, inspeciona o conteúdo das mensagens para fornecer segurança adicional.

Benefícios:

- **Proteção contra ataques externos**: Bloqueia acessos não autorizados e ataques, como o *DDoS*.

- **Controle de Acesso**: Garante que apenas usuários e serviços autorizados possam se conectar à rede.
- **Monitoramento de Tráfego**: Permite monitorar o tráfego de rede para detectar atividades suspeitas.
- **Políticas Personalizadas**: Administradores podem definir regras específicas para diferentes tipos de tráfego e usuários.

Limitações:

- **Ameaças internas**: Firewalls são mais eficazes contra ameaças externas. Se um atacante conseguir contornar o firewall ou já estiver dentro da rede, sua eficácia pode ser limitada.

Explicação: Firewall é uma solução de segurança de rede que monitora e controla o tráfego de rede com base em regras de segurança predefinidas. O principal objetivo de um firewall é criar uma barreira entre uma rede confiável e outra rede externa, como a internet, protegendo os sistemas contra acessos não autorizados.

Os firewalls são fundamentais para qualquer estratégia de segurança de rede, protegendo contra uma ampla gama de ameaças e garantindo que apenas tráfego seguro e autorizado possa acessar os sistemas internos de uma organização.

Honeypot
Exemplo:

Tipos de Honeypots:

Honeypots de Produção: São colocados dentro da rede de uma organização para monitorar e atrair possíveis ataques reais. O foco é a segurança da rede e a detecção de invasores.

Honeypots de Pesquisa: Usados por pesquisadores para estudar métodos e tendências de ataques. O objetivo é coletar o máximo de informações possível sobre técnicas de ataque sem interferir diretamente na proteção de uma rede.

Benefícios dos Honeypots:

Detecção de ameaças desconhecidas: Como os honeypots não são utilizados por usuários legítimos, qualquer interação com eles é considerada suspeita, ajudando a identificar novas ameaças.

Análise de comportamento: Os honeypots fornecem insights sobre como os atacantes operam, suas motivações e as ferramentas que utilizam.

Redução de falsos positivos: Como o honeypot é projetado para não ter tráfego legítimo, ele facilita a identificação de atividades maliciosas sem muitos falsos alarmes.

Limitações:

Risco de exploração: Se mal configurado, o honeypot pode ser usado como ponto de entrada para ataques mais profundos na rede.

Alvo restrito: Um honeypot só detecta ataques direcionados a ele, o que significa que pode não capturar ameaças que visam outros sistemas ou áreas da rede.

Explicação: **Honeypots** são sistemas ou recursos de segurança que são deliberadamente configurados para parecer vulneráveis a ciberataques, com o objetivo de atrair potenciais atacantes. Eles são usados para monitorar, registrar e estudar comportamentos maliciosos, ajudando especialistas de segurança a entender táticas de invasores e desenvolver melhores defesas.

Um honeypot é implantado como um "alvo fácil" dentro de uma rede. Ele simula uma vulnerabilidade

ou fraqueza que pode atrair hackers ou malwares. Quando um atacante interage com o honeypot, suas atividades são monitoradas, permitindo que os administradores coletem informações valiosas, como técnicas de invasão e ferramentas utilizadas.