Modelo de "Contramedidas e Hardening" para a Disciplina de Segurança Cibernética

Introdução

Este modelo tem como objetivo fornecer um guia prático de contramedidas e hardening para aumentar a segurança dos sistemas e redes, abordando medidas que podem ser implementadas para mitigar vulnerabilidades comuns. Este guia é destinado aos alunos do curso de graduação em T.I. na disciplina de Segurança Cibernética.

1. Hardening de Sistemas Operacionais

1.1. Windows

- **Atualizações:** Mantenha o sistema operacional e todos os softwares atualizados.
- **Configuração de Política de Grupo (GPO):**
  - Desative contas de usuário padrão.
  - Configure políticas de senha (complexidade, expiração).
  - Limite tentativas de login.
- **Firewall do Windows:**
  - Habilite e configure regras de entrada e saída.
- **Desativação de Serviços Desnecessários:**
  - Desative serviços não utilizados para reduzir a superfície de ataque.
- **Controle de Conta de Usuário (UAC):**
  - Ative e configure o UAC para limitar ações administrativas.

1.2. Linux

- **Atualizações:** Use gerenciadores de pacotes (apt, yum) para manter o sistema e softwares atualizados.
- **Configuração do SSH:**
  - Desative o login de root via SSH.
  - Use autenticação baseada em chave pública.
- **Firewall (iptables/ufw):**
  - Configure regras restritivas para portas e serviços.
- **Desativação de Serviços Desnecessários:**
  - Desative serviços e daemons não utilizados.
- **Configurações de Senha:**
  - Configure políticas de senha no /etc/security/pwquality.conf.
- **SELinux/AppArmor:**
  - Ative e configure um dos frameworks de segurança para controle de acesso.

2. Hardening de Rede

2.1. Segmentação de Rede

- **Sub-redes:** Divida a rede em sub-redes menores para limitar a propagação de ataques.
- **VLANs:** Use VLANs para segmentar o tráfego de rede por função ou departamento.

2.2. Configuração de Firewall

- **Regras de Tráfego:** Configure regras para permitir apenas o tráfego necessário.
- **DMZ:** Utilize uma zona desmilitarizada (DMZ) para serviços públicos, isolando-os da rede interna.

2.3. IDS/IPS

- **Instalação e Configuração:** Implante e configure sistemas de detecção/prevenção de intrusões (Snort, Suricata).

3. Hardening de Aplicações Web

3.1. Configurações do Servidor Web

- **Apache/Nginx:**
  - Desative listagem de diretórios.
  - Limite o tamanho de uploads e downloads.
  - Use cabeçalhos de segurança (X-Frame-Options, X-Content-Type-Options, Content-Security-Policy).
- **SSL/TLS:**
  - Use certificados válidos.
  - Force HTTPS.
  - Desative protocolos e cifras fracas.

3.2. Sanitização de Entrada

- **Validação de Dados:** Valide todas as entradas de usuário no lado do servidor.
- **Preparação de Consultas:** Use consultas preparadas para prevenir SQL Injection.

4. Contramedidas Gerais

4.1. Backup

- **Políticas de Backup:** Defina políticas de backup regulares e testes de restauração.
- **Armazenamento Seguro:** Armazene backups em locais seguros e separados da rede principal.

4.2. Gerenciamento de Patches

- **Automação de Patches:** Use ferramentas de gerenciamento de patches para automatizar a aplicação de atualizações críticas.

4.3. Monitoramento e Logging

- **Soluções de SIEM:** Implante sistemas de gerenciamento de eventos e informações de segurança (SIEM) para monitorar e analisar logs.

- **Auditoria de Logs:** Realize auditorias regulares de logs para identificar atividades suspeitas.

4.4. Treinamento e Conscientização

- **Programas de Treinamento:** Implemente programas de treinamento contínuo em segurança para todos os funcionários.
- **Simulações de Phishing:** Realize simulações de phishing para aumentar a conscientização.