Manual de Correção e Prevenção de Vulnerabilidades

1. Servidores Web - Apache e Nginx

Apache:

Atualizações e Patches:

- Mantenha o servidor Apache atualizado. Use sudo apt-get update && sudo apt-get upgrade para sistemas baseados em Debian ou sudo yum update para sistemas Red Hat.
- Instale os patches de segurança assim que estiverem disponíveis.

Configurações Seguras:

- Desative módulos desnecessários no arquivo httpd.conf para reduzir o risco de exposição.
- Use ServerTokens Prod e ServerSignature Off para minimizar as informações sobre a versão do servidor.

SSL/TLS:

- Implemente HTTPS para criptografar as comunicações. Use certificados SSL/TLS de uma CA confiável.
- Configure redirecionamentos de HTTP para HTTPS para garantir que todos os dados trafeguem criptografados.

Proteção contra-ataques Comuns:

- Configure limites para evitar DoS, como LimitRequestBody, RequestReadTimeout, e MaxRequestWorkers.
- Use mod_security e mod_evasive para proteção adicional.

Nginx:

Atualizações e Patches:

- Mantenha o Nginx atualizado utilizando comandos apropriados para o seu gerenciador de pacotes.
- Acompanhe as notas de versão para instalar patches relevantes prontamente.

Configurações Seguras:

- Edite o arquivo de configuração nginx.conf para ocultar a versão do servidor usando server_tokens off;.
- Configure cabeçalhos de segurança como add_header X-Frame-Options "SAMEORIGIN"; para proteger contra cliques em frames.

SSL/TLS:

- Configure SSL/TLS com um certificado válido e diretrizes de segurança robustas, incluindo parâmetros como ssl_protocols, ssl_ciphers, e ssl_prefer_server_ciphers on;.

Restrições de Acesso:

- Utilize autenticação básica ou outros métodos para controlar o acesso a áreas administrativas.
- Implemente regras para bloquear acessos suspeitos ou maliciosos.

2. Firewall

Implementação e Configuração:

- Utilize um firewall de hardware ou software (como iptables ou firewalld) para controlar o tráfego de entrada e saída.
- Defina regras específicas para permitir apenas o tráfego necessário e bloquear as portas não utilizadas.

Monitoramento e Manutenção:

- Regularmente, revise as regras do firewall para ajustar às mudanças na infraestrutura de rede.
- Use ferramentas de monitoramento para identificar e responder rapidamente a tentativas de intrusão.

3. Logs

Configuração de Logs:

- Configure a rotação de logs para evitar o uso excessivo de espaço em disco.
- Garanta que os logs de erro e acesso de Apache, Nginx e firewall estejam ativos e capturando informações relevantes.

Análise de Logs:

- Use ferramentas como GoAccess, AWStats ou Graylog para analisar logs periodicamente.
- Estabeleça procedimentos para revisão regular de logs em busca de atividades suspeitas.

Segurança dos Logs:

- Proteja arquivos de log com permissões adequadas para evitar acessos não autorizados.
- Considere o uso de criptografia para logs sensíveis.