SSH Hardening Baseline

Objetivo

Estabelecer um baseline mínimo de segurança para o Serviço SSH, reduzindo riscos associados a ataques de força bruta, acesso não autorizado e exploração de configurações padrão.

Este baseline deve ser aplicado preventivamente, independentemente da existência de incidentes ativos.

Escopo

Este baseline aplica-se a:

- Servidores Linux
- Ambientes de laboratório, homologação e produção
- Hosts expostos a rede internas ou externas

Ameaças Endereçadas

Este baseline visa mitigar, principalmente:

- Brute Force SSH
- Credential Guessing
- Enumeração de usuário
- Abuso de serviços administrativos
- Ataques automatizados (Hydra, scripts, bots)

Referência MITRE ATT&CK:

- T1110 – Brute Force
- T1021.004 - Remote Services: SSH

Controle de Segurança (Baseline)

4.1 Porta SSH não padrão

Descrição:
Alterar a porta padrão do SSH (22) para uma porta não comum.

Objetivo:
Reduzir exposição a scanners automáticos e ataques oportunistas.

Risco mitigado:
Descoberta automática de serviço via varredura padrão.

4.2 Limitação de Tentativas de Autenticação (MaxAuthTries)

Descrição:
Definir um número máximo reduzido de tentativas de autenticação por conexão.

Objetivo:
Diminuir a eficácia de ataques de tentativa e erro.

Risco mitigado:
Força bruta manual ou automatizada.

4.3 Rate-limit de Conexões SSH

Descrição:
Implementar limitação de conexões por IP no firewall.

Objetivo:
Reduzir a taxa de tentativas por segundo, protegendo o serviço SSH de abuso.

Observação:
Este controle atua **antes do serviço SSH**, funcionando como medida preventiva.

Risco mitigado:
Ataques de alta frequência e negação de serviço leve.

4.4 Bloqueio Automático por Abuso (Fail2ban)

Descrição:
Bloquear automaticamente endereços IP que excedam o número permitido de falhas de autenticação.

Objetivo:
Interromper ataques persistentes após confirmação de abuso.

Observação:
Este controle é **reativo**, baseado em análise de logs.

Risco mitigado:
Ataques de brute force persistentes

4.5 Autenticação Segura

Descrição:
Preferir autenticação por chave SSH sempre que possível.

Objetivo:
Eliminar dependência de senhas fracas ou reutilizadas.

Risco mitigado:
Comprometimento por credenciais vazadas.

Monitoramento e Visibilidade,

- Logs de autenticação devem ser monitorados por um SIEM (ex: Wazuh)
- Alertas devem ser gerados para:
    - Falhas repetidas de login
    - Bloqueios automáticos
    - Tentativas em portas não padrão

Este baseline **não substitui monitoramento ativo**

Validação do Baseline

Após a aplicação do baseline, deve-se validar:

- Tentativas de brute force são desaceleradas
- Ataques persistentes são bloqueados
- Alertas são registrados corretamente
- Acesso legítimo continua funcional

Testes podem incluir:

- Simulação de brute force controlada
- Tentativas de acesso legítimo

Relação com Incident Response

Este baseline reduz significativamente a probabilidade de incidentes de brute force.

Caso um incidente ocorra:

- Deve-se seguir o *Brute Force SSH – Incident Response Playbook*
- Validar se o baseline estava corretamente aplicado

Revisão e Melhoria Contínua

Este baseline deve ser:

- Revisado periodicamente
- Ajustado conforme novos ataques
- Alinhado a frameworks como CIS Controls