Playbook – Brute Force SSH

Informações Gerais:

Categoria:

- Acesso não autorizado / Credential Access
- Password Guessing

MITRE ATT&CK:

- T1110.001 - Password Guessing
- T1021.004 - SSH

Fonte:

- SIEM(Wazuh)

Ambiente Afetado:

- Linux Server / Linux Workstation

Classificação:

- 5 ou >

Critério de Disparo

Este playbook deve ser utilizado quando ocorrer:

- Múltiplas falhas de autenticação SSH
- Mesmo IP de origem ou usuário
- Janela de tempo curta (ex: minutos)
- Alerta classificado como Brute Force (ex: rule.mitre.technique = Brute force)

Identificação

O analista deve validar:

- Host Afetado
- Usuário(s) Alvo
- IP de origem
- Quantidade de tentativas e frequência (ex: 3 tentativas em 5 minutos ou 100 tentativas em 10 minutos)

- Período em que ocorreu (ex: de que horas até que horas)
- Origem do log (/var/log/auth.log)

Pergunta essencial:

Isso é comportamento legítimo ou suspeito?

Análise

O analista deve responder:

- Houve login bem-sucedido?
- O usuário existe?
- O IP é interno ou externo?
- O mesmo IP aparece em outros hosts?
- O alerta é recorrente?

Decisão:

Não houve sucesso – Tentativa de brute force

Houve sucesso – Incidente confirmado

Classificação de Severidade

Situação	Severidade
Poucas tentativas	Baixa
Múltiplas tentativas sem sucesso	Média
Login bem-sucedido	Alta
Reincidência / Múltiplos hosts	Crítica

Contenção

Dependendo do cenário:

- Bloqueio do IP de origem
- Rate-limit no SSH
- Fail2Ban
- Restrição por firewall
- Desativação temporária do serviço (Caso extremo)

Seguir políticas da empresa antes de executar ações de impacto.

Erradicação

Se houve indício de comprometimento:

- Reset de senha do usuário
- Revisão de contas existentes
- Remoção de chave SSH suspeita
- Hardening do serviço SSH

Recuperação

- Validar acesso legítimo
- Restaurar serviços (se afetados)
- Monitorar o host por período definido
- Confirmar normalização dos alertas

Escalonamento

Escalar para:

- Time de Segurança Sênior
- Time de Infraestrutura
- Gestão (se impacto relevante)

Conforme:

- SLA
- Severidade
- Política interna

Lições Aprendidas

- SSH precisa estar exposto?
- Threshold de alerta é adequado?
- MFA é possível?
- Playbook precisa de ajuste?

Registrar melhorias propostas.