**APÊNDICES**

**APÊNDICE A – README T1110 – BRUTE FORCE: SSH**

**Objetivo**

Este filtro foi criado para detectar tentativas de autenticação não autorizadas via SSH, incluindo usuários inválidos, falhas de senha e desconexões antes do login (pré-auth).

**Testes realizados**

Comando de teste:

fail2ban-regex /var/log/auth.log /etc/fail2ban/filter.d/mitre-t1110.conf

Resultado obtido:

Total de linhas processadas: 22.177  
Linhas correspondentes (matched): 12.161  
Linhas ignoradas: 0  
Linhas não correspondentes (missed): 10.016

**Cobertura**

Cálculo da cobertura:

cobertura = linhas correspondentes / total de linhas  
cobertura = 12.161 / 22.177 ≈ 54.8 %

Interpretação:

- Cerca de 55% das linhas do log são capturadas pelo filtro.  
- Isso é esperado, pois nem todas as linhas de /var/log/auth.log representam tentativas de login.  
- O filtro está focado em capturar \*\*tentativas de acesso SSH maliciosas ou inválidas\*\*.

**Considerações**

- Cobertura de ~55% é \*\*normal e adequada\*\*, considerando que grande parte do log contém eventos legítimos.  
- O filtro captura:  
 - Falhas de autenticação PAM  
 - Tentativas de senha inválidas (usuário válido ou inválido)  
 - Usuários inválidos  
 - Desconexões pré-auth  
- Nenhum ignoreregex foi definido, garantindo que todas as tentativas suspeitas sejam analisadas.

**Status atual**

- Filtro válido (sem erros de sintaxe).  
- Captura de ataques SSH confirmada.  
- Cobertura estimada em ~55% do log analisado (27/Set/2025).  
- Chain MITRE-T1110 no iptables recebendo corretamente os IPs banidos.

**Roadmap de evolução**

1. Monitoramento contínuo  
 - Verificar periodicamente fail2ban-client status mitre-t1110 para garantir bloqueio de novos IPs.

2. Aprimoramento do filtro  
 - Adicionar padrões adicionais se forem identificadas novas formas de ataque (ex.: tentativas com usuários comuns "ubuntu", "admin", "test", etc.).

3. Exceções e Ignore  
 - Definir ignoreregex se houver IPs confiáveis ou faixas internas que não devem ser bloqueadas.

4. Métricas contínuas  
 - Executar testes semanais com fail2ban-regex para monitorar evolução da cobertura.  
 - Documentar percentual de cobertura ao longo do tempo (histórico).

**APÊNDICE B – README T1046 – PORTSCAN DETECTION**

**Título**

MITRE ATT&CK: T1046 - Network Service Scanning (Portscan)  
Autor: root@onrutas  
Data: 09 de outubro de 2025  
Local: /etc/fail2ban/filter.d/mitre-t1046.conf

**Objetivo**

Este apêndice apresenta a documentação técnica referente ao filtro Fail2Ban associado à técnica MITRE ATT&CK T1046 - Network Service Scanning (Portscan). O objetivo é detalhar o funcionamento, resultados de teste e cálculo de cobertura obtidos na análise do log de mensagens do sistema.

**Testes realizados**

Comando executado:

fail2ban-regex /var/log/messages /etc/fail2ban/filter.d/mitre-t1046.conf

Resultados obtidos:

Failregex: 11735 total  
|- 1) [11735] ^.\*Portscan( (tentativa|detectado))?:.\*SRC=<HOST>.\*$  
Ignoreregex: 0 total  
Linhas processadas: 13.863  
Linhas correspondentes (matched): 11.735  
Linhas ignoradas: 0  
Linhas não correspondentes (missed): 2.128  
Tempo de processamento: 1,70 segundos

**Cálculo de Cobertura**

cobertura = linhas correspondentes / total de linhas  
cobertura = 11.735 / 13.863 ≈ 84,6 %

Interpretação:

- O filtro apresenta cobertura aproximada de 85%, valor considerado excelente.  
- As linhas não correspondentes referem-se a mensagens do sistema que não indicam atividade de Portscan.  
- Nenhum padrão de ignorância (ignoreregex) foi definido, permitindo análise completa de todas as ocorrências relevantes.

**Considerações técnicas**

- Cobertura elevada (~85%) indica desempenho satisfatório do filtro.  
- O padrão failregex captura corretamente eventos contendo as palavras:  
 "Portscan tentativa" ou "Portscan detectado" seguidas de "SRC=<HOST>".  
- Teste realizado sem erros de sintaxe.  
- Log analisado com codificação UTF-8.  
- Ausência de linhas ignoradas demonstra compatibilidade desejada com o formato de log do sistema.

**Status atual**

✔️ Filtro validado e ativo.  
✔️ Captura confirmada de eventos de varredura de portas (Portscan).  
ℹ️ Cobertura estimada em ~84,6% sobre o log /var/log/messages.  
✔️ Chain MITRE-T1046 corretamente vinculada ao iptables.

**Roadmap de evolução**

1. Monitoramento contínuo  
 - Revisar semanalmente o status da jail 'mitre-t1046' via fail2ban-client.  
2. Expansão do regex  
 - Incluir novos padrões provenientes de ferramentas como Suricata ou Zeek.  
3. Ajuste de falsos positivos  
 - Definir ignoreregex para hosts internos confiáveis.  
4. Histórico de cobertura  
 - Registrar mensalmente a taxa de cobertura e número de eventos detectados.

**Conclusão**

O filtro mitre-t1046.conf demonstrou excelente desempenho, com taxa de cobertura aproximada de 85%. O resultado confirma sua eficácia na detecção de atividades de varredura de portas (Portscan) e sua integração correta ao Fail2Ban e iptables. O apêndice reforça a confiabilidade e estabilidade da configuração utilizada no ambiente monitorado.