Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

snortchallenges2– TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | snortchallenges2– Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 11/10/2024 |
| **Link** | https://tryhackme.com/r/room/snortchallenges2 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico Santarelli | Membro |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 11/10/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

Contextualização 3

Desenvolvimento 3

Stop the attack and get the flag 3

What is the name of the service under attack? 4

What is the used protocol/port in the attack? 4

Stop the attack and get the flag 5

What is the used protocol/port in the attack? 5

Which tool is highly associated with this specific port number? 6

Conclusão 6

**Contextualização**

O CTF compões a trilha de SOC Level 1. A ideia da sala é treinar as habilidades de usar a ferramenta de Snort para armazenar logs de pacotes (Sniffer) e bloquear ataques (IPS).

**Desenvolvimento**

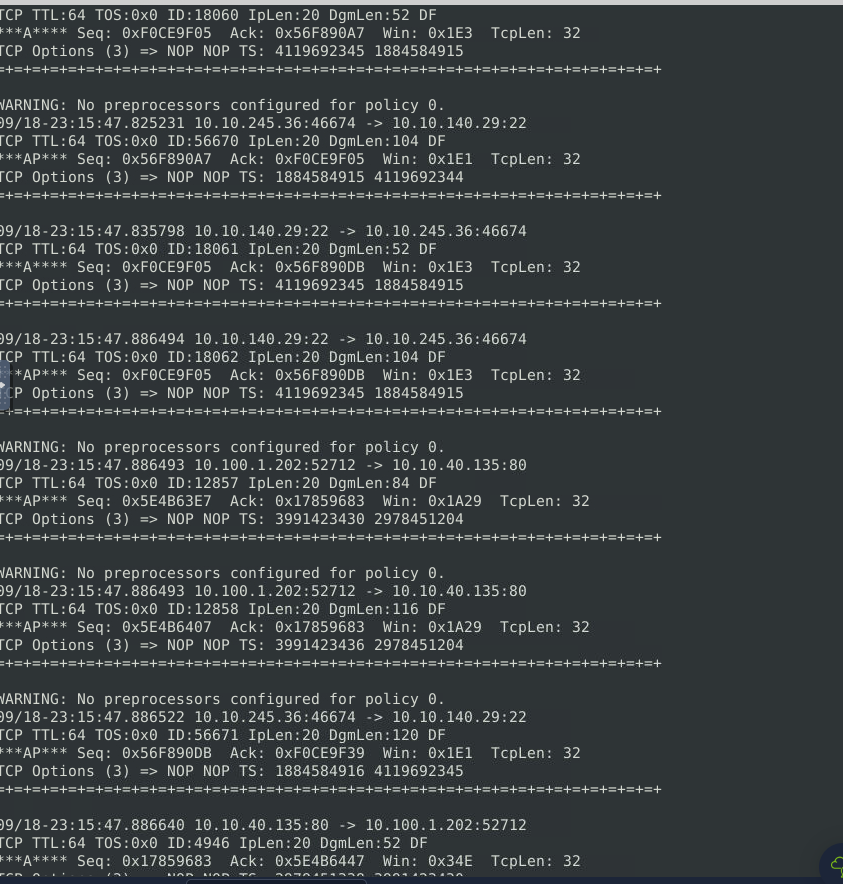
**Scenario 1 | Brute Force**

O primeiro cenário é voltado para usar o Snort como sniffer para localizar o ataque brute force e como IPS para ativamente bloquear o ataque.

**Stop the attack and get the flag**

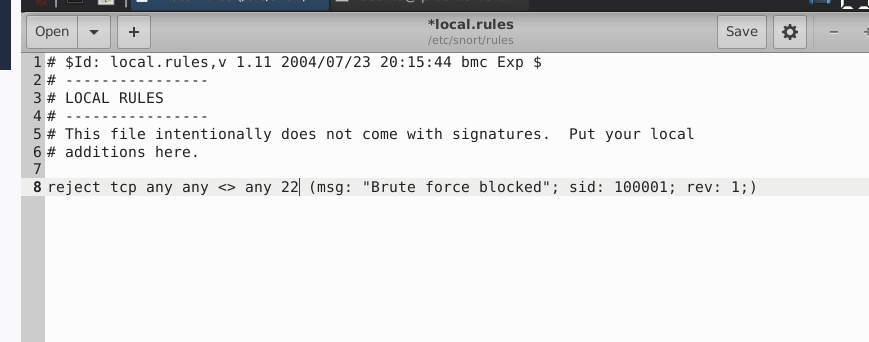
Primeiramente, vamos iniciar o Snort como Sniffer na interface de rede eth0.

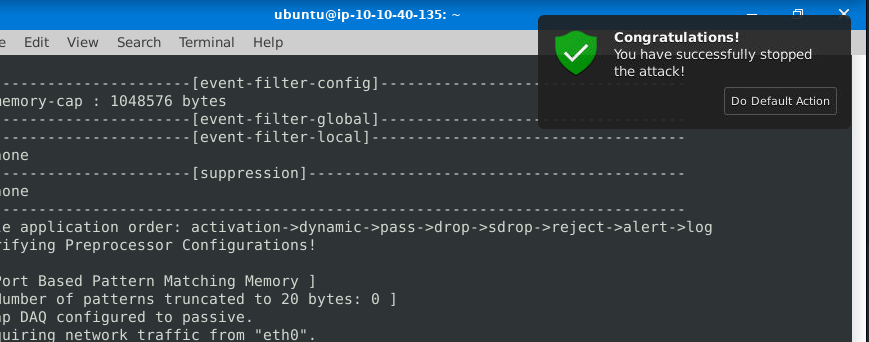
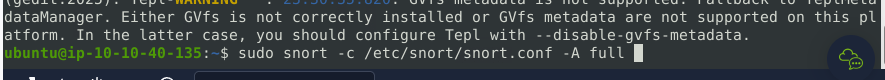




Visualizamos pelo resultado que a porta 22 está sendo usada para o ataque de brute force, então podemos utilizar esse padrão para bloquear o ataque.

Devemos, então, alterar o arquivo de configuração do Snort.

Rodando o Snort em modo IPS com o arquivo de configuração editado é possível bloquear o ataque. A flag, então, aparece no Desktop.



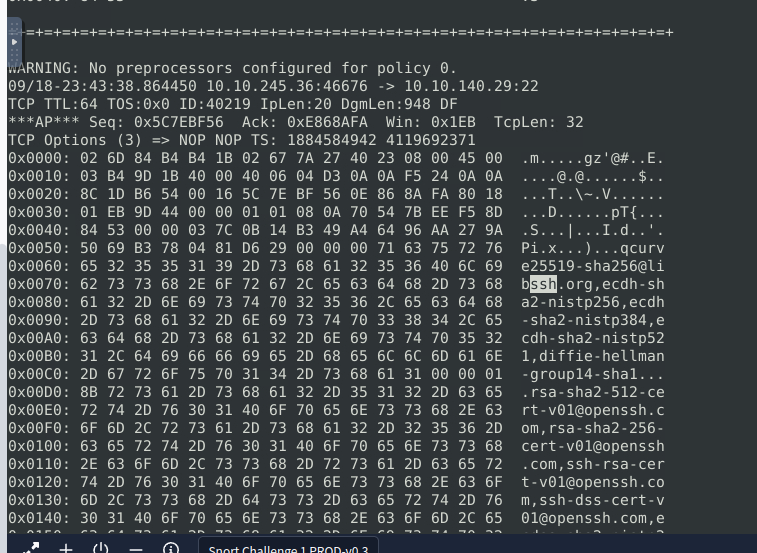
**What is the name of the service under attack?**

Para reconhecer o serviço, devemos procurar nos logs gerados da execução do Sniffer.

Para ler o log, usamos o próprio Snort e utilizamos a flag –X para ler profundamente o arquivo.



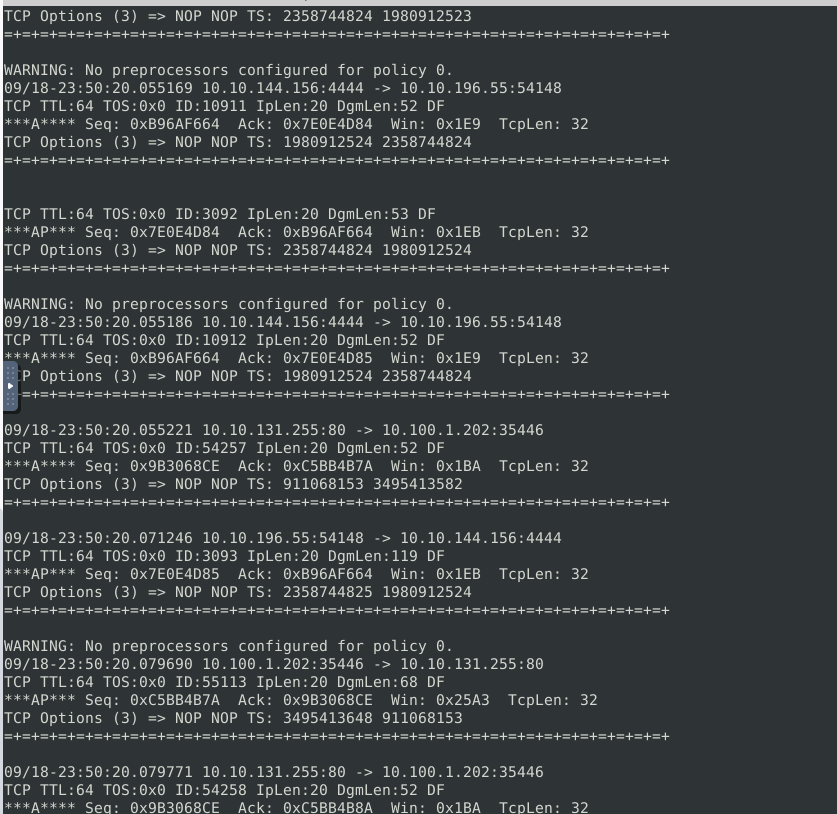
No pacote da porta 22 encontramos o serviço utilizado



R: SSH.

**What is the used protocol/port in the attack?**

Para responder a isso, podemos analisar a resposta obtida ao executar o Snort como sniffer no primeiro questionamento.

R: TCP/22.

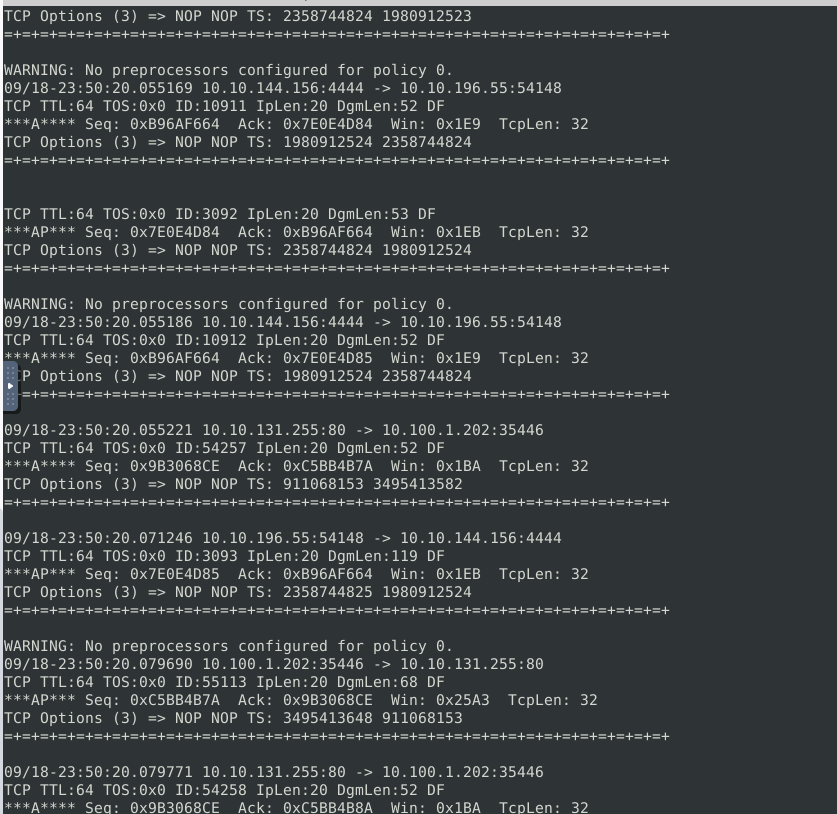
**Scenario 2 | Reverse Shell**

Nesse contexto novamente devermos analisar os logs de Snort como Sniffer e após isso criar regras para bloquear o ataque utilizando a aplicação de IPS do Snort.

**Stop the attack and get the flag**

Rodando o Snort como Sniffer na interface eth0.

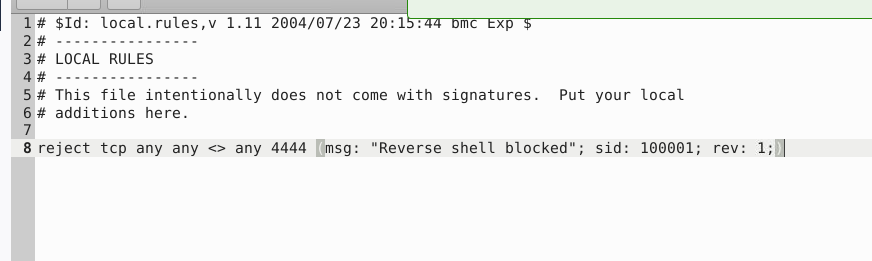




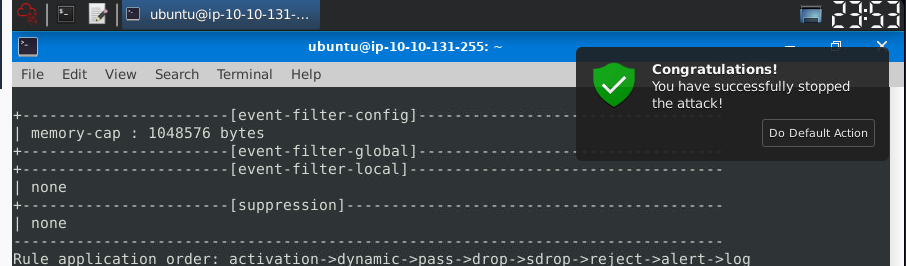
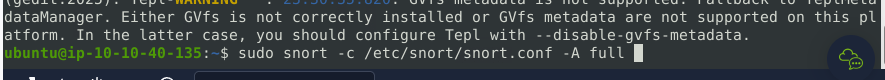
Os logs indicam uma atividade na porta 4444, que é a porta padrão utilizada pelo Metasploit para Reverse Shell.

Devemos, então, criar uma regra na configuração do Snort para bloquear a porta 4444 no destino.



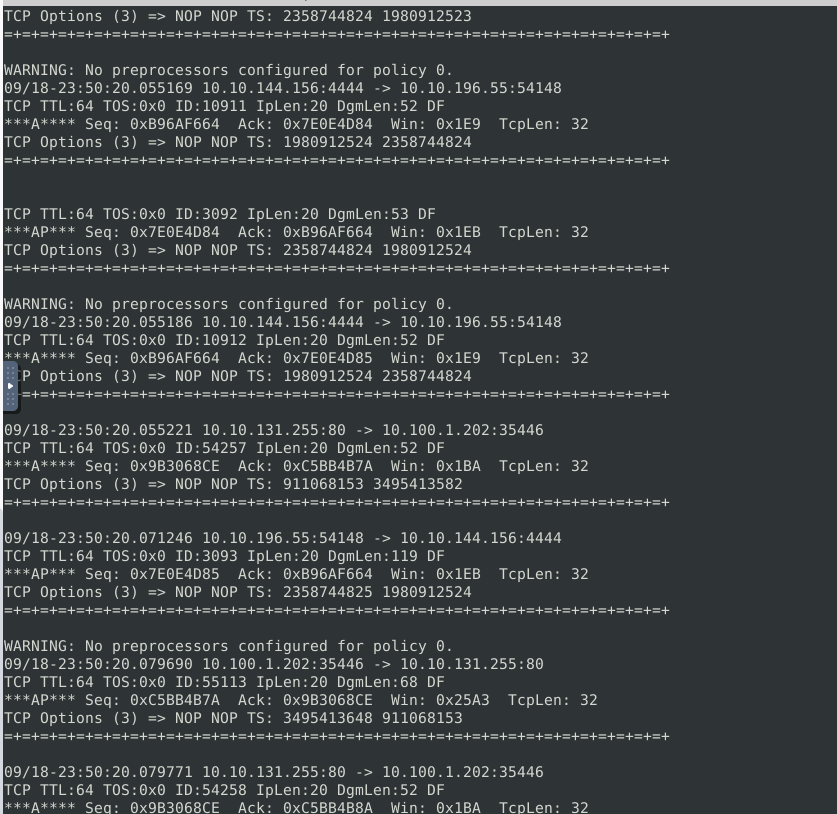


Logo, utilizando esse arquivo, podemos rodar o Snort como IPS para bloquear o ataque.



**What is the used protocol/port in the attack?**

Avaliando o log gerado pelo Snort em modo sniffer obtemos o protocolo e a porta.

R: tcp/4444.

**What is the used protocol/port in the attack?**

Como visto o Metasploit foi a ferramenta utilizada, já que sua porta padrão é a 4444.

R: metasploit

**Conclusão**

Este CTF oferece uma experiência prática de nível fácil, ideal para iniciantes na área de Blue Team que desejam colocar em prática os aprendizados das salas teóricas de Snort.