Instituto Superior de Engenharia

Politécnico de Coimbra

Guião Laboratorial do uso do Suricata como sistema de deteção de intrusões (IDS)

Segurança

Autores:

Henrique Dias Neves Simões Ferreira - 2023135147
João Pedro Vila Pomar - 2023140947
Rodolfo Miguel de Sousa Belchior Brás Oliveira - 2023155660

Professor:

Luís Eduardo Faria dos Santos

Ano Letivo:
2024/2025
Tempo Dispendido:
40 horas

Conteúdo

Lista de Figuras

1 Introdução

A crescente complexidade e frequência das ameaças informáticas tornam essencial a adoção de mecanismos eficazes de monitorização e proteção das redes. No mundo digital, onde a informação é um dos ativos mais críticos, as organizações e os indivíduos estão constantemente expostos a perigos. Estes vão desde software malicioso (malware) e tentativas de acesso não autorizado, até ataques de negação de serviço (Dos/DDoS) que visam indisponibilizar sistemas, ou explorações de vulnerabilidades que podem levar a fugas de dados massivas. Tais incidentes podem comprometer seriamente a confidencialidadeat, a integridade e a disponibilidade, pilares fundamentais da segurança da informação.

Os sistemas de deteção e prevenção de intrusões (IDS/IPS) desempenham um papel fundamental neste contexto, ao permitir identificar e responder a comportamentos suspeitos ou maliciosos no tráfego de rede. Um Sistema de Deteção de Intrusões (IDS) funciona como um vigilante, monitorizando o tráfego da rede em tempo real, analisando-o em busca de padrões anómalos ou assinaturas de ataques conhecidos e, ao detetar uma potencial ameaça, gera um alerta para que os administradores possam tomar as devidas providências. Um Sistema de Prevenção de Intrusões (IPS), por sua vez, partilha estas capacidades de deteção, mas adiciona a capacidade de intervir ativamente, podendo bloquear ou mitigar o tráfego malicioso identificado antes que este cause danos.

Para explorar experimentalmente estas tecnologias de defesa, este trabalho foca-se no Suricata, um motor de deteção de ameaças de código aberto (Open Source) reconhecido pelo seu alto desempenho. Uma das suas capacidades mais importantes é a Monitorização Profunda de Pacotes (Deep Packet Inspection - DPI), que lhe permite não só analisar os cabeçalhos do tráfego (como endereços IP e portas) mas também o conteúdo das comunicações. Esta análise profunda é crucial para detetar uma ampla gama de ataques, tais como ataques DDoS e explorações de vulnerabilidades, que poderiam passar despercebidas numa análise mais superficial.

O principal objetivo deste guião laboratorial é, proporcionar uma compreensão prática do funcionamento e da operação do Suricata no modo IDS. Ao longo das experiências procurar-se-á entender como o Suricata deteta diferentes tipos de intrusões, como gera e estrutura os seus logs e alertas, e como as suas regras podem ser geridas e configuradas, para potencialmente responder a ameaças em tempo real.

2 Configuração da Testbed (Ambiente de Simulação)

Nesta secção, detalha-se a testbed criada no GNS3, os recursos utilizados, e o processo geral de configuração. Esta testbed servirá de base para todas as experiências de deteção e análise de intrusões com o Suricata.

2.1 Objetivo e Visão Geral da Testbed

A testbed, criada integralmente na plataforma GNS3, tem como principal objetivo simular um ambiente de rede corporativa simplificado. Este ambiente permite testar e analisar a eficácia do sistema de deteção de intrusões Suricata contra diversas ameaças simuladas, originadas a partir de um segmento de rede dedicado que representa uma rede externa hostil.

A topologia geral (conforme a Figura 1) é composta por:

- Uma zona interna ("área verde") contendo dispositivos de utilizadores finais (VPCS), switches de acesso (Switch2, Switch3), um router principal (Router1), e a máquina de deteção de intrusões (Ubuntu com Suricata).
- Uma zona de interligação, gerida pelo Router2, que liga a zona interna (via Router1 e SPAN-CentralSwitch) à rede do atacante (via Router3).
- Uma zona de ataque ("área vermelha"), contendo a máquina Kali Linux (o atacante), o seu switch de acesso (Switch1) e o seu router de acesso (Router3).
- Um switch central com capacidade SPAN (SPAN-CentralSwitch), estrategicamente posicionado entre o Router1 e o Router2 para espelhar o tráfego relevante para a máquina Suricata.

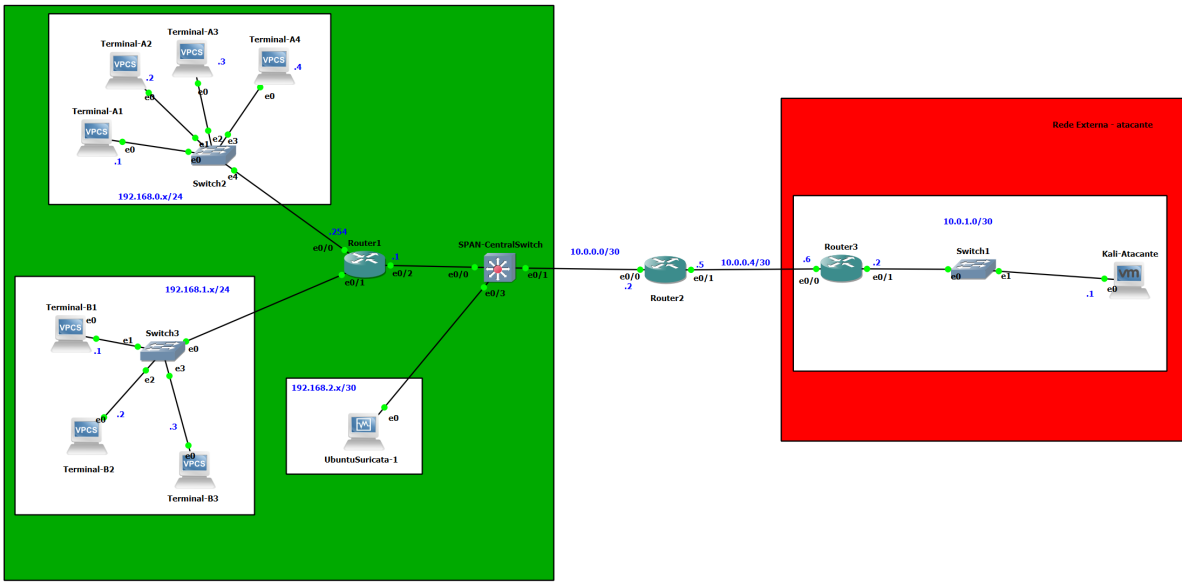

Figura 1: Topologia GNS3

2.2 Recursos Utilizados

Para a construção desta testbed no GNS3, foram utilizados os seguintes recursos:

Software Principal

- GNS3 (2.2.54)
- Hipervisor para Máquinas Virtuais: VirtualBox (ou VMware, conforme a preferência)

Dispositivos de Rede (Imagens GNS3)

- Routers (R1, R2, R3): Imagem Cisco IOU L3 (`i86bi-linux-l3-adventerprisek9-15.5.2T.bin`)
- Switch de Espelhamento (SPAN-CentralSwitch): Imagem Cisco IOU L2 `i86bi_linux_l2-ipbasek9-ms.may8-2013-team_track`, com suporte para SPAN.
- Switches de Acesso (Switch1, Switch2, Switch3): Switches Ethernet genéricos e não geríveis do GNS3

Máquinas Virtuais (VMs)

- Máquina Atacante: Kali Linux, a correr no VirtualBox/VMware
- Máquina IDS: Ubuntu Server/Desktop com Suricata instalado

Terminais Cliente

- Sete VPCS para simular utilizadores finais nas LANs internas (Terminal-A1 a A4, Terminal-B1 a B3)

3 Arquitetura de Rede e Configurações Chave

Segmentação da Rede:
A rede foi dividida em várias sub-redes para simular diferentes zonas funcionais, como ilustrado no diagrama da topologia.

- Separação entre LANs de utilizadores, rede do atacante, interligações entre routers e canal de monitorização.

Gamas de Endereçamento IP:

- 192.168.0.0/24 e 192.168.1.0/24 — LANs internas de utilizadores (área verde).
- 192.168.2.0/30 — Ligação dedicada entre a VM Suricata e o SPAN-CentralSwitch.
- 10.0.0.0/30 e 10.0.0.4/30 — Redes de interligação entre os routers.
- 10.0.1.0/30 — Rede do atacante (Kali Linux).

Encaminhamento de Tráfego:

- Configuração de rotas nos routers R1, R2 e R3.
- Permite o encaminhamento de pacotes entre todas as zonas da rede.

Monitorização com SPAN:

- O SPAN-CentralSwitch (IOU L2) espelha o tráfego das seguintes portas:
  - Ethernet0/0 — Ligada ao Router1.
  - Ethernet0/1 — Ligada ao Router2.
- O tráfego é redirecionado para a porta Ethernet0/3, conectada à VM Suricata.
- Isto permite que o Suricata monitorize o tráfego entre a rede interna e a rede do atacante sem interferir diretamente nas comunicações.

4 Anatomia das Regras do Suricata

4.1 Cabeçalho da Regra

A anatomia das regras utilizadas pelo *Suricata* começa com a seguinte estrutura:
<ação> <protocolo> <endereço_origem> <porta_origem> -> <endereço_destino> <porta_destino>

Onde:

- **ação**: Representa o que deve ser feito quando a condição da regra for satisfeita. Exemplos incluem:
  - `alert` – gera um alerta;
  - `drop` – descarta o pacote;
  - `pass` – permite o pacote.
  - `reject` – rejeita o pacote.
- **protocolo**: Define o tipo de tráfego que será inspecionado, como tcp, udp, icmp ou ip.
- **endereço_origem** e **porta_origem**: Indicam o endereço IP e a porta da origem do tráfego.
- `->`: Indica a direção do tráfego, da origem para o destino.
- **endereço_destino** e **porta_destino**: Especificam o destino do tráfego.

Após essa estrutura básica, a regra prossegue com a definição das condições dentro de parênteses, conhecidas como **opções da regra**.

4.2 Opções da Regra

Após o cabeçalho, entre parênteses `()`, vêm as **opções da regra**, separadas por ponto e vírgula. Essas opções definem as condições específicas que o tráfego deve atender para que a regra seja acionada.
Cada opção segue o formato:

`palavra-chave:valor;`

Abaixo estão algumas das opções mais importantes:

- `msg:<texto>;`
  Mensagem descritiva exibida no alerta.
- `content:<padrão>;`
  Procura por uma sequência específica de bytes no payload.
- `sid:<número>;`
  Signature ID, um identificador único da regra.

  Exemplo: `sid:2101411;`
- `rev:<número>;`
  Número de revisão da regra.

  Exemplo: `rev:13;`
- `classtype:<classificação>;`
  Classifica o tipo de ameaça ou ataque.

  Exemplo: `classtype:attempted-recon;`
- `flow:<opções_de_fluxo>;`
  Verifica o estado de uma sessão TCP.

5 Experiências Realizadas

5.1 Ataque DoS e DDoS

Um ataque DoS/DDoS (*(Distributed) Denial of Service)* visa tornar um sistema ou serviço indisponível ao sobrecarregá-lo com tráfego proveniente de uma ou múltiplas origens, respetivamente. Este tipo de ataque impede o acesso legítimo ao serviço, explorando a limitação de recursos do servidor alvo, seja a sua capacidade de processamento, largura de banda ou número de conexões que consegue gerir. Nesta experiência, foram simulados dois cenários de ataque SYN flood utilizando a ferramenta hping3 a partir da máquina Kali Linux (10.0.1.1), visando o Terminal-B2 (192.168.1.2) na porta 80 (HTTP). O objetivo foi observar as diferentes respostas do Suricata.

5.1.1 DDoS: SYN Flood com IPs de Origem Aleatórios (–rand-source)

Comando Executado (Kali):

sudo hping3 -S –flood –rand-source -p 80 192.168.1.2

Descrição: Este comando gera um fluxo intenso de pacotes TCP SYN com endereços IP de origem falsificados e aleatórios, característico de um ataque DDoS distribuído.

Deteção e Análise Observada no Suricata: Durante este ataque, o eve.json do Suricata (ver Figura 2) registou numerosos eventos. Estes incluíram múltiplos registos de fluxo ("event_type":"flow") com diversos IPs de origem aleatórios direcionados ao alvo 192.168.1.2:80, com flags SYN e terminando em timeout, o que é consistente com um SYN flood. Crucialmente, associados a este tráfego, foram gerados vários alertas ("event_type":"alert") por regras da comunidade baseadas na reputação dos IPs de origem. Especificamente, foram observados alertas como ET DROP Spamhaus DROP Listed Traffic Inbound group XX (com SIDs como 2400022, 2400024, 2400026, etc.), todos com ação DROP.


attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:03.801031+0000","src_ip":"152.189.22.22","dest_ip":"192.168.1.2","src_port":47641,"dest_port":80}}
{"timestamp":"2025-06-05T18:07:03.810010+0000","flow_id":207159275247732,"in_iface":"enp0s3","event_type":"alert","src_ip":"150.141.29.19","src_port":47892,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400025,"rev":4358,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 26","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:03.810010+0000","src_ip":"150.141.29.19","dest_ip":"192.168.1.2","src_port":47892,"dest_port":80}}
{"timestamp":"2025-06-05T18:07:03.831360+0000","flow_id":21632933651S1284,"in_iface":"enp0s3","event_type":"alert","src_ip":"116.144.20.115","src_port":48372,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400020,"rev":4358,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 21","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:03.831360+0000","src_ip":"116.144.20.115","dest_ip":"192.168.1.2","src_port":48372,"dest_port":80}}
{"timestamp":"2025-06-05T18:07:03.859854+0000","flow_id":200419624S902220,"in_iface":"enp0s3","event_type":"alert","src_ip":"155.66.57.66","src_port":49903,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400026,"rev":4358,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 27","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:03.859854+0000","src_ip":"155.66.57.66","dest_ip":"192.168.1.2","src_port":49903,"dest_port":80}}
{"timestamp":"2025-06-05T18:07:03.917729+0000","flow_id":197129368094251S,"in_iface":"enp0s3","event_type":"alert","src_ip":"148.148.110.221","src_port":51655,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400024,"rev":4358,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 25","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:03.917729+0000","src_ip":"148.148.110.221","dest_ip":"192.168.1.2","src_port":51655,"dest_port":80}}
{"timestamp":"2025-06-05T18:07:04.015009+0000","flow_id":64464107023777,"in_iface":"enp0s3","event_type":"alert","src_ip":"169.129.143.158","src_port":55007,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400030,"rev":4358,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 31","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:04.015009+0000","src_ip":"169.129.143.158","dest_ip":"192.168.1.2","src_port":55007,"dest_port":80}}
{"timestamp":"2025-06-05T18:07:04.029676+0000","flow_id":127461049776168,"in_iface":"enp0s3","event_type":"alert","src_ip":"58.14.116.246","src_port":55721,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400006,"rev":4358,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 7","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2025_05_30"]}},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-06-05T18:07:04.029676+0000","src_ip":"58.14.116.246","dest_ip":"192.168.1.2","src_port":55721,"dest_port":80}}

Figura 2: DDoS

Lógica da Regra: Esta regra (drop ip ...) descarta tráfego IP originado de endereços conhecidos por atividades maliciosas (listados pela Spamhaus) e destinados à rede interna ($HOME_NET). O threshold limita os alertas (um por hora por IP de origem) e os flowbits adicionam uma lógica de estado à deteção. No ataque, IPs aleatórios gerados pelo hping3 que constavam na lista da Spamhaus acionaram esta regra.

cisco@Ubuntu-Suricata: $ sudo grep 'sid:2400020;' /var/lib/suricata/rules/suricata.rules
[sudo] password for cisco:
alert ip [113.26.202.0/24,113.89.186.0/24,113.212.128.0/19,114.99.0.0/20,114.134.28.0/22,114.231.48.0/22,114.231.216.0/22,114.239.188.0/24,115.144.69.0/24,116.30.217.0/24,116.144.0.0/15,116.146.0.0/15,117.18.0.0/24,117.58.0.0/17,117.60.11.0/24,118.107.16.0/20,119.13.179.0/24,119.27.192.0/18,119.58.0.0/16,119.82.12.0/22] any -> $HOME_NET any (msg:"ET DROP Spamhaus DROP Listed Traffic Inbound group 21"; reference:url,www.spamhaus.org/drop/drop.txt; threshold: type limit, track by_src, seconds 3600, count 1; classtype:misc-attack; flowbits:set,ET.Evil; flowbits:set,ET.DROPIP; sid:2400020; rev:4358; metadata:affected_product Any, attack_target Any, deployment Perimeter, tag Dshield, signature_severity Minor, created_at 2010_12_30, updated_at 2025_05_30;)
cisco@Ubuntu-Suricata: $

Figura 3: Regra Suricata (sid:2400020) responsável pela deteção do tráfego malicioso

5.1.2 DoS: SYN Flood com IP de Origem Único (Kali Linux)

Comando a Executar (Kali):

sudo hping3 -S –flood -p 80 192.168.1.2

Descrição: Descrição: Este comando gera um fluxo intenso de pacotes TCP SYN direcionados ao alvo (192.168.1.2 na porta 80). Todos os pacotes de ataque têm como origem o endereço IP real da máquina Kali (10.0.1.1), caracterizando um ataque de Negação de Serviço (DoS) de fonte única.

Deteção Esperada/A Observar no Suricata: Deteção e Análise Observada no Suricata: Durante a execução deste ataque DoS, a análise do ficheiro eve.json do Suricata (ver Figura 4) demonstrou que o Suricata registou a atividade de ataque. Foram observados numerosos registos de fluxo ("event_type":"flow") com as seguintes características:

IP de origem: 10.0.1.1 (Kali Linux).
IP de destino: 192.168.1.2 (o alvo).
Porta de destino: 80 (HTTP).
Protocolo: TCP.
Estes fluxos frequentemente apresentavam flags TCP SYN, estado "new"e terminavam com a razão "timeout", o que é consistente com o comportamento de um ataque SYN flood.

{"timestamp":"2025-06-05T18:04:12.523810+0000","flow_id":918438996963490,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":4321,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":8,"pkts_toclient":0,"bytes_toserver":480,"bytes_toclient":0,"start":"2025-06-05T18:02:43.803664+0000","end":"2025-06-05T18:03:10.751695+0000","age":27,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523835+0000","flow_id":145660053687116O,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":52795,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":11,"pkts_toclient":0,"bytes_toserver":660,"bytes_toclient":0,"start":"2025-06-05T18:02:45.076997+0000","end":"2025-06-05T18:03:10.418070+0000","age":25,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523859+0000","flow_id":162838364550865,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":1336,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":15,"pkts_toclient":0,"bytes_toserver":900,"bytes_toclient":0,"start":"2025-06-05T18:02:45.379137+0000","end":"2025-06-05T18:03:10.688603+0000","age":25,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523884+0000","flow_id":136207699531830 2,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":37182,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":7,"pkts_toclient":0,"bytes_toserver":420,"bytes_toclient":0,"start":"2025-06-05T18:02:44.644813+0000","end":"2025-06-05T18:03:11.495506+0000","age":27,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523907+0000","flow_id":893502351897431,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":4218,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":9,"pkts_toclient":0,"bytes_toserver":540,"bytes_toclient":0,"start":"2025-06-05T18:02:43.797858+0000","end":"2025-06-05T18:03:10.748548+0000","age":27,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523933+0000","flow_id":141483318346904 64,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":64308,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":13,"pkts_toclient":0,"bytes_toserver":780,"bytes_toclient":0,"start":"2025-06-05T18:02:45.329416+0000","end":"2025-06-05T18:03:09.262852+0000","age":24,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523958+0000","flow_id":192197878385553 6,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":59495,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":11,"pkts_toclient":0,"bytes_toserver":660,"bytes_toclient":0,"start":"2025-06-05T18:02:46.775175+0000","end":"2025-06-05T18:03:11.967024+0000","age":25,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.523982+0000","flow_id":642922048287910,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":12500,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":7,"pkts_toclient":0,"bytes_toserver":420,"bytes_toclient":0,"start":"2025-06-05T18:02:50.018619+0000","end":"2025-06-05T18:03:09.543320+0000","age":19,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T18:04:12.524015+0000","flow_id":507283344550 3,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":22141,"dest_ip":"192.168.1.2","dest_port":80,"proto":"TCP","flow":{"pkts_toserver":9,"pkts_toclient":0,"bytes_toserver":540,"bytes_toclient":0,"start":"2025-06-05T18:02:48.787612+0000","end":"2025-06-05T18:03:11.150531+0000","age":23,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}

Figura 4: DoS

5.2 Ataque SNMP

O protocolo SNMP (*Simple Network Management Protocol*) é amplamente utilizado para monitorização e gestão de dispositivos de rede. No entanto, versões mais antigas como o SNMPv1 e SNMPv2c utilizam uma *community string* para autenticação, frequentemente mantida com o valor predefinido "public". Esta configuração representa uma vulnerabilidade significativa, pois permite acesso não autorizado à informação de gestão do dispositivo.

5.2.1 Reconhecimento via SNMP com snmpwalk

Comando Executado (Kali):

snmpwalk -v2c -c public 10.0.0.1

Descrição: O comando snmpwalk é utilizado para interagir com dispositivos que utilizam o protocolo SNMP. Neste caso, a consulta foi realizada usando a versão 2c do protocolo (-v2c) e a community string padrão "public", sendo a requisição direcionada ao endereço IP 10.0.0.1.

Este comando simula uma tentativa de enumeração de informações do dispositivo remoto, constituindo uma técnica comum de reconhecimento. O ataque foi executado a partir da máquina Kali, com o objetivo de aceder a dados de gestão do dispositivo alvo.

Deteção e Análise no Suricata:
Durante a execução do ataque, o Suricata demonstrou eficácia na deteção do tráfego suspeito, tendo gerado múltiplos alertas com base na seguinte regra da comunidade.

Regra:

- GPL SNMP public access udp
- SID: 2101411

Esta regra é ativada sempre que há tráfego UDP com destino à porta 161 (porta padrão do SNMP). A sua definição é a seguinte (ver Figura 6):

alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"GPL SNMP public access udp"; content:"public"; fast_pattern; sid:2101411; classtype:attempted-recon; priority:2;)

Lógica da Regra:

- `msg:"GPL SNMP public access udp";`
  Mensagem de alerta que indica uma tentativa de acesso ao serviço SNMP utilizando a community string padrão `"public"`.
- `content:"public";`
  Otimiza o desempenho do mecanismo de deteção, utilizando o conteúdo como ponto de indexação para uma análise mais eficiente.
- `fast_pattern;`
  Otimiza o desempenho do mecanismo de deteção, utilizando o conteúdo como ponto de indexação para uma análise mais eficiente.
- `sid:2101411;`
  Identificador único da assinatura, usado para rastreamento e correlação em sistemas de monitorização.
- `classtype:attempted-recon;`
  Classifica o alerta como uma tentativa de reconhecimento, neste caso, de sondagem via SNMP.
- `priority:2;`
  Atribui uma prioridade média ao alerta, indicando que o evento deve ser analisado, embora não represente uma ameaça crítica imediata.

A classificação do alerta foi *Attempted Information Leak*, com prioridade 2, sinalizando uma tentativa de recolha de informações potencialmente sensíveis sem autenticação adequada.

A Figura 5 mostra os alertas gerados pelo Suricata durante o ataque, onde se observam múltiplas tentativas de acesso ao serviço SNMP no IP 10.0.0.1, originadas a partir do IP 10.0.1.1 (interface da máquina atacante).

Este ataque demonstra como configurações inseguras, como o uso da community string padrão em serviços SNMP, podem ser facilmente exploradas para fins de reconhecimento.

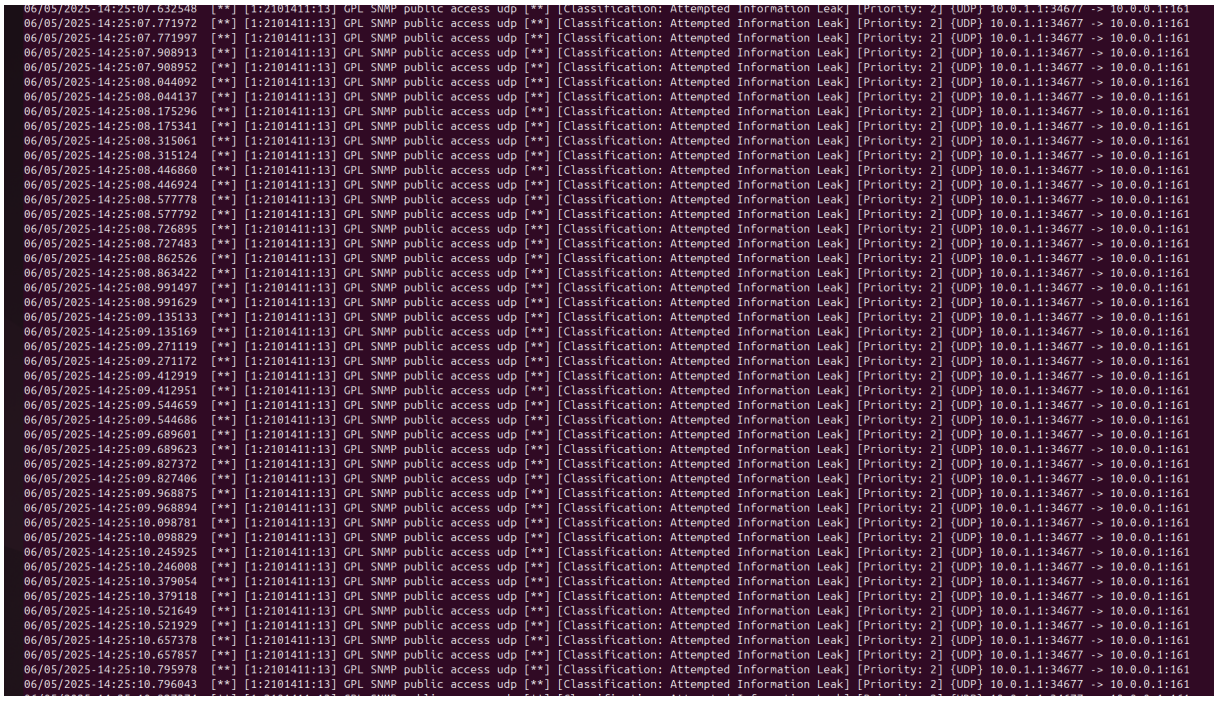

Figura 5: Alertas gerados pelo Suricata durante o ataque SNMP

Figura 6: Regra Suricata responsável pela deteção do ataque SNMP (sid:2101411)

5.3 Ataque Port Scanning com Nmap

Um ataque de *Port Scanning* tem como objetivo descobrir quais portas estão abertas num sistema, permitindo ao atacante inferir quais serviços estão em execução e, possivelmente, identificar vulnerabilidades exploráveis. Ferramentas como o *Nmap* são amplamente usadas para esse fim, especialmente na fase de reconhecimento de um ataque.

Nesta experiência, foi simulado um ataque de *Port Scanning*, no qual foi utilizado o comando nmap -sS a partir da máquina com o IP 192.168.0.2, tendo como alvo a máquina 10.0.1.1. O objetivo foi identificar quais portas TCP estavam abertas nesse host, explorando a técnica *SYN scan* (meia-conexão), que é rápida e menos intrusiva, dificultando a sua deteção em alguns casos.

5.3.1 Comando Executado (Kali):

nmap -sS 10.0.1.1

Descrição: O comando executa uma varredura TCP do tipo *SYN Scan*, enviando pacotes com o flag *SYN* para várias portas do *host* destino. Com base na resposta recebida (por exemplo, SYN/ACK, RST, etc.), é possível inferir o estado da porta (aberta, fechada ou filtrada). Esta técnica é considerada discreta porque não estabelece uma conexão TCP completa, tornando-se mais difícil de detetar por sistemas de monitorização simples.

5.3.2 Deteção e Análise Observada no Suricata

Durante o ataque, o sistema de deteção de intrusões Suricata foi capaz de identificar tráfego anómalo através da geração de múltiplos alertas associados à seguinte assinatura:

- **Mensagem:** SURICATA TCPv4
- **Classificação:** Generic Protocol Command Decode
- **Prioridade:** 3
- **SID:** 2200074

Esta assinatura identifica pacotes TCP com *checksums* inválidos, que são muitas vezes o resultado de técnicas de evasão utilizadas por ferramentas como o *Nmap* para contornar mecanismos de deteção convencionais.

Abaixo apresenta-se a definição da regra que permitiu a sua deteção:

```
alert tcp any any -> any any (msg:"SURICATA TCPv4";
tcpv4-csum:invalid; classtype:protocol-command-decode; sid:2200074; rev:2;)
```

5.3.3 Lógica da Regra

- `msg:"SURICATA TCPv4";`
  Mensagem de alerta que será exibida ao detetar um pacote com erro no checksum TCPv4.
- `tcpv4-csum:invalid;`
  Indica que a regra deteta pacotes IPv4 com checksum TCP inválido — o que pode indicar corrupção de dados, tráfego malformado ou evasão de análise.
- `classtype:protocol-command-decode;`
  Classifica o evento como um problema durante a decodificação do protocolo — geralmente relacionado a anomalias de baixo nível ou pacotes malformados.
- `sid:2200074;`
  Identificador único da assinatura (Signature ID).
- `rev:2;`
  Número da revisão da regra. Indica que esta é a segunda versão publicada ou ajustada dessa regra.

Como evidenciado pelos registos (ver Figura 7), foram gerados diversos alertas associados a pacotes com origem na máquina `192.168.0.2` e destino ao IP 10.0.1.1 na porta 34454, oriundos de várias portas de origem aleatórias.

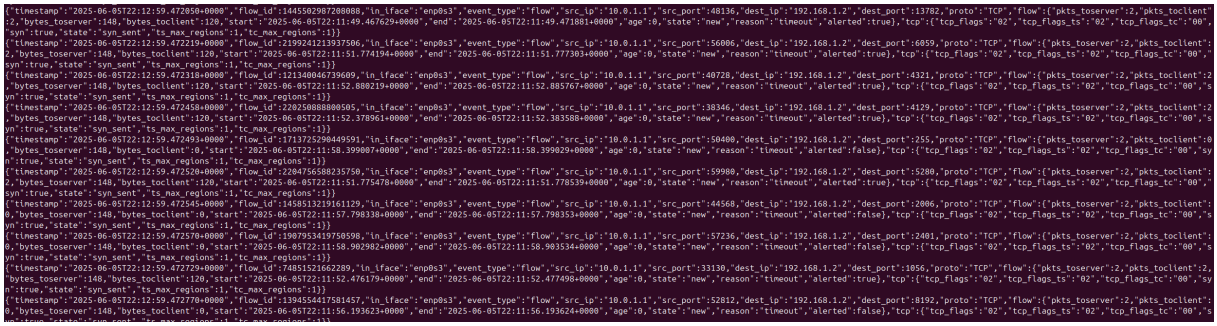
{"timestamp":"2025-06-05T22:12:59.472850+0000","flow_id":1445502987280888,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":48136,"dest_ip":"192.168.1.2","dest_port":13782,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":148,"bytes_toclient":120,"start":"2025-06-05T22:11:49.467629+0000","end":"2025-06-05T22:11:49.471881+0000","age":0,"state":"new","reason":"timeout","alerted":true},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472219+0000","flow_id":219924121393750 6,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":56006,"dest_ip":"192.168.1.2","dest_port":6059,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":148,"bytes_toclient":120,"start":"2025-06-05T22:11:51.774194+0000","end":"2025-06-05T22:11:51.777303+0000","age":0,"state":"new","reason":"timeout","alerted":true},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472318+0000","flow_id":121340046739609,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":40728,"dest_ip":"192.168.1.2","dest_port":4321,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":148,"bytes_toclient":120,"start":"2025-06-05T22:11:52.880219+0000","end":"2025-06-05T22:11:52.885767+0000","age":0,"state":"new","reason":"timeout","alerted":true},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472458+0000","flow_id":220250888800505,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":38346,"dest_ip":"192.168.1.2","dest_port":4129,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":148,"bytes_toclient":120,"start":"2025-06-05T22:11:52.378961+0000","end":"2025-06-05T22:11:52.383588+0000","age":0,"state":"new","reason":"timeout","alerted":true},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472493+0000","flow_id":171372529044959 1,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":50400,"dest_ip":"192.168.1.2","dest_port":255,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":0,"bytes_toserver":148,"bytes_toclient":0,"start":"2025-06-05T22:11:58.399807+0000","end":"2025-06-05T22:11:58.399829+0000","age":0,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472520+0000","flow_id":220475688235750,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":59980,"dest_ip":"192.168.1.2","dest_port":5280,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":148,"bytes_toclient":120,"start":"2025-06-05T22:11:51.775478+0000","end":"2025-06-05T22:11:51.778539+0000","age":0,"state":"new","reason":"timeout","alerted":true},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472545+0000","flow_id":145851321916 1129,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":44568,"dest_ip":"192.168.1.2","dest_port":2086,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":0,"bytes_toserver":148,"bytes_toclient":0,"start":"2025-06-05T22:11:57.798338+0000","end":"2025-06-05T22:11:57.798353+0000","age":0,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472570+0000","flow_id":190795341975059 8,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":57236,"dest_ip":"192.168.1.2","dest_port":2401,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":0,"bytes_toserver":148,"bytes_toclient":0,"start":"2025-06-05T22:11:58.902982+0000","end":"2025-06-05T22:11:58.903534+0000","age":0,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472729+0000","flow_id":748515216622 89,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":33130,"dest_ip":"192.168.1.2","dest_port":1056,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":148,"bytes_toclient":120,"start":"2025-06-05T22:11:52.476179+0000","end":"2025-06-05T22:11:52.477498+0000","age":0,"state":"new","reason":"timeout","alerted":true},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","syn":true,"state":"syn_sent","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-06-05T22:12:59.472770+0000","flow_id":139455441758145 7,"in_iface":"enp0s3","event_type":"flow","src_ip":"10.0.1.1","src_port":52812,"dest_ip":"192.168.1.2","dest_port":8192,"proto":"TCP","flow":{"pkts_toserver":2,"pkts_toclient":0,"bytes_toserver":148,"bytes_toclient":0,"start":"2025-06-05T22:11:56.193623+0000","end":"2025-06-05T22:11:56.193624+0000","age":0,"state":"new","reason":"timeout","alerted":false},"tcp":{"tcp_flags":"02","tcp_flags_ts":"02","tcp_flags_tc":"00","s

Figura 7: Alertas relacionados com *Port Scanning*


root@Ubuntu-Suricata:/home/cisco# sudo grep 'sid:2010935' /var/lib/suricata/rules/suricata.rules
alert tcp $EXTERNAL_NET any -> $HOME_NET 1433 (msg:"ET SCAN Suspicious inbound to MSSQL port 1433"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; classtype:bad-unknown; sid:2010935; rev:3; metadata:created_at 2010_07_30, confidence Medium, signature_severity Informational, updated_at 2019_07_26;)
root@Ubuntu-Suricata:/home/cisco#

Figura 8: Exemplo Alerta *Port Scanning* no porto 1433

5.4 Ataque de Força Bruta

Um ataque de força bruta (*Brute Force*) consiste na tentativa repetida e sistemática de adivinhar credenciais de acesso (nome de utilizador e palavra-passe), com o objetivo de obter acesso não autorizado a um sistema. Este tipo de ataque é frequentemente dirigido a serviços remotos como Telnet, SSH ou interfaces de administração web.

5.4.1 Comando Executado (Kali):

Na simulação realizada, a máquina Kali-Atacante tentou estabelecer uma ligação Telnet com o dispositivo Router1 (IP 10.0.0.1), utilizando credenciais predefinidas comuns como "admin"e "1234".
Este tipo de ataque explora a negligência na alteração das credenciais padrão, frequentemente presentes em dispositivos de rede, como routers residenciais e empresariais.

O Suricata foi capaz de detetar a atividade suspeita, gerando um alerta com base na seguinte assinatura:

- **Mensagem:** ET EXPLOIT Zyxel DSL CPE Management Interface Default Credentials (admin) (CVE-2025-0890)
- **SID:** 2060090
- **Serviço alvo:** Telnet (porta 23)
- **Gravidade:** Major
- **Confiança:** High

Esta regra está direcionada a equipamentos de rede Zyxel que mantêm credenciais padrão ativas. A análise incide sobre tráfego TCP com destino à porta 23 (Telnet), procurando sequências específicas no conteúdo da comunicação, como o nome de utilizador "admin"seguido da palavra-passe "1234".

```
alert tcp any any -> $HOME_NET 23 ( msg:"ET EXPLOIT Zyxel DSL CPE Management
Interface Default Credentials (admin) (CVE-2025-0890)";
flow:established,to_server; content:"admin|0d 00|1234"; sid:2060090; rev:1; )
```

5.4.2 Lógica da Regra

- `msg:"ET EXPLOIT Zyxel DSL CPE Management Interface Default Credentials (admin) (CVE-2025-0890)";`
  Mensagem de alerta exibida quando a regra é acionada, descrevendo uma tentativa de exploração por credenciais padrão *admin*. Está associada à vulnerabilidade **CVE-2025-0890**.
- `flow:established,to_server;`
  Define condições relacionadas ao estado da conexão TCP e à direção do tráfego.
- `content:"admin|0d 00|1234";`
  Define a sequência de bytes que a regra procura no tráfego: o nome de utilizador "admin", seguido pela palavra-passe "1234". O uso de `|0d 00|` representa bytes literais entre os dois campos.
- `sid:2060090;`
  Signature ID único da regra, que permite identificá-la em logs, sistemas SIEM e atualizações de repositórios de regras.
- `rev:1;` Número da revisão da regra.

A gravidade da assinatura foi classificada como *"Major"*, com nível de confiança *"High"*, o que indica forte probabilidade de exploração bem-sucedida. A utilização de credenciais padrão representa uma falha de configuração crítica, frequentemente explorada por atacantes.

A Figura 9 apresenta a linha da regra conforme configurada no ficheiro do Suricata, demonstrando que o sistema está corretamente preparado para detetar este tipo de ameaça.

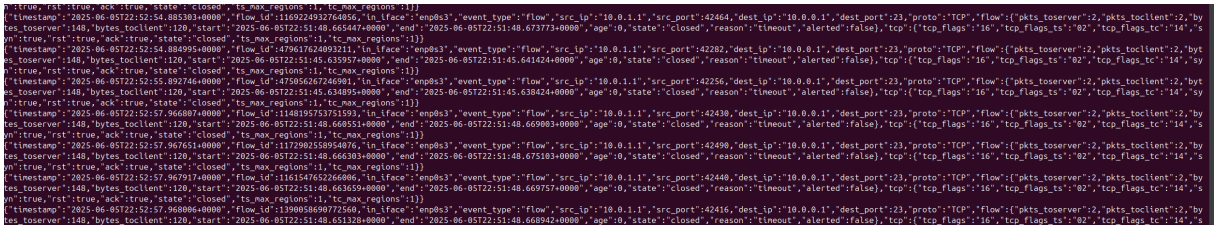

Figura 9: Alerta relacionado com Ataque de Força Bruta via Telnet

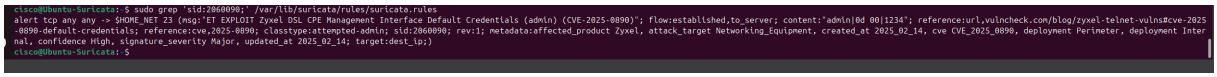

Figura 10: Regra do Suricata para deteção de tentativas de login Telnet com credenciais padrão (sid:2060090)

6 Perguntas

6.1 Quão eficaz é o Suricata na deteção de diferentes tipos de ataques na rede?

O suricata demonstrou ser uma ferramenta bastante eficaz na deteção de diferentes tipos de ataques. No contexto dos testes realizados neste projeto, o sistema, a funcionar como IDS, foi capaz de identificar com sucesso, os diferentes tipos de ataque realizados (port scanning, brute force via Telnet, DDoS, DoS, reconnaissance SNMP).

6.2 Será o Suricata capaz de detetar, com eficiência, ataques em tempo real?

Sim, o Suricata é projetado para realizar a deteção de intrusões em tempo real. Na configuração adotada (IDS), o suricata mostrou ser eficaz na análise em tempo real, tendo sido capaz de gerar alertas imediatamente após a deteção de padrões maliciosos.

6.3 O desempenho do Suricata pode ser afetado por um elevado volume de tráfego na rede?

O desempenho do Suricata pode ser afetado por um elevado volume de tráfego, especialmente em ambientes com limitação de recursos. Durante os testes realizados, o Suricata conseguiu detetar os ataques em tempo útil, ainda assim o elevado volume de pacotes fez o sistema utilizar mais recursos como é visível nos gráficos 10 e 11.

- Num cenário real, com tráfego intenso e variado, o volume de pacotes pode comprometer a capacidade de análise em tempo real;
- O Suricata faz análise profunda dos pacotes, o que é exigente em termos de CPU e memória — se os recursos forem insuficientes, pode haver perda de pacotes ou atraso na geração de alertas;
- A quantidade de regras ativas também afeta diretamente o desempenho: quanto mais regras, mais tempo o Suricata leva para analisar cada pacote.

Apesar disso, em ambiente de laboratório como o utilizado no GNS3, o tráfego é controlado e limitado, o que permite ao Suricata manter um bom desempenho. Contudo, esta limitação deve ser tida em conta ao extrapolar os resultados para contextos reais.

Figura 11: CPU antes do Ataque - ≈ 50%

Figura 12: CPU após o Ataque - ≈ 80%

7 Conclusão

As experiências conduzidas ao longo deste guião laboratorial demonstraram, de forma inequívoca, a eficácia e a relevância do Suricata na monitorização de tráfego de rede e na deteção de uma variedade de comportamentos anómalos e maliciosos. Através da simulação de diversos tipos de ataques, desde o reconhecimento com scans de portas até tentativas de negação de serviço e força bruta, foi possível observar na prática a capacidade do Suricata em identificar estas ameaças e gerar alertas correspondentes.

A capacidade intrínseca do Suricata de realizar Inspeção Profunda de Pacotes (*Deep Packet Inspection* - DPI) revelou-se fundamental, permitindo uma análise granular não apenas dos cabeçalhos, mas também do conteúdo das comunicações. Esta funcionalidade mostrou-se essencial na deteção de assinaturas específicas (por exemplo, comandos SNMP) e padrões presentes em tráfego de aplicação.

Adicionalmente, a exploração da sintaxe das regras do Suricata e a experimentação com a sua ativação sublinharam a flexibilidade da ferramenta, bem como a importância de compreender os seus mecanismos de deteção para otimizar a segurança da rede. A análise das regras acionadas pelos diferentes ataques permitiu descortinar a lógica subjacente à deteção, desde simples correspondências de conteúdo até mecanismos mais avançados baseados em estado e em limiares.

Em suma, este guião proporcionou uma base sólida para a compreensão prática do Suricata como uma ferramenta poderosa e essencial no arsenal de segurança de redes. A capacidade de adaptação, a profundidade analítica e a riqueza das suas funcionalidades fazem do Suricata um recurso indispensável para qualquer profissional na área da cibersegurança.

Referências

[1] VulnCheck. (2025, 20 de março). *Zyxel Hardcoded Credentials & Telnet Command Injection Vulnerabilities*. VulnCheck Blog. Disponível em: `https://vulncheck.com/blog/zyxel-telnet-vulns#cve-2025-0890-default-credentials`. Acedido em: 5 de junho de 2025.

[2] Cisco Networking Academy. (2025). *Network Security, Módulo 11: IPS Technologies*. Material do curso online. Acedido em: 5 de junho de 2025.

[3] Luo, Carrie. (2023, 13 de novembro). *Open-Source IDS/IPS: Suricata for Beginners*. DEV Community (dev.to). Disponível em: `https://dev.to/carrie_luo1/open-source-idsips-suricata-for-beginners-5d42`. Acedido em: 2 de junho de 2025.

[4] Moyle, Ed. (2024, 18 de julho). *Top 15 Kali Linux tools and how to use them*. SearchSecurity (TechTarget). Disponível em: `https://www.techtarget.com/searchsecurity/tip/Top-Kali-Linux-tools-and-how-to-use-them`. Acedido em: 5 de junho de 2025.

[5] Open Information Security Foundation. (2025). *Suricata Rules Documentation*. Disponível em: `https://docs.suricata.io/en/latest/rules/intro.html`. Acedido em: 3 de junho de 2025.