Instituto Superior de Engenharia

Politécnico de Coimbra

Segurança

2024/2025

Splunk

Diogo Coutinho Amor Antunes 2018016615 a20180425@isec.pt
Duarte Jorge Ferreira Rodrigues 2022150190 a2022150190@isec.pt

Licenciatura de Engenharia Informática
Coimbra, 06 de Junho de 2025

Conteúdo

Capítulo 1

Introdução

A monitorização e análise de sistemas informáticos deixaram de ser tarefas meramente reativas para se tornarem componentes estratégicos na gestão de infraestruturas tecnológicas. À medida que as redes se tornam mais complexas, a variedade de dispositivos e as ameaças cada vez mais sofisticadas, torna-se crucial o uso de ferramentas especializadas que proporcionem uma visão em tempo real do que acontece nos sistemas.

Neste projeto, examinamos uma ferramenta frequentemente utilizada no campo da cibe segurança e análise operacional: o Splunk. Ao invés de nos concentrarmos apenas nas suas características teóricas, criámos uma estratégia prática que reproduz um cenário real, utilizando routers, servidores web e máquinas virtuais configuradas numa rede simulada. A meta principal é ilustrar, por meio de exemplos práticos, como o Splunk pode ser empregue para recolher, tratar, visualizar e responder a eventos significativos, com ênfase especial em registros de autenticação, tráfego de rede e detecção de comportamentos duvidosos.

O projeto não se concentra só na coleta e análise de dados, mas também em cenários práticos, como a elaboração de paineis, o envio de logs de várias origens (via Syslog e Forwarders) e a configuração de notificações automáticas baseadas em critérios de segurança. Esta estratégia possibilita não só entender a operação técnica do instrumento, mas também avaliar o seu efeito em termos de prevenção, auditoria e resposta a incidentes.

Neste documento, buscamos ilustrar como a incorporação do Splunk numa infraestrutura pode aprimorar consideravelmente a segurança, a eficácia operacional e a agilidade na resposta em ambientes de negócios ou acadêmicos.

Capítulo 2

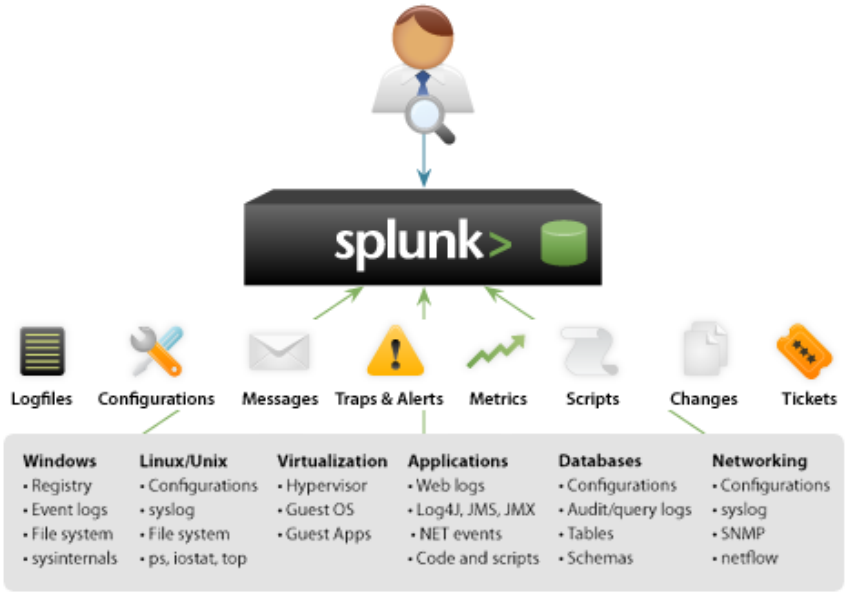
Desenvolvimento

2.1 Splunk

No atual contexto do desenvolvimento tecnológico, a quantidade de dados gerados pelas infraestruturas é enorme. Servidores, aplicações e diversos equipamentos geram constantemente informações que descrevem o seu funcionamento. Podem ser logs, notificações ou até métricas de desempenho. Este tipo de informação é conhecido como dados de máquina (*machine data*).

O Splunk é uma plataforma que permite juntar, indexar, armazenar e mais tarde consultar e analisar dados de máquinas. Isto em tempo real, ou para uma análise posterior. Foi desenvolvido para transformar dados complexos em algo fácil, acessível e útil, permitindo que os profissionais tomem decisões rápidas e responsáveis.

Desenhado para lidar com qualquer tipo de dado computacional, como logs de aplicações, registos de rede, eventos em sistemas operativos, erros em bases de dados, entre outros. Estes dados não estão normalmente estruturados, mas o Splunk consegue facilitar o seu processamento de forma automática e eficiente.



2.2 Funcionalidades Principais do Splunk

O Splunk inclui inúmeras funcionalidades tais como a angariação de dados sejam logs de servidores, logs de segurança, logs de bases de dados, equipamentos de rede, serviços cloud ou sistemas operativos. Isto pode ser feito

através de agentes chamados Forwarders ou por meio de conexões diretas a ficheiros e serviços.

Uma vez coletados, os dados são indexados pelo Splunk e organizados em estruturas chamadas buckets, e classificados em diferentes categorias (Hot, Warm, Cold, Frozen e Thawed) de acordo com a sua idade e frequência de acesso. Este armazenamento é feito com compressão o que garante alto desempenho e escalabilidade.

A consulta e análise dos dados é feita a partir da Search App, usando uma linguagem própria, a SPL (Search Processing Language). Com o SPL é possível procurar por erros ou eventos específicos, filtrar resultados por tempo, origem, tipo de evento etc, realizar correlações entre diferentes sistemas e extrair campos e padrões automaticamente.

É possível ainda criar gráficos interativos e paineis personalizados de forma a visualizar a informação de maneira clara e objetiva. Estes paineis podem ser utilizados para monitoramento em tempo real dos sistemas, acompanhamento de métricas de desempenho ou a visualização de incidentes de segurança.

Existe também a possibilidade de criar alertas com base em condições específicas como um número de tentativas falhadas de login (para prevenir os ataques *brute-force*), uso excessivo de CPU ou RAM, erros recorrentes no sistema ou a ausência de dados expectados (serviço offline). Quando um alerta é disparado, o Splunk pode enviar uma notificação ao administrador ou até executar scripts de correção.

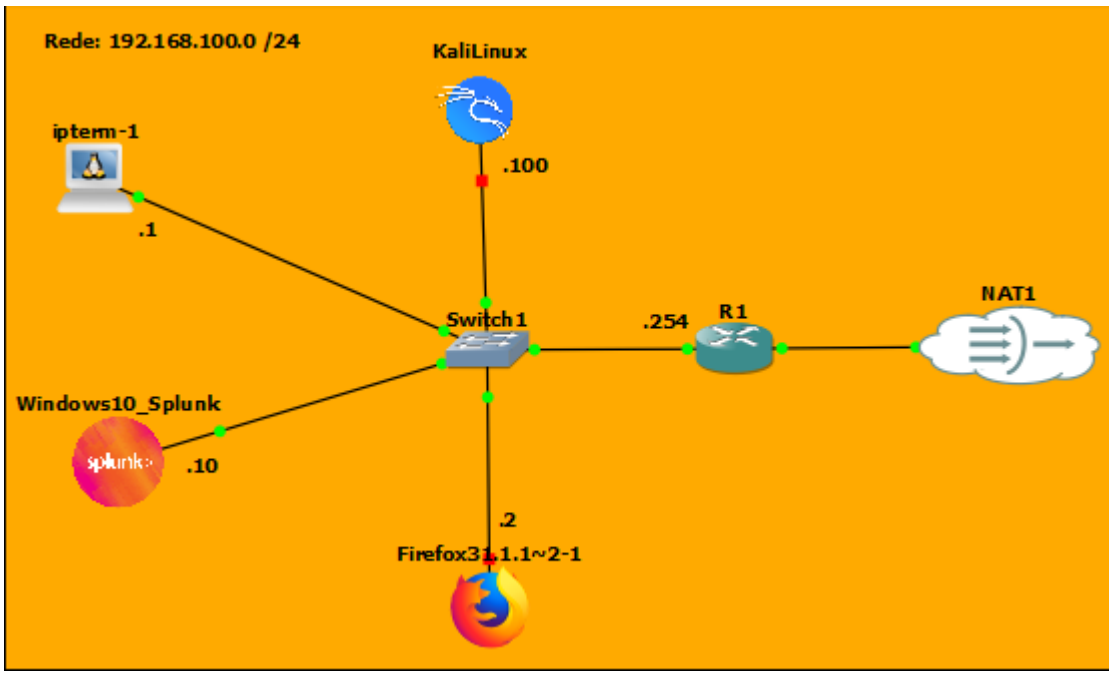
Na prática o Splunk serve para a detecção de falhas técnicas antes de se tornarem problemas críticos, análise forense de segurança (resposta a ataques e rastreamento de acessos suspeitos), monitoramento de performance de aplicações e servidores, acompanhamento de KPIs de negócio e automatização de auditorias e relatórios em conformidade com o RGPD, ISO etc.

Capítulo 3

Testbed

3.1 Ambiente para as experiências

Para serem feitas algumas experiências foi criada uma topologia no gns3, com vários dispositivos e máquinas virtuais para criar um ambiente mais realista. Estes estão todos presentes na mesma rede.



- Router 1 - 192.168.100.254
- Ip Term 1 - 192.168.100.1
- WebTerm Firefox - 192.168.100.2
- Máquina Virtual Windows 10 - 192.168.100.10
- Máquina Virtual Kali - 192.168.100.100
- NAT - Para puder ter acesso à internet em toda a rede.

3.2 Configurações do router

No router para poder obter uma maior variedade de logs, foi configurado para receber comunicação ssh, e também foi criado um http server. Além disso, foram criados 3 utilizadores locais, *admina* e *adminb*, para gerar logs a partir de

comunicações ssh e acessos diretamente ao router e o *webadmin*, para gerar logs para acessos ao webserver do router.

```
R1(config)#username admina secret ciscoadmin
R1(config)#ip domain-name span.com
R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R1(config)#
*May 31 16:40:29: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#ip ssh version 2
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
```

```
R1(config)#username adminb secret ciscoadmin
```

```
R1(config)#enable secret cisco
```

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

```
R1(config)#ip http server
R1(config)#ip http authentication local
R1(config)#username webadmin privilege 15 secret webadmin
```

Por fim, configurei o router para poder gerar as mensagens log e consequentemente as enviasse com base no protocolo syslog para o servidor splunk, presente na máquina virtual windows 10 (192.168.100.10), para que este as armazene.

```
R1(config)#logging host 192.168.100.10
R1(config)#
*May 30 18:56:49.930: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.100.10 port 514
 started - CLI initiated
```

```
*Jun  2 11:37:18: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.100.10 port 514 res
tored CLI initiated
R1(config)#logging trap debugging
R1(config)#logging console informational
R1(config)#
*Jun  2 11:38:06: %SYS-5-LOG_CONFIG_CHANGE: Console logging: level informational, xml disab
led, filtering disabled
R1(config)#
```

```
R1(config)#login on-succes log
R1(config)#login on-failure log
```

Como se pode verificar nas imagens acima, configurei, para que o router possa gerar logs de acesso, tanto de falha como de sucesso. Coloquei para enviar mensagens de log de nível gravidade “debugging”, para ser mais detalhado e gerar

o máximo de logs. As mensagens de log são enviadas para servidor splunk utilizando o protocolo UDP na porta 514.

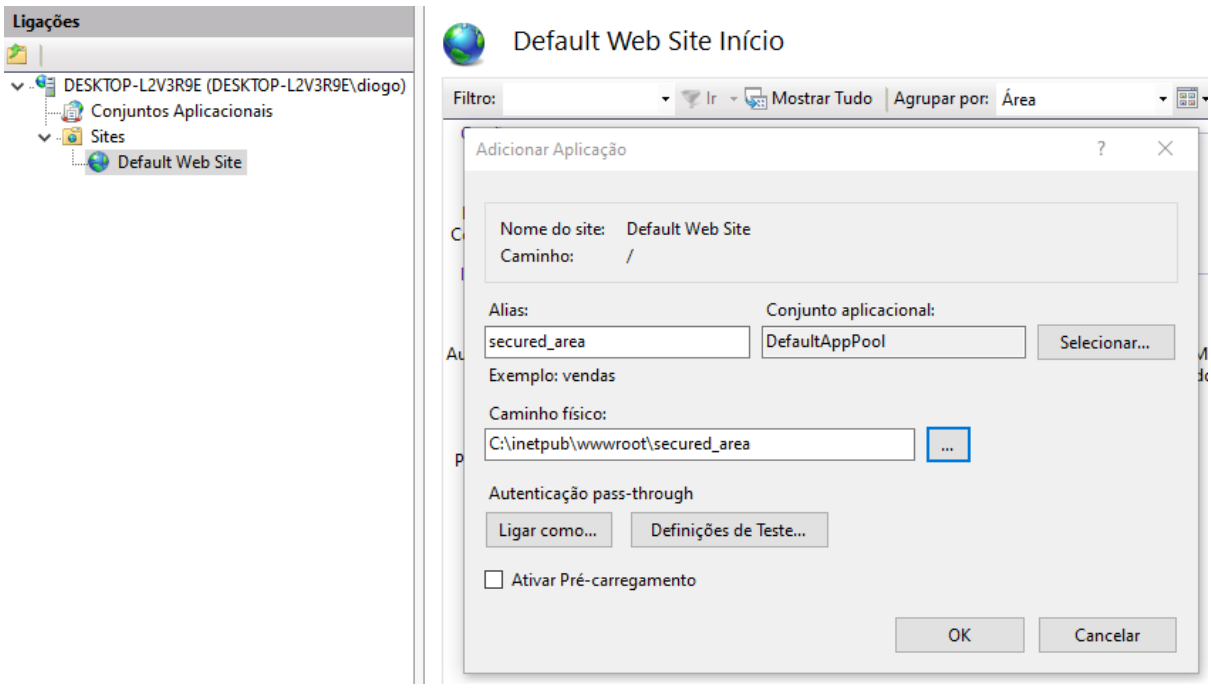
3.2 Configuração da Máquina Virtual Windows 10

3.2.1 Configuração do Web Server (IIS)

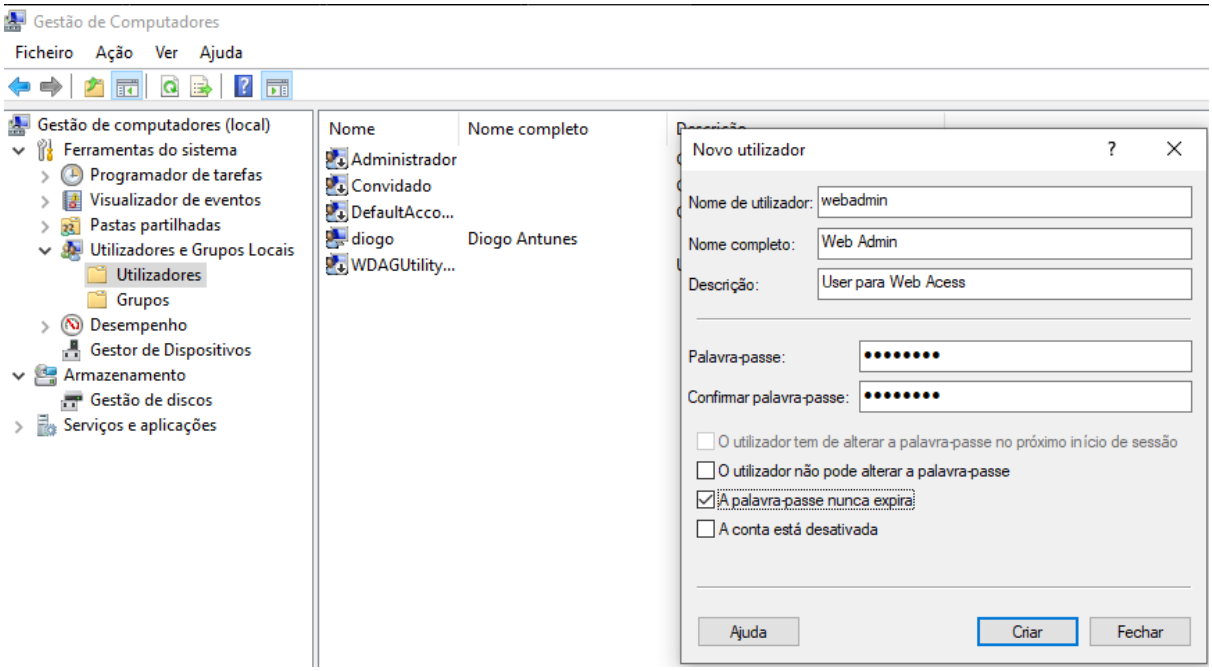
Primeiramente foi criado um web server (IIS), para poder ter mais uma fonte de logs de autenticação http e tornar o ambiente da experiência mais completo e realista. Para isso precisei de instalar e configurar o *Internet Information Services (IIS)*.

Após a instalação, é criado o diretório padrão para sites web **C:\inetpub\wwwroot** onde depois criei uma pasta (area_segura), onde coloquei o ficheiro html do site.

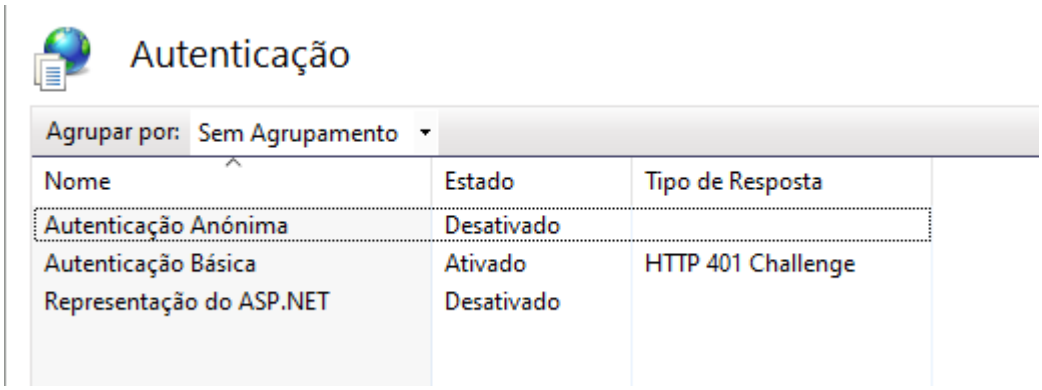
A seguir criei o web server no gestor IIS, começando por criar um diretório autenticado (secured_area) e associo à pasta que criei.

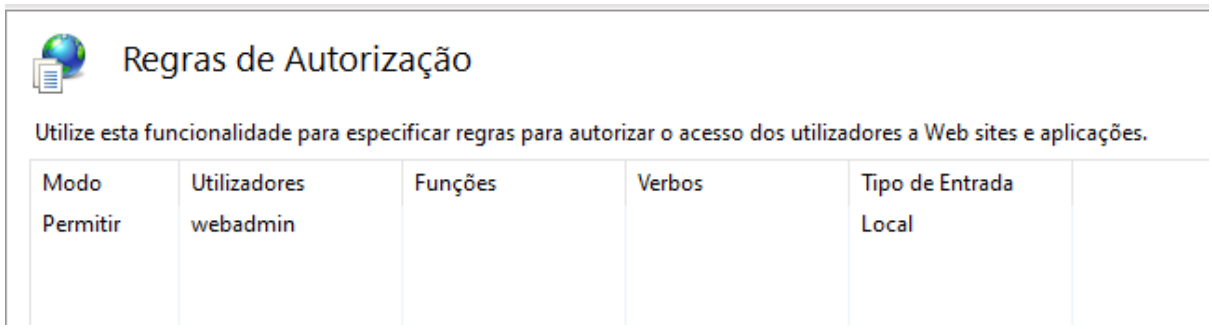


A seguir foi criado o utilizador webadmin no windows 10, para testar os acessos por autenticação ao site.



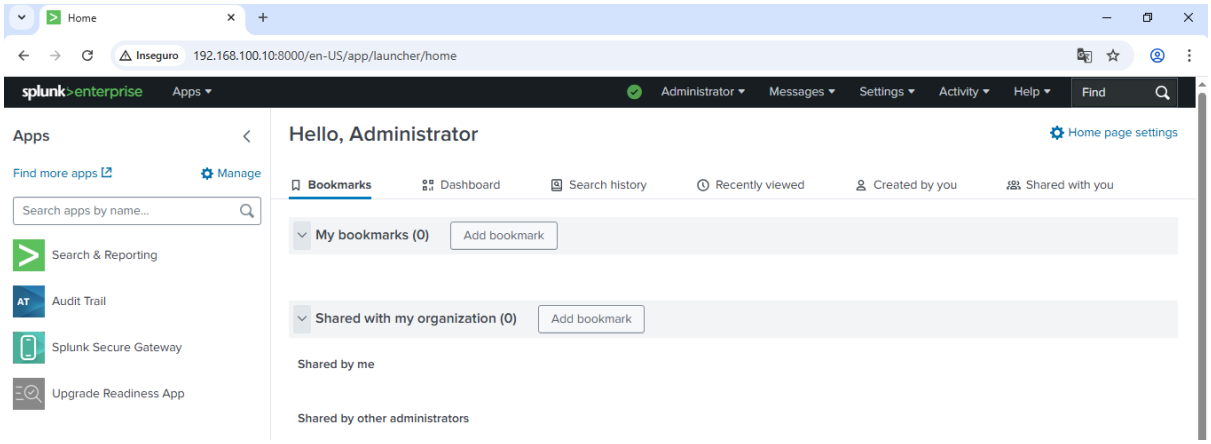
Por fim, mudei as regras de autenticação do site para autenticação básica, para ser necessário haver autenticação e alterei também as regras de autorização para permitir que o utilizador criado possa ter acesso ao site.





3.2.2 Configuração do servidor Splunk

Primeiramente instalei o Splunk Enterprise no windows 10. Após a instalação, para aceder ao servidor splunk web criado, basta aceder via web ao endereço **http://<IP_da_máquina>:8000**, neste caso, http://192.168.100.10:8000, que nos leva à página inicial do servidor Splunk.



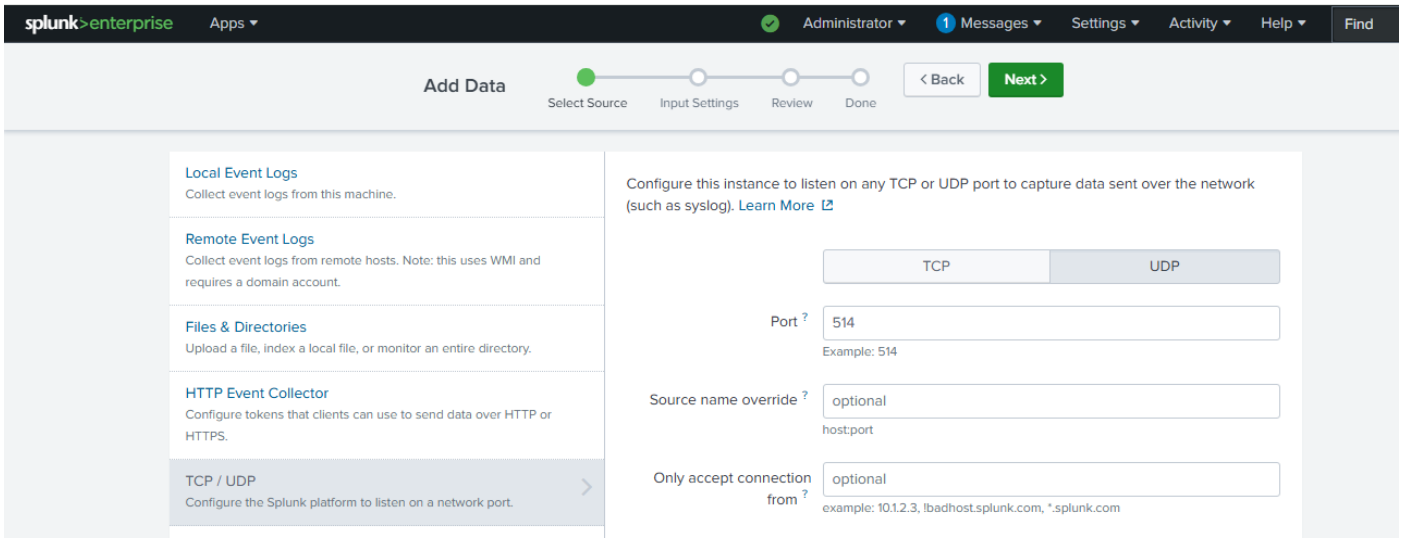
Capítulo 4

Experiências

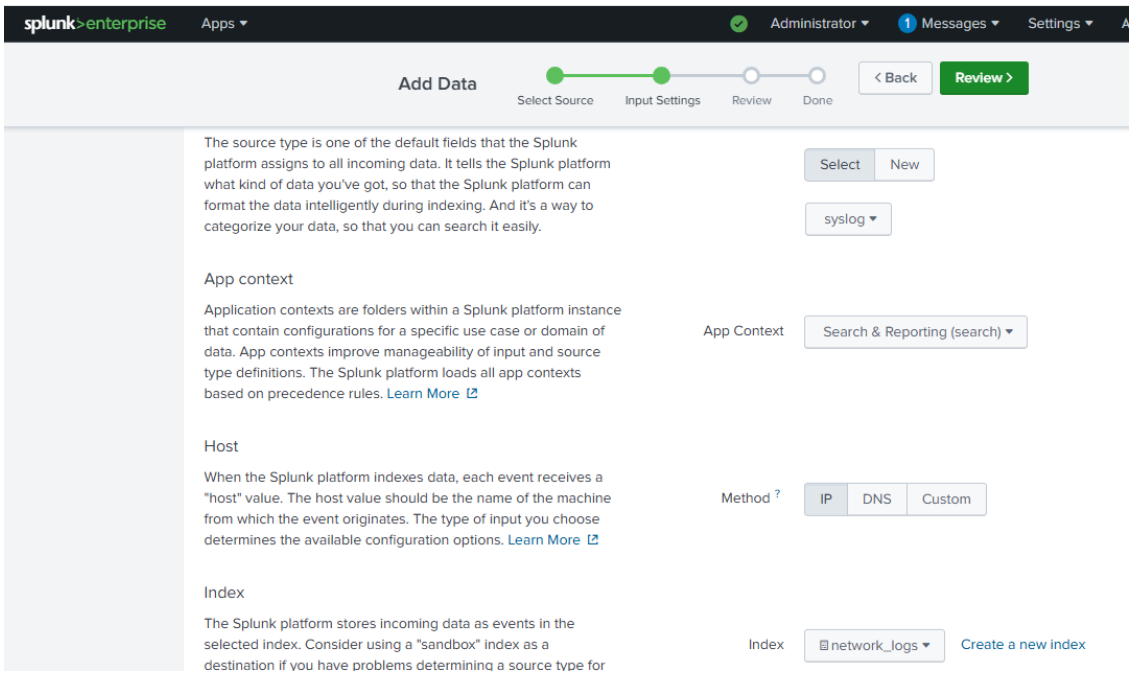
4.1 Experiência 1

Nesta experiência, tentamos mostrar como os dados de log gerados no router, podem ser enviados para o Splunk Indexer. Como é que os dados podem ser pesquisados e visualizados, assim como indexados de maneira que a pesquisa dos mesmos seja facilitada.

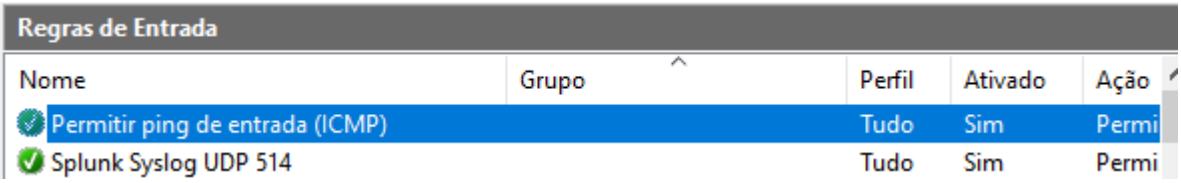
Primeiramente foi configurada uma entrada de dados para que o Splunk pudesse reconhecer que estavam a ser enviadas mensagens syslog a partir do Router, neste caso via comunicação UDP na porta 514.



Estes dados obtidos pelo router vão ser armazenados num índice à parte com o nome *network_logs* para facilitar e otimizar a organização.



Como não estávamos a conseguir fazer o ping até ao router, nem a conseguir receber os logs vindos do router, foi preciso criar regras na firewall do Windows 10 para permitir mensagens ICMP e para permitir a entrada de comunicações UDP vindas da porta 514.



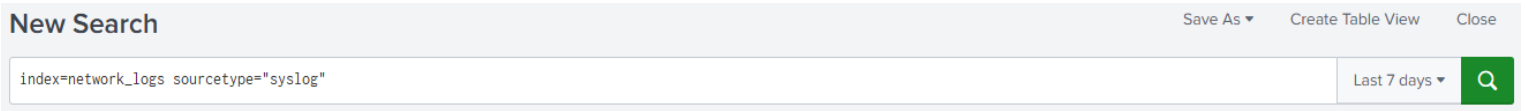
Após serem feitas as configurações para que o Splunk pudesse receber e armazenar os logs gerados pelo router corretamente, começámos a gerar os vários tipos de logs que eram possíveis neste ambiente:

- Logs de autenticação, ssh a partir do ipterm, com autenticações erradas e com sucesso;
- Logs de autenticação, http a partir do webterm para o http server do router
- logs de configuração.

Para poder visualizar os logs, basta ir ao *Search & Reporting* na página principal do Splunk.

A pesquisa dos dados para ser facilitada temos de especificar ao splunk, que tipos de dados e que dados queremos visualizar. Os campos fundamentais para filtrar e direcionar a pesquisa são:

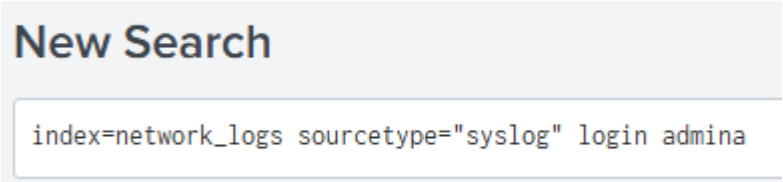
- **Index** - O repositório onde os dados são armazenados, no caso dos dados gerados pelo router, estes foram indexados no índice network_logs;
- **sourcetype** - É o tipo de fonte que identifica o formato dos dados de entrada, neste caso é syslog;
- **host** - nome ou ip do dispositivo de onde os dados ou logs são enviados;
- **source** - Identifica o caminho do arquivo de onde os dados foram coletados, neste caso, udp:514.



Como se pode verificar na imagem acima, comecei por procurar todos os eventos syslog, indexados no índice network_logs e do tipo syslog, ou seja, todos os logs gerados pelo router. Como se pode ver também pode-se filtrar as pesquisas por tempo.

i	Time	Event
>	6/1/25 3:20:41.000 PM	Jun 1 15:20:41 192.168.100.254 57: *Jun 1 14:20:41: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: webadmin] [Source: 192.168.100.2] [localport: 80] at 14:20:41 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:20:04.000 PM	Jun 1 15:20:04 192.168.100.254 56: *Jun 1 14:20:03: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: webadmin] [Source: 192.168.100.2] [localport: 80] at 14:20:03 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:42.000 PM	Jun 1 15:13:42 192.168.100.254 55: *Jun 1 14:13:41: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admina] [Source: 192.168.100.1] [localport: 22] at 14:13:41 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:37.000 PM	Jun 1 15:13:37 192.168.100.254 54: *Jun 1 14:13:36: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admina] [Source: 192.168.100.1] [localport: 22] [Reason: Login Authentication Failed] at 14:13:36 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:33.000 PM	Jun 1 15:13:33 192.168.100.254 53: *Jun 1 14:13:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admina] [Source: 192.168.100.1] [localport: 22] [Reason: Login Authentication Failed] at 14:13:32 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:19.000 PM	Jun 1 15:13:19 192.168.100.254 52: *Jun 1 14:13:19: %SYS-6-LOGOUT: User adminb has exited tty session 2(192.168.100.1) host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 1:28:16.000 PM	Jun 1 13:28:16 192.168.100.254 63: *Jun 1 12:28:15: %SYS-5-CONFIG_I: Configured from console by admina on vty0 (192.168.100.1) host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 1:27:28.000 PM	Jun 1 13:27:28 192.168.100.254 62: *Jun 1 12:27:27: %SYS-5-CONFIG_I: Configured from console by admina on console host = 192.168.100.254 source = udp:514 sourcetype = syslog

A imagem acima, mostra o output da pesquisa, onde se podem verificar os vários tipos de logs gerados pelo router. No entanto se quisermos a pesquisa pode ser ainda mais detalhada, por exemplo, se quisermos pesquisar apenas os logs de autenticação gerados pelo router basta adicionar login ao comando de pesquisa que utilizei para gerar estes dados. O método de pesquisa do Splunk facilita bastante a filtragem de logs. Pode-se verificar na imagem abaixo, como exemplo, os logs de autenticação do admina.



i	Time	Event
>	6/1/25 3:23:02.000 PM	Jun 1 15:23:02 192.168.100.254 62: *Jun 1 14:23:02: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admina] [Source: UNKNOWN] [localport: 0] at 14:23:02 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:42.000 PM	Jun 1 15:13:42 192.168.100.254 55: *Jun 1 14:13:41: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admina] [Source: 192.168.100.1] [localport: 22] at 14:13:41 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:37.000 PM	Jun 1 15:13:37 192.168.100.254 54: *Jun 1 14:13:36: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admina] [Source: 192.168.100.1] [localport: 22] [Reason: Login Authentication Failed] at 14:13:36 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog
>	6/1/25 3:13:33.000 PM	Jun 1 15:13:33 192.168.100.254 53: *Jun 1 14:13:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admina] [Source: 192.168.100.1] [localport: 22] [Reason: Login Authentication Failed] at 14:13:32 UTC Sun Jun 1 2025 host = 192.168.100.254 source = udp:514 sourcetype = syslog

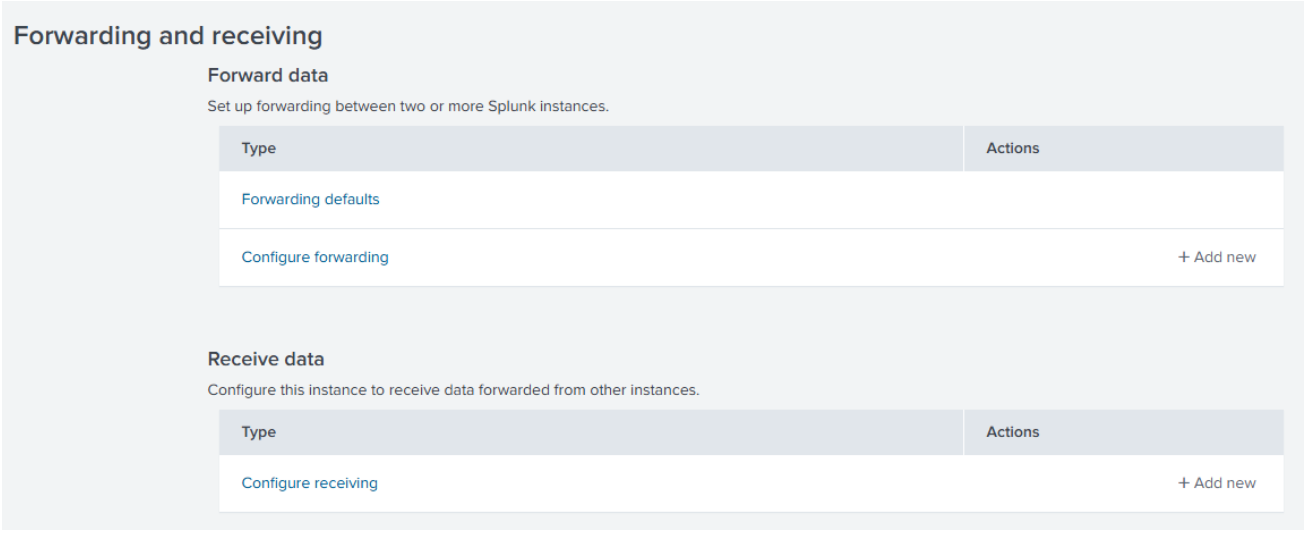
Como se pode verificar na imagem, foram filtrados todos os logs de autenticação do admina, entre eles, autenticação por ssh (localport: 22) e diretamente no router.(localport: 0).

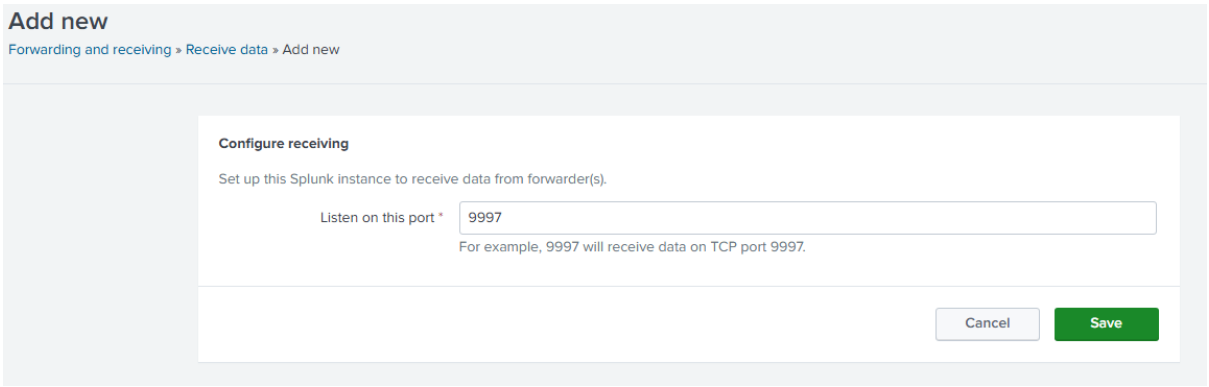
4.2 Experiência 2

Nesta segunda experiência, o objetivo é tentar enviar os logs gerados pelo web server IIS, criado no Windows 10. Ao contrário dos dados gerados pelo router, que podem ser enviados diretamente para o Splunk Indexer através da rede, os logs gerados pelo web server IIS necessitam de um agente externo para coletar os dados dos logs e enviar para o Splunk Indexer.

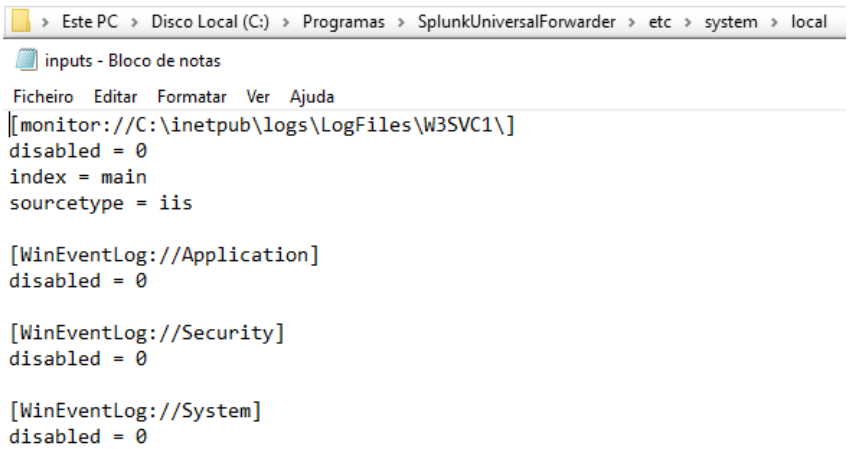
Para realizar essa tarefa, foi instalado o Universal Forwarder do Splunk para poder aceder aos logs gerados pelo web server do windows 10 que são guardados na diretoria **C:\inetpub\logs\LogFiles\W3SVC1**.

Após instalar e configurar o Universal Forwarder, foi necessário configurar o splunk para que este possa receber os dados dos logs do web server, ou seja, teve de se dizer ao splunk para “escutar” a comunicação UDP da porta 9997, porta padrão que é utilizada para transmissão de dados pelo Universal forwarder do Splunk.





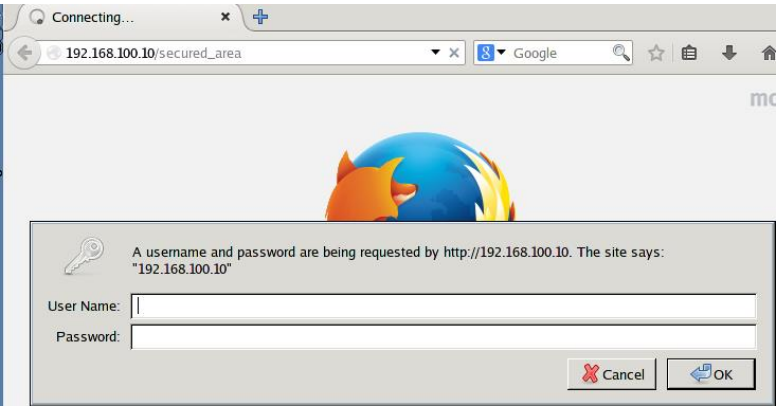
Como se pode verificar nas imagens acima, foi configurado o splunk para escutar a porta 9997, porta utilizada para o encaminhamento de dados (data forwarding), utilizando a comunicação TCP. Neste caso estes dados são armazenados no index **main**.

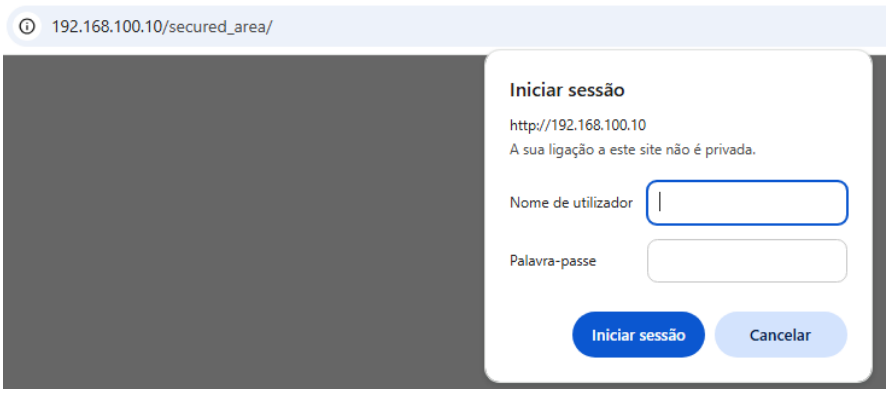


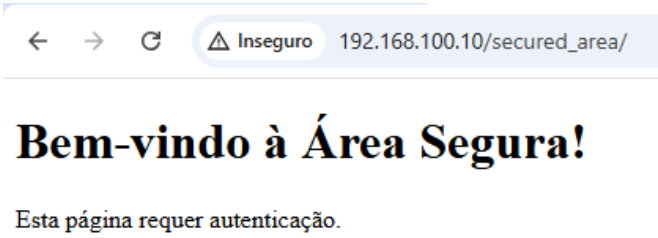
Na imagem acima, pode-se visualizar a configuração dos dados enviados pelo Universal Forwader. Aqui é especificado a diretoria onde estão armazenados

os logs gerados pelo web server, onde os dados vão ser indexados no splunk indexer, neste caso, no indice main, e o sourcetype que é iis.

Após finalizar a configuração, para gerar vários logs de autenticação acedemos ao site a partir do windows 10 e do webterm com autenticações falhadas e com sucesso.



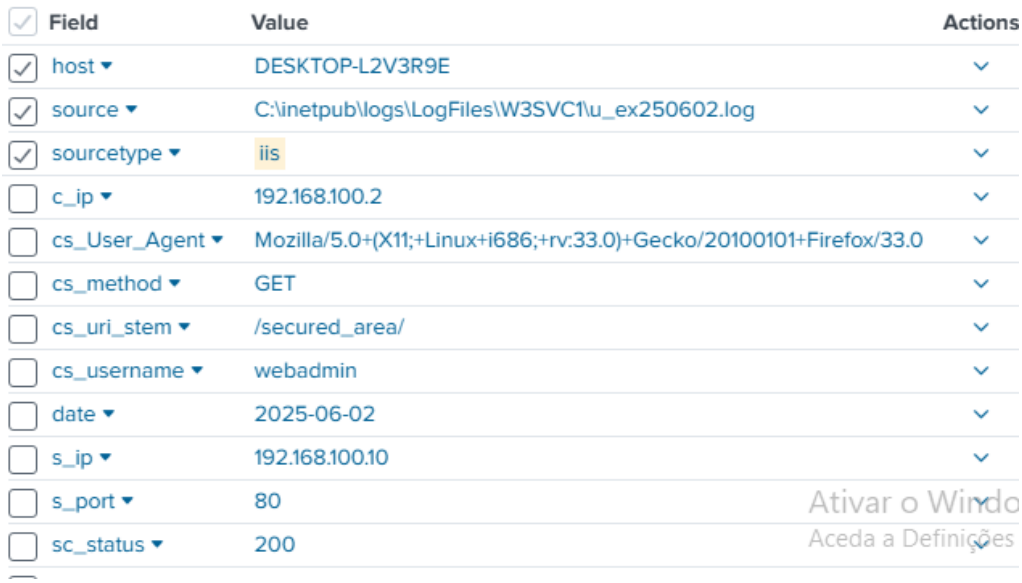




A seguir, fomos ao splunk visualizar os logs gerados, para procurar os logs criados pelo web server. Para isso, basta no motor de busca do splunk, filtrar os dados com o comando index =" main" e sourcetype="iis".

i	Time	Event
>	6/2/25 8:45:27.000 PM	2025-06-02 19:45:27 192.168.100.10 GET /secured_area/ - 80 webadmin 192.168.100.2 Mozilla/5.0+(X11;+Linux+i686;+rv:33.0)+Gecko/20100101+Firefox/33.0 - 200 0 0 1 host = DESKTOP-L2V3R9E source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex250602.log sourcetype = iis
>	6/2/25 8:45:27.000 PM	2025-06-02 19:45:27 192.168.100.10 GET /secured_area - 80 webadmin 192.168.100.2 Mozilla/5.0+(X11;+Linux+i686;+rv:33.0)+Gecko/20100101+Firefox/33.0 - 301 0 0 1 host = DESKTOP-L2V3R9E source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex250602.log sourcetype = iis
>	6/2/25 8:45:11.000 PM	2025-06-02 19:45:11 192.168.100.10 GET /secured_area - 80 - 192.168.100.2 Mozilla/5.0+(X11;+Linux+i686;+rv:33.0)+Gecko/20100101+Firefox/33.0 - 401 2 5 1 host = DESKTOP-L2V3R9E source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex250602.log sourcetype = iis
>	6/2/25 8:43:55.000 PM	2025-06-02 19:43:55 192.168.100.10 GET /favicon.ico - 80 - 192.168.100.10 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/137.0.0.0+Safari/537.36+Edg/137.0.0.0 http://192.168.100.10/secured_area/ 404 0 2 0 host = DESKTOP-L2V3R9E source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex250602.log sourcetype = iis
>	6/2/25 8:43:55.000 PM	2025-06-02 19:43:55 192.168.100.10 GET /secured_area/ - 80 webadmin 192.168.100.10 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/137.0.0.0+Safari/537.36+Edg/137.0.0.0 - 200 0 0 0 host = DESKTOP-L2V3R9E source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex250602.log sourcetype = iis

Na imagem acima pode-se ver uma parte dos logs gerados pelo web server, no entanto, em relação aos logs gerados pelo router, estes são um pouco mais confusos, não estão tão legíveis. No entanto, se abrirmos os detalhes do log, conseguimos entender e perceber melhor os dados.



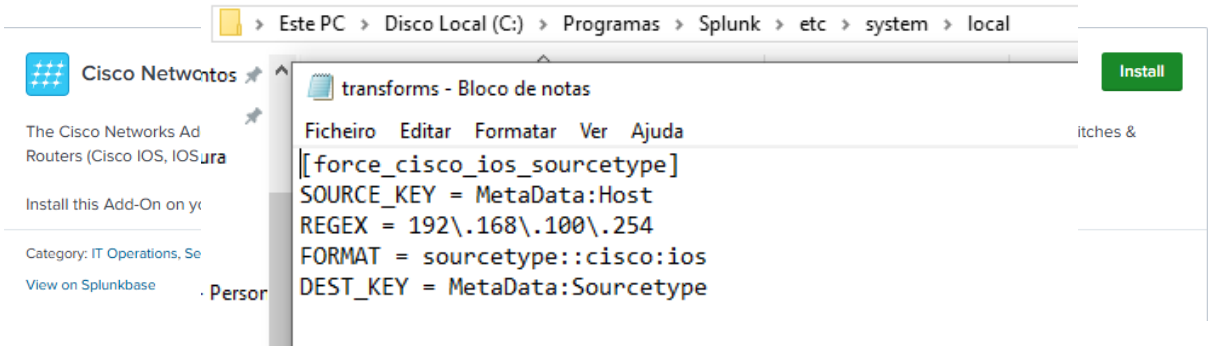
Field	Value	Actions
host	DESKTOP-L2V3R9E	
source	C:\inetpub\logs\LogFiles\W3SVC1\u_ex250602.log	
sourcetype	iis	
c_ip	192.168.100.2	
cs_User_Agent	Mozilla/5.0+(X11;+Linux+i686;+rv:33.0)+Gecko/20100101+Firefox/33.0	
cs_method	GET	
cs_uri_stem	/secured_area/	
cs_username	webadmin	
date	2025-06-02	
s_ip	192.168.100.10	
s_port	80	
sc_status	200	

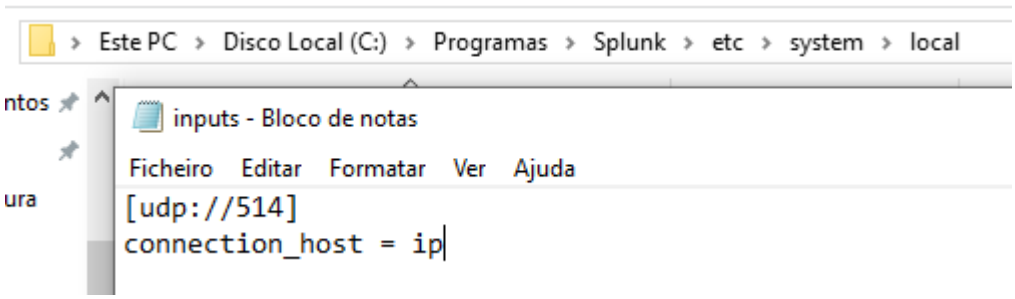
Aqui pode-se perceber melhor, os dados dos logs, por exemplo c_ip, mostra o ip de onde foi acessado o site (webterm), o username do utilizador (webadmin), protocolo (80, http), e o status (200), que indica que o acesso foi bem-sucedido.

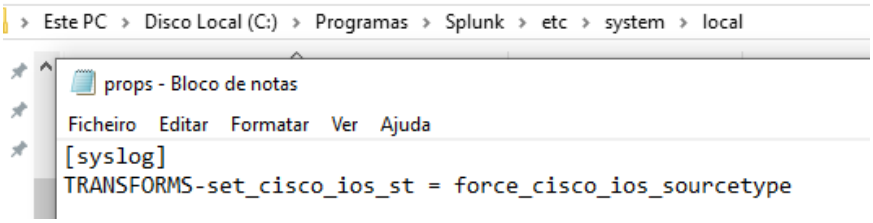
4.3 Experiência 3

Na terceira experiência, o objetivo foi configurar novos sourcetypes e definições de fonte mais corretas, para que a pesquisa dos dados seja mais fácil. Por exemplo, na última pesquisa os dados estavam confusos, menos legíveis e o objetivo é otimizar esse aspecto. Além disso, criámos uma dashboard, para visualizar aspectos específicos.

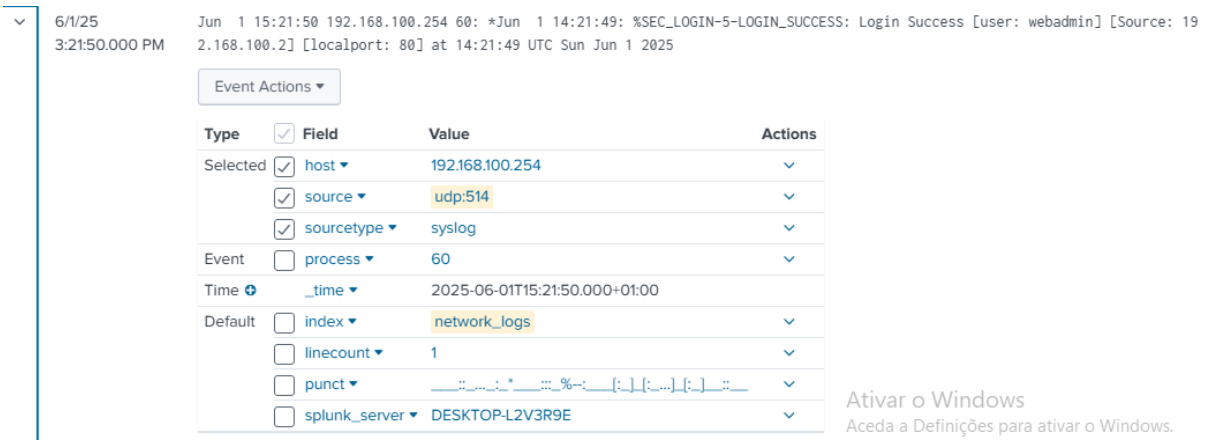
Primeiramente foi instalado o add-on para otimizar os dados recebidos pelo router. O add-on traduz os dados de uma maneira mais eficiente, e adiciona novos tipos de dados que podem ser legíveis no splunk, o que nos vai facilitar a criação de dashboards.





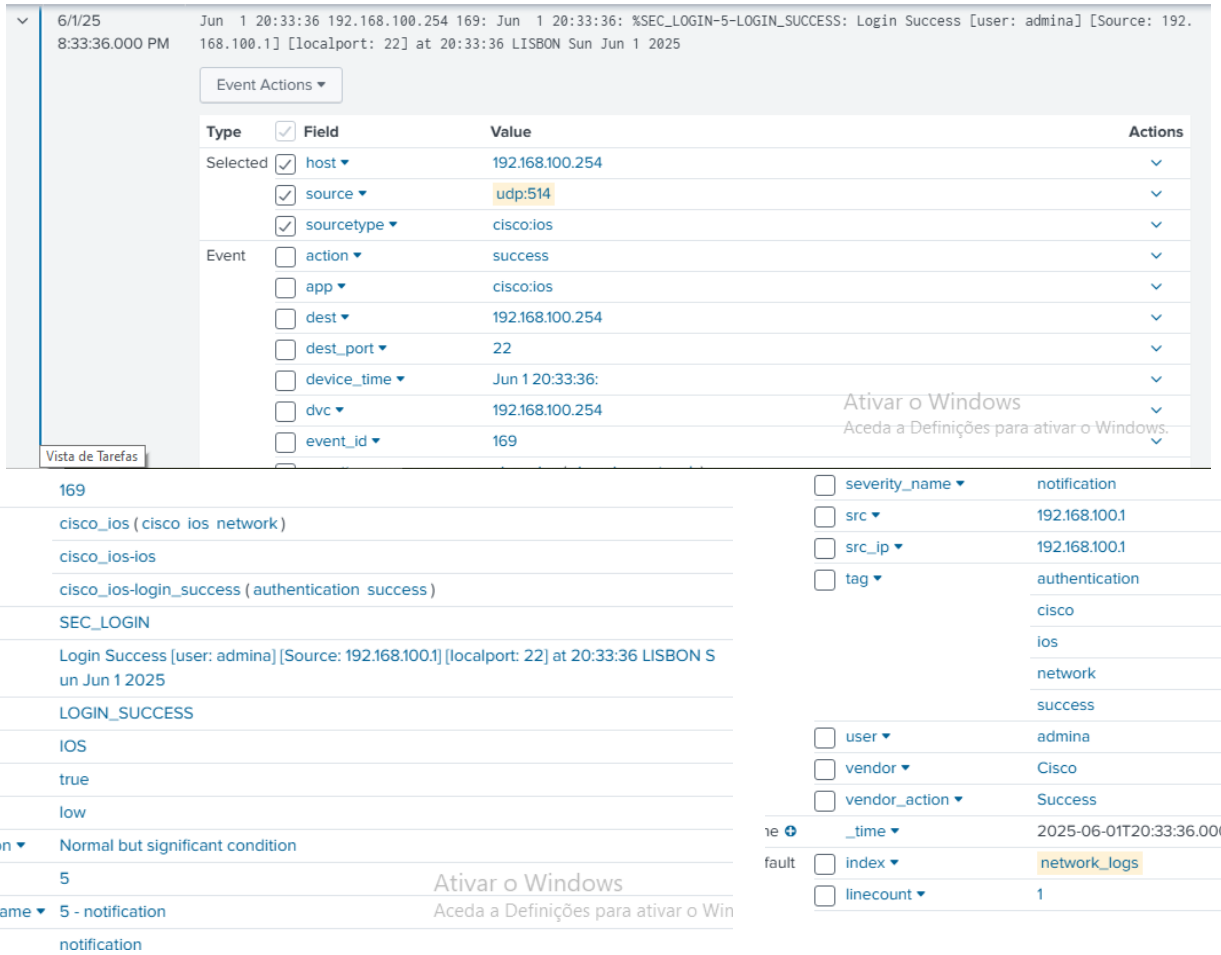


Após configurar os add-os, foram gerados novos logs no router, e neste momento quando abrimos os detalhes dos logs, os dados estão muito mais completos, comparado aos antigos.



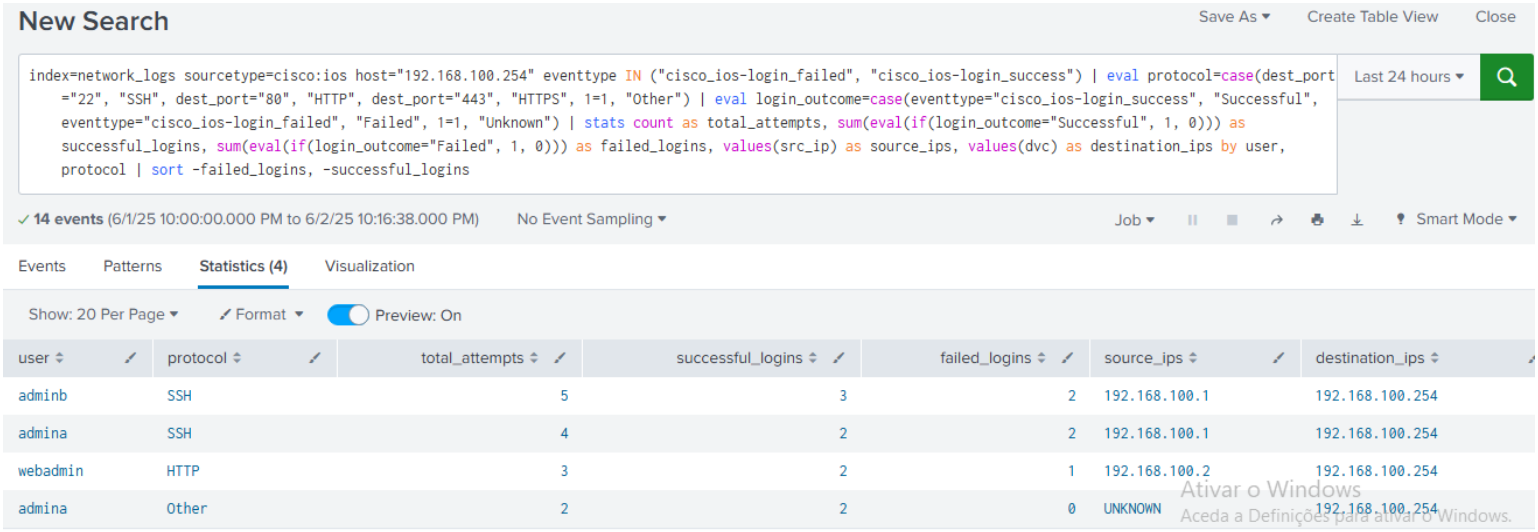
Como se pode verificar, nos detalhes dos logs antigos, não nos aparecem dados que nos permitam interpretar a mensagem do log. Sendo um log de autenticação, está em falta, por exemplo, o user, source_ip, o tipo de log, etc.

Os logs gerados após adicionar o add-on do cisco são muito mais detalhados como se pode ver nas imagens abaixo. O número de dados de um log aumentou imenso.



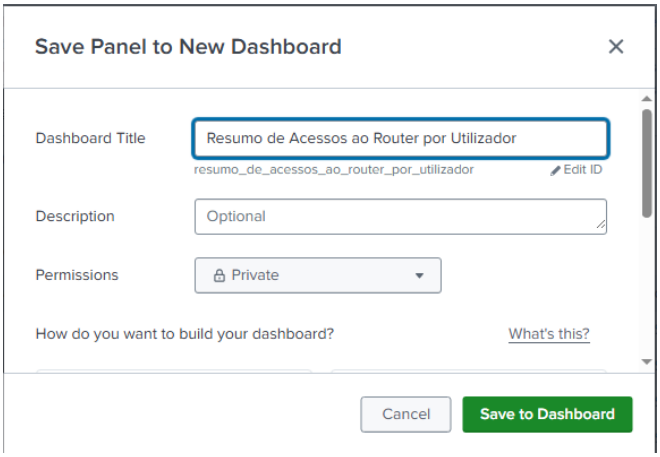
Por fim, foi criado um dashboard, onde se pode visualizar um resumo dos acessos ao router, detalhando para cada utilizador em cada tipo de acesso ao mesmo, diretamente, por ssh, http, o número de tentativas de autenticação, as bem-sucedidas e as falhadas.

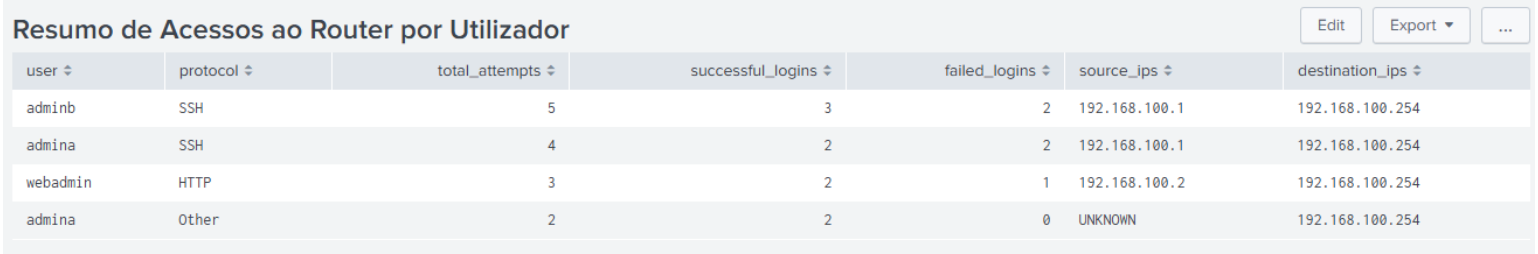
Para criar o dashboard, vai-se ao motor de busca do splunk e configura-se utilizando a linguagem SPL, o tipo de tabela que queremos criar.



Com a criação desta tabela, pode-se analisar os dados de acesso ao router de cada utilizador muito mais rápido, dando detalhes do tipo de protocolo de comunicação utilizado além do ip da máquina de onde foi feito o acesso.

Estas tabelas podem ser gravadas como dashboards, onde depois, podem ser acedidas mais facilmente, além de serem atualizadas na hora.



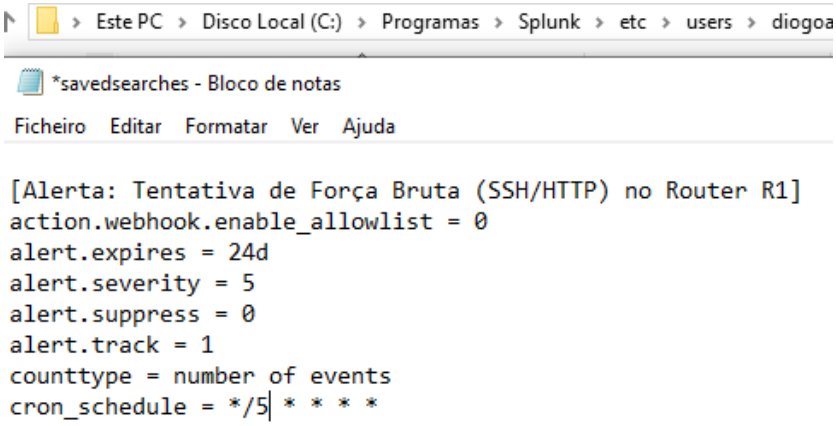


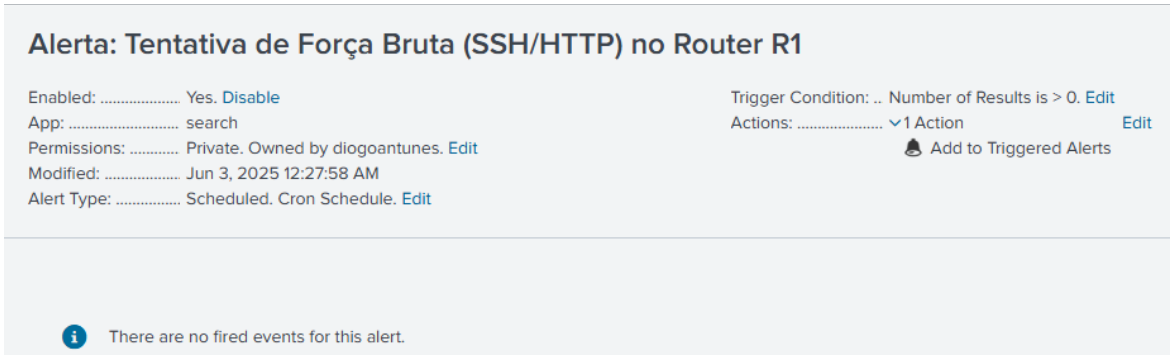
4.4 Experiência 4

Nesta última experiência, o objetivo é fazer com que o splunk identifique ataques de força bruta ao router e crie um alerta. Para isso, vamos utilizar os dados disponibilizados pelo splunk e quando um determinado utilizador tiver mais de 5 tentativas de autenticação falhadas em 15 minutos ele gera um trigger alert.

A criação do alerta é semelhante aos dashboards, cria-se uma tabela, onde tem o source ip, o número de tentativas falhadas e o tipo de acesso utilizado.

A seguir, é só ir a save e gravar como alerta. Como estou a utilizar a versão trial do Splunk, o alerta apenas se verifica de hora a hora, no entanto indo ao ficheiro de configuração dá para configurar manualmente. Para ser mais realista coloquei essa verificação a cada 5 minutos.

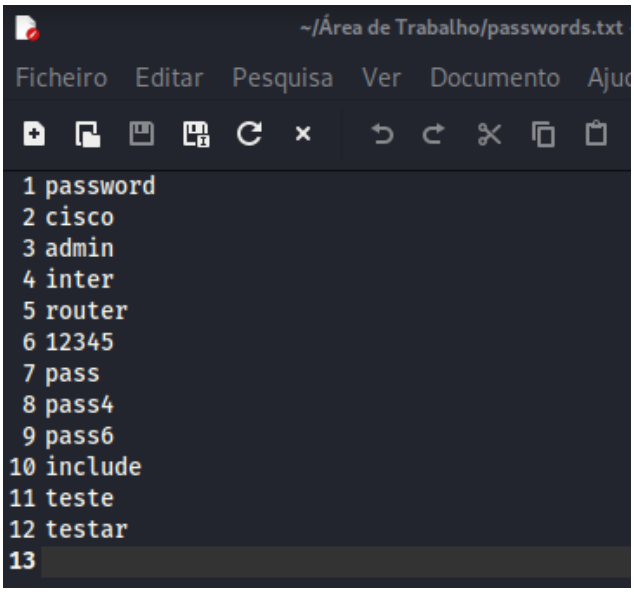


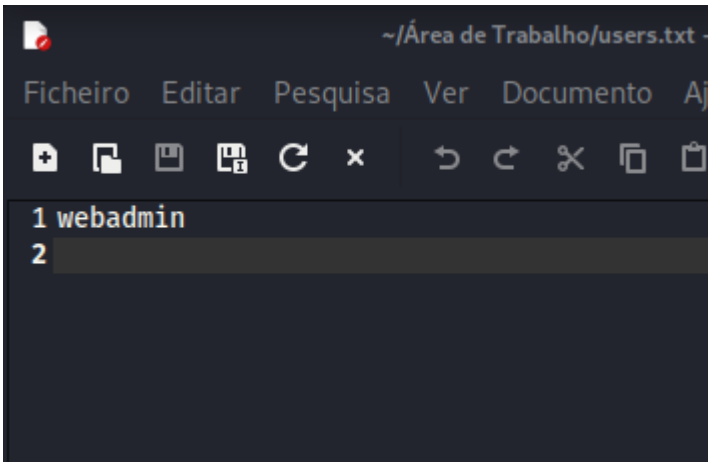


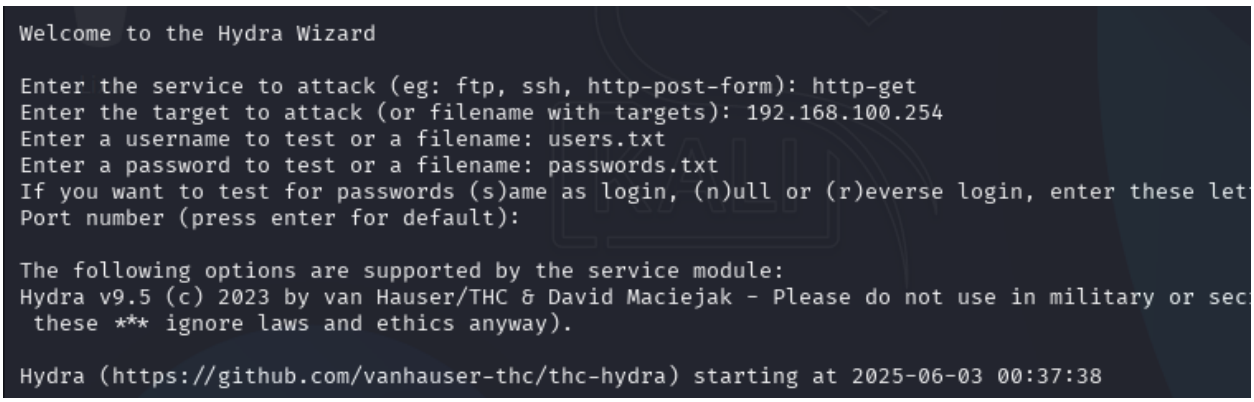
O alerta foi configurado, para quando um ataque for detectado, este emita um trigger alert.

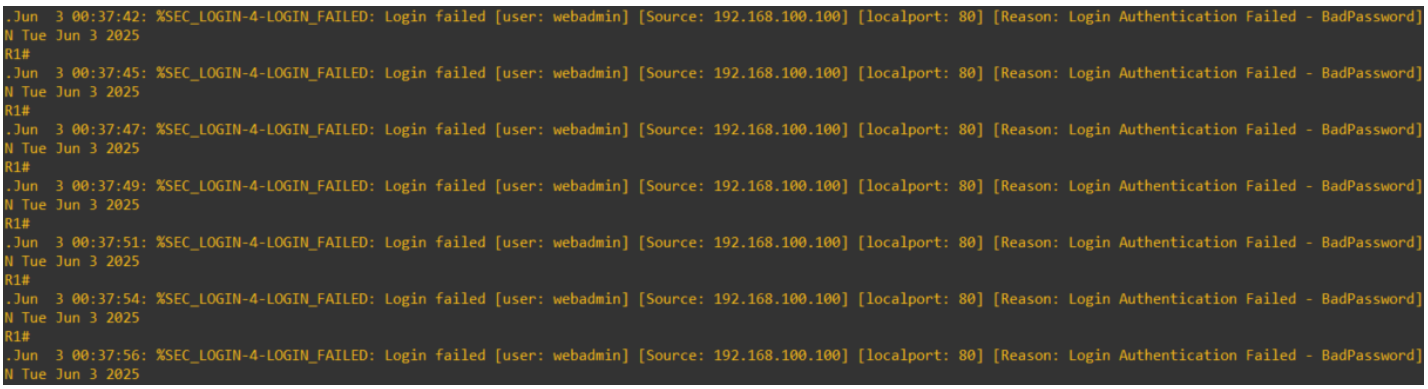
Para realizar o ataque de força vamos utilizar a ferramenta hydra presente na máquina virtual do Kali Linux. Tentei fazer o ataque de força bruta por acesso ssh, no entanto deu erro por incompatibilidade dos algoritmos ssh. Pois, o router utilizado na topologia apresenta algoritmos ssh mais antigos. Para mostrar o alerta fiz o ataque por acesso http ao http server do router.

Para realizar o ataque criei um ficheiro user.txt, onde coloquei o username do webadmin criado no router e outro ficheiro passwords.txt onde tenho uma lista de passwords que o atacante vai utilizar para tentar fazer o ataque por força bruta.



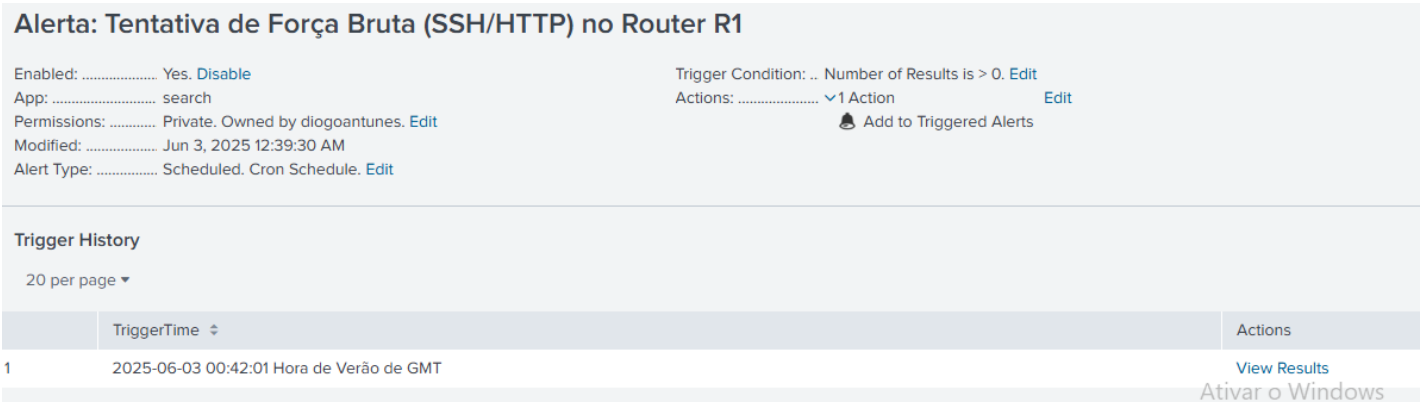






Como se pode verificar na imagem acima, estão a ser gerados logs de tentativas de autenticação falhas, causadas pelo ataque vindo da máquina do Kali Linux (ip 192.168.100.100).

Após 5 minutos foi gerado um tigger alert, como se pode verificar na imagem abaixo.



Após clicar em visualizar resultados, pode-se ver 12 tentativas de autenticação sem sucesso, vindas da máquina com o endereço ip 192.168.100.100 em uma tentativa de acesso http, como demonstrado no ataque.

Capítulo 5

Bibliografia

https://www.devmedia.com.br/splunk-monitorando-o-ambiente-de-ti-parte-1-revista-infra-magazine-10/27418
https://www.youtube.com/watch?v=IfHgKvDUWoQ&list=PL8vOoYAs_ySxS_b0mFeSbPe8q-VDyX55w&index=5
https://docs.uipath.com/automation-suite/automation-suite/2022.4/installation-guide/setting-up-splunk
https://brainwork.com.br/2016/05/13/usando-o-splunk-como-syslog-server/