**Splunk**: é uma plataforma de software que permite a coleta, indexação, pesquisa, análise e visualização de dados de máquina em grande escala. É amplamente utilizado para análise de segurança, monitoramento de TI, análise de negócios e outras aplicações que exigem o processamento e análise de dados em tempo real.

**Introdução ao Comando Top**

Agora, também podemos criar e usar o comando top. Isso realmente criará uma tabela em ordem decrescente. Quero ver quais são os principais eventos de requisição com base no endereço IP de origem. Posso simplesmente definir um limite, talvez 20, e então o endereço IP de origem. Isso mostrará o endereço IP que tem o maior número de contagens nas horas decrescentes.

Você pode ver que há 66 contagens. Viu isso? E depois temos 64. Isso é ainda mais útil, como mencionei, no caso de um ataque de força bruta, ajudando a identificar qualquer ataque de força bruta ou qualquer tipo de movimento lateral. Portanto, a tabela e o comando top são muito, muito poderosos.

**Utilizando o Comando D Dub**

Podemos também utilizar o comando d dub. Por exemplo, se você tiver o endereço IP de origem e DST\_ip, isso mostrará a saída. Mas você pode remover qualquer duplicata, caso exista alguma entrada duplicada. Você também pode usar novamente o comando transform.

Você pode dizer d sorry\_ub e, em seguida, pode novamente especificar com base no endereço IP de origem e no destino. Assim, você dirá que deseja uma combinação única de endereço IP de origem e endereço IP de destino. Se isso existir, você verá uma redução no número. Caso contrário, verá os mesmos números exatos. Essa é a maneira de visualizar os eventos únicos.

**Construindo um Dashboard**

Agora, vamos aprender a construir um dashboard. Como você pode ver, este é o nosso resultado para os logs DSCP. Agora, seu gerente pediu para você construir um dashboard para que você ou sua equipe não precisem executar a mesma consulta repetidamente.

O que você pode fazer é, com base nos resultados que vê agora, considerar alguns endereços IP de origem. Vamos usar isso como o endereço IP de origem. Adicionei o endereço IP de origem na consulta de busca. Agora quero salvar isso para que, na próxima vez, não precise executar a mesma consulta ou lembrar dela.

**Salvando o Dashboard**

Posso clicar em “Salvar como” e, em seguida, ir para “Novo Dashboard”. Clicarei nele e isso me pedirá para inserir o nome do dashboard. Direi “DSCP” e talvez adicione o endereço IP de origem, então direi “host externo” e talvez o nome do host.

Tenho duas opções: posso optar pela opção de construtor, onde posso visualizar, pois há muitos painéis e personalizações, ou posso optar pelo dashboard clássico. Posso clicar no dashboard clássico. Também tenho a opção de privado ou compartilhado no aplicativo. Posso selecionar o privado para que ele fique visível apenas para mim. Se eu selecionar o compartilhado no aplicativo, nesse caso, ele será compartilhado entre diferentes aplicativos.

**Acessando o Dashboard**

Portanto, selecionarei o privado para mantê-lo assim e, em seguida, posso clicar em “Salvar Dashboard”. Uma vez feito isso, posso clicar em “Ver Dashboard” e isso me levará ao dashboard aqui.

Na próxima vez que você quiser acessar ou ver os mesmos resultados, não precisará executar a consulta novamente. Você pode simplesmente ir à seção de dashboards e, aqui, encontrará “DSCP host externo”. Assim que fizer isso, poderá ver os resultados dessa forma.

**Opções Adicionais no Dashboard**

Uma vez que você clique nisso, poderá ver as permissões de edição. Você também pode definir isso como o dashboard inicial, caso seja realmente importante para você.

No dashboard, você tem mais algumas opções. Você pode clonar o mesmo dashboard, agendar a entrega em PDF, editar as permissões, mudar o título e tudo mais, além de adicionar diferentes painéis. Você pode adicionar diferentes painéis com base em diferentes dados que você tem.

Você tem a opção de editar, pois não temos dados complexos com múltiplos campos, então não veremos muitas informações. Mas você pode adicionar e personalizar clicando na seção de adicionar painel, onde há diferentes opções, como novos relatórios, novos a partir de relatórios, clonar do dashboard ou construir um novo estilo de painel.

Talvez seja um painel baseado em eventos estatísticos, gráfico ou baseado em PI. Você só precisa selecionar, inserir algumas informações e isso mostrará o resultado. No nosso caso, é um dado simples. Não veremos muitas informações aqui, mas espero que você tenha entendido a ideia.