

## Laboratório - Isolar host comprometido usando 5 tuplas

### Objetivos

Neste laboratório, você analisará os logs que foram coletados durante a exploração de uma vulnerabilidade documentada para determinar os hosts e arquivos comprometidos.

**Parte 1: Revisar alertas em Sguil**

**Parte 2: Pivô para Wireshark**

**Parte 3: Pivô para Kibana**

### Histórico/Cenário

A tupla de 5 é usada por administradores de TI para identificar requisitos para criar um ambiente de rede operacional e seguro. Os componentes da tupla 5 incluem um endereço IP de origem e número de porta, endereço IP de destino e número de porta, e o protocolo em uso na carga de dados. Este é o campo de protocolo do cabeçalho do pacote IP.

Neste laboratório, você também analisará os logs para identificar os hosts comprometidos e o conteúdo do arquivo comprometido.

### Recursos necessários

- Máquina virtual Security Onion

### Instruções

Após o ataque, os usuários não têm mais acesso ao arquivo chamado **confidential.txt**. Agora você analisará os logs para determinar como o arquivo foi comprometido.

**Observação:** Se esta era uma rede de produção, recomenda-se que **analysts** e usuários root alterem suas senhas e estejam em conformidade com a política de segurança atual.

### Parte 1: Avaliação Alertas em Sguil

- Inicie a VM Security Onion e faça login. Faça login com o **analyst** de usuário e **cyberops** de senha
- Abra o **Sguil** e faça login. Clique em **Select All** para selecionar as interfaces e, em seguida, **Start SGUIL**.
- Revise os eventos listados na coluna Event Message . Uma dessas mensagens é **GPL ATTACK\_RESPONSE id check returned root**. Esta mensagem indica que o acesso root pode ter sido obtido durante um ataque. O host em 209.165.200.235 retornou acesso root para 209.165.201.17. O ID de alerta **5.1** é usado como exemplo neste laboratório.

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Δ	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20		209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root
RT	351	seconion-ossec	1.1	2020-06-19 18:09:28		0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.
RT	23	seconion-ossec	1.2	2020-06-19 18:09:29		0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.

## Laboratório - Isolar host comprometido usando 5 tuplas

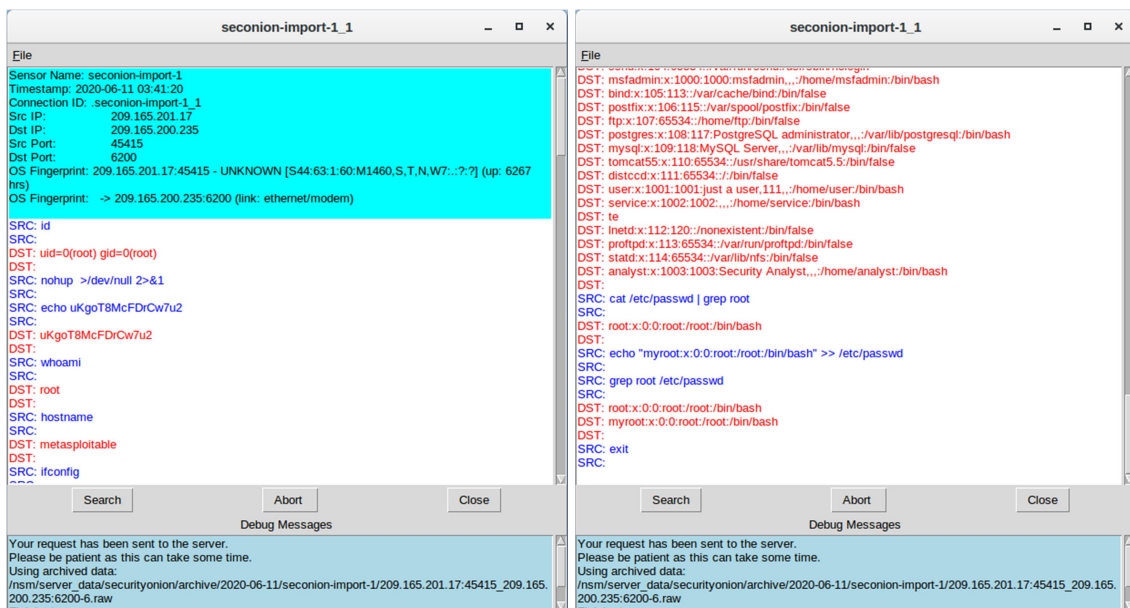
- d. Marque as caixas de seleção **Show Packet Data** e **Mostrar Regra** para exibir cada alerta com mais detalhes.



- e. Clique com o botão direito no ID de alerta 5.1 e selecione **Transcrip**.

RealTime Events		Escalated Events						
ST	CNT	Sensor	Alert ID	Date/Time	Δ	Src IP	SPort	Dst IP
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20		209.165.200.235	6200	209.165.201.17
RT	351	seconion-ossec	Event History	09:28	0.0.0.0			0.0.0.0
RT	23	seconion-ossec	Transcript	09:29	0.0.0.0			0.0.0.0
RT	7	seconion-ossec	Transcript (force new)	10:04	0.0.0.0			0.0.0.0
RT	7	seconion-ossec	Wireshark	10:04	0.0.0.0			0.0.0.0

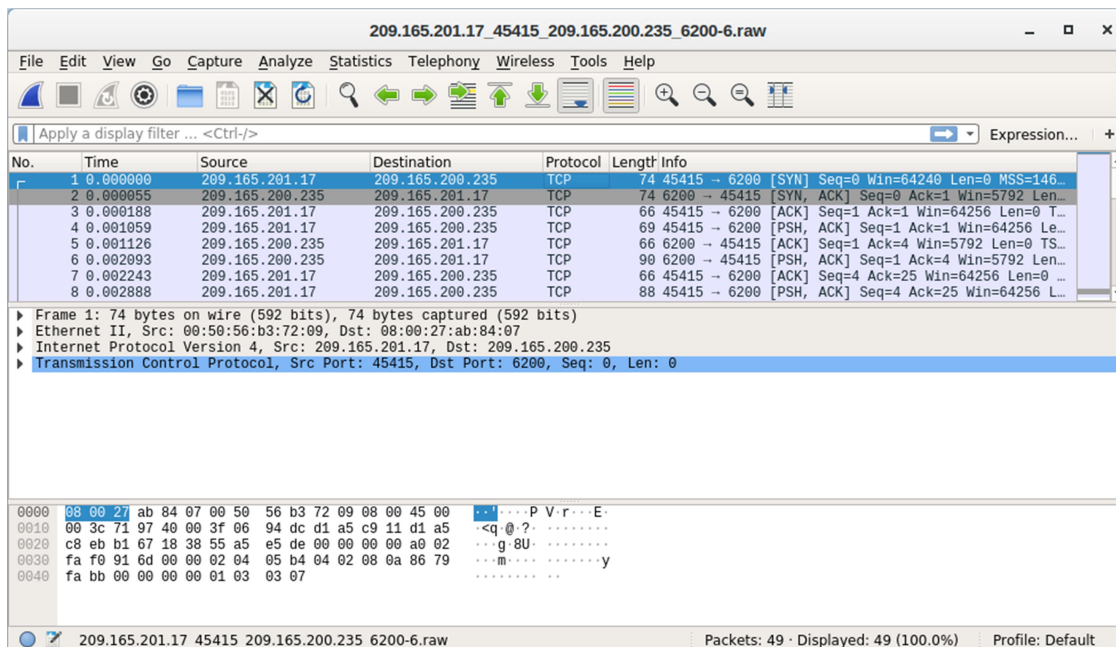
- f. Revise as transcrições para o alerta. A transcrição exibe as transações entre a origem do agente de ameaça (SRC) e o destino (DST) durante o ataque. O ator de ameaça está executando comandos do Linux no destino.



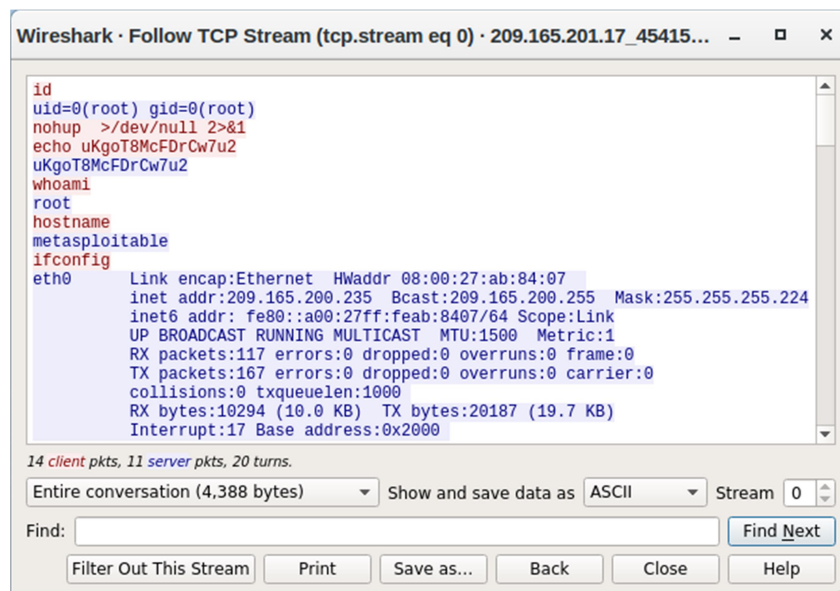
Que tipo de transações ocorreram entre o cliente e o servidor neste ataque?

## Parte 2: Pivô para Wireshark

- a. Selecione o alerta que forneceu a transcrição da etapa anterior. Clique com o botão direito do mouse no ID de alerta 5.1 e selecione **Wireshark**. A janela principal do Wireshark exibe três visualizações de um pacote.



- b. Para exibir todos os pacotes montados em uma conversa TCP, clique com o botão direito do mouse em qualquer pacote e selecione **Follow > TCP Stream**.



O que você observou? O que as cores de texto vermelho e azul indicam?

## Laboratório - Isolar host comprometido usando 5 tuplas

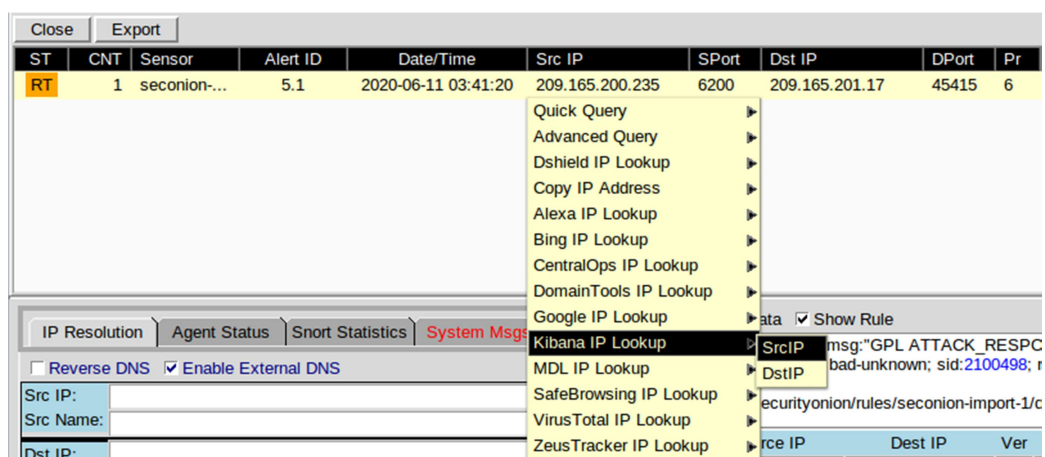
O atacante emite o comando **whoami** no alvo. O que isso mostra sobre a função de invasor no computador de destino?

Percorra o fluxo TCP. Que tipo de dados o ator da ameaça tem lido?

- c. Saia da janela de fluxo TCP. Feche o **Wireshark** quando terminar de analisar as informações fornecidas.

### Parte 3: Pivô para Kibana

- a. Volte para Sguil. Clique com o botão direito do mouse no IP de origem ou de destino do ID de alerta 5.1 e selecione **Kibana IP Lookup > SrcIP**. Digite o nome de usuário **analyst** e a senha **cyberops**, se solicitado por Kibana.

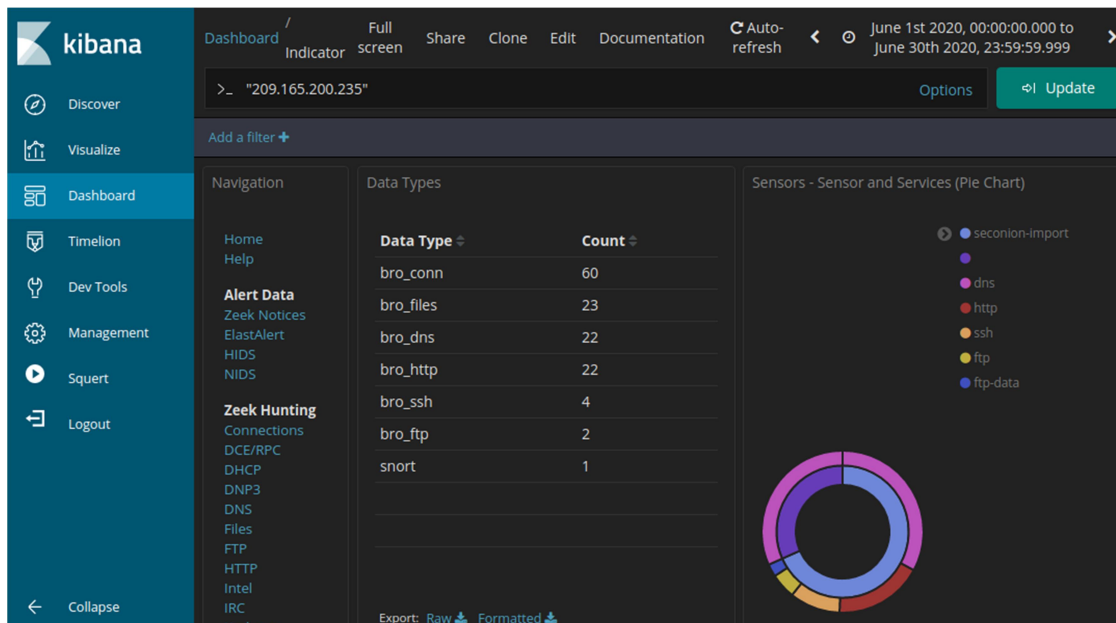


**Observação:** Se você recebeu a mensagem "Your connection is not private", clique em **ADVANCED > Proceed to localhost (unsafe)** para continuar.

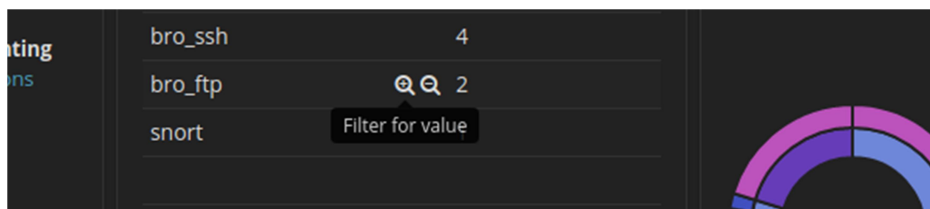
- b. Se o intervalo de tempo for as últimas 24 horas, altere-o para junho de 2020 para que 11 de junho seja incluído no intervalo de tempo. Use a guia **Absolute** para alterar o intervalo de tempo.

## Laboratório - Isolar host comprometido usando 5 tuplas

- c. Nos resultados exibidos, há uma lista de diferentes tipos de dados. Você foi informado de que o arquivo **confidential.txt** não está mais acessível. Nos Sensores - Sensores e Serviços (Gráfico de Pizza), ftp e ftp-data estão presentes na lista, como mostrado na figura. Vamos determinar se o FTP foi usado para roubar o arquivo.



- d. Vamos filtrar para **bro\_ftp**. Passe o mouse sobre o espaço vazio ao lado da contagem de tipos de dados **bro\_ftp**. Selecione **+** para filtrar apenas o tráfego relacionado ao FTP, conforme mostrado na figura.



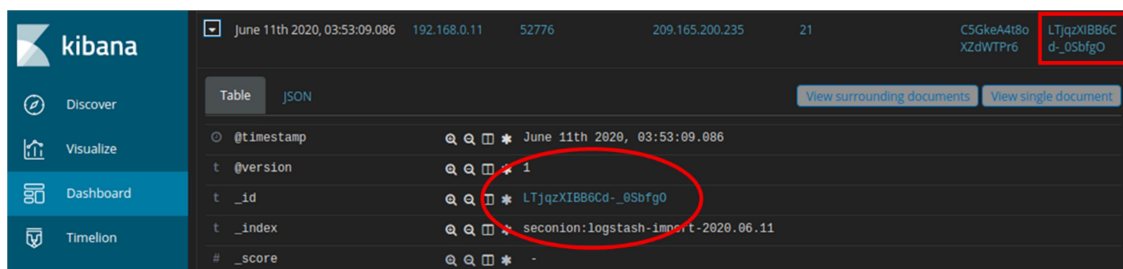
- e. Role para baixo até a seção **All Logs** Há duas entradas listadas.

Quais são os endereços IP de origem e destino e os números das portas para o tráfego FTP?

- f. Expanda e examine ambas as entradas de log. Em uma dessas entradas, o **ftp\_argument** tem uma entrada de **ftp://209.165.200.235/./confidential.txt**. Revise também a mensagem na entrada de log para saber mais sobre esse evento.

## Laboratório - Isolar host comprometido usando 5 tuplas

- g. Dentro da mesma entrada de log, role para cima até o campo `_id` de alerta e clique no link.



- h. Revise a transcrição para as transações entre o invasor e o destino. Se desejar, você pode baixar o pcap e revisar o tráfego usando o Wireshark.

Quais são as credenciais do usuário para acessar o site FTP?

- i. Agora que você verificou que o invasor usou FTP para copiar o conteúdo do arquivo confidential.txt e, em seguida, excluí-lo do destino. Então, qual é o conteúdo do arquivo? Lembre-se de que um dos serviços listados no gráfico de pizza é ftp\_data.
- j. Navegue até a parte superior do painel. Selecione **Files** sob o título Zeek Hunting no painel esquerdo, conforme mostrado na figura. Isso permitirá que você revise os tipos de arquivos que foram registrados.

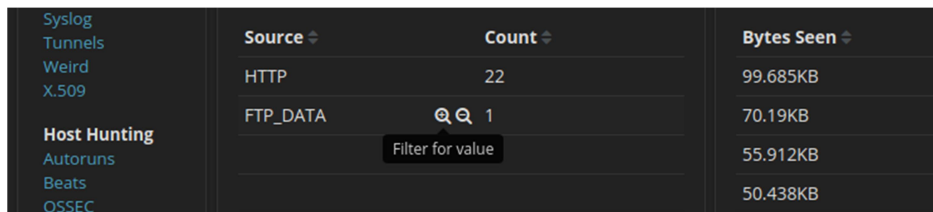


Quais são os diferentes tipos de arquivos? Veja a seção Tipo MIME da tela.

Role até o cabeçalho **Files - Source**. Quais são as fontes de arquivo listadas?

## Laboratório - Isolar host comprometido usando 5 tuplas

- k. Filtre para **FTP\_DATA** passando o mouse sobre o espaço vazio ao lado do Count for FTP\_DATA e clique em **+**.



Source	Count	Bytes Seen
HTTP	22	99.685KB
FTP_DATA	1	70.19KB
		55.912KB
		50.438KB

- l. Role para baixo para revisar os resultados filtrados.

Qual é o tipo MIME, endereço IP de origem e destino associado à transferência dos dados de FTP? Quando essa transferência ocorreu?

- m. Nos logs de arquivo, expanda a entrada associada aos dados de FTP. Clique no link associado ao alerta **\_id**.

Qual é o conteúdo de texto do arquivo que foi transferido usando FTP?

Com todas as informações recolhidas até agora, qual é a sua recomendação para impedir mais acesso não autorizado?