Laboratório - Extraia um executável de um PCAP

Objetivos

Parte 1: Analisar logs pré-capturados e capturas de tráfego

Parte 2: Extrair arquivos baixados do PCAP

Histórico/Cenário

Olhar para registros é muito importante, mas também é importante entender como as transações de rede acontecem no nível do pacote.

Neste laboratório, você analisará o tráfego em um arquivo pcap capturado anteriormente e extrairá um executável do arquivo.

Recursos necessários

- Máquina virtual CyberOps Workstation

Instruções

Parte 1: Analisar registros pré-capturados e capturas de tráfego

Na Parte 2, você trabalhará com o arquivo **nimda.download.pcap**. Capturado em um laboratório anterior, o **nimda.download.pcap** contém os pacotes relacionados ao download do malware Nimda. Sua versão do arquivo, se você a criou no laboratório anterior e não reimportou sua VM CyberOps Workstation, será armazenada no diretório /home/analyst. No entanto, uma cópia desse arquivo também é armazenada na **VM do CyberOps Workstation**, no diretório **/home/analyst/lab.support.files/pcaps**, para que você possa concluir este laboratório. Para consistência da saída, o laboratório usará a versão armazenada no diretório **pcaps**.

Enquanto o **tcpdump** pode ser usado para analisar arquivos capturados, a interface gráfica **do Wireshark** torna a tarefa muito mais fácil. Também é importante notar que **tcpdump** e **Wireshark** compartilham o mesmo formato de arquivo para capturas de pacotes; portanto, arquivos PCAP criados por uma ferramenta podem ser abertos pela outra.

a. Altere o diretório para a pasta **lab.support.files/pcaps** e obtenha uma listagem de arquivos usando o comando **ls —l**.

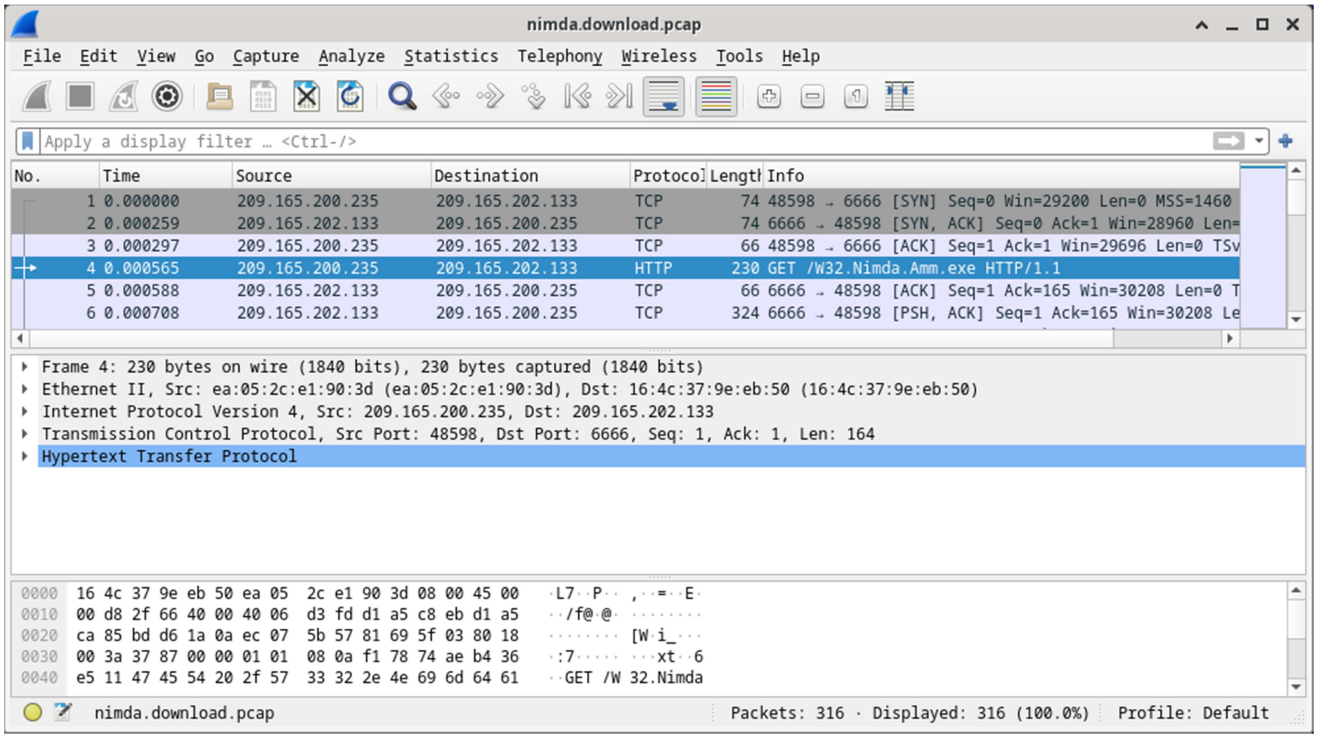
```
[analyst@secOps ~] $ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 7460
-rw-r—r— 1 analyst 3510551 ago 7 15:25 lab_prep.pcap
-rw-r—r— 1 analyst 371462 jun 22 10:47 nimda.download.pcap
-rw-r—r— 1 analyst 3750153 25 de maio 11:10 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$
```

b. Execute o comando abaixo para abrir o arquivo **nimda.download.pcap** no Wireshark.

```
[analyst@secOps pcaps] $ wireshark nimda.download.pcap &
```

© 2017 - aa Cisco e/ou suas afiliadas. Todos os direitos reservados. Página Pública da Cisco

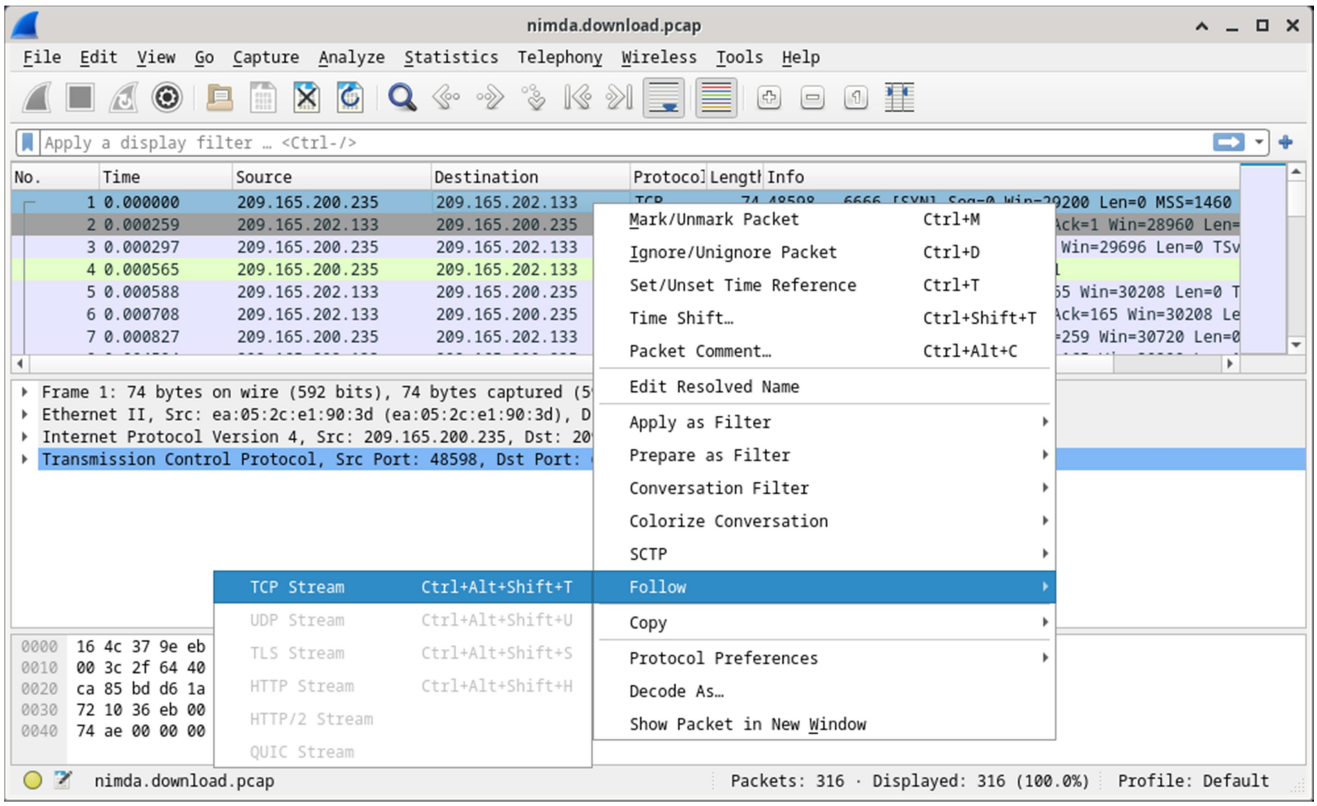
c. O arquivo **nimda.download.pcap** contém a captura de pacote relacionada ao download de malware realizado em um laboratório anterior. O **pcap** contém todos os pacotes enviados e recebidos enquanto o **tcpdump** estava em execução. Selecione o quarto pacote na captura e expanda o Hypertext Transfer Protocol para exibir como mostrado abaixo.



d. Os pacotes de um a três são o handshake TCP. O quarto pacote mostra a solicitação para o arquivo de malware. Confirmando o que já era conhecido, a solicitação foi feita por HTTP, enviada como uma solicitação GET.

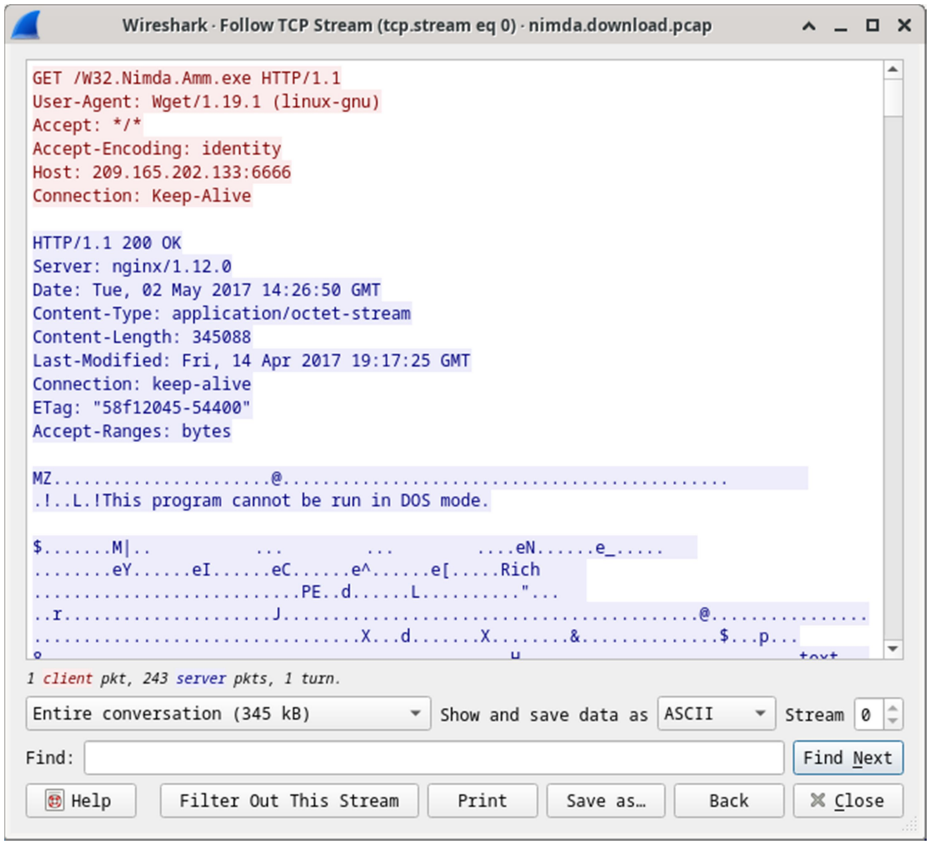
© 2017 - aa Cisco e/ou suas afiliadas. Todos os direitos reservados. Página Pública da Cisco

e. Como HTTP é executado sobre TCP, é possível usar o recurso **Seguir TCP Stream**do **Wireshark** para reconstruir a transação TCP. Selecione o primeiro pacote TCP na captura, um pacote SYN. Clique com o botão direito do mouse e escolha **Seguir** > **TCP Stream**



© 2017 - aa Cisco e/ou suas afiliadas. Todos os direitos reservados. Página Pública da Cisco

f. Wireshark exibe outra janela contendo os detalhes de todo o fluxo TCP selecionado.



Quais são todos esses símbolos mostrados na janela **Seguir TCP Stream** ? Eles são ruído de conexão? Dados? Explique.

Existem algumas palavras legíveis espalhadas entre os símbolos. Por que estão lá?

Pergunta do desafio: Apesar do **nome W32.Nimda.amm.exe, este executável não é o famoso worm. Por razões de segurança, este é outro arquivo executável que foi renomeado como W32.Nimda.amm.exe. Usando os fragmentos de palavras exibidos pela** janela Seguir TCP Streamdo Wireshark, você pode dizer qual executável isso realmente é?

g. Clique em **Fechar** na janela Seguir fluxo TCP para retornar ao arquivo Wireshark nimda.download.pcap.

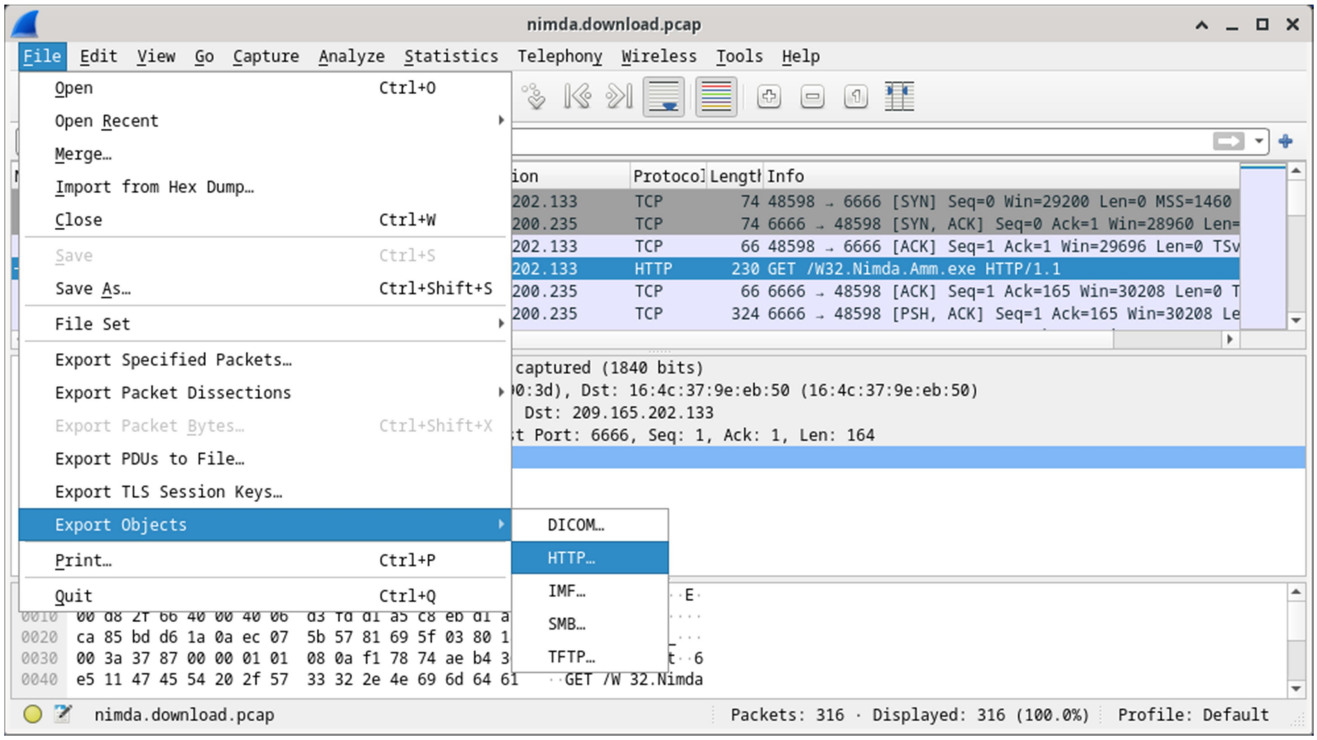
© 2017 - aa Cisco e/ou suas afiliadas. Todos os direitos reservados. Página Pública da Cisco

Parte 2: Extrair arquivos baixados do PCAP

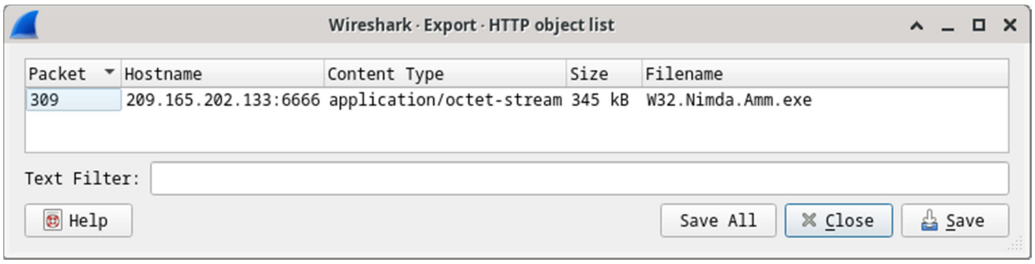
Como os arquivos de captura contêm todos os pacotes relacionados ao tráfego, um PCAP de um download pode ser usado para recuperar um arquivo baixado anteriormente. Siga as etapas abaixo para usar o **Wireshark** para recuperar o malware Nimda.

a. Nesse quarto pacote no arquivo **nimda.download.pcap**, observe que a solicitação **HTTP GET** foi gerada de **209.165.200.235** para **209.165.202.133**. A coluna Informações também mostra que isso é, de fato, a solicitação GET para o arquivo.

b. Com o pacote de solicitação GET selecionado, navegue até **Arquivo > Exportar objetos > HTTP**, no menu do **Wireshark**.



c. Wireshark exibirá todos os objetos HTTP presentes no fluxo TCP que contém a solicitação GET. Nesse caso, somente o arquivo **W32.Nimda.amm.exe** está presente na captura. Levará alguns segundos até que o arquivo seja exibido.



Por que **W32.Nimda.amm.exe** é o único arquivo na captura?

© 2017 - aa Cisco e/ou suas afiliadas. Todos os direitos reservados. Página Pública da Cisco

d. Na janela de **lista de objetos HTTP**, selecione o arquivo **W32.Nimda.amm.exe** e clique em **Salvar como** na parte inferior da tela.

e. Clique na seta para a esquerda até ver o botão **Início**. Clique em Início e, em seguida, clique na pasta **analyst** (não na guia analista). Salve o arquivo lá.

f. Retorne à janela do terminal e verifique se o arquivo foi salvo. Altere o diretório para a pasta **/home/analyst** e liste os arquivos na pasta usando o comando **ls -l**.

```
[analyst@secOps pcaps] $ cd /home/analista
[analyst@secOps ~]$ ls –l
total 364
drwxr-xr-x 2 analyst analyst 4096 Sep 26 2014 Desktop
drwx– 3 analyst analyst 4096 May 25 11:16 Downloads
drwxr-xr-x 2 analyst analyst 4096 Maio 22 08:39 extra
drwxr-xr-x 8 analyst analyst 4096 jun 22 11:38 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 3 15:56 second_drive
-rw-r–r– 1 analyst 345088 jun 22 15:12 W32.Nimda.amm.exe
[analyst@secOps ~] $
```

O arquivo foi salvo?

g. O comando **file** fornece informações sobre o tipo de arquivo. Use o comando file para aprender um pouco mais sobre o malware, como mostra abaixo:

```
[analyst@secOps ~] $ arquivo w32.nimda.amm.exe
W32.Nimda.amm.exe: PE32+ executável (console) x86-64, para MS Windows
[analyst@secOps ~] $
```

Como visto acima, **W32.Nimda.amm.exe** é de fato um arquivo executável do Windows.

No processo de análise de malware, qual seria o próximo passo provável para um analista de segurança?

© 2017 - aa Cisco e/ou suas afiliadas. Todos os direitos reservados. Página Pública da Cisco