Lab 7 : Análise Forense em Rede de Computadores

Introdução

A análise do tráfego de rede é uma ferramenta poderosa não só para o aprendizado de redes, protocolos, camadas e resolução de problemas, mas também para investigação quando se deseja conhecer os elementos envolvidos ou detectar e examinar ataques a computadores e redes, visto que ele contém tudo que seu computador está realmente comunicando através da rede.

Neste laboratório vocês irão exercitar um processo inverso do que já realizado em outras oportunidades com a ferramenta de análise de pacotes Wireshark. Ao invés de capturar o tráfego em uma rede já conhecida, vocês iniciarão a partir de um conjunto de capturas de tráfego específico para poder chegar na rede correspondente e reconstruir o cenário.

Atividade: Dissecando as Evidências

A Figura 1 mostra a topologia da rede utilizada para a atividade deste laboratório, entretanto os sistemas finais e os equipamentos da rede não estão identificados nos blocos da figura.

Sua tarefa é analisar os arquivos de captura (*.pcap) fornecidos que contêm o tráfego em cada enlace da rede, e identificar os equipamentos, as funções/serviços que eles realizam e sua localização na topologia, a partir da análise dos pacotes e protocolos. Por exemplo, o arquivo 1-2.pcap contém o tráfego no enlace entre as interfaces 1 e 2 indicadas na figura, e assim por diante.

No relatório inclua:

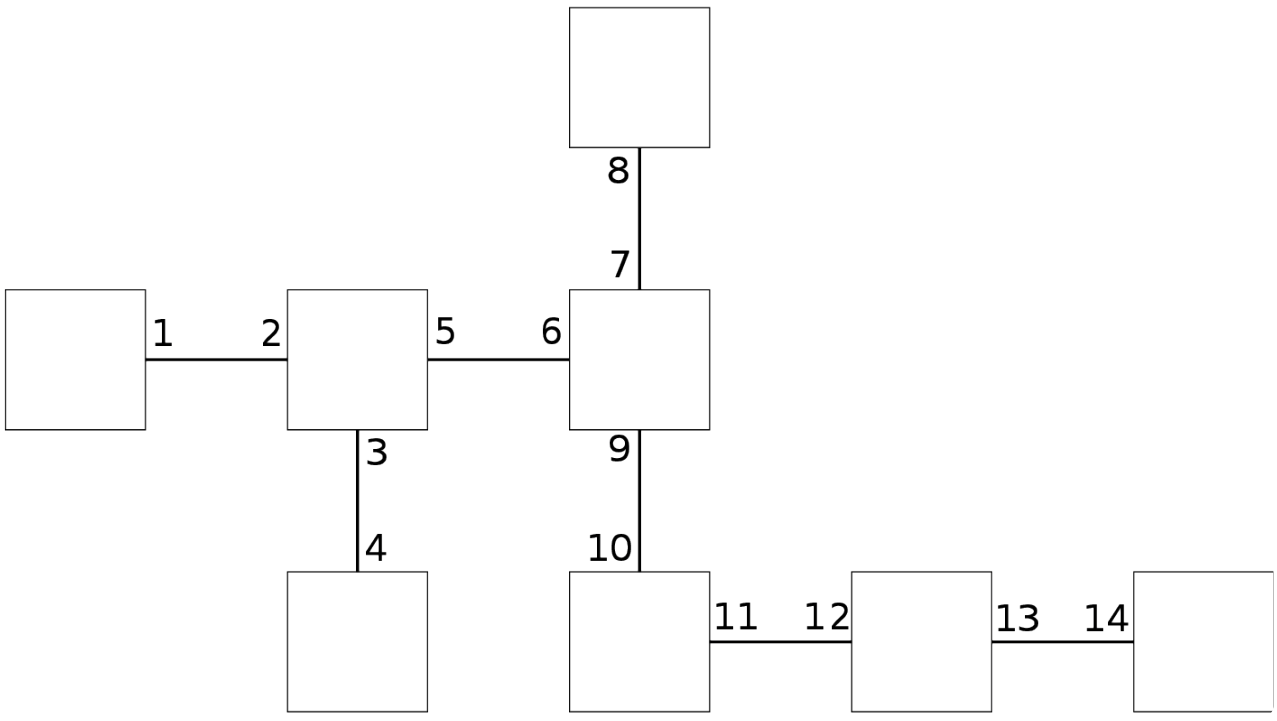
• uma versão da Figura 1 identificando os equipamentos, sistemas finais e serviços ou aplicações, assim como os endereços das camadas 2 e 3 de todas as interfaces;

• um texto objetivo descrevendo o seu processo de análise e os acontecimentos observados a partir das capturas;

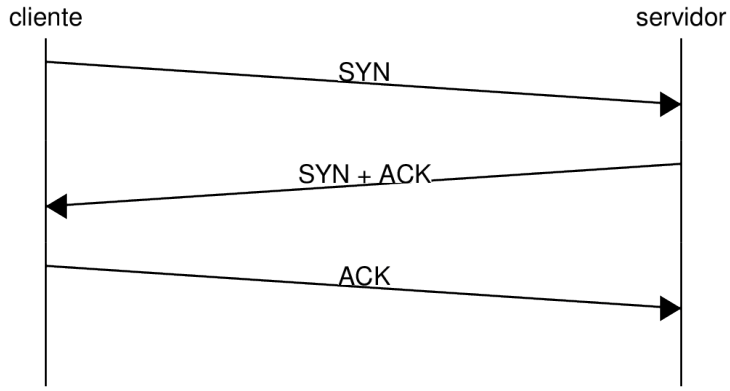
• um diagrama de sequência de tempo (vide exemplos na Figura 2) com os protocolos e mensagens trocadas entre os nós identificados na rede, por exemplo: sistemas finais, roteadores, servidores de aplicação, servidor de resolução de nomes (DNS).
Obs.: Eventuais equipamentos de camada 2 identificados na topologia podem ser omitidos da representação no diagrama de sequência.

Dica: o Wireshark geralmente apresenta os pacotes com tempo relativo ao início da captura, então para ter uma visão melhor da ordem dos acontecimentos, sugerimos mudar o formato de exibição de tempo para a hora do dia (menu View > Time Display Format > Time of Day, ou atalho Ctrl+Alt+2)

Figura 1:



A Figura 2 mostra um simples exemplo do estilo de diagrama que deve ser feito, neste exemplo é mostrado o estabelecimento de uma conexão TCP (3-way handshake).



(Opcional) Atividade Extra: Reconstrução da Cena

Construa o ambiente identificado usando o Mininet. Observe que além da definição da topologia, a atividade exige configuração das interfaces, serviços e protocolos de rede. Para fins de verificação, compare as capturas de pacotes e acontecimentos no seu ambiente.