EA080 - O — Análise Forense em Redes de Computadores

Professor: Christian Esteve Rothenberg

Leonardo Rodrigues Marques `RA: 178610`

1 Processo de Reconhecimento dos Componentes da Rede.

Para resolver essa questão, adotamos a seguinte técnica. Em primeiro lugar, abrimos todos os arquivos e verificamos os tipos de mensagens trocadas entre as interfaces. As interfaces que mais nos chamaram atenção foi **9-10** devido a presença de mensagens BGP. Isso mostrou que haviam duas sub-redes na topologia e que, dois roteadores estavam ligados através dessas interfaces. Também foi possível obter os endereços MACs e IP deles, mas sem especificar qual na figura. Após isso, outras interfaces que nos chamaram a atenção foram **7-8**. Essas interfaces trocavam mensagens ARP e DNS,sendo a DNS típica de servidores DNS. Como as interfaces **7 e 9** estavam em apenas um componente e esse componente era um roteador, foi fácil decidir quem era o servidor DNS e os endereços respectivos das interfaces. O próximo passo foi concluir quais eram os componentes dos lado esquerdo e direito. Essa etapa foi um pouco demorada, já que a presença de switches deixou a interpretação das interfaces um pouco confusas. Mesmo assim, começamos pelo lado esquerdo, interfaces **1-2**. Haviam várias mensagens DHCP com endereços MACs e IPs diferentes, oque levou a constatar que ali haviam dois hosts. As interfaces **5-6** e **1-2** mostravam, além de DHCP e ARP, mensagens TCP, enquanto a interface **3-4** apenas broadcast de DHCP. Usando-se desse dado, foi fácil descobrir o IP de cada componente e associá-los com os endereços MACs obtidos nas mensagens DHCP anteriores. Consequentemente conseguimos os endereços da interface 6. Após isso, verificamos as mensagens TCP SYN, e elas partiam do componente mais a esquerda(host 1) e fluíam até o componente mais a direita. Isso, de fato, ajudou a resolver os endereços das interfaces **9-10**, anteriormente descobertos(roteadores), mas não especificados. Também ajudou a definir que o componente mais a direita era um host. De mão disso e de mensagens ARP entre as interfaces **11-12** e **13-14**, conseguimos resolver os endereços daqueles componentes. Enfim, conseguimos descobrir todos os componentes e resolver todos os endereços MAC e IP. De toda a topologia, a região mais difícil e confusa de ser interpretadão foi a parte esquerda, interfaces **1-2**, **3-4** e **5-6** devido a presença de switches e mensagens DHCP. Apesar dessa dificuldade, ela foi resolvida pelo fato de esses componentes apenas comutarem os pacotes entre a rede interna, sem alterar as propriedades(IP e MAC) das interfaces.