CURSO DE TECNOLOGIA EM DEFESA CIBERNÉTICA

Cap 16 - O protocolo TCP/IP sob ataque! - Quem é o culpado?

Kraków – Polônia

Abril/2021

Ian Alberto Ribeiro Christani

Cap 16 - O protocolo TCP/IP sob ataque! - Quem é o culpado?

Kraków – Polônia

Abril/2021

SUMÁRIO

1 INTRODUÇÃO

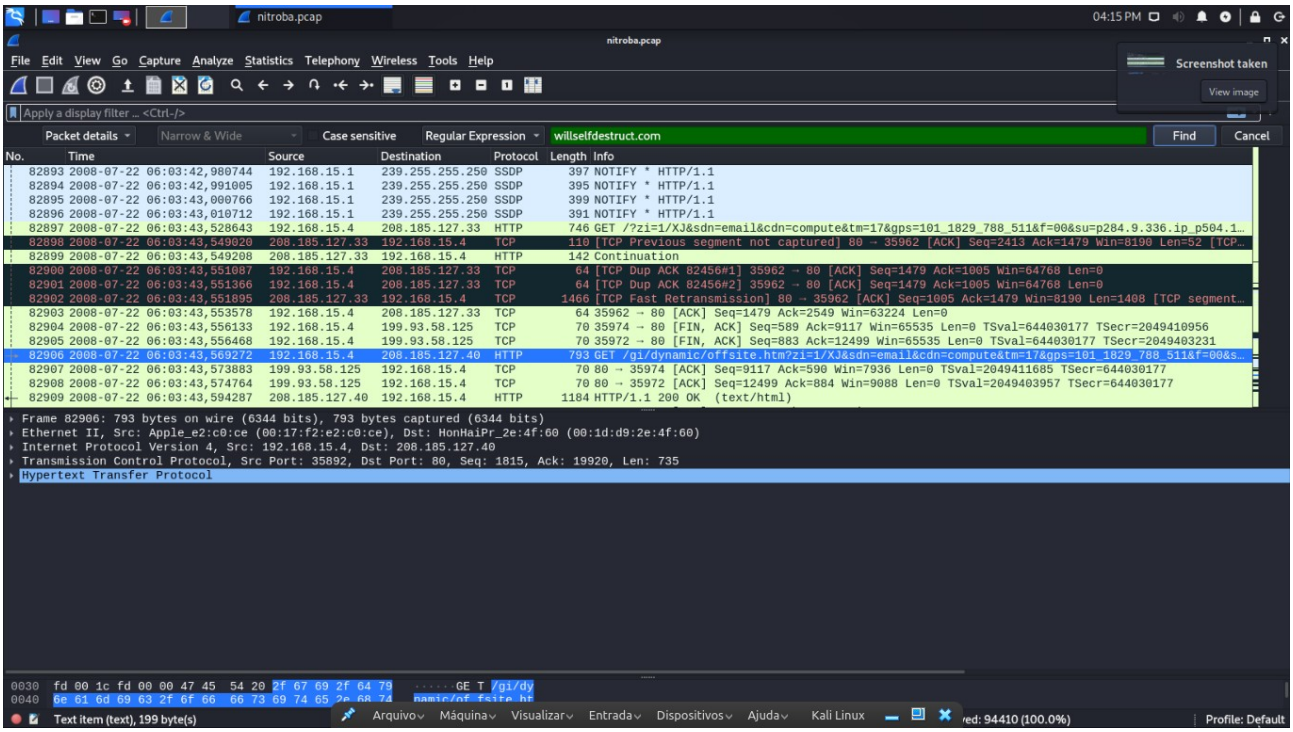
A proposta dessa atividade é familiarizar-se com a ferramenta Wireshark, usada também para analisar fluxo de pacotes em uma rede, bem como aplicar os conhecimentos sobre redes, pacotes, e procotolos recém adquiridos no curso. Para isso, temos um caso em que uma pessoa, enviou uma série de e-mails em anonimato praticando bullying com uma professora e tem-se como objetivo descobrir tal pessoa.

2 DESENVOLVIMENTO

Nesse momento temos as informações: endereço do site no qual foi enviado o e-mail para a professora (www.willselfdestruct.com), o e-mail da mesma (lilytuckrige@yahoo.com) e o IP do dormitório: 140.247.62.34. Vale ressaltar que o sniffer não conterá dados referentes ao primeiro e-mail enviado.

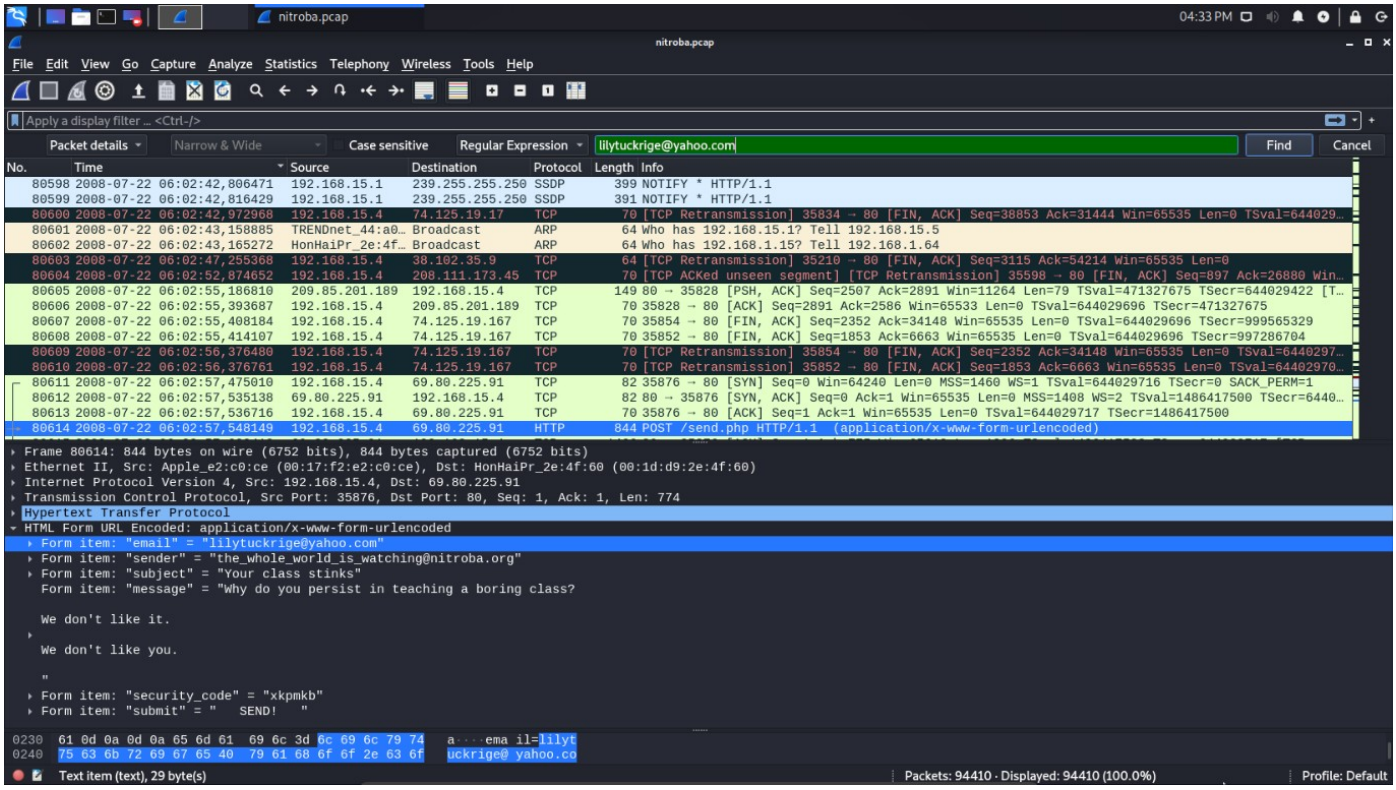
Vamos começar nossa investigação no tentando colher informações provenientes do site, pois ele esta diretamente relacionado com o evento. Já o IP do dormitório, como não há senha de proteção de acesso ao roteador, teremos diversos acessos e eventos não relevantes e devido à quantidade de informações não relacionadas, por uma questão de estratégica, deixaremos para explorar tal endereço de IP mais adiante, se necessário.

Filtrando os dados do arquivo .pcap usando **willselfdestruct.com** temos:

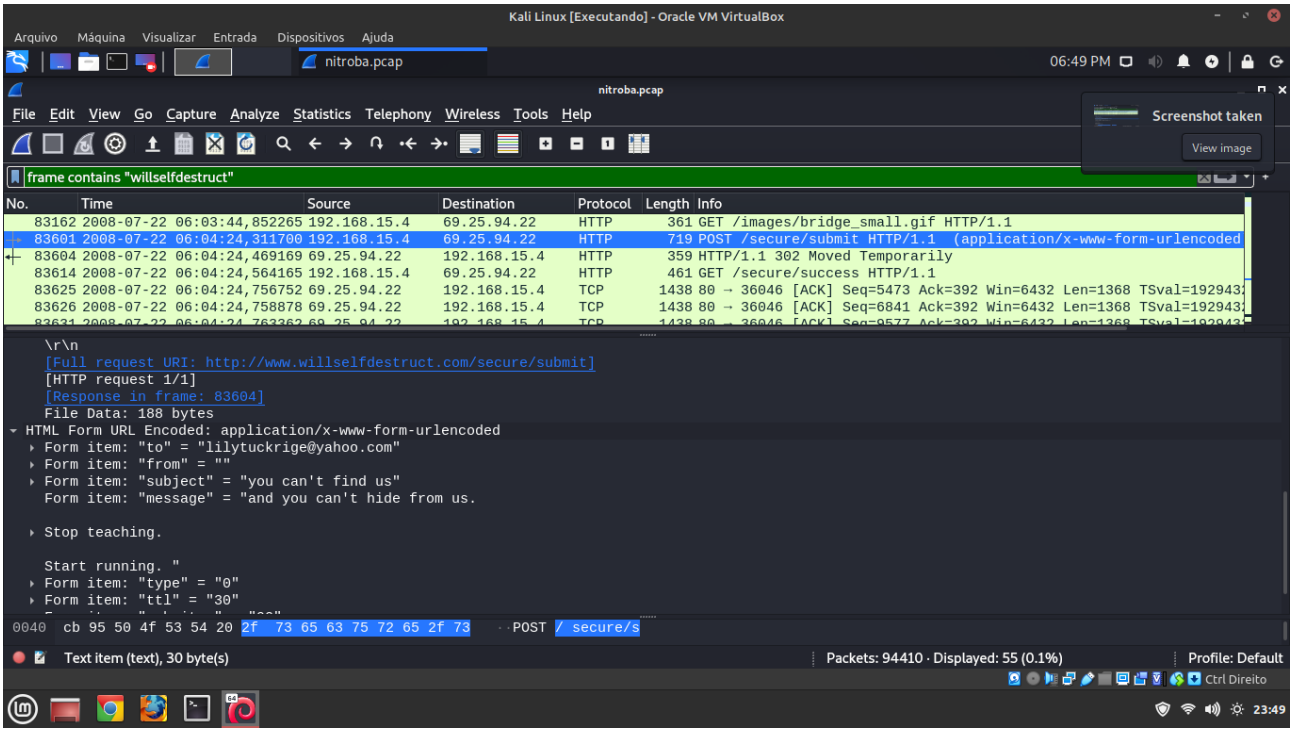


Podemos ver através de inúmeros pacotes analisados que o IP: 192.168.15.4 sendo o *source* é uma constante.

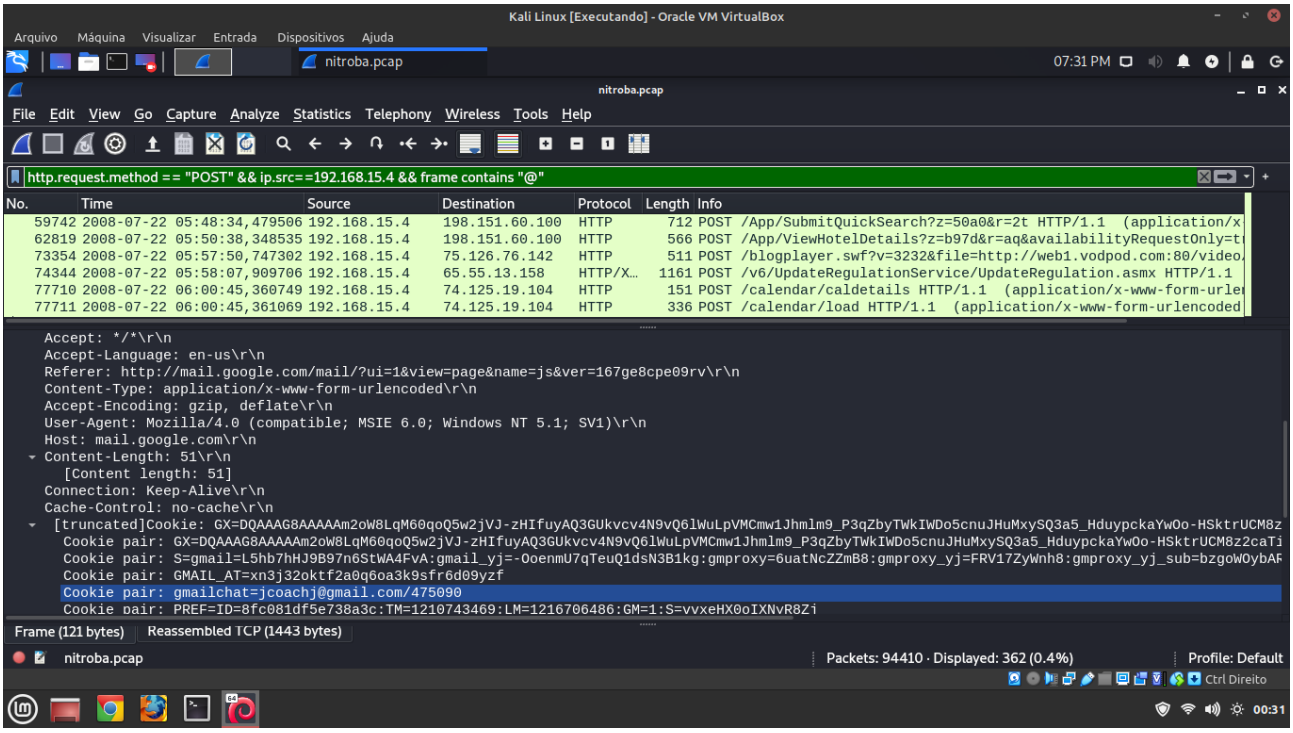
A prova que esse IP esta envolvido vem quando filtramos pelo e-mail da professora, pois tal IP aparece no pacote relacionado com a mensagem que a professora recebeu (n. 80614):



Temos aqui então um possível IP do atacante. A possibilidade de rastreamento do atacante usando o MAC address é descartada, porque o mesmo é do roteador e não do dispositivo do atacante. Aplicando o mesmo parâmetro de pesquisa no filtro de string, podemos comprovar que em ambos e-mails de *bullying* capturados o IP é o mesmo.



Na situação do bulling, tem-se um e-mail enviado, envio de informação via protocolo HTTP – no caso o texto do e-mail, podemos tentar pegar mais informações filtrando pelo método POST. A combinação dos filtros que usaremos (http.request.method == "POST" && ip.src==192.168.15.4 && frame contains "@"). Vale ressaltar aqui, que foi utilizado no lugar de apenas o @, o e-mail da professora, mas como não acrescentou nenhuma informação relevante, decidiu-se manter o foco em e-mail, mas de uma maneira mais genérica. Poderia ser usado o método GET, mas nesse caso estaríamos considerando as navegações em sites de uma maneira geral e tendo muito mais pacotes para serem analisados e não estaríamos considerando o envio do e-mail em si. Que fique bem claro que o uso do @ não está aqui pressupondo que o e-mail saiu da conta do atacante e sim considerando a estrutura de um endereço de e-mail, que irá ajudar a não pegar na pesquisa outros métodos POSTs usados e não relacionados. A idéia básica é restringir cada vez mais a cada informação relevante for encontrada.



Analisando TODOS os pacotes (já que a quantidade não é grande e boa parte deles são bem parecidos) que obedeceram o filtro, dentre eles, alguns chamam a atenção, os pacotes 83326 e 80842. Aparece apenas um e-mail envolvido: jcoach@gmail.com . Ele foi encontrado na parte de informações de cookie, que armazena informações do usuário no site, nas informações referentes à camada 7. É possível ver também que tal e-mail estava usando o chat do gmail (hangouts) entre outros serviços do Google e Facebook. Como não há nesse filtro algo que possa acrescentar mais alguém na lista, temos que ver se há possibilidade de encontrarmos alguém que possa ser o proprietário de tal e-mail. Caso não, devemos prosseguir usando outros artifícios, idéias e filtros.

Olhando a lista dos possíveis candidatos chegamos no **Johnny Coach - jcoach@gmail.com**. O embasamento para supor que foi ele é: um e-mail apenas que está ligado ao endereço de IP que enviou o e-mail à professora, esse endereço de IP enviou informações através (método POST).

Vale aqui ressaltar que tive problemas com relação ao registro de horários dos pacotes (veja os screenshots). Depois de diversas tentativas de reconfiguração na coluna TIME, não foi possível ajustar para que o horário ficasse compatível com o da

história contada no site, por isso não considerei tal dado para a análise, porém reconheço que é fundamental dado dessa natureza.

3 CONCLUSÃO

Podemos ver que a vivência com ferramentas específicas, no caso o Wireshark, além do conhecimentos de redes, pacotes, modelo OSI entre outros mais específicos, são essenciais para desempenhar a atividade de análise de fluxo de dados em uma rede.

REFERÊNCIAS

https://wiki.wireshark.org/DisplayFilters

https://www.wireshark.org/docs/wsug_html_chunked/ChWorkFindPacketSection.html

https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html