SNIFFERS DE REDES: APRENDENDO SOBRE O WIRESHARK E EXEMPLIFICANDO UM TIPO DE ATAQUE

Miriane Aparecida Batista
Tecnólogia em Análises e Desenvolvimento de Sistemas
Instituto Federal do Triangulo Mineiro Campus Paracatu

Resumo: Nesse trabalho será apresentados conceitos importantes sobre o que são sniffers de redes e como se torna mais fácil acompanhar o tráfico de sua rede utilizando essa ferramenta. Ao inserirmos nossos dados em um site, temos o hábito de verificar se o mesmo possui certificado de segurança? Usuários com pouco conhecimento em defesas são vitimas de ataques e acabam tendo suas informações confidenciais acessadas por pessoas maliciosas. A ferramenta Wireshark pode ser utilizada tanto para proteger a rede quanto para atacá-la, logo, mostraremos uma forma de ataque na qual se tem acesso a dados confidenciais da conta de um usuário da rede.

Palavras-Chave: Sniffers. Wireshark. Tráfego de dados.

Paracatu, 2016

1. Introdução

É reconhecido de fato que a tecnologia aumentou gradativamente a competitividade entre as empresas. Informações sendo enviadas com maior velocidade resultando em menor gasto de tempo, está diretamente ligado ao lucro empresarial. Porém, mesmo que tenha muitas vantagens, a tecnologia também tem suas vulnerabilidades podendo sofre vários tipos de ataques.

No Brasil o órgão responsável por tratar incidentes que ocorram em nosso país é o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), ele recebe todas as notificações de invasões e desenvolve táticas de segurança e tratamento de incidentes, mas ainda sim ataques acontecem diariamente. " Além do processo de tratamento aos incidentes, o CERT.br também atua conscientizando os usuários da Internet sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet ."(COUTO, Felipe; SANTOS, Alex; LOVATO, Agnaldo, 2012)[1].

Sniffers de Redes também definidos como 'analisador de pacotes', 'analisador de protocolos' ou 'analisador de redes', nada mais é que um software que tem como função interceptar e registrar os dados que estejam trafegando por uma rede. É uma ferramenta que pode ser utilizada por exemplo, por administradores de redes que queiram diagnosticar problemas em sua rede, como também pode ser usado por pessoas maliciosas para terem acesso a informações confidenciais, em outras palavras, com essa ferramenta pode-se "capturar o tráfego da rede interna, podem revelar senhas, esquemas de autenticação de serviços, além de dados processados e enviados por aplicações que necessitam de sigilo na transação". (CURVELO, 1999, p. 2)[2].

O funcionamento dos sniffers se baseiam em capturar todos os pacotes que estejam trafegando na rede e não apenas as pacotes que estejam destinados a ele.

[1] Retirado do artigo " Estudo Comparativo de Ferramentas Analisadoras de Pacotes em Rede Tpc/Ip ".
[2] Referente ao artigo " Sobre a Detecção Remota de Sniffers para Detectores de Intrusão em Redes TCP/IP ".

> Como estão em um mesmo meio físico compartilhado, é possível configurar esta interface para que capture todo os pacotes, independente para qual endereço o mesmo tenha sido destinado. Esta condição de funcionamento é definida como "modo promíscuo", e sob estas circunstancias as estações podem monitorar e capturar o tráfego de rede, mesmo que o endereço de destino não seja o seu. (ANTONIO, Rogerio, 2003, p. 25).

Umas das ferramentas mais utilizadas para analisar o tráfico da rede é o wireshark principalmente por ser um software livre.

> Possui uma interface gráfica bastante simples e intuitiva. A visualização dos pacotes capturados é baseada em um sistema de cores, no qual cada cor corresponde a um protocolo diferente, recurso que não foi encontrado nas outras ferramentas. Com a ferramenta Wireshark, a empresa evitará custos com a compra de licença, e poderá utilizar de funcionalidades como a decodificação de pacotes, a montagem de sessões TCP, diagrama de toda conexão TCP, entre outros. (COUTO, Felipe; SANTOS, Alex; LOVATO, Agnaldo, 2012, p. 53).

Será mostrado como podemos capturar pacotes na rede com informações confidenciais dos usuários utilizando essa ferramenta.

2. Alguns softwares

Como qualquer outro software, para os Sniffers também possui ferramentas gratuitas e pagas, abaixo será mostrado alguns exemplos:

2.1. Ntop

O Ntop é um programa de monitoramento e gerenciamento em sistemas UNIX/Linux e Win32, que monitora passivamente uma rede coletando dados sobre os protocolos e sobre os hosts da rede.

As informações são exibidas em gráficos de forma bem detalhada que facilita o entendimento dos dados coletados sobre os protocolos e hots. Os protocolos que são monitorados por ele são: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, TCP/UDP.

2.2. SniffPass

Como já explicito no próprio nome, esse software faz a captura de senhas básicas dos protocolos: POP3, IMAP4, SMTP, FTP e HTTP e as exibem na tela. Porém, está limitado ao uso HUB para conectar os computadores da rede, pois switches e roteadores não enviam as informações para todos os computadores (broadcast), logo, a máquina que estiver executando o SniftPass não conseguir ver as senhas dos usuários do demais computadores de sua rede caso estajam conectadas por um switcher.

2.3. NetworkMiner

Com essa ferramenta é possível detectar o sistema operacional, hostname (nome da maquina) e quais portas estão abertas em um computador da rede e também capturar pacotes que estejam trafegando. Na tela inicial do sistema, em cada uma das abas pode se obter diversas informações como: consumo da banda, downloads, senhas e etc. Esse é um exemplo em que as informações seriam usadas apenas para analisar a rede, porém, também pode ser usada para fins maliciosos.

2.4. Wireshark

Também conhecida como tubarão dos fios, é umas das ferramentas gratuitas mais utilizadas pelos administradores de redes para ter o controle geral do tráfico da rede. Com isso, é possível monitorar tudo o que entra e sai nos hosts.

Foi desenvolvida em 1998 pelo Gerald Combs que possui bacharel em Ciências da Computação pela University of Missouri-Kansas City na empresa em que trabalhava **Network Integration Services (ISP)**.

> No final de 1997, o estudante de ciência de computação da University of Missouri – Kansas City, Gerald Combs, trabalhava para um pequeno provedor de Internet. Problemas de rede em tais provedores eram comuns e Gerald buscava ferramentas que pudessem lhe auxiliar na resolução dos mesmos. Porém, naquela época, produtos

> para análise de protocolos de rede eram caros (custavam em média $1500) e não funcionavam nos sistemas operacionais de sua companhia (Solaris e Linux). Dessa forma, com o intuito de rastrear os problemas ocorridos nos sistemas e aperfeiçoar seus conhecimentos em redes de computadores, Gerald começou a escrever seu próprio analisador de tráfego de rede, batizando o software de Ethereal. (SANCHES, Rodrigo, 2013).

Gerald aceitou uma proposta de emprego na **CACE Technologies** e por isso alterou o nome da ferramenta para Wireshark.

É um projeto do software livre liberado sob a licença GNU General Public Licence (GPL), desenvolvida em linguagem C++ e é suportada pelas plataformas: UNIX, Linux, Solaris, FreeBSD, NetBSD, OpenBSD, MAC OS X, Windows. Todas as informações buscadas são reorganizadas pelo sistema de forma que facilite o entendimento visual para o usuário, podendo ser representado em linhas ou gráficos.

3. Metodologia

Para exemplificarmos o funcionamento do wireshark e mostrar como é possível obter pacotes com informações confidencias de outros hosts da rede, criaremos uma rede interna com mascara de 24 bits (255.255.255.0) na qual utilizaremos 3 máquinas sendo 2 delas virtuais com o sistema operacional Linux, e 01 máquina física com sistema operacional Windows.

As três máquinas chamamos respectivamente de Host 1 com IP 192.168.0.102, Host 2 com IP 192.168.0.106 e o Host 3 com IP 192.168.0.100. O wireshark será instalado no Host 1 com o comando *sudo apt-get install wireshark.*

Depois de instalado digitamos no terminal 'wireshak' para abri-lo. A tela inicial possui 04 abas para acesso rápido, que são: Capture, Files, Online e Capture Help. Na aba *Capture* ficam listadas todas as interfaces reconhecidas pelo wireshark e tem também as opções de capturas; Na aba *Capture Help* é mostrado como fazer a captura e o passo a passo para configurá-la; Na opção *Files* podemos abrir as capturas feitas anteriormente e também tem um link que

mostra exemplos de capturas; E por ultimo a opção *Online* onde podemos visualizar os projetos de websites, guias de usuários e segurança para podermos trabalhar com o wireshark de uma forma segura.

O próximo passo e determinar qual a interface de rede que receberá as capturas de pacotes que pode ser definida na barra de menu -> capture -> Interfaces ou na própria tela inicial na aba *Capture* selecionamos a interface e clicamos em start.

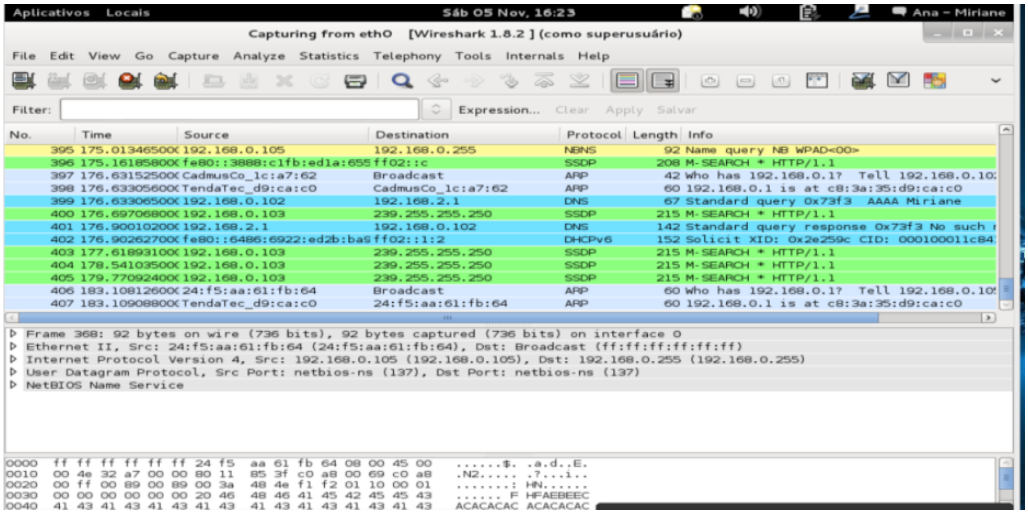

Figura 1 - Tela após start

Após iniciarmos a busca e pacotes aparecerá esta tela, com algumas ferramentas na barra de menu que são mais utilizadas. Temos a opção Filter para que possamos escrever uma expressão ou protocolo que quero filtrar. Por exemplo, se quisermos visualizar apenas os pacotes relacionados ao protocolo 'arp', então digitamos na barra do filtro 'arp' e colocamos para filtrar.

Logo abaixo terá três painéis, o *Painel de Lista de Pacotes* um que exibirá todos os pacotes filtrados com suas informações básicas:

- **Nº:** o número do pacote no arquivo de captura (não sofre alterações, mesmo usando um filtro).
- **Time:** o tempo do pacote. O formato de apresentação desse tempo pode ser mudado.
- **Source:** o endereço de origem do pacote.

- **Destination:** o endereço de destino do pacote.
- **Protocol:** abreviação do nome do protocolo.
- **Info:** informações adicionais sobre o pacote.

O *Painel de Detalhes dos Pacotes* que mostra mais detalhadamente as informações do pacote selecionado no painel anterior, podendo expandir ou comprimir esses detalhes, e também temos o *Painel de Byts dos Pacotes* que representa os dados do pacote selecionado em hexadecimal. O lado esquerdo apresenta o equivalente no pacote de dados, o centro mostra uma representação hexadecimal, enquanto o lado direito exibe os caracteres ASCII correspondentes.

Em baixo temos a *Barra de Status* que mostra mensagens informativas, nela é mostrada qual interface está sendo utilizada para a captura de pacotes, e também os:

- **Packets:** Mostra o numero de pacotes capturados.
- **Displayed:** Mostra o numero de pacotes sendo exibidos atualmente no painel de lista de pacotes.
- **Marked:** Mostra o numero de pacotes selecionado no painel.

Por exemplo, através do terminal do Host 1 utilizar o comando 'ping' para o Host 2, serão listados no painel de lista de pacotes.

Ao selecionar qualquer pacote, são listada detalhes sobre ele, como: a origem dele, destino, tempo, protocolo relacionado a ele, e etc. Selecionei um pacote qualquer para observar as informações detalhadas que serão exibidas e entende-las melhor. O pacote selecionado foi o de nº 70, na qual possui detalhes sobre o: Frame, Ethernet II, Internet Protocol, User Datagrama Protocol, Hypertext Translater Protocol. Ao lado de cada uma dessas informações à uma setinha que ao ser clicada abre mais informações sobre cada item:

- **Frame:** Refere-se a primeira camada do modelo OSI, a camada física.

- **Ethernet II:** Refere-se a segunda camada, logo, está mostrando o o endereço MAC de destino e o de origem.
- **Internet Protocol:** Refere-se a terceira camada do modelo OSI, mostrando informações sobre o endereço IP de origem e o de destino.
- **User Datagrama Protocol:** Refere-se a quarta camada do modelo OSI, que é a camada de transporte (TCP e UDP). Nela também são exibidas outras informações como porta de destina e origem.
- **Hypertext Translater Protocol:** Esse é um protocolo da camada de aplicação o HTTP porta 80, mostra também algumas informações como o que o ele está buscando no google, e etc.

Todas as buscas de pacotes podem ser salva, porem suponhamos que ao invés de analisarmos uma rede pequena de 03 máquinas como a do nosso exemplo, tenhamos que analisar uma rede maior de uma empresa com mais de 100 computadores. Para facilitar o controle, podemos fazer algumas alterações nas configurações do wireshark:

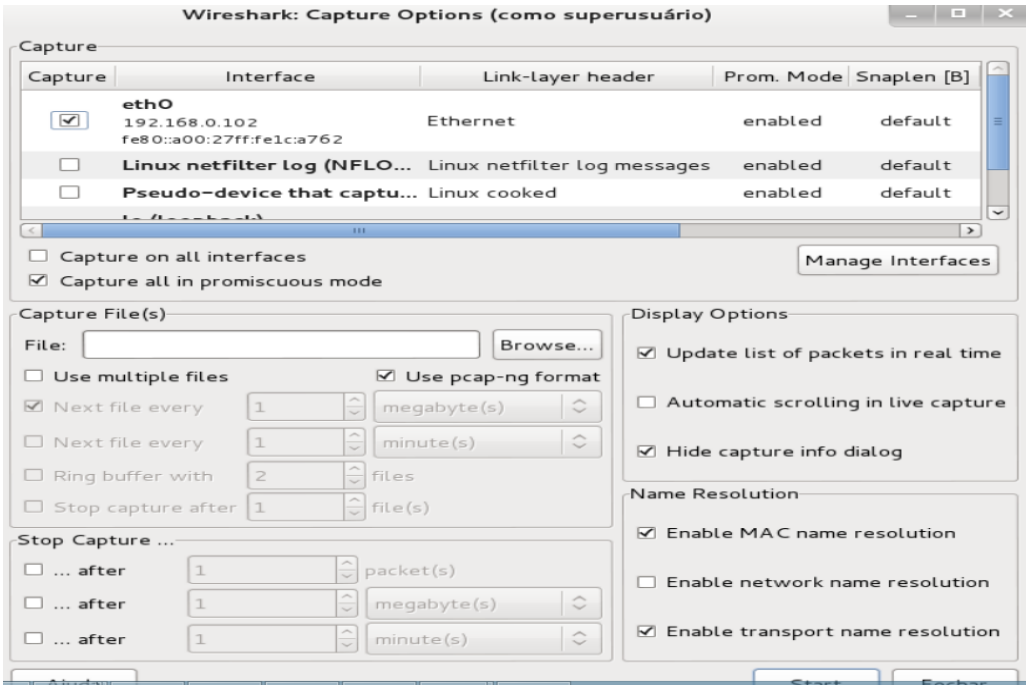

Figura 2 - Capture Options

Na parte superior podemos selecionar a interface; Logo abaixo temos a opção marcada 'Capture all in promiscuous mode' que habilita a interface selecionada à receber todos os pacotes da rede.

Temos a opção 'Use multiple files' que quando marcada, torna as opções abaixo editáveis. Suponhamos que queremos que seja criado um novo arquivo a cada 20 Mb de pacotes que forem captado ou então a cada 30 minutos de busca, então basta marcar essa opção e determinar abaixo o tempo ou o tamanho que desejarmos. Isso facilita a análise do arquivo ao invés de salvar um único arquivo com todas as informações.

Há também a opção 'Stop capture' na qual podemos determinar a quantidade de pacotes buscados, tamanho ou o tempo como limite de parada, ou seja, quando a busca atingir o limite que determinarmos nessa opção ela será finalizada.

4. Exemplo prático

O protocolo HTTP (*HyperText Transfer Protocol*) é o protocolo padrão da web; através dele é definido como são requisitadas as páginas, como serão enviadas os dados de usuários digitados em formulários, e etc. Todas essa informações são enviadas em forma de texto, e por isso são vulneráveis a intercepção de dados por terceiros.

Um meio de segurança para sites e aplicações web é aderir o 'certificado de segurança', ou seja, o HTTPs que possui mecanismos de segurança como a confidencialidade, integridade e autenticação, que protejam o site e as informações dos usuários inseridas nele.

- **Confidencialidade:** As mensagens são protegidas para que nenhum outro usuário possa lê-la a não ser o próprio destinatário.
- **Integridade:** Protege para que a mensagem original não sofra nenhuma alteração e seja entregada do mesmo jeito que foi enviada.
- **Autenticação:** Provar que o servidor de onde veio a mensagem, é realmente quem diz ser e não um invasor tentado se passar por ele.

A grande defesa dos sites que possuem o certificado de segurança é que suas mensagens são criptografadas, o que torna mais segura o seu meio de comunicação. São criadas duas chaves e por isso as mensagens enviadas são criptografadas e somente o servidor terá a outra chaves para descriptografá-la.

Ainda há muitos sites que não possui esse certificado de segurança os tornando um alvo mais vulnerável para sofre ataques. Por exemplo, utilizando a ferramenta wireshark, vou capturar todos os pacotes da minha rede para descobrir o login e senha de um dos usuários **Host 3** que estiver acessando um site não seguro.

Primeiro coloco o wireshark para começar a receber os pacotes por um tempo, para que possamos analisar os pacotes que ele irá capturar na rede. Vamos supor que o usuário do Host 3 acesse o site http://www.rstextil.com.br/ e coloque seu usuário e senha:

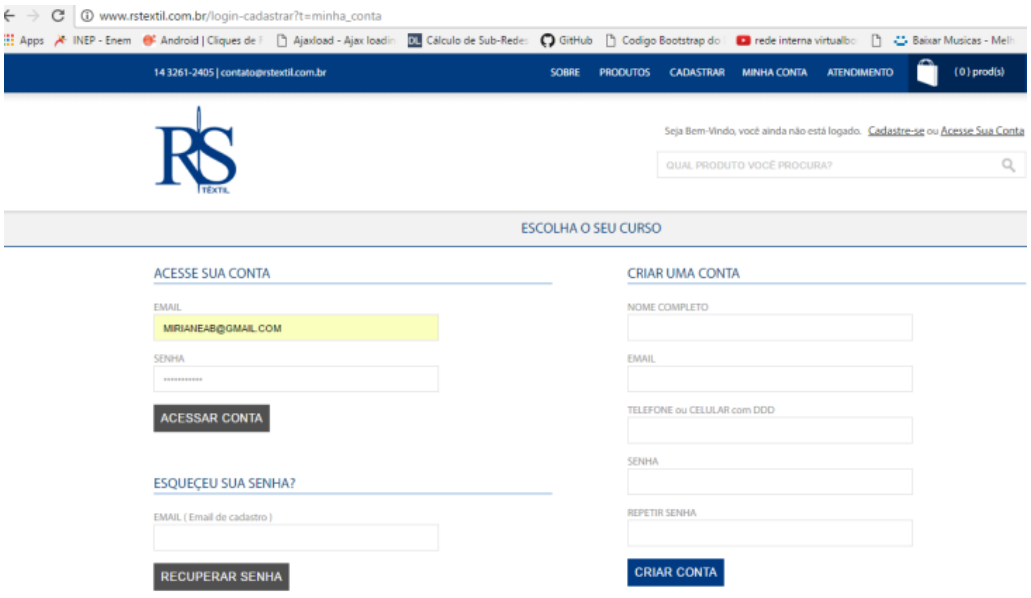

Figura 3 - Entrando com o usuario e senha

Agora voltamos para o wireshark, lembrando que ele está instalado no **Host 1**, e paramos a busca de pacotes para analisar todos que recebemos.

Para filtrarmos as informações vamos digitar filter o seguinte comando: *ip.addr == 192.168.0.105 and http.request.method == "POST"*, ou seja, estamos buscando todos os pacotes que tenham originado do Host 3 e que tenham sido enviados através do metodo POST. Depois clicamos em Apply para filtrar a busca:

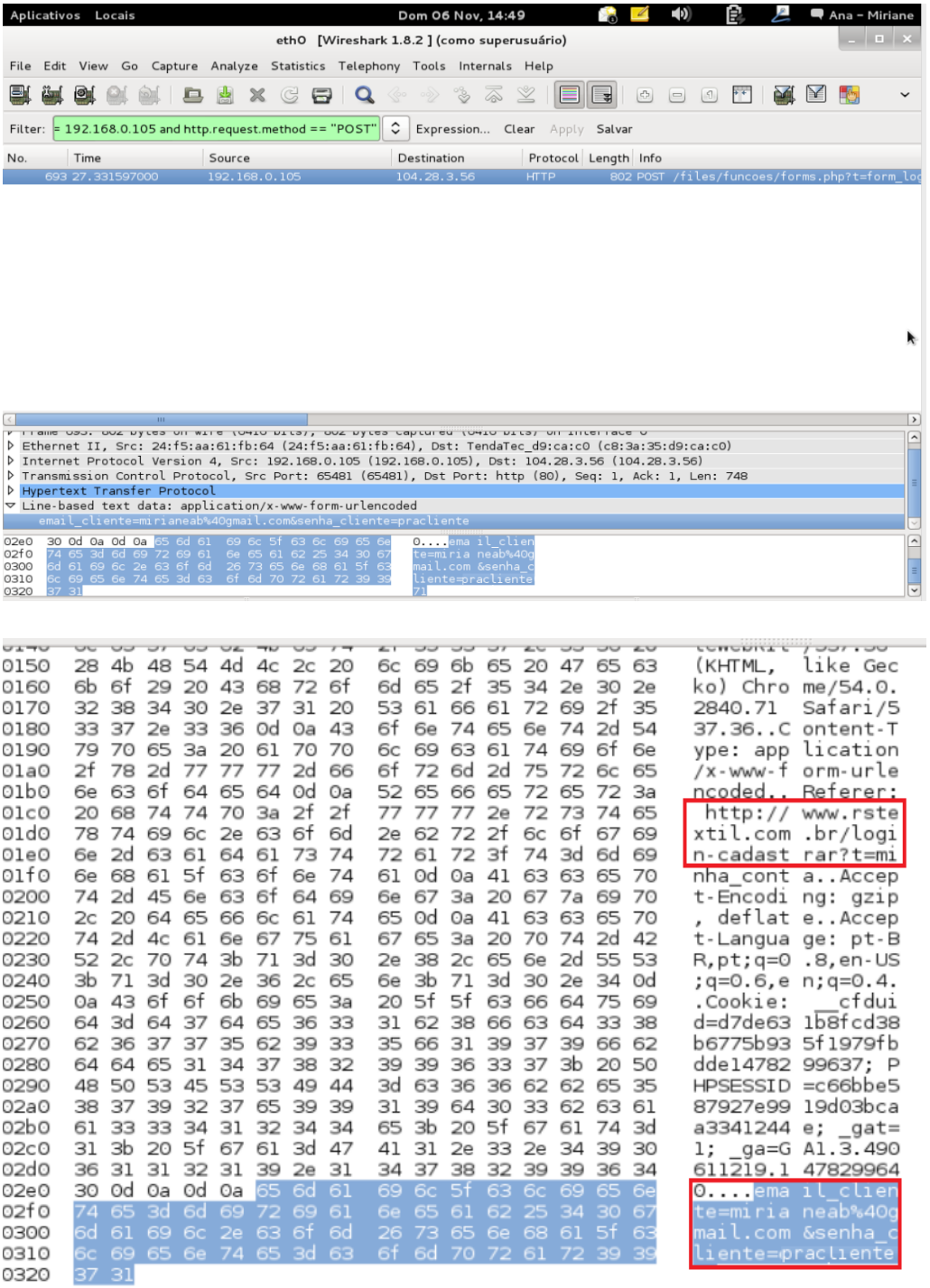

Figura 4 - Filtragem

Após a busca ele nos retornou um pacote acima que nos mostra em seus detalhes todas as informações que precisamos, como o site de acesso, o usuario (mirianeab@gmail.com) e a senha (pracliente). Logo, facilmente podemos tambem entrar no mesmo site como a conta desse usuário.

É de extrema importância que ao logarmos em um site, verificarmos se é um site com certificado de segurança que possua um cadeado ao lado do 'http', pois caso contrário, outras pessoas podem conseguir ter acesso a sua conta roubando seus dados que trafegam na rede.

5. Conclusão

As empresas hoje buscam sempre acompanhar a tecnologia porque mesmo que isso gere um custo à elas, ainda sim as vantagens adquiridas se tornam compensadoras. Sniffers de Rede são exemplos de ferramentas que auxiliam muito os administradores de redes à monitorarem o tráfico de dados e gerenciar as informações em suas redes.

Porém, como tudo na internet, esse softwares também possuem suas desvantagens pois podem ser usados para fins maliciosos no intuito de adquirir informações confidencias de outros usuários, como no exemplo mostrado nesse artigo. Tomar medidas de segurança é essencial para que naveguemos na internet sem sermos vítimas de alguma ataque, então, sempre ao inserir informações confidenciais em formulários de algum site, devemos primeiramente verificar se o mesmo possui certificado de segurança ou alguma outra medida de segurança para o usuário.

Administra uma rede criando o hábito de analisar seu tráfico de pacotes é interessante, pois assim sempre teremos o controle de quem está na rede, identificaremos possíveis ataques ou algumas atividades suspeitas, encontraremos aplicações inseguras em hosts dentre outras vantagens.

6. Referências Bibliográficas

CASTRO, Julia; RIBEIRO, Leonardo. **Manual de Funcionamento Wireshark.** Universidade Cátolica de Brasília, 2008. Disponível em: < http://www.cleberjean.com.br/downloads/Manual_Wireshark.pdf >.

CURVELO, Evandro. **Sobre a Detecção Remota de Sniffers para Detectores de Intrusão em Redes TCP/IP.** Universidade Federal de Pernambuco. Dissertação de Mestrado, 1999. Disponível em: < http://repositorio.ufpe.br/bitstream/handle/123456789/2550/arquivo4949_1.pdf?sequence=1&isAllowed=y>.

PISA, Pedro. **Qual a diferença entre HTTP e HTTPs,** 2013. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/07/qual-a-diferenca-entre-http-e-https.html >.

SANCHES, Rodrigo. **Análise do tráfego de rede com o Wireshark - Revista Infra Magazine 10**. Doutorado em Engenharia Elétrica. Universidade Estadual de Campinas. Disponível em:< http://www.devmedia.com.br/analise-do-trafego-de-rede-com-o-wireshark-revista-infra-magazine-10/27417>.

COUTO, Felipe; SANTOS, Alex; LOVATO, Angelo. **Estudo Comparativo de Ferramentas Analisadoras de Pacotes em rede TCP/IP.** Universidade Estadual do Sudoeste da Bahia (UESB). 2012. Disponível em: < http://200.19.105.203/index.php/reavi/article/view/2561/2088>.

CASAGRANDE, Rogério. **Técnicas de Detecção de Sniffers.** Universidade Federal do Rio Grande do Sul. Dissertação de Mestrado em Ciência da Computação. 2003. Disponível em: <http://index-of.es/Sniffers/Sniffers_pdf/000400345.pdf>.

FARRUCA, Nuno Miguel. **Wireshark para sistemas distribuídos.** Universidade Nova de Lisboa. Dissertação em Mestrado em Engenharia Informática. 2008/2009. Disponível em: < https://run.unl.pt/bitstream/10362/2288/1/Farruca_2009.pdf>.