

Roteiro 1 Análise tráfego de rede

Tecnologias Hacker

Objetivo: Desenvolver a habilidade analítica do tráfego de redes de computadores por meio da interpretação de um arquivo de log real.

Carga horária: 3 horas

Prazo para entrega: até 24 de fevereiro

Os sniffing de rede são ferramentas que permitem o profissional realizar uma avaliação sobre o comportamento de um ambiente de rede, e os protocolos que trafegam nesta. Entretanto, estas ferramentas pode ser utilizadas com propósitos maliciosos por invasores que tentam capturar o tráfego da rede com diversos objetivos, dentre os quais podem ser citados, obter cópias de arquivos importantes durante sua transmissão, obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real.

Vários protocolos populares presentes nas redes de computadores e sobretudo na Internet, ainda continuam a enviar informações sensíveis e importantes pela rede em texto claro, ou seja, sem criptografia.

Um ótimo instrumento pró ativo para os administradores de rede e profissionais de segurança, são os detectores de intrusão (IDS - Intrusion Detection System), que também são baseados em um sniffer para a captura das redes, e utilizam uma base de dados de regras para detectar redes suspeitas.

Antes de utilizar um sniffing é importante entender alguns conceitos básicos de rede, como a diferença entre o modo promíscuo e não promíscuo em uma interface de rede. Em uma rede local, os dados são enviados a todas as máquinas da rede. Entretanto, as máquinas ignoram os pacotes que lhes não são destinados. Para que seja possível alterar este comportamento e permitir que uma máquina analise todos os pacotes que passam por ela, devemos configurar a interface em um modo específico chamado "promiscuous", ou modo promíscuo.

Pergunta 1: Pesquise e registre aqui dois exemplos de IDS.

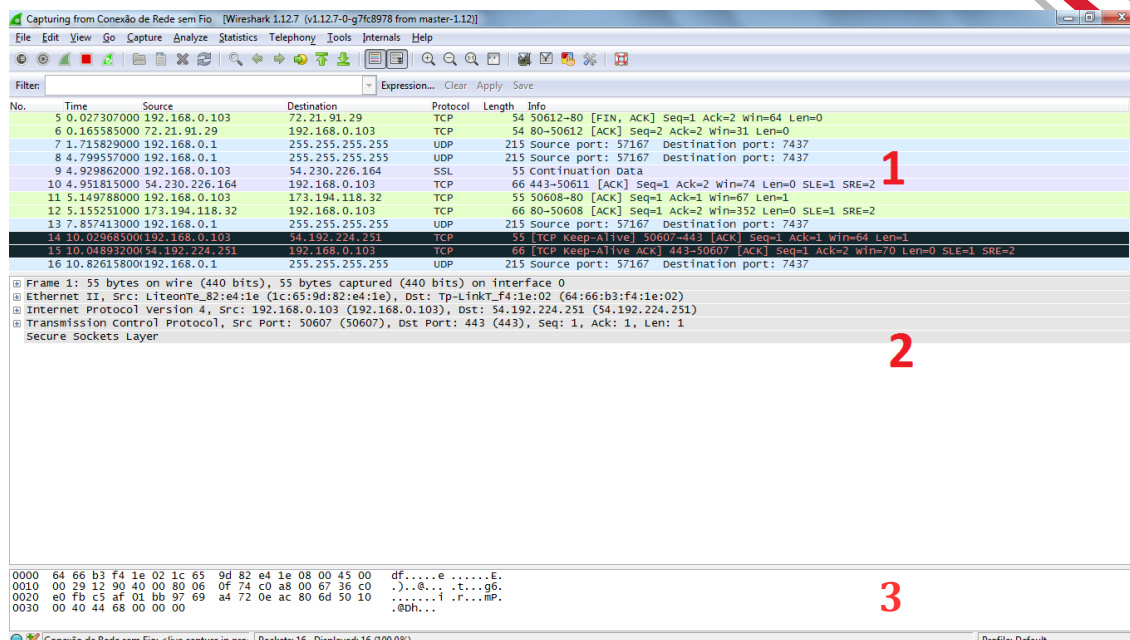
Pergunta 2: Quais as diferenças entre IDS e IPS?



Introdução ao Wireshark

Um dos analisadores de protocolos mais conhecidos por profissionais de tecnologia é o Wireshark. Sucessor do Ethereal desde junho de 2006, ele é um analisador de protocolos (sniffer), distribuído gratuitamente, a partir do endereço <http://www.wireshark.com>. Pode ser executado em diversas plataformas, incluindo sistemas Unix e Windows. Para ambiente Windows, é necessário instalar a biblioteca de captura de pacotes WinPcap (confirmar na instalação). Ela é uma versão da biblioteca libpcap (existente para ambientes Unix), para o Windows.

O Wireshark faz análise dos pacotes no momento da recepção e da transmissão das informações, permite organizar os dados de acordo com os protocolos utilizados (suporte para centenas de protocolos), possui função para filtrar apenas os resultados que interessam, exporta os dados capturados para arquivos de texto, além de outras funcionalidades.

Sua tela inicial apresenta um atalho para os principais recursos da ferramenta. É possível iniciar uma captura de tráfego de forma rápida e simples. Ainda, sua interface de saída está dividida em três partes:

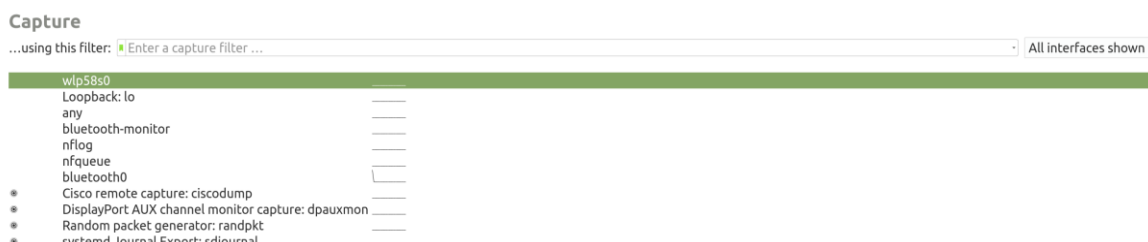



- A primeira contém uma relação dos pacotes capturados, um por linha. Selecione um dos pacotes 
- A segunda contém informações sobre o pacote que está selecionado, onde cada linha contém um protocolo, na ordem em que eles são empilhados. Dentro de cada protocolo, são mostrados os campos do seu cabeçalho. 
- A terceira parte contém os dados, ou seja, a carga útil (payload) do pacote, que será utilizada pela aplicação. A carga útil é apresentada no formato hexadecimal e o seu correspondente para ASCII.

Acesse a lista com os analisadores de pacotes mais usados, por meio do endereço: sectools.org/tag/sniffers/

Utilizando o Wireshark

Abra o Wireshark e ative a captura de pacotes (Menu Capture -> Start). Você também acessar no painel inicial o nome da interface que você deseja iniciar a captura.



- Inicie a captura (pressionando em Start). Depois de selecionarmos a interface, começamos de imediato a visualizar os pacotes que passam na rede. Caso já exista algum tráfego passando pela interface, este será apresentado na tela de captura.
- Abra um navegador e acesse algumas páginas web por volta de 2 minutos. Entre as páginas acesse www.google.com.
- Pare a captura de pacotes clicando no botão Stop. 

Observe que no campo que apresenta os pacotes capturados existem diversos detalhes nas informações (Info). Várias destas informações estão relacionadas com as conexões do protocolo de transporte TCP e nelas aproveite para observar as fases de abertura de uma conexão TCP por meio do Three-way Handshake.

Recordando:

Os três passos do Three-way Handshake

- I. O cliente que pretende abrir uma conexão com um servidor ou serviço envia um pacote com a flag **SYN**;
- II. O servidor ou serviço, se disponível para novas conexões, responde com um pacote com as flags **SYN + ACK**;
- III. O cliente ao receber esta confirmação então responde com o último para a abertura de conexão, um pacote **ACK**.

Vale lembrar que o TCP é um protocolo que garante a entrega dos dados a origem, ou seja, é um protocolo orientado à conexão. Isto significa que, antes que os dados sejam transmitidos, uma conexão confiável deve ser obtida e confirmada, conforme observamos com os passos do Three-way handshake. As transmissões de dados em nível de Transporte, durante uma comunicação mantêm alguns parâmetros de controle específicas da conexão. Estes controles são listados a seguir:

URG: informar uma estação receptora de que certos dados dentro de um segmento é urgente e deve ser priorizada.

ACK: Reconhecimento – Reconhece dados recebidos.

PSH: Este mecanismo que pode ser acionado pela aplicação, informa ao TCP origem e destino que a aplicação solicita a transmissão rápida dos dados enviados.

RST: Interrompe uma conexão em resposta a um erro.

SYN: Sincronizar – inicia uma conexão.

FIN: Nenhum dado a mais do emissor, finaliza a conexão

- Selecione os vários pacotes e observe os seus campos e valores. 

Aplicando Filtros

Agora vamos estabelecer alguns filtros para obter saídas específicas do volume de pacotes capturados. Estes filtros serão aplicados no “display filter”.

Atenção: alguns filtros podem não mostrar nenhum pacote, em função da atividade da rede naquele momento.

Faça um teste utilizando o filtro. Digite no campo filtro a sintaxe `ip.addr==192.168.0.1` (ou o ip de sua máquina)

Para ativar o filtro pressione ENTER.

Para desativar o filtro (antes de digitar outro), pressione no botão “Clear”. Os filtros devem ser digitados em letras minúsculas.

Construa filtros para as situações abaixo. **Este exercício é fundamental não só para que você se familiarize com a ferramenta, mas você compreenda a as característica da comunicação em rede e de seus protocolos.** (dica: clique no botão “Filter” e depois em “Add Expression” ou “Expression”):

- A. Apenas pacotes do protocolo DNS
- B. Apenas pacotes do protocolo HTTP
- C. Apenas pacotes do protocolo UDP
- D. Apenas pacotes do protocolo TCP
- E. Todos os pacotes enviados ou recebidos pelo seu host (forneça o seu IP)
- F. Apenas os pacotes HTTP enviados ou recebidos pelo seu host (forneça o seu IP)
- G. Apenas pacotes do host `www.google.com`.
- H. Todos os pacotes originados (enviados) pelo seu host.

Estatísticas e análise de dados

Com os dados obtidos, utilize as ferramentas de estatísticas disponíveis no Wireshark para descrever o comportamento da rede no período analisado. Encontre quais foram os principais serviços utilizado, principais hosts de origem e destino, protocolos usados, tamanho de pacotes, entre outros resultados.

Utilize as opções dentro do menu “Statistics”. A opção Summary mostra um resumo da coleta de informações. Verifique as estatísticas disponíveis nas opções “Conversations”, “Endpoints”, “Packet length”, “IP addresses”, “IP destinations”, “IP protocol types”, “HTTP”.

Para geração de estatísticas personalizadas na forma de gráficos, use a opção “IO Graphs”. No campo “Filter” insira o filtro desejado. Gere pelo menos 3 gráficos diferentes para mostrar as estatísticas.^[1]Ex: compare o tráfego gerado por diferentes protocolos: dns, arp, udp, tcp, etc.

Desafio 1

Nome do arquivo para análise: analise trafego malware 1.pcap

Informações sobre o Cenário Problema

Segmento de LAN: 192.168.2.0/24 (192.168.2.0 a 192.168.2.255)

Domínio: dnipromotors.com

Controlador de domínio: 192.168.2.4 - Dnipromotors-DC

Gateway de segmento de LAN: 192.168.2.1

Endereço de transmissão do segmento LAN: 192.168.2.255

Cliente Windows para investigar: 192.168.2.147

Sua tarefa:

Você deverá analisar o arquivo e responder as seguintes perguntas:

Pergunta 3: Qual é o endereço MAC do cliente Windows em 192.168.2.147?

Pergunta 4: Qual é o nome do host para o cliente Windows em 192.168.2.147?

Pergunta 5: Com base no tráfego do protocolo Kerberos, qual é o nome da conta de usuário do Windows usado em 192.168.2.147?

Pergunta 6: Qual a função do protocolo Kerberos?

Pergunta 7: Qual é a URL que retornou um arquivo executável do Windows?

Pergunta 8: Qual data e hora que a URL foi acessada?

Pergunta 9: Depois de receber o arquivo executável, com qual endereço IP o host infectado do Windows tentou estabelecer uma conexão TCP?

Desafio 2

Nome do arquivo para análise: analise trafego malware 2.pcap

Informações sobre o Cenário Problema

Segmento LAN: 172.17.1.0/24

Domínio: kyivartworks.com

Controlador de Domínio: 172.17.1.2 - Kyivartworks-DC

Gateway de rede: 172.17.1.1

Broadcast LAN: 172.17.1.255

Cliente Windows para investigar: 172.17.1.129

Sua tarefa:

Você deverá analisar o arquivo e responder as seguintes perguntas:

Pergunta 10: Qual é o endereço MAC do cliente Windows em 172.17.1.129?

Pergunta 11: Qual é o nome do host para o cliente Windows em 172.17.1.129?

Pergunta 12: Com base no tráfego Kerberos, qual é o nome da conta de usuário do Windows usado em 172.17.1.129?

Pergunta 13: Qual URL no pcap retornou um documento do Microsoft Word?

Pergunta 14: Qual data e hora que a URL foi criada?

Pergunta 15: Qual URL no pcap retornou um arquivo executável do Windows?