Insper

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: Aproximadamente 3 horas

Prazo para entrega: Até dia 29 de fevereiro de 2024 às 11h45.

As ferramentas de monitoramento de rede são utilizadas para avaliar o comportamento e os protocolos em uso dentro de um ambiente de rede. No entanto, é importante notar que essas mesmas ferramentas podem ser exploradas com intenções maliciosas por invasores, que buscam capturar dados de tráfego com objetivos diversos, como acessar arquivos importantes durante sua transmissão, obter senhas para expandir sua presença em uma rede invadida ou até mesmo monitorar conversas em tempo real.

Muitos dos protocolos comuns usados em redes de computadores, especialmente na Internet, ainda transmitem informações sensíveis em texto claro, sem criptografia, tornando-as vulneráveis a interceptação.

Para os administradores de rede e profissionais de segurança, os Sistemas de Detecção de Intrusões (IDS) são uma ferramenta proativa valiosa. Eles também utilizam técnicas de sniffing para capturar dados de rede e, com base em uma base de dados de regras, identificar atividades suspeitas.

Antes de empregar ferramentas de monitoramento de rede, é essencial compreender conceitos fundamentais, como a diferença entre os modos promíscuo e não promíscuo em uma interface de rede. Normalmente, em uma rede local, os dados são enviados para todas as máquinas, mas apenas as destinatárias processam esses pacotes. Para permitir que uma máquina analise todos os pacotes que passam por ela, é necessário configurar a interface para operar em modo promíscuo.

Insper

Pergunta 1: Pesquise e registre aqui dois exemplos de IDS (0,25 pontos).

Tanto Cisco quanto Trend Micro oferecem soluções para IDS, sendo a Trend Micro a nº1 no mercado.

- https://www.trendmicro.com/en_us/ciso/22/l/intrusion-detection-prevention-systems.html
- https://www.cisco.com/c/pt_br/products/security/ngips/index.html

Pergunta 2: Quais as diferenças entre IDS e IPS (0,25 pontos)?

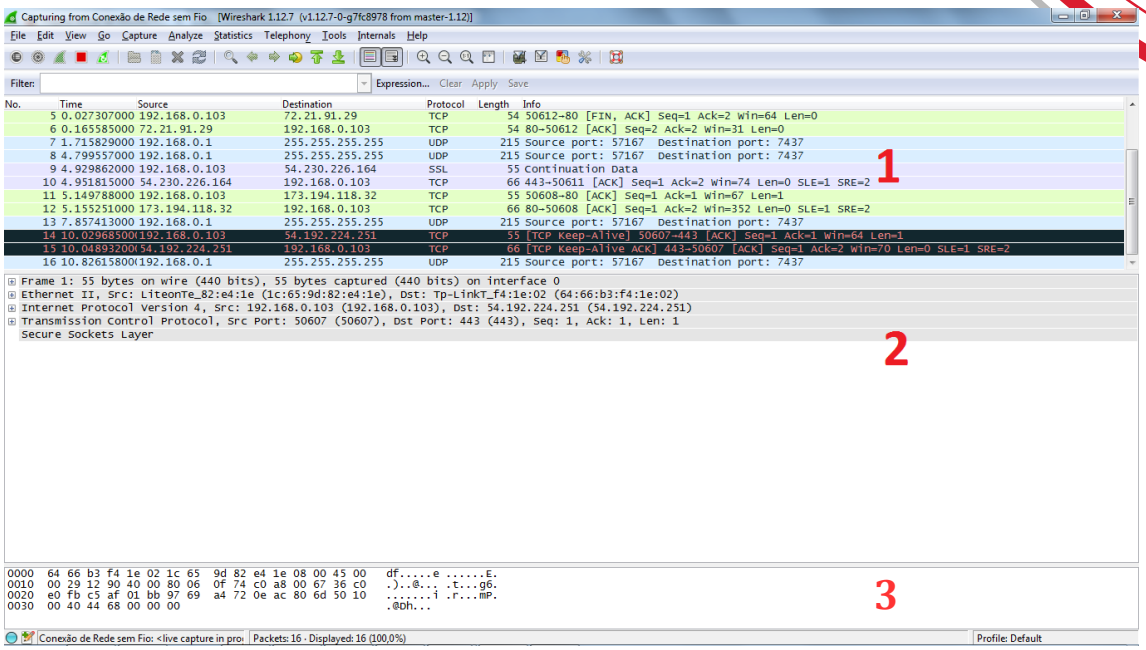
Enquanto o IDS fornece somente alertas sobre possíveis ameaças e intrusões, e portanto demanda intervenção manual, o IPS também bloqueia conexões que possam apresentar comportamento suspeito, com base em “digital vaccine signatures". Além disso, também é possível configurar o IPS com parâmetros específicos para quarentenar ou bloquear conexões.

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.

Insper

Recordando:

Os três passos do Three-way Handshake

O Three-way Handshake é fundamental nas redes TCP/IP, pois possibilita a criação e o término de conexões confiáveis e organizadas. Esse procedimento assegura que todos os dispositivos envolvidos na comunicação estejam em sincronia quanto aos seus números de sequência iniciais e estabeleçam os parâmetros necessários para a transmissão de dados.

Entender o funcionamento do handshake de três etapas é crucial para administradores de rede, analistas de segurança e desenvolvedores que lidam com aplicativos baseados em TCP, pois é a base para uma comunicação segura e eficiente pela Internet.

O processo de três etapas garante que ambas as extremidades da conexão estejam preparadas e cientes dos números de sequência e parâmetros de comunicação um do outro. Isso estabelece uma conexão confiável e sincronizada antes que a transmissão de dados comece minimizando as chances de perda ou corrupção de dados. A seguir é apresentada as três etapas para abertura de uma conexão de rede:

1. **Solicitação inicial de conexão SYN (Synchronize):**
    - O cliente envia um segmento SYN para o servidor, indicando que deseja iniciar uma conexão.
    - Este segmento contém um número de sequência inicial gerado aleatoriamente pelo cliente, que será usado para sincronizar os números de sequência entre o cliente e o servidor.
2. **Resposta do servidor SYN-ACK (Synchronize-Acknowledgment):**
    - O servidor recebe o segmento SYN, reconhece a solicitação de conexão e responde com um segmento SYN-ACK.
    - O segmento SYN-ACK também contém um número de sequência inicial gerado aleatoriamente pelo servidor.

- Além disso, o servidor incrementa o número de sequência enviado pelo cliente (adicionando 1) e inclui esse número de sequência na resposta SYN-ACK, indicando que recebeu corretamente a solicitação SYN do cliente.

3. **Confirmação do cliente ACK (Acknowledgment):**
   - Finalmente, o cliente recebe o segmento SYN-ACK do servidor e envia um segmento ACK em resposta.
   - Este segmento ACK confirma a recepção do segmento SYN-ACK pelo servidor.
   - O número de sequência enviado pelo cliente é então incrementado (adicionando 1) e incluído no segmento ACK, confirmando que ele recebeu corretamente o SYN-ACK do servidor.

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 mantém 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 para você compreender as características 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 adresses”, “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. Ex: compare o tráfego gerado por diferentes protocolos: dns, arp, udp, tcp, etc.

Insper

DESAFIOS

Todas as respostas dos 5 desafios deverão seguir com o print completo do desktop (não serão aceitos prints apenas da janela do Wireshark). O código do portscan deverá estar no github e o link para ele deverá estar no documento de entrega.

Desafio 1 (1 ponto)

Nome do arquivo para análise: desafio1.pcap

Informações sobre o Cenário Problema

No dia 21 de março de 2022 a estação de trabalho de Patrick Zimmerman foi infectada pelo malware IceID. Analise as conexões realizadas nesta data em busca de comportamentos suspeitos que permitiram a instalação de uma ferramenta de segurança ofensiva.

Sua tarefa:

Você deverá analisar o arquivo e responder as seguintes perguntas:

Pergunta 3: Qual o IP do servidor DHCP desta rede?

O IP do DHCP desta rede é 10.0.19.14.

Pergunta 4: Qual o nome do controlador de domínio desta rede?

O nome do controlador de domínio (DC) desta rede é BURNINCANDLE-DC.

Pergunta 5: Liste duas conexões suspeitas realizadas neste arquivo.

Tráfego sobre o UDP data pode ser perigoso, pois não existe uma aplicação definida.

Insper

Desafio 2 (1,5 pontos)

Nome do arquivo para análise: analise trafego desafio2.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

Você deverá analisar o arquivo e responder as seguintes perguntas:

Pergunta 6: Qual é o endereço MAC do host 192.168.2.4?

Pergunta 7: Qual é o hostname do cliente Windows em 192.168.2.147?

Pergunta 8: Com base no tráfego do protocolo Kerberos, qual é o nome da conta de usuário do Windows usado em 192.168.2.147?

Pergunta 9: Qual a função do protocolo Kerberos?

Pergunta 10: Qual é a URL que retornou um arquivo executável do Windows? Qual o nome do arquivo?

Pergunta 11: Qual data e hora que a URL foi acessada?

Insper

Pergunta 12: Depois de receber o arquivo executável, com qual endereço IP o host infectado do Windows tentou estabelecer uma conexão TCP?

Desafio 3 (1 ponto)

Nome do arquivo para análise: analise trafego desafio3.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 13: Qual é o endereço MAC do cliente Windows em 172.17.1.129?

Pergunta 14: Qual é o nome do host para o cliente Windows em 172.17.1.129?

Pergunta 15: Com base no tráfego Kerberos, qual é o nome da conta de usuário do Windows usado em 172.17.1.129?

Pergunta 16: Qual URL no pcap retornou um documento do Microsoft Word?

Pergunta 17: Qual data e hora que a URL foi criada?

Insper

Pergunta 18: Qual URL no pcap retornou um arquivo executável do Windows?

Desafio 4 (1 ponto)

Nome do arquivo para análise: analise trafego desafio4.pcap

Informações sobre o Cenário Problema

Segmento LAN: 192.168.1.0/24 (10.9.10.0 through 10.9.10.255)

Domínio: SPOONWATCH-DC

Gateway de rede: 192.168.1.1

Broadcast LAN: 192.168.1.255

Cliente Windows para investigar: 172.17.1.129

Você deverá analisar o arquivo e responder as seguintes perguntas:

Pergunta 19: Qual o IP do Controlador de domínio?

Pergunta 20: Qual o user account do IP 192.168.1.216?

Pergunta 21: Qual o hostname do IP 192.168.1.216?

Pergunta 22: Qual IP no pcap retornou arquivos suspeitos?

Pergunta 23: Em qual porta de comunicação do servidor destino as conexões foram realizadas?

Insper

Desafio 5

Criação de Escaneamento de Portas com Python.

Descrição: Desenvolvimento de uma aplicação que realize o escaneamento de portas de comunicação de um destino por meio de bibliotecas de desenvolvimento da Linguagem de programação Python.

Você deverá realizar uma pesquisa dos módulos e bibliotecas que permitem o desenvolvimento de uma ferramenta para o escaneamento de portas TCP de acordo com as premissas a seguir:

- Ser em linguagem Python;
- Deverá possuir uma interface amigável e de fácil utilização (user-friendly interface); **(1 ponto)**
- Permitir o escaneamento de um host ou uma rede; **(1 ponto)**
- Permitir inserir o range (intervalo) de portas a serem escaneadas; **(1 ponto)**
- Além da função de escaneamento, espera-se que seu código relacione as portas Well-Know Ports e seus serviços, e apresente em sua saída (imprimir) o número da porta e o nome do serviço associado. **(2 pontos)**
- Existem diversos projetos e documentações relacionados com esta atividade. Aproveite para analisar os códigos já desenvolvidos para teu projeto.

Insper

Introdução

As ferramentas de escaneamento permitem a descoberta de vulnerabilidades em ambientes computacionais, entre outras funcionalidades. Os escaneadores estão disponíveis como ferramentas especializadas projetadas apenas para “escanear” vulnerabilidades em um host, como por exemplo determinar se suas portas de comunicação estão sendo ou não usadas. São extremamente úteis no processo de descoberta e reconhecimento do alvo em um PENTEST, bem como, para a administração de ambientes computacionais. Muitas portas estão associadas a serviços específicos de rede. Para isso, é fundamental o conhecimento sobre sockets e dos protocolos de transporte, bem como, suas características como cabeçalho e *flags*.

Existem basicamente três tipos de escaneamento:

- **Escaneamento de porta (*port scanner*):** Seu objetivo é verificar portas abertas e serviços disponíveis em um host.
- **Escaneamento de rede:** Permite identificar os hosts que estão ativos em uma rede.
- **Escaneamento de vulnerabilidades:** Busca por vulnerabilidades conhecidas em um host.

Neste roteiro vamos trabalhar com o *port scanner.*

Port scanner

É a técnica mais popular e usada por Hackers/Crackers para descobrir serviços vulneráveis em um sistema e o NMAP a mais popular das ferramentas.

Insper

Indicação para pesquisa:

Capítulo 1 : O'CONNOR, T. J. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, 2012, ISBN-13: 978-1597499576

DUFFY, Christopher. Aprendendo Pentest com Python. Novatec, 2015, ISBN: 978-85-7522-505-9

Tutoriais Wireshark:

Changing Your Column Display:

https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/

Identifying Hosts and Users:

https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/

Display Filter Expressions:

https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/

Exporting Objects from a Pcap:

https://unit42.paloaltonetworks.com/using-wireshark-exporting-objects-from-a-pcap/

Wireshark Workshop Videos Now Available:

https://unit42.paloaltonetworks.com/wireshark-workshop-videos/