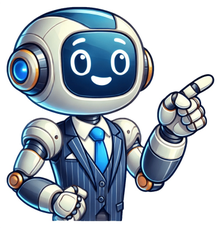
I'm not a bot



Como usar o wireshark

O Wireshark permite capturar e analisar todo o tráfego de rede no Windows, facilitando a solução de problemas, a otimização do desempenho e o aprendizado sobre protocolos. Sua interface intuitiva e múltiplas opções de filtragem e personalização o tornam uma ferramenta útil tanto para iniciantes quanto para especialistas em rede e segurança cibernética. O uso responsável e ético do Wireshark, juntamente com a adoção de medidas de segurança e conformidade legal, é essencial para proteger a privacidade e evitar riscos. Você já imaginou O que realmente acontece na sua rede quando você navega, joga online ou gerencia dispositivos conectados? Se você está simplesmente curioso sobre os mistérios que circulam em seu WiFi, ou se você simplesmente precisa de uma ferramenta profissional para Analise o tráfego da rede e detecte problemas com sua conexão, certamente o nome de Wireshark já chamou sua atenção. Pois bem, neste artigo você descobrirá sem rodeios todos os detalhes sobre o Wireshark: O que é, para que serve no Windows, como instalar e as melhores dicas antes de começar a capturar dados. Vamos lá. O que é Wireshark? Desvendando o titã da análise de rede O Wireshark é o analisador de protocolo de rede mais popular e reconhecido no mundo todo.. Esta ferramenta gratuita, de código aberto e poderosa permite que você capturar e examinar todo o tráfego de rede que passa pelo seu computador, seja ele uma máquina Windows, Linux, macOS ou até mesmo sistemas como FreeBSD e Solaris. Com o Wireshark, você pode ver, em tempo real ou após a gravação, exatamente quais pacotes estão entrando e saindo do seu computador, sua origem, destino, protocolos e até mesmo dividi-los para obter detalhes de cada camada de acordo com o modelo OSI. Ao contrário de muitos analisadores, O Wireshark se destaca pela sua interface gráfica intuitiva, mas também oferece uma versão de console poderosa chamada TShark para aqueles que preferem a linha de comando ou precisam executar tarefas automatizadas. A flexibilidade do Wireshark Ele permite que você analise uma conexão enquanto navega, realize auditorias de segurança profissionais, resolva gargalos de rede ou aprenda do zero sobre como funcionam os protocolos da Internet, tudo isso no seu próprio PC! Baixe e instale o Wireshark no Windows Instalar o Wireshark no Windows é um processo simples., mas é aconselhável fazer isso passo a passo para não deixar pontas soltas, principalmente quanto a permissões e drivers adicionais para a captura. Download oficial: Acesso a o site oficial do Wireshark e escolha a versão do Windows (32 ou 64 bits, dependendo do seu sistema). Execute o instalador: Clique duas vezes no arquivo baixado e siga o assistente. Aceite as opções padrão se tiver alguma dúvida. Motivadores essenciais: Durante a instalação, o instalador irá perguntar-lhe instalar Npcap. Este componente é essencial, pois permite que sua placa de rede capture pacotes em modo "promíscuo". Aceite sua instalação. Encerrar e reiniciar: Quando o processo estiver concluído, reinicie o computador para garantir que todos os componentes estejam prontos. Conteúdo exclusivo - Clique aqui Como excluir fotos da nuvemPreparar! Agora você pode começar a usar o Wireshark no menu Iniciar do Windows. Observe que este programa é atualizado com frequência, por isso é uma boa ideia verificar novas versões de tempos em tempos. Como funciona o Wireshark: captura e exibição de pacotes Quando você abre o Wireshark, A primeira coisa que você verá é a lista de todas as interfaces de rede disponíveis no seu sistema.: Placas de rede com fio, WiFi e até mesmo adaptadores virtuais se você usar máquinas virtuais como VMware ou VirtualBox. Cada uma dessas interfaces representa um ponto de entrada ou saída de informações digitais. Para começar a capturar dados, Basta clicar duas vezes na interface desejada. Desde esse momento, O Wireshark exibirá em tempo real todos os pacotes que circulam por esse cartão, classificando-os por colunas como número do pacote, hora da captura, origem, destino, protocolo, tamanho e detalhes adicionais. Quando quiser parar de capturar, pressione o botão botão vermelho Parar. Você pode salvar suas capturas no formato .pcap para análise posterior, compartilhamento ou até mesmo exportá-las em vários formatos (CSV, texto, compactado, etc.). Essa flexibilidade é o que torna O Wireshark é uma ferramenta indispensável tanto para análises pontuais quanto para auditorias completas.. Introdução: Dicas antes de fazer uma captura de tela no Windows Para garantir que suas primeiras capturas do Wireshark sejam úteis e não acabem cheias de ruído irrelevante ou dados confusos, há várias recomendações importantes a serem seguidas: Feche programas desnecessários: Antes de iniciar uma captura, feche os aplicativos que geram tráfego em segundo plano (atualizações, chats, clientes de e-mail, jogos, etc.). Dessa forma você evitará misturar tráfego irrelevante. Controlar o firewall: Firewalls podem bloquear ou modificar o tráfego. Considere desativá-lo temporariamente se quiser uma captura completa. Capture apenas o que é relevanteSe você quiser analisar um aplicativo específico, espere um ou dois segundos após iniciar a captura para iniciá-lo e faça o mesmo ao fechá-lo antes de interromper a gravação. Conheça sua interface ativa: Certifique-se de selecionar a placa de rede correta, especialmente se você tiver vários adaptadores ou estiver em uma rede virtual. Seguindo essas diretrizes, suas capturas de tela ficarão muito mais limpas e úteis para qualquer análise posterior.. Filtros no Wireshark: como focar no que realmente importa Um dos recursos mais poderosos do Wireshark são os filtros. Existem dois tipos básicos: Filtros de captura: Elas são aplicadas antes de começar a capturar, permitindo que você colete apenas o tráfego que lhe interessa desde o início. Filtros de exibição: Elas se aplicam à lista de pacotes já capturados, permitindo que você exiba apenas aqueles que atendem aos seus critérios. Entre os filtros mais comuns estão: Por protocolo: Filtra apenas pacotes HTTP, TCP, DNS, etc. Por endereço IP: Por exemplo, exiba apenas pacotes de ou para um IP específico usando ip.src == 192.168.1.1 o ip.dst == 8.8.8.8. Pelo porto: Limita os resultados a uma porta específica (tcp.porta == 80). Por sequência de texto: Localiza pacotes que contêm uma palavra-chave em seu conteúdo. Por endereço MAC, comprimento do pacote ou intervalo de IP. Conteúdo exclusivo - Clique aqui Como copiar e colar de um PDFAlém disso, os filtros podem ser combinados com operadores lógicos (e, or, não) para pesquisas muito precisas, como tcp.port == 80 e ip.src == 192.168.1.1. O que você pode capturar e analisar com o Wireshark no Windows? Wireshark é capaz de interpretar mais de 480 protocolos diferentes, desde conceitos básicos como TCP, UDP, IP, até protocolos específicos de aplicação, IoT, VoIP e muitos outros. Isso significa que você pode examinar todos os tipos de tráfego de rede, desde simples consultas DNS até sessões SSH criptografadas, conexões HTTPS, transferências FTP ou tráfego SIP de telefonia pela Internet. Além disso, O Wireshark suporta formatos de captura padrão, como tcpdump (libpcap), pcapng e outros, e permite que você compacte e descompacte capturas de tela rapidamente usando GZIP para economizar espaço. Para tráfego criptografado (TLS/SSL, IPsec, WPA2, etc.), se você tiver as chaves corretas, poderá até descriptografar os dados e visualizar seu conteúdo original. Captura detalhada de tráfego: recomendações adicionais Antes de iniciar qualquer captura importante, siga este protocolo para maximizar a utilidade das informações coletadas.: Escolha a interface certa: Normalmente, seu adaptador ativo será aquele para a conexão que você está usando. Caso tenha alguma dúvida, verifique qual está conectado nas configurações de rede do Windows. Definir a cena: Abra apenas os programas ou aplicativos que gerarão o tráfego que você deseja analisar. Isolar o fenômenoSe você deseja analisar o tráfego do aplicativo, siga esta sequência: inicie o aplicativo depois de iniciar a captura, execute a ação que deseja analisar e feche o aplicativo antes de interromper a gravação. Salve a captura de tela: Pare a gravação, vá em Arquivo > Salvar e escolha .pcap ou seu formato preferido. É assim que você vai conseguir arquivos limpos e fáceis de analisar, sem nenhum tráfego indesejado misturado. Exemplos ilustrativos: análise de tráfego com Wireshark Digamos que você tenha dois computadores em sua rede local e um deles para de acessar a Internet. Você pode usar o Wireshark para capturar tráfego dessa máquina. e veja se há erros na resolução de endereços DNS, se os pacotes não estão chegando ao roteador ou se um firewall está bloqueando as comunicações. Outro caso típico: detectar se um site não criptografa corretamente seu login. Se você fizer login em um site sem HTTPS e aplicar um filtro HTTP combinado com seu nome de usuário, poderá até ver sua senha circulando sem criptografia pela rede, uma demonstração real do risco de sites inseguros. Wireshark e Segurança: Riscos, Ataques e Medidas de Proteção O poder do Wireshark também é seu maior risco: Nas mãos erradas, pode facilitar a captura de credenciais, espionagem ou revelar informações confidenciais.. Aqui estão algumas ameaças e recomendações: Credential stuffing (ataques de força bruta de credenciais): Se você capturar tráfego SSH, Telnet ou outro serviço, poderá observar tentativas de login automatizadas. Preste atenção às sessões mais longas (elas geralmente são bem-sucedidas), aos tamanhos dos pacotes e ao número de tentativas para detectar padrões suspeitos. Risco de tráfego externo: Filtre todo o tráfego SSH que não esteja vindo da sua rede interna: se você vir conexões de fora, fique alerta! Senhas em texto simples:Se um site transmitir nomes de usuário e senhas não criptografados, você verá isso na captura de tela. Nunca use o Wireshark para obter esses dados em redes estrangeiras. Lembre-se de que fazer isso sem permissão é ilegal. Consentimento e legalidade: Analisa somente tráfego de redes próprias ou com autorização explícita. A lei é muito clara sobre esse ponto, e o uso indevido pode ter consequências sérias. Transparência e ética:Se você trabalha em um ambiente corporativo, informe os usuários sobre a análise e sua finalidade. O respeito à privacidade é tão importante quanto a segurança técnica. Como abrir um arquivo pcap no Windows 10 Alternativas ao Wireshark: Outras opções para análise de rede O Wireshark é a referência indiscutível, mas existem outras ferramentas que podem complementar ou, em situações específicas, substituir seu uso: tcpdump: Ideal para ambientes Unix/Linux, funciona na linha de comando. É leve, rápido e flexível para capturas rápidas ou tarefas automatizadas. Tubarão das Nuvens: Plataforma web para upload, análise e compartilhamento de capturas de pacotes do navegador. Muito útil para ambientes colaborativos. SmartSniff: Focado no Windows, fácil de usar para capturas pontuais e visualização de conversas entre clientes e servidores. ColaSoft Capsa: Analisador gráfico de redes que se destaca pela simplicidade de sua interface e opções específicas para escaneamento de portas, exportação e visualização compacta. A escolha da melhor alternativa depende de suas necessidades específicas.: velocidade, interface gráfica, colaboração on-line ou compatibilidade com hardware específico. Configurações avançadas: Modo promíscuo, monitor e resolução de nomes O modo promíscuo permite que a placa de rede capture não apenas os pacotes destinados a ela, mas todo o tráfego que circula pela rede à qual está conectado. É crucial para analisar redes corporativas, hubs compartilhados ou cenários de testes de penetração. No Windows, vá para Capturar > Opções, selecione a interface e marque a caixa de modo promíscuo. Tenha em mente que em redes Wi-Fi, exceto por hardware muito específico, você só verá tráfego do seu próprio dispositivo. Além disso, A resolução de nomes converte endereços IP em nomes de domínio legíveis (por exemplo, 8.8.8.8 em google-public-dns-a.google.com). Você pode habilitar ou desabilitar esta opção em Editar > Preferências > Resolução de Nomes. Ajuda muito a identificar dispositivos durante uma varredura, embora possa tornar o processo mais lento se houver muitos endereços sendo resolvidos. Sou um entusiasta da tecnologia que transformou seus interesses "geek" em profissão. Passei mais de 10 anos da minha vida usando tecnologia de ponta e mexendo em todos os tipos de programas por pura curiosidade. Agora me especializei em informática e videogames. Isto porque há mais de 5 anos escrevo para diversos sites sobre tecnologia e videojogos, criando artigos que procuram dar-lhe a informação que necessita numa linguagem compreensível para todos. Se você tiver alguma dúvida, meu conhecimento vai desde tudo relacionado ao sistema operacional Windows até Android para celulares. E meu compromisso é com você, estou sempre disposto a dedicar alguns minutos e te ajudar a resolver qualquer dúvida que você possa ter nesse mundo da internet. Wireshark es reconocido mundialmente como el analizador de paquetes más popular y ampliamente utilizado. Este software permite la captura y análisis exhaustivo de todo el tráfico de red que fluye hacia y desde un PC. Una característica distintiva de Wireshark es su compatibilidad multiplataforma. Lo que significa que está disponible para una variedad de sistemas operativos, incluyendo Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, entre otros. En este artículo de informática tutoriales, ofreceremos una guía básica para realizar capturas de tráfico de red y cómo usar wireshark, analizar para identificar cualquier anomalía potencial. ¿Alguna vez has querido echar un vistazo detrás de las cortinas de tu red? Con Wireshark, esto no solo es posible, ¡sino también sorprendentemente fácil y completamente gratis! Este programa es un verdadero todoterreno en el mundo del análisis de redes, capaz de inspeccionar cientos de protocolos. Ya sea que estés lidiando con protocolos de la capa física, de enlace, de red, de transporte o de aplicación, Wireshark lo tiene cubierto. Imagina poder capturar, en tiempo real, todo lo que pasa por tu red cableada o inalámbrica. Con Wireshark, puedes hacer exactamente eso. Y lo mejor de todo es que, una vez terminada la captura, puedes analizar todo a fondo, offline, en el mismo ordenador o en otro, cuando te convenga. Wireshark no es solo una cara bonita. Aunque cuenta con una GUI intuitiva para ver el tráfico capturado, también ofrece TShark, una herramienta de consola para los amantes de la línea de comandos. ¿Quieres ver el tráfico a través de SSH? ¡Con TShark es pan comido! La magia de Wireshark también reside en sus filtros. Puedes configurarlos para ver exactamente lo que necesitas, sin distracciones. Además, es un camaleón en cuanto a formatos de captura: desde tcpdump (libpcap) y pcap ng hasta muchas otras extensiones. Y si te preocupa el espacio, Wireshark puede comprimir y descomprimir al vuelo tus capturas con GZIP. En un mundo de datos cifrados, Wireshark también brilla. Con la clave privada adecuada, puede descifrar una variedad de protocolos como IPsec, SSL/TLS, WEP y WPA/WPA2. Además, es compatible con tecnologías de red desde Ethernet hasta Bluetooth y USB. Y si te preocupa la complejidad, descuida. Wireshark es sorprendentemente sencillo de usar, sin importar si eres un profesional de TI o simplemente un curioso de la tecnología. Funciona de maravilla en Windows, macOS y Linux, lo que te permite disfrutar de su potencia en el sistema operativo que prefieras. ¡Sumérgete en el fascinante mundo del análisis de redes con Wireshark, tu compañero de confianza para descubrir los secretos que esconde tu red! Interfaz Gráfica Intuitiva: Wireshark cuenta con una interfaz de usuario fácil de entender, lo que facilita su uso tanto para principiantes como para usuarios avanzados. Soporte Multiplataforma: Disponible para varios sistemas operativos, incluyendo Windows, macOS y Linux, lo que amplía su accesibilidad. Amplia Comunidad y Documentación: Wireshark cuenta con una comunidad activa y una amplia documentación en línea, lo que facilita la resolución de problemas y el aprendizaje. Potente Filtrado y Análisis: Ofrece opciones avanzadas de filtrado para centrarse en datos específicos, junto con herramientas de análisis poderosas para inspeccionar el tráfico de red. Captura en Tiempo Real: Permite la captura en tiempo real de paquetes de red, lo que facilita la detección inmediata de problemas y amenazas. Compatibilidad con Múltiples Protocolos: Es capaz de analizar una amplia variedad de protocolos de red, permitiendo la detección de problemas en diversas capas del modelo OSI. Curva de Aprendizaje: Para usuarios principiantes, la cantidad de funciones y opciones puede resultar abrumadora al principio, requiriendo tiempo para familiarizarse completamente. Riesgo de Sobrecarga: Al capturar y analizar todo el tráfico de red, puede generar grandes cantidades de datos, lo que podría afectar el rendimiento del sistema. Requiere Permisos Elevados: En algunos sistemas operativos, como Windows, puede requerir permisos elevados para acceder a ciertas funciones, lo que podría presentar limitaciones en entornos controlados. Limitaciones en Redes Inalámbricas: La captura de tráfico inalámbrico puede presentar desafíos y requerir hardware específico, y la capacidad de Wireshark para analizar ciertos protocolos inalámbricos puede ser limitada. Posibles Preocupaciones de Privacidad: El monitoreo del tráfico de red plantea preocupaciones de privacidad, y su uso indebido podría infringir leyes y regulaciones. Crea filtros personalizados para centrarte en tipos específicos de tráfico o paquetes que cumplen con ciertos criterios. Estos filtros se pueden guardar para futuras sesiones. Aquí encontraras muchos de los filtros que puedes usar para wireshark. Configura las columnas en la lista de paquetes de Wireshark. Añade, elimina o reordena columnas para resaltar la información más relevante para tu análisis. Información sobre preferencias de columna Aquí encontraras como funcionan los filtros de columna de wireshark Ajusta las configuraciones de Wireshark, incluyendo la resolución de nombres, formatos de tiempo, colores y fuentes, para adaptar la interfaz a tus necesidades. Preferencias de Wireshark Aquí encontraras todo sobre el menú de preferencias. Personaliza las reglas de colorización para identificar rápidamente patrones o problemas en el tráfico de red. Personalización de colores Aquí encontraras todo sobre la personalización de los colores para las tramas de wireshark. Crea perfiles de usuario con configuraciones, filtros y preferencias únicos. Ideal para diferentes tareas o usuarios compartiendo la misma instalación de Wireshark. Aquí encontraras como crear perfiles para wireshark Extiende las capacidades de Wireshark con Lua scripts o desarrollando tus propios plugins, añadiendo funcionalidades específicas. Solo para profesionales dentro del mundo de la programación. Sirve para automatizar tareas. Exporta los datos capturados por Wireshark y utiliza herramientas externas de visualización y análisis de datos para obtener perspectivas más detalladas. Para poder activar el modo monitor en wireshark primero deberemos saber que es. El modo promiscuo es una característica importante en el ámbito de las redes informáticas y de la herramienta Wireshark. Cuando una interfaz de red está configurada en modo promiscuo, puede capturar y ver todo el tráfico de red que pasa a través de esa interfaz, incluso si los paquetes de datos no están destinados específicamente a la dirección MAC de esa interfaz. Para poder activarlo en wireshark nos iremos a la pestaña de captura =>opciones y se nos abrirá el siguiente menú donde podremos ver todas las conexiones y cuales esta activadas en modo monitor, para poder activar el modo monitor de una conexión lo único que deberemos hacer es marcar la siguiente casilla. En Wireshark, la resolución de nombres se refiere al proceso de convertir direcciones IP en nombres de dominio legibles para los humanos. Por ejemplo, cuando ves una dirección IP en un paquete capturado en Wireshark, la resolución de nombres te permite ver el nombre de host asociado con esa dirección IP, lo que facilita la comprensión de qué dispositivos están involucrados en la comunicación de red. Para poder activar estas opciones no iremos a la pestaña edición y abajo del todo preferencias, una vez dentro nos iremos a la pestaña de name resolution y marcaremos las siguientes casillas. Y con esto terminaría nuestro apartado de personalización como puedes ver mucho por hacer! Descarga e Instalación en Diferentes Sistemas Operativos: Wireshark es compatible con varios sistemas operativos, lo que facilita su acceso desde diversas plataformas. A continuación, se detallan los pasos para descargar e instalar Wireshark en Windows, macOS y distribuciones Linux como Ubuntu. 1. Windows: Visita el sitio oficial de Wireshark. Selecciona la versión compatible con tu sistema (32 o 64 bits). Haz clic en «Installer for Windows» para descargar el instalador. Ejecuta el instalador descargado y sigue las instrucciones en pantalla. Durante la instalación, se te pedirá seleccionar los componentes. Puedes dejar las opciones predeterminadas para una instalación estándar. Una vez completada la instalación, Wireshark estará listo para su uso en tu sistema Windows. 2. macOS: En el sitio oficial de Wireshark, selecciona «macOS» en la sección de descargas. Descarga el archivo DMG (instalador) correspondiente. Abre el archivo DMG y arrastra el icono de Wireshark a la carpeta de Aplicaciones. Ejecuta Wireshark desde la carpeta de Aplicaciones. Durante la primera ejecución, es posible que se requieran permisos adicionales. Sigue las instrucciones para permitir el acceso. 3. Linux (Ubuntu): Abre la terminal. Ejecuta los siguientes comandos uno por uno: Durante la instalación, se te pedirá configurar Wireshark para permitir el acceso sin privilegios de superusuario. Selecciona «Sí» para esta opción. Estos pasos cubren las instalaciones básicas en los sistemas operativos mencionados. Adaptarlos para otras distribuciones Linux o sistemas operativos específicos es similar, y se puede encontrar información adicional en la documentación oficial de Wireshark. sudo apt update sudo apt install -y wireshark Wireshark: Wireshark es un analizador de protocolos de red que permite capturar y examinar datos en una red en tiempo real. Proporciona una interfaz gráfica de usuario (GUI) intuitiva y potente para el análisis de tráfico de red. Wireshark es capaz de mostrar información detallada sobre varios protocolos, filtrar paquetes según criterios específicos y ofrecer herramientas avanzadas para inspeccionar y entender el tráfico de red. TShark: TShark es la interfaz de línea de comandos de Wireshark. A diferencia de la interfaz gráfica de Wireshark, TShark opera en la línea de comandos y es ideal para situaciones en las que se necesita realizar análisis de tráfico de red de manera automatizada o en entornos sin interfaz gráfica. Permite realizar las mismas funciones que Wireshark pero de forma más automatizada y programática. External Capture Tools: Estos son componentes adicionales que complementan las capacidades de Wireshark y TShark. Cada uno de ellos tiene un propósito específico: androiddump: Captura tráfico de red en dispositivos Android. etwdump: Herramienta de captura para dispositivos ETW (Event Tracing for Windows). randpktdump: Genera paquetes de red aleatorios y los captura. sshdump: Captura tráfico de red relacionado con SSH (Secure Shell). ciscodump: Especializado en la captura de tráfico en redes Cisco. wifidump: Se centra en la captura de tráfico de redes Wi-Fi. udpdump: Captura paquetes UDP (User Datagram Protocol). Estas herramientas externas permiten extender las capacidades de Wireshark para abordar casos de uso específicos. Por ejemplo, si estás trabajando en una red Wi-Fi, wifidump puede ser una herramienta valiosa, mientras que ciscodump sería útil para analizar el tráfico en entornos basados en dispositivos Cisco. La selección de estas herramientas depende de los requisitos particulares de tu análisis de tráfico y del tipo de redes que estés investigando. Utilizamos Windows 11 para nuestras capturas de tráfico con Wireshark, pero en Linux o macOS, la experiencia es la misma gracias a su interfaz gráfica uniforme. Al iniciar Wireshark, lo primero que ves son todas las interfaces de red disponibles en tu ordenador. Por ejemplo, en nuestro caso, contamos con tres tarjetas de red y varias interfaces de red virtuales de VMware y Virtual Box. Wireshark te permite capturar tráfico de cualquier tarjeta de red, tanto física como virtual. Simplemente selecciona la tarjeta de red activa que deseas monitorizar a la cual accedemos con un doble clic. Si optas por una tarjeta de red Wi-Fi, Wireshark capturará todo el tráfico entrante y saliente, pero recuerda que no pondrá la tarjeta en modo monitor, así que solo verás los paquetes de tu dispositivo. Cuando haces doble clic en la interfaz de red seleccionada en Wireshark, la captura de tráfico, tanto entrante como saliente, comienza automáticamente. Sin embargo, para asegurarte de que esta captura sea lo más eficiente y relevante posible. Cerrar Programas Innecesarios: Antes de iniciar la captura, cierra todas las aplicaciones que puedan generar tráfico de fondo indeseado. Esto incluye clientes de correo, aplicaciones de mensajería instantánea, actualizaciones automáticas, etc Desactivar el Firewall Temporalmente: Los firewalls pueden bloquear o alterar el tráfico de red. Para una captura completa y sin restricciones, considera desactivar tu firewall. Capturar Tráfico Específico de Aplicaciones: Si tu objetivo es analizar el tráfico generado por una aplicación específica, sigue este protocolo: Espera un segundo después de iniciar la captura en Wireshark. Ejecuta la aplicación cuyo tráfico deseas capturar. Una vez finalizado tu análisis o prueba, cierra la aplicación. Espera otro segundo antes de detener la captura en Wireshark. Este proceso ayuda a aislar el tráfico de la aplicación, facilitando un análisis más específico y detallado. Uso de Filtros Durante la Captura: Aunque Wireshark captura todo el tráfico por defecto, puedes configurar filtros para capturar solo tipos específicos de tráfico. Monitorización de Redes Wi-Fi: Si estás capturando tráfico de una red Wi-Fi, ten en cuenta que Wireshark capturará solo el tráfico de tu dispositivo a menos que la tarjeta de red esté en modo monitor. Y dicho todo esto empezaremos a analizar paquetes, seleccionaremos la interfaz que os interese y empezara a funcionar; Explora el poder de Wireshark para capturar meticulosamente cada paquete de tu conexión. Esta herramienta no solo recoge la información, sino que la clasifica de manera intuitiva en categorías como «Origen», «Destino», «Protocolo», longitud e información adicional. Esta organización detallada te permite navegar y ordenar el tráfico capturado con una facilidad asombrosa. Ya sea que estés buscando por protocolo específico o rastreando una dirección IP particular, Wireshark hace que el análisis de tus datos sea una tarea sencilla y eficiente Con Wireshark, cada paquete de datos se convierte en un libro abierto. Esta herramienta te permite desplegar y explorar con gran detalle cada fragmento de información, desde la capa de aplicación hasta la física. Wireshark organiza la información por capas, facilitando la identificación y el análisis del contenido que necesitas. Ya sea que estés investigando en la capa de transporte o profundizando en los misterios de la capa de enlace, Wireshark te guía a través de estos niveles con facilidad y precisión, asegurando que no te pierdas nada importante en tus datos.. Wireshark va más allá en el análisis de red, proporcionándote detalles cruciales como los puertos de origen y destino en conexiones TCP o UDP. Además, te ofrece una visión avanzada de aspectos como los números de secuencia, identificando situaciones clave como reinicios de conexión (RST) o la necesidad de retransmitir segmentos debido a problemas en la red. Esta herramienta te brinda una perspectiva completa y detallada, esencial para entender a fondo el comportamiento y los eventos dentro de tu red. En la siguiente captura veréis como voy a hacer un login dentro de una página web y no solo se verá la solicitud http y la consulta DNS si no que si la página está mal securizada también veremos el login a través de wireshark lo que puede resultar bastante peligroso si es a ti a quien se lo hacen. Primero hemos visto como se ve perfectamente a través de la consulta DNS que es lo que el equipo de la red está buscando, pero lo que es mucho más asombroso es... y si filtramos http y en el filtro de cadena de texto ponemos el nombre de dicha página que nos ha mostrado la consulta DNS. Exacto tenemos el usuario y la contraseña increíble ¿verdad? Esta es una de las cosas mas básicas de wireshark imagina lo lejos que puede llegar. Por ultimo vamos a realizar una prueba básica, vamos a realizar un PING a google.es y veréis como wireshark captura perfectamente los ICMP Realizar y guardar una captura de tráfico con Wireshark es sencillo. Después de capturar los datos, pulsa el botón de «Stop» y luego guarda la captura desde «File / Save». Ten en cuenta que al compartir estas capturas debes hacerlo con alguien de confianza, ya que contendrán todo el tráfico capturado. Para tráfico encriptado como TLS, IPsec o WPA/WPA2, se necesitará la clave de descifrado para acceder a los datos. Además, algunos sistemas operativos de routers y firewalls tienen capturadores de paquetes integrados que permiten capturar tráfico específico, reduciendo la cantidad de datos capturados. Estas capturas se pueden exportar en formato pcap y luego analizar en Wireshark con todos sus filtros, facilitando la identificación de problemas o configuraciones incorrectas en la red. Protocolo: Puedes filtrar por protocolo utilizando su nombre. Por ejemplo, «tcp», «udp», «http», «dns», etc. Dirección IP: Para filtrar por una dirección IP específica, puedes utilizar los operadores «src» (fuente) y «dst» (destino). Por ejemplo, «ip.src == 192.168.1.1» o «ip.dst == 8.8.8.8». Puerto: Puedes filtrar por puertos utilizando los operadores «srcport» y «dstport». Por ejemplo, «tcp.srcport == 80» o «udp.dstport == 53». Dirección MAC: Puedes filtrar por dirección MAC utilizando los operadores «ether.src» y «ether.dst». Filtros lógicos: Puedes combinar múltiples condiciones utilizando operadores lógicos como «and», «or» y «not». Por ejemplo, «tcp.port == 80 and ip.src == 192.168.1.1». Filtros de rango de direcciones IP: Puedes filtrar direcciones IP dentro de un rango utilizando la notación CIDR. Por ejemplo, «ip.src == 192.168.0.0/16» para filtrar todas las direcciones IP en el rango 192.168.x.x. Filtros de longitud de paquete: Puedes filtrar por la longitud de los paquetes utilizando los operadores «len». Por ejemplo, «tcp.len > 100» para filtrar paquetes TCP con longitud mayor a 100 bytes. Filtros de tiempo: Puedes filtrar por tiempo utilizando el operador «time». Por ejemplo, «frame.time_relative > 10» para filtrar paquetes capturados más de 10 segundos después del inicio de la captura. Wireshark es una herramienta versátil que se puede utilizar en diversos escenarios para analizar y diagnosticar problemas en redes. Aquí tienes algunos posibles usos: Identifica y resuelve problemas de conectividad, rendimiento o seguridad en una red. Cómo utilizar: Captura paquetes durante el período del problema y analiza el tráfico para identificar posibles anomalías. Analiza el tráfico para mejorar el rendimiento de la red y optimizar el uso del ancho de banda. Cómo utilizar: Identifica patrones de tráfico, detecta cuellos de botella y ajusta la configuración de la red según sea necesario. Detecta actividades maliciosas, intrusiones o amenazas en la red. Cómo utilizar: Examina el tráfico en busca de patrones sospechosos, identifica posibles ataques y fortalece la seguridad de la red. Estudia el comportamiento de los protocolos utilizados en la red. Cómo utilizar: Examina la información de los paquetes para entender cómo interactúan los dispositivos y aplicaciones en la red. Ayuda en el desarrollo y la depuración de aplicaciones que utilizan la red. Cómo utilizar: Captura paquetes generados por la aplicación, analiza las interacciones y corrige posibles problemas de comunicación. Observa el tráfico web para entender el comportamiento de los usuarios o solucionar problemas de carga. Cómo utilizar: Filtra los paquetes relacionados con el tráfico web y analiza las solicitudes y respuestas HTTP. Garantiza que la red cumpla con políticas y estándares establecidos. Cómo utilizar: Analiza el tráfico para verificar el cumplimiento de políticas de seguridad y protocolos establecidos. Estos son solo algunos ejemplos de cómo Wireshark puede ser una herramienta valiosa en diferentes situaciones. Su versatilidad y capacidad para proporcionar información detallada hacen que sea esencial en el arsenal de cualquier profesional de redes. En nuestra página web, destacamos la importancia de la seguridad en la autenticación SSH. Es crucial reconocer que, si un atacante logra acceder a un sistema que opera un servidor SSH, podría realizar ataques de credential stuffing con relativa facilidad. Este riesgo se agrava por la tendencia generalizada de usar contraseñas predecibles o, lo que es más riesgoso, repetir la misma contraseña en múltiples cuentas. Esta práctica facilita que los ataques de credential stuffing pasen inadvertidos en muchos casos. Identificar intentos de acceso SSH exitosos de los fallidos puede no ser evidente a primera vista en herramientas como Wireshark. Sin embargo, hay ciertos indicadores clave que pueden ayudarnos a discernir entre ambos: Duración de la Sesión: Una sesión SSH exitosa tiende a ser más larga que una fallida. Observar la longitud de la sesión puede proporcionar pistas sobre su éxito. Tamaño del Paquete: Los servidores SSH generan respuestas específicas para autenticaciones exitosas y fallidas. Al examinar el tamaño de los paquetes SSH, podemos inferir que aquellos de mayor tamaño suelen corresponder a sesiones exitosas. Tiempo de Vida del Paquete: Los paquetes que implican interacción del usuario en una autenticación exitosa generalmente tienen un tiempo de vida más prolongado que aquellos generados por intentos automatizados y fallidos. Además, recomendamos monitorear el número de intentos de inicio de sesión. Un volumen inusual de estos puede ser un indicativo de un posible ataque de credential stuffing. Mantenerse alerta a estas señales es crucial para la seguridad de tu infraestructura SSH. Te presento un análisis de Wireshark, pero con un toque más dinámico. Imagina que estás frente a una pantalla de cine, y en ella, ¡zas!, una sesión de Telnet captada por Wireshark se despliega ante tus ojos. Aquí, cada paquete es un susurro en el vasto mundo de la red, contándonos historias de intentos de inicio de sesión. ¡Atención aquí! Estamos viendo algo que huele a credential stuffing: una serie de intentos de autenticación que llegan uno tras otro, rápidos como centellas. Es como una carrera de velocidad en el mundo digital, donde los patrones de tráfico nos dan pistas jugosas. Momento clave: Algunos de estos intentos podrían ser más robóticos que tu aspiradora inteligente, automatizados al máximo. Si ves sesiones que se repiten con la precisión de un reloj suizo, levanta la ceja, porque algo automatizado está en marcha. Aquí va un dato curioso: Las sesiones que se extienden más que un maratón de tu serie favorita suelen significar «¡Bingo, acceso conseguido!», mientras que las que son más cortas que un video de TikTok suelen terminar en un «Intento fallido». Y para rematar, ese variado tiempo de respuesta entre paquetes nos susurra al oído la diferencia entre un ser humano tecleando y un script de ataque que trabaja a toda máquina. Uno de los mayores inconvenientes y riesgos generados a partir del auge de tecnologías emergentes como el Internet de las Cosas es que los dispositivos habilitados cuentan con SSH habilitado en primera instancia. Normalmente, sus sistemas asociados acostumbran a utilizar las credenciales por defecto o con alguna modificación mínima. ¿Por qué esto es un riesgo? Cualquiera que tenga conocimiento acerca de esas contraseñas o la capacidad de adivinar las usuarios y contraseñas, puede fácilmente acceder remotamente a las máquinas. Cómo Detectar Vulnerabilidades: Filtrando en Wireshark las solicitudes y el tráfico SSH interno, además del proveniente de direcciones IP externas, ayudará a identificar situaciones sospechosas. Identifica tráfico SSH proveniente de direcciones IP desconocidas a tu red interna como señal de una posible vulneración de la red. Patrones de Acceso Inusual: Analiza todo el tráfico SSH para establecer patrones de acceso, tanto usuales como inusuales. Un alto nivel de tráfico proveniente de una sola máquina o solicitudes a sistemas que normalmente no lo haría son señales de posibles ataques. Monitoreo en Redes Corporativas: Controla y bloquea el tráfico SSH en la red según sea necesario. Monitorea las comunicaciones y el tráfico en general para detectar cualquier anormalidad. Uso en Educación: Wireshark puede ser útil en la educación para estudiantes y profesores, ayudándoles a comprender cómo transcurren los paquetes por las redes y formándolos en diferentes aspectos, desde técnicos de redes hasta hackers éticos. Haz clic en «Inicio» para iniciar la captura de paquetes. Realiza las acciones en la red que deseas analizar mientras Wireshark está en ejecución. Examina los paquetes capturados para identificar patrones, comportamientos anómalos o posibles problemas de seguridad. Utiliza las estadísticas y gráficos de Wireshark para un análisis más profundo. Exporta los resultados de la captura en un formato legible. Puedes guardarlos como archivos .pcap para revisarlos más tarde o compartirlos con otros expertos en seguridad. Documenta tus hallazgos de manera detallada. Si encuentras vulnerabilidades, informa al propietario de la red y ofrece recomendaciones para solucionar los problemas. Si durante el escaneo se capturó información sensible, asegúrate de eliminarla de manera segura y notificar a las partes afectadas si es necesario. Recuerda siempre actuar dentro de los límites éticos y legales al realizar escaneos de accesos remotos. La transparencia y la colaboración son clave para garantizar un uso adecuado de esta poderosa herramienta de análisis de redes. La exportación de datos en Wireshark es esencial para analizar y compartir información capturada. Aquí te guiamos a través del proceso de exportación y las opciones disponibles. Antes de exportar, selecciona los paquetes específicos que deseas incluir. Puedes utilizar filtros para refinar tu selección y centrarte en la información relevante. Ve a «Archivo»: Abre Wireshark y selecciona la pestaña «Archivo» en la barra de menú. Selecciona «Exportar»: En el menú desplegable de «Archivo», elige la opción «Exportar». Wireshark ofrece varios formatos de exportación. Las opciones comunes incluyen: Archivo de Texto: Ideal para exportar texto plano con información básica sobre los paquetes. Archivo CSV: Útil para exportar datos en formato de valores separados por comas, facilitando su apertura en hojas de cálculo. Archivos de Captura Comprimidos: Permite empaquetar múltiples capturas en un solo archivo comprimido, simplificando el intercambio. Exportación de Datos Específicos: Dependiendo de tus necesidades, puedes exportar solo datos específicos, como las conversaciones, seguimiento TCP, o información sobre paquetes seleccionados. Algunos formatos permiten opciones de personalización. Por ejemplo, al exportar como CSV, puedes elegir qué campos incluir. Asegúrate de revisar y ajustar estas opciones según tus requerimientos. Finaliza el proceso seleccionando la ubicación de guardado y confirmando la exportación. Asegúrate de guardar el archivo en un lugar accesible y con un nombre descriptivo. Wireshark te permite aplicar filtros incluso durante el proceso de exportación. Esto significa que puedes exportar solo los datos que cumplen con ciertos criterios, haciendo que la información sea más manejable. La exportación de datos en Wireshark es una herramienta poderosa para analizar, compartir y archivar información capturada. Aprovecha las diversas opciones de exportación para adaptar la salida a tus necesidades específicas. En la vanguardia de la ética en la seguridad de redes, establecemos directrices claras para el uso responsable de herramientas de análisis como Wireshark. Aquí destacamos las prácticas esenciales: Consentimiento Informado: El primer paso y no negociable es obtener el consentimiento explícito del propietario de la red. Sin él, no hay análisis ético posible. Uso Legal y Responsable: Adhiriéndose a la legalidad, Wireshark debe ser una herramienta de análisis, nunca un medio para comprometer la seguridad de la red. Transparencia Operativa: La transparencia no solo es ética, sino que también es estratégica. Informar a los usuarios sobre la naturaleza y el propósito del análisis de tráfico refuerza la confianza. Protección de la Privacidad: Es vital respetar y proteger la información personal. Si se capturan datos sensibles, es esencial que se eliminen de manera segura y eficiente. Colaboración Proactiva: La detección de vulnerabilidades debe ser seguida de una comunicación inmediata con los administradores de la red, ofreciendo asistencia para solucionar cualquier problema. Educación Continuada: Mantente actualizado sobre las mejores prácticas y las últimas actualizaciones en el campo de la seguridad de redes para garantizar un uso efectivo y ético de las herramientas de análisis. La seguridad al utilizar Wireshark es crucial para evitar riesgos y proteger la integridad de la red. Aquí hay algunas medidas de seguridad que debes considerar al emplear Wireshark: Fuentes Confiables: Descarga Wireshark solo desde fuentes confiables, como el sitio web oficial. Evita versiones modificadas o no verificadas que podrían contener malware. Actualizaciones Regulares: Mantén Wireshark actualizado con las últimas versiones y parches de seguridad. Las actualizaciones periódicas suelen corregir vulnerabilidades. Firewalls y Antivirus: Asegúrate de tener un firewall y software antivirus activos. Estas medidas adicionales ayudarán a proteger tu sistema mientras utilizas Wireshark. Entorno Controlado: Realiza capturas de red en un entorno controlado o en redes de prueba. Evita utilizar Wireshark en redes de producción sin la debida autorización. Análisis Seguro: Al analizar paquetes capturados, hazlo en un entorno seguro. Evita exponer información sensible y utiliza mecanismos de cifrado si es necesario. Contraseñas Seguras: Usa contraseñas fuertes para proteger archivos de capturas y configuraciones de Wireshark. Limita el acceso a usuarios autorizados. El uso de Wireshark debe ser legal y ético. Aquí hay algunas consideraciones legales y éticas importantes al emplear esta herramienta: Consentimiento Informado: Obtén el consentimiento informado antes de realizar capturas en una red. Asegúrate de que los propietarios de la red y los usuarios afectados estén al tanto y den su permiso. Cumplimiento Legal: Asegúrate de cumplir con todas las leyes y regulaciones locales relacionadas con el monitoreo de redes. El incumplimiento puede tener consecuencias legales. Privacidad del Usuario: Respeta la privacidad de los usuarios al evitar la captura y análisis de datos sensibles. Evita actividades que puedan comprometer la seguridad y privacidad. Propósito Legítimo: Utiliza Wireshark solo con propósitos legítimos y autorizados. Evita el uso malicioso o la violación de la seguridad de la red. No Desencriptar sin Autorización: No intentes desencriptar el tráfico cifrado sin la debida autorización. Este acto puede ser ilegal y violar la privacidad. Educación Continua: Mantente informado sobre las leyes y prácticas éticas en constante evolución relacionadas con el monitoreo de redes. La educación continua es esencial. Al seguir estas medidas de seguridad y consideraciones legales, podrás utilizar Wireshark de manera segura, ética y legal, contribuyendo así a un entorno de red más seguro y protegido. Wireshark es una herramienta poderosa, pero existen otras alternativas que también ofrecen características destacadas para el análisis de tráfico de red. Aquí te presentamos algunas opciones: Tcpdump es una herramienta de línea de comandos que proporciona captura y análisis de paquetes en sistemas basados en Unix. Ventajas: Ligero y eficiente. Ideal para entornos basados en texto. Ofrece una variedad de opciones de filtrado. CloudShark: Network Analysis, Evolved. Cloudshark es una plataforma en línea que permite cargar, compartir y analizar capturas de paquetes directamente desde el navegador. Ventajas: Acceso remoto a análisis de tráfico. Colaboración en tiempo real. Interfaz intuitiva basada en web. SmartSniff es una herramienta de captura de paquetes para Windows que muestra la información detallada de los paquetes capturados. Ventajas: Interfaz gráfica fácil de usar. Filtrado y búsqueda avanzados. Compatible con varias versiones de Windows. Capsa es una solución de análisis de red que ofrece funciones avanzadas, incluyendo diagnóstico de red, detección de problemas y análisis de seguridad. Ventajas: Análisis en tiempo real. Informes detallados y gráficos.. es una herramienta de línea de comandos que forma parte del conjunto de herramientas Wireshark, que se utiliza para el análisis de tráfico de red. Ventajas Análisis en tiempo rea. Flexibilidad y personalización. Estas alternativas ofrecen diferentes enfoques y características, por lo que la elección dependerá de tus necesidades específicas y preferencias. Experimenta con varias herramientas para encontrar la que mejor se adapte a tu entorno y objetivos de análisis de red. ¡Wireshark, el héroe oculto de la red! Con su capacidad para desentrañar los misterios del tráfico de red, es como el detective astuto que siempre está un paso adelante. Pero no te preocupes, aunque nos despidamos, siempre estará ahí, listo para sumergirse en los entresijos de los paquetes de datos. ¡Hasta la próxima aventura, querido Wireshark! Que tus capturas sean siempre claras y tus filtrados, precisos. Se, algum dia, você estiver solucionando problemas de rede e precisar inspecionar pacotes individuais, use o Wireshark. O Wireshark é uma ferramenta padrão e essencial para capturar e analisar tráfego de rede que você precisa conhecer. Já que o Wireshark é a ferramenta mais importante para esse trabalho, vamos falar sobre alguns pontos principais: onde baixar, como capturar pacotes de rede, como usar os filtros do Wireshark entre outros. O que é o Wireshark? O Wireshark é um programa de software para análise de protocolo de rede em código aberto criado por Gerald Combs em 1998. Uma organização mundial de especialistas em rede e desenvolvedores de software mantém o Wireshark e continua disponibilizando atualizações tanto para novas tecnologias de rede quanto para novos métodos de criptografia. O uso do Wireshark é completamente seguro. Órgãos públicos, empresas, organizações sem fins lucrativos e instituições de ensino usam o Wireshark para solução de problemas e com fins pedagógicos. Não há uma forma melhor de aprender redes do que observar o tráfego através do microscópio do Wireshark. Há dúvidas sobre a legalidade do Wireshark, visto que se trata de um poderoso analisador de pacotes. O lado luminoso da Força afirma que você só deve usar o Wireshark nas redes em que tem permissão para inspecionar pacotes de dados. Recorrer ao Wireshark para examinar pacotes sem permissão é um caminho para o lado Sombrio. Como o Wireshark funciona? O Wireshark é uma ferramenta de análise de pacotes e sniffer de rede. Ele captura o tráfego de rede na rede local e armazena esses dados para análise offline. O Wireshark captura o tráfego de rede Ethernet, Bluetooth, sem fio (IEEE.802.11), token ring, conexões frame relay, entre outros. N.E.: um "pacote" é uma mensagem unitária de qualquer protocolo de rede (ou seja, TCP, DNS etc.) N.E. ²: O tráfego de LAN fica em modo de transmissão. Isso significa que um único computador com Wireshark instalado pode monitorar o tráfego entre dois outros computadores. Se você quiser analisar o tráfego de um site externo, precisará capturar os pacotes no computador local. O Wireshark permite filtrar o log antes do início da captura ou durante a análise. Assim, você pode afunilar e focar aquilo que procura no rastreamento da rede. Por exemplo, é possível definir um filtro para monitorar o tráfego em rede TCP entre dois endereços IP. Você pode configurar o filtro para mostrar apenas os pacotes enviados de um computador. Os filtros no Wireshark são um dos principais motivos que fizeram dele a ferramenta padrão para análise de pacotes. Como baixar o Wireshark Baixar e instalar o Wireshark é fácil. O primeiro passo é consultar a página oficial de download do Wireshark para o sistema operacional que você usa. A versão básica do Wireshark é gratuita. Wireshark para Windows O Wireshark tem duas versões para o Windows: 32 bits e 64 bits. Selecione a correta para o seu sistema operacional. Até a data de publicação deste artigo, a versão atual é a 3.0.3. A instalação é muito simples e não deve causar problemas. Wireshark para Mac O Wireshark está disponível para o Mac através do Homebrew. Para instalar o Homebrew, é preciso executar o seguinte comando no Terminal: /usr/bin/ruby -e "$(curl -fsSL " Após instalar o sistema Homebrew, é possível acessar vários projetos de código aberto para o seu Mac. Para instalar o Wireshark, execute o comando a seguir no Terminal: brew install wireshark O Homebrew fará o download e instalará o Wireshark e quaisquer dependências para que o programa seja executado corretamente. Wireshark para Linux Instalar o Wireshark no Linux pode variar um pouco dependendo da distribuição. Se você não estiver usando uma das distribuições abaixo, verifique os comandos. Ubuntu No terminal, execute estes comandos: sudo apt-get install wireshark sudo dpkg-reconfigure wireshark-common sudo adduser $USER wireshark Além de baixarem e atualizarem o pacote, esses comandos concedem privilégios de nível administrativo para executar o Wireshark. Red Hat Fedora No terminal, execute estes comandos: sudo dnf install wireshark-qt sudo usermod -a -G wireshark username O primeiro comando instala as versões de interface GUI e CLI do Wireshark, enquanto o segundo concede permissões para usar o Wireshark. Kali Linux O Wireshark provavelmente já está instalado! Ele faz parte do pacote básico. Vá até o menu para confirmar. Fica na opção "Sniffing & Spoofing". Pacotes de dados no Wireshark Agora que o Wireshark está instalado, vamos ver como habilitar o sniffer de pacotes do Wireshark e como analisar o tráfego de rede. Como capturar pacotes de dados no Wireshark Ao abrir o Wireshark, uma lista de todas as conexões de rede que você pode monitorar aparece na tela. Há também um campo para filtro de captura, assim você captura apenas o tráfego de rede que deseja monitorar. É possível selecionar uma ou mais interfaces de rede com a tecla "shift" e o botão esquerdo do mouse. Após selecionar a interface de rede, você pode iniciar a captura. Há várias maneiras de fazer isso. Clique em "Start Capturing Packets", o primeiro botão da barra de ferramentas. Uma opção é clicar em Capture -> Start no menu. Outra é apertar as teclas "Ctrl" + "E". Durante a captura, o Wireshark mostrará os pacotes que está capturando em tempo real. Quando todos os pacotes que você precisa tiverem sido capturados, use as mesmas teclas ou clique nas mesmas opções de menu para interromper a captura. É recomendado interromper a captura de pacotes no Wireshark antes de fazer a análise. Como analisar pacotes de dados no Wireshark O Wireshark exibe três painéis diferentes para inspecionar dados de pacotes. O painel superior, intitulado "Packet List", tem uma lista com todos os pacotes da captura. Ao clicar em um pacote, os outros dois painéis se alteram para mostrar detalhes sobre o pacote selecionado. Também é possível ver se o pacote faz parte de uma conversation, ou seja, o tráfego entre dois endpoints específicos. Alguns detalhes sobre cada coluna do painel superior: No.: representa a posição numérica do pacote capturado. O colchete indica que este pacote faz parte de uma conversation. Time: mostra quanto tempo levou do início da captura até a captura do pacote. É possível mudar o formato de exibição desses números, caso você queira algo diferente. Source: é o endereço do sistema que enviou o pacote. Destination: é o endereço de destino do pacote. Protocol: indica o tipo de pacote, por exemplo, TCP, DNS, DHCPv6 ou ARP. Length: exibe o tamanho do pacote em bytes. Info: apresenta mais informações sobre o conteúdo do pacote. Essa coluna varia de acordo com o tipo de pacote. "Packet Details", o painel do meio, exibe o máximo possível de informações legíveis sobre o pacote, dependendo do tipo de pacote. Clicando com o botão direito do mouse, você pode criar filtros com base no texto destacado neste campo. O painel inferior, "Packet Bytes", mostra o pacote exatamente como ele foi capturado em hexadecimal. Ao examinar um pacote que faz parte de uma conversation, você pode clicar no pacote com o botão direito do mouse e selecionar "Follow" para ver apenas os pacotes que fazem parte dessa conversation. Filtros do Wireshark Uma das melhores funcionalidades do Wireshark são os filtros de captura e os filtros de exibição. Os filtros permitem que você visualize a captura da maneira necessária para solucionar os problemas em questão. Como uma forma de incentivo, compilamos alguns filtros. Veja abaixo. Filtros de captura do Wireshark Os filtros de captura restringem os pacotes capturados ao filtro. Ou seja, se os pacotes não corresponderem ao filtro, não serão salvos pelo Wireshark. Confira agora alguns exemplos de filtros de captura: host IP-address: limita a captura ao tráfego com origem no e destino ao endereço IP. net 192.168.0.0/24: captura todo o tráfego na subnet. dst host IP-address: captura pacotes enviados para o host especificado. port 53: captura o tráfego apenas na porta 53. port not 53 and not arp: captura todo o tráfego, exceto tráfego DNS e ARP. Filtros de exibição do Wireshark Os filtros de exibição do Wireshark alteram a visualização da captura durante a análise. Depois de interromper a captura de pacotes, use os filtros de exibição para filtrar os pacotes no painel Packet List. Assim, você pode solucionar o problema. O filtro de exibição mais útil (de acordo com a minha experiência) é: ip.src==IP-address and ip.dst==IP-address Esse filtro mostra os pacotes de um computador (ip.src) para outro (ip.dst). Também é possível usar o ip.addr para mostrar pacotes com origem no e destino ao endereço IP. Confira mais alguns filtros a seguir: tcp.port eq 25: mostrará todo o tráfego na porta 25, que geralmente é tráfego SMTP. icmp: exibirá apenas o tráfego ICMP na captura. Provavelmente são pings. ip.addr != IP_address: apresenta todo o tráfego, com exceção do tráfego de ou para o computador especificado. Analistas até criam filtros para detectar ataques específicos, como o seguinte filtro para detectar o Sasser: ls_ads.opnum==0x09 Funcionalidades adicionais do Wireshark Além da captura e dos filtros, há várias outras funcionalidades do Wireshark que podem facilitar sua vida. Configurações de Cores no Wireshark É possível configurar o Wireshark para colorir os pacotes no painel Packet List de acordo com o filtro de exibição. Isso permite evidenciar os pacotes que você deseja destacar. Confira alguns exemplos aqui. Modo Promiscuous no Wireshark Como padrão, o Wireshark captura apenas pacotes com destino ao ou origem no computador onde está sendo executado. Quando você selecionar "run Wireshark in Promiscuous Mode" nas configurações de captura, é possível capturar a maior parte do tráfego na rede local (LAN). Linha de comando do Wireshark O Wireshark disponibiliza uma interface de linha de comando (ILC), caso o seu um sistema operacional não tenha uma GUI. O recomendado seria usar a ILC para capturar e salvar um log e, assim, revisar esse log com a GUI. Comandos do Wireshark wireshark : executa o Wireshark no modo GUI. wireshark –h : exibe os parâmetros disponíveis para linha de comandos no Wireshark. wireshark –a duration:300 –i eth1 –w wireshark. : captura o tráfego na interface Ethernet 1 por 5 minutos. "–a" significa parar automaticamente a captura, "-i" especifica qual interface capturar. Métricas e estatísticas Na opção "Statistics" do menu, você encontrará uma infinidade de opções para mostrar detalhes sobre sua captura. Propriedades do arquivo de captura: Gráfico I/O do Wireshark: Recursos e tutoriais extras para o Wireshark Há muitos tutoriais e vídeos que ensinam como usar o Wireshark para fins específicos. Seu ponto de partida deve ser o site do Wireshark. Lá, você encontrará a documentação oficial do programa e uma página colaborativa no modelo Wiki. Embora o Wireshark seja uma ótima ferramenta de análise e sniffer de rede, é melhor utilizado, na minha opinião, quando você sabe o que está procurando. Você não vai usar o Wireshark para encontrar um novo problema. Há muito ruído na rede. Você precisa de uma ferramenta como o Edge da Varonis, que vai ajudar a entender a situação geral e indicar uma ameaça para ser investigada. Em seguida, o Wireshark pode ser utilizado para se aprofundar e entender exatamente o que há nos pacotes perigosos. Por exemplo, quando os pesquisadores de segurança da Varonis descobriram o Norman CryptoMiner, eles receberam um alerta da Varonis que indicava atividades suspeitas na rede e nos arquivos de várias máquinas. Durante a análise do minerador de criptomoedas, os pesquisadores da Varonis usaram o Wireshark para inspecionar as atividades de rede em algumas das máquinas que estavam se comportando de forma inadequada. O Wireshark mostrou à equipe de pesquisa que um novo minerador de criptomoedas, o Norman, estava se comunicando ativamente com servidores de comando e controle (C&C) usando o DuckDNS. No Wireshark, a equipe da Varonis conseguiu ver todos os endereços IP dos servidores C&C utilizados pelos invasores. Dessa forma, a empresa desligou a comunicação e interrompeu o ataque. Para ver a equipe da Varonis em ação, inscreva-se em uma demonstração de ataque cibernético em tempo real. Escolha o horário que for melhor para você! Tener el tráfico de una red controlado, es algo que nos puede ayudar en muchas circunstancias diferentes. Es por ello que es de vital importancia contar con herramientas de escaneo que sean eficientes, y sean altamente adaptables a las necesidades de cada sistema donde se implementen. Entre las opciones que tienes disponible para escanear de manera eficiente los paquetes de red lo cierto es que puedes utilizar Wireshark. Por esto mismo, en este artículo te explicaremos todos los detalles más importantes, entre ellos, cómo se descarga y se instala, al igual que los diferentes usos que te ofrece esta herramienta. Qué es Wireshark Este programa que es completamente gratuito, nos permite realizar inspección profunda de cientos de protocolos, ya que soporta protocolos de capa física, de enlace, protocolos de red, capa de transporte y también capa de aplicación. Nos permitirá realizar una captura en tiempo real, y cuando hayamos terminado de capturar todos los paquetes que entran y salen de nuestra tarjeta de red cableada o inalámbrica, podremos realizar un análisis en profundidad de manera offline, es decir, en otro ordenador (o en el mismo) y en cualquier momento. Wireshark permite ver todo el tráfico capturado vía GUI con el propio programa, no obstante, también podremos ver toda la información capturada con el programa TShark, una herramienta que funciona a través de consola y nos permitirá leer todo a través de la línea de comandos CLI, para ver todo vía SSH, por ejemplo. Una característica fundamental de cualquier analizador de paquetes son los filtros, para que únicamente nos muestre lo que queremos que nos muestre, y ninguna información más que nos generaría un trabajo extra. Wireshark es capaz de leer y escribir en diferentes formados de captura, como en formato tcpdump (libpcap), pcap ng, y otras muchas extensiones, para adaptarse perfectamente a los diferentes programas para su posterior análisis. Otro aspecto importante es que la captura realizada se puede comprimir con GZIP al vuelo, y, por supuesto, descomprimirla al vuelo también en caso de que estemos leyendo la captura. Por supuesto, es capaz de leer datos de diferentes tecnologías de redes como Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI y otros. Hoy en día tenemos muchos protocolos con datos cifrados, con la clave privada adecuada, Wireshark es capaz de descifrar el tráfico de diferentes protocolos como IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, y WPA/WPA2. Hay que tener en cuenta que esta herramienta lo cierto es que resulta bastante sencilla de usar. Por lo que no tiene ningún tipo de misterio. Además, puedes usarla desde un PC con Windows si quieres o también llegar a ejecutarla desde macOS o Linux. Por lo que podrás hacer uso de este programa desde diferentes sistemas operativos sin ningún tipo de inconveniente. Ventajas de Wireshark En el momento de usar esta herramienta en particular, hay que hablar de las distintas ventajas que ofrece, ya que de esta manera se puede conseguir saber si merece o no la pena. Y es que, sin duda alguna, utilizar Wireshark tiene muchos beneficios y es un programa que nos va a aportar muchas ventajas en el día a día… Versátil: Se trata de un programa muy versátil que puede soportar más de 480 protocolos diferentes, que nos da la opción de trabajar con los datos que capturemos en una red durante una sesión, mediante la utilización de paquetes. Estos los podemos almacenar para luego analizar. tcpdump: Soporta un formato de archivos estándar llamado tcpdump, que nos permite reconstruir sesiones TCP. Todo esto apoyado por una interfaz gráfica bastante accesible si se tiene un poco de práctica, y relativamente sencilla de aprender si es la primera vez que le damos uso. Muchas funciones: Sus funciones son muy buenas de cara a los administradores, que lo pueden usar para resolver problemas en sus redes de forma que se pueden ver excesos de tráfico o sobreconsumos. También puede ayudar a resolver fallos en la seguridad y a su vez, ayudar a prevenirlos. A niveles de desarrollo. A niveles de desarrollo se puede usar para realizar la depuración de la implementación de protocolos de red. A nivel educativo. Es una buena herramienta para aprender cómo funciona una red, e ir descifrando la información que pueden contener los paquetes de los dispositivos que están conectados a la red que estamos analizando. Podremos ver información como usuarios, contraseñas, mensajes, incluso podemos averiguar la marca y modelo de los dispositivos que se encuentran en la red. Multiplataforma. Se puede ejecutar en los sistemas operativos más conocidos como Windows, Linux, OS X, entre otros. Actualizado. Se sigue actualizando con frecuencia. Esto no solo incluye nuevas funcionalidades, si no que también recibe muchos parches de seguridad. Desventajas de Wireshark Una vez que ya se conocen las diferentes ventajas que hay con el uso de esta herramienta en particular, está claro que también es importante conocer los puntos en contra que tiene este programa. Por lo tanto, si hablamos de las desventajas, hay que mencionar los 'contras'. Pero, lo positivo de esta opción es que no encontramos grandes inconvenientes, incluso tratándose de un programa con tantas características y potente, no resulta complejo de utilizar. Pero podemos decir que si es la primera vez que lo usamos o somos novatos en el mundo de las redes, descifrar los

paquetes puede resultar complicado hasta que se toman un tiempo para comprender completamente la forma en que funciona el software, pero creemos que la mayoría de las personas se encontraran bien con la forma en que funciona el software. No hay mucho que podamos decir en general que nos disguste, ya que el software funciona bien y cumple con la función para la que fue creado que no es otra que leer los paquetes, seguirlos y rastrear todos los datos que pasan por la red. En todo caso esto con el paso del tiempo, aprenderemos a interpretarlo. Otra posible desventaja que podemos encontrarnos con Wireshark, es el hecho de que requiere privilegios elevados para realizar la captura de paquetes, esta característica puede resultar ser mala o buena según la perspectiva desde la que se observe, ya que a nivel de seguridad, puede ser ventajosa, pero a nivel de usuario puede ser un engorro tener que solicitar autorización para realizar una simple revisión o rastreo de paquetes. Además de esto, tiene también la desventaja estándar de capturar paquetes que podrían no reflejar el tráfico real de la red porque los datos se capturan localmente, esto no es un fallo de Wireshark, específicamente, sino de cualquier software de rastreo ejecutado localmente. La aplicación a pesar de que es bastante buena en lo que hace, y además de eso no tiene ningún competidor claro al menos a nivel gratuito, se le agradecería aplicar un procesamiento de datos más potente, ya que en muchas ocasiones a pesar de tener un equipo en condiciones, puede pecar en este aspecto a la propia aplicación y dar la impresión de que le falta un poco de potencia para dicho procesamiento de datos. Y por último, destacar que puede ralentizar el rendimiento de nuestro equipo cuando tenemos que lidiar con mucho tráfico y un período de monitoreo prolongado, ya que a pesar de que la aplicación, insistimos, es muy buena en lo que hace, a pesar de tener un equipo con buenas prestaciones, en muchas ocasiones parece que consume muchos más recursos de los que deberían ser necesarios para un simple análisis de tráfico. Capacidad de personalización Wireshark ofrece una gran gama de opciones que nos permiten personalizar la experiencia de usuario, adaptándose así a las necesidades de cada uno. Esto nos permite aprovechar todas sus características al máximo, así como las funciones que el programa nos proporciona. Algunos de los puntos más importantes son: Interfaz: La interfaz de Wireshark es bastante personalizable. Esta se puede establecer con otra disposición, o incluso con otra apariencia gráfica para el usuario. Entre los cambios más utilizados, están el ajuste de tamaño y la ubicación de todos los paneles, así como la elección de diferentes esquemas de colores para que la visibilidad sea diferente. Filtros: Es uno de los apartados más amplios de esta solución. Cuenta con gran cantidad de filtros en todo su paquete. Pero eso no es algo que nos limite si falta alguno, y es que tendremos la posibilidad de crear nuevos filtros personalizados. En estos, podremos establecer también un gran abanico de parámetros para que los resultados que nos proporciona sean diferentes. Perfiles de configuración: Que cada usuario cuente con su propio entorno de trabajo es muy útil. Esto por lo general incluye los cambios que hemos visto previamente, así como otras personalizaciones al gusto de cada uno. Con la posibilidad de cambiar perfiles, se puede optimizar el flujo de trabajo de una forma mucho más eficiente. Columnas: Wireshark cuenta con unas columnas que se muestran en la vista de resumen de paquetes. Esto es algo que cada usuario puede eliminar y reorganizar de la forma que más se adapta al mismo. También es posible cambiar el formato, así como la información que nos muestra cada una de las columnas dependiendo de nuestras preferencias. Scripts y complementos: Esta herramienta permite la creación de scripts, los cuales se pueden escribir en LUA y en Python. Principalmente siempre es buscando automatizar tareas, crear nuevos tipos de análisis, o incluso agregar nuevas características personalizadas. Una vez que hemos visto las principales características, solo queda saber cómo podemos descargarlo e instalarlo. Descarga e instalación Este programa es completamente gratuito, podemos acceder directamente a la web oficial de Wireshark donde podréis encontrar los enlaces para su descarga. La instalación de este programa es muy sencilla, simplemente deberemos seguir el asistente de instalación paso a paso, y reiniciar el ordenador al finalizar. Además, como decíamos anteriormente, esta herramienta se puede usar en diferentes softwares sin inconvenientes. Wireshark es un programa que se actualiza constantemente, por lo que es muy recomendable tener siempre la última versión instalada en nuestro equipo para disfrutar de las últimas novedades. Si tienes un sistema operativo basado en Linux, es muy probable que en tu gestor de paquetes tengas Wireshark, y simplemente tengas que ejecutar un comando como este: sudo apt install wireshark Una vez que ya hemos visto cómo descargar e instalar Wireshark, vamos a utilizarlo para realizar una captura de datos. Junto con la instalación de WireShark se realiza también la instalación de Npcap, los drivers necesarios para poner la tarjeta de red en modo «promiscuo» y capturar todo el tráfico que nos llega y que enviamos, Npcap es un programa fundamental y se encuentra actualmente en su versión 1.50. En el pasado cuando Npcap estaba en fase beta, había problemas de cuelgues e incluso no te funcionaba bien la conexión a la red local e Internet, por este motivo, se ha utilizado durante muchos años WinPcap en lugar de Npcap, sin embargo, hoy en día se recomienda utilizar este último porque es el que está más actualizado y dispone de todas las mejoras. Debemos recordar que este programa es multiplataforma, de hecho, en la mayoría de distribuciones Linux orientadas a la ciberseguridad está incorporado de manera predeterminada, porque es ampliamente utilizado por los profesionales de la ciberseguridad, los administradores de redes y también los administradores de sistemas. En todas las distribuciones Linux podremos ejecutar programas similares como tcpdump, sin embargo, WireShark no solamente permite capturar todos los datos que entran y salen de la tarjeta de red, sino que también podremos ver la captura con una interfaz gráfica de usuario muy intuitiva. Por último, WireShark nos permite también ejecutar complejos filtros para solamente mostrar las capturas de datos que nos interesan. Hacer una captura de tráfico con Wireshark Nosotros hemos utilizado el sistema operativo Windows 10 para la realización de la captura de tráfico, pero en sistemas Linux o macOS es exactamente igual, ya que tenemos exactamente la misma interfaz gráfica de usuario. Lo primero que veremos al iniciar este programa son todas las tarjetas de red e interfaces de red de nuestro ordenador, en nuestro caso tenemos un total de tres tarjetas de red cableadas (ASUS XG-C100C, Realtek 2.5G y Intel 1G), una tarjeta de red Wi-Fi (WiFi 2), además, tenemos diferentes interfaces de red virtuales que se corresponden con las interfaces de VMware y Virtual Box. Wireshark nos permite capturar el tráfico de cualquier tarjeta de red, ya sea física o virtual, simplemente tenemos que tener claro cuál es nuestra tarjeta de red que actualmente está en uso, y de la cual queremos capturar tráfico de red. En nuestro caso es la ASUS XG-C100C, por lo que simplemente hacemos doble click sobre esta tarjeta. En el caso de que quieras utilizar una tarjeta de red WiFi también podrás hacerlo sin problemas, todo el tráfico entrante y saliente de esta tarjeta WiFi será capturado por WireShark, pero un detalle muy importante es que WireShark no pondrá la tarjeta en modo monitor para ver también los paquetes de otros clientes inalámbricos, solamente capturará y mostrará los paquetes propios. Al hacer doble click, de manera automática empezará a capturar todo el tráfico de red, tanto entrante como saliente. Algunas recomendaciones ANTES de realizar una captura de tráfico, son las siguientes: Cerrar todos los programas que generen tráfico de red, el cual no queremos capturar Asegurarnos de que el firewall se encuentra desactivado, ya que podría bloquear cierto tráfico y no aparecerá en Wireshark, o solamente aparecerá parte del tráfico generado. Si queremos capturar un cierto tráfico de datos que genere una aplicación, es recomendable esperar 1 segundo antes de iniciarlo y que capture tráfico de red del equipo, a continuación, ejecutamos esa aplicación, y por último, cerramos la aplicación y esperamos 1 segundo antes de detener la captura de tráfico. Con estas recomendaciones, estamos seguros que la captura de tráfico que hagáis será un éxito. En esta captura de tráfico, podéis ver tráfico de diferentes protocolos, tanto tráfico del protocolo Spanning-Tree Protocol de la red, como también tráfico TCP y tráfico TLSv1.2 de diferentes aplicaciones que tenemos abiertas. Tal y como podéis ver, con WireShark vamos a poder capturar en detalle todos los paquetes de la conexión y va a ponerlo en categorías de «Origen», «Destino», «Protocolo», longitud e información adicional, de esta forma, podremos ordenar fácilmente toda la captura de datos por protocolo, dirección IP de origen o destino etc. Con cada entrada de datos, podremos desplegar y ver en detalle todo el paquete de datos, tanto a nivel de aplicación, transporte, a nivel de red, enlace y también a nivel físico, es decir, Wireshark nos proporcionará la información por capas, para encontrar más fácilmente la información que nosotros necesitamos saber. Por supuesto, también nos indicará cuáles son los puertos de origen y destino si usamos TCP o UDP, e incluso podremos ver de manera avanzada los números de secuencia, y si ha habido un RST en la conexión o se ha tenido que reenviar un segmento debido a un problema. En la siguiente captura, podéis ver el resultado de ejecutar el comando «nslookup www.redeszone.net» a través de consola, realiza la solicitud DNS a nuestro servidor DNS, y automáticamente nos contestará con la resolución DNS hecha del dominio anterior. Por supuesto, este tráfico se «mezcla» con otro tráfico que tenemos en nuestro ordenador de diferentes aplicaciones, por este motivo es tan importante cerrar todas las aplicaciones que utilicen conectividad a Internet antes de empezar con la captura de tráfico. Aquí podéis ver la respuesta del servidor DNS a la solicitud DNS anterior: Si hacemos el típico ping, utilizando el protocolo ICMP, también nos lo mostrará perfectamente, nos mostrará tanto los «Echo request» como también los «Echo reply». Tal y como habéis visto, es muy fácil realizar una captura de datos con Wireshark para analizar todo el tráfico de red. Si queremos guardar esta captura, simplemente tenemos que pinchar en el botón rojo de «Stop» para parar la captura de datos, y posteriormente pinchar en «File / Save» para guardarla. Esta captura podremos guardarla en nuestro ordenador o en un soporte externo para su posterior análisis, o enviarla a algún experto que sea capaz de detectar el problema, aunque debes tener en cuenta que tendrá acceso a todo el tráfico capturado, por lo que debes enviar esta captura a alguien de confianza. Si hemos capturado tráfico con TLS o IPsec, necesitará la correspondiente clave de descifrado, por lo que eso no lo podrá «leer» sin esta información, lo mismo ocurre con el tráfico WPA/WPA2, sin la clave, no podrá leer el tráfico interno. Existen algunos sistemas operativos para routers y firewalls que incorporan un capturador de paquetes, este capturador de paquetes incorporados nos permitirán coger todo el tráfico de red de una o varias interfaces físicas o lógicas, e incluso podremos definir que solamente queremos capturar el tráfico desde o hacia una determinada IP/puerto, de esta forma, la captura que realicemos no será tan extensa que ocupe muchos MB o GB de información. Estos sistemas operativos siempre nos van a permitir exportar la captura en formato pcap, por tanto, posteriormente podremos abrir esta captura con Wireshark y examinarla en detalle. Por ejemplo, pfSense incorpora un capturado de paquetes bastante completo para limitar la captura de datos por interfaz, y tendremos un botón que nos permitirá descargar esta captura para su posterior análisis. Gracias al uso de Wireshark, podremos cargar esta captura recién creada de forma externa, y aplicar todos los filtros de Wireshark para solamente ver lo que nos interesa y no toda la captura realizada por pfSense. Lo mismo ocurre con algunos firmwares de routers como AVM, el cual dispone de un analizador de paquetes internos para detectar malas configuraciones o problemas a nivel de red. Posibles usos de Wireshark Como hemos visto, Wireshark es un software que nos permite conocer mucha información sobre los paquetes que transcurren por la red. Esto puede ser de mucho beneficio tanto con fines legales o ilegales. En el caso de los legales, puede ser una gran herramienta para administradores de redes. Entre las funciones que se pueden desempeñar con este programa podemos encontrar: Capturar tramas directamente desde la red. Mostrar y filtrar las tramas capturadas. Editar las tramas y transmitirlas por la red. Realizar capturas de tramas usando un equipo remoto. Llevar a cabo análisis y estadísticas. Filtrar todo tipo de datos. Exportar las capturas en diferentes formatos. Seguir flujos, parámetros y patrones de tráfico. Inspección profunda de protocolos Captura de información en el momento para posterior análisis Análisis de VoIP Posibilidad de lectura y modificación de archivos de captura de información como tcpdump, Microsoft Network Monitor, NetScreen snoop y más. Acceso a visualización en vivo de información proveniente de los protocolos de Ethernet, Bluetooth, USB, IEEE 802-11 (Wi-Fi), Frame Relay etc. Exportación de información a los formatos XML, PostScript, CSV y texto plano. Uno de los usos más interesantes e importantes para los que puedes utilizar Wireshark, es para el incident response (respuesta a incidencias) relacionado al tráfico SSH. Recordemos que este es un protocolo muy poderoso especialmente por la encriptación con la que cuenta por defecto. Podrás contar con acceso remoto y claro está, encriptado, a cualquier dispositivo que tenga habilitada la función de servidor SSH. Puedes realizar ataques de tipo Credential-Stuffing, escaneo de máquinas que estén funcionando con servidores SSH vulnerables y el establecimiento de shells reversos. Haremos énfasis en los dos primeros a continuación. Ataques Credential-Stuffing Considerando que SSH requiere la autenticación del usuario, un atacante que tenga acceso a una máquina que ejecute un servidor SSH podrá realizar ataques de este tipo sin mayores problemas. Pero, ¿qué hay con las contraseñas de las distintas credenciales? Por desgracia, la mayoría de las personas tienden a utilizar contraseñas muy fáciles de adivinar o peor aún, a optar siempre por la misma contraseña para todas sus cuentas. Esto hace que los ataques de tipo credential stuffing pasen, en la mayoría de los casos, completamente desapercibidos. De buenas a primeras no es sencillo diferenciar los intentos de acceso vía SSH exitosos de los no exitosos en Wireshark. Sin embargo, existen algunas características que nos ayudarán a revelar qué registros son exitosos: Longitud del flujo (de la sesión): si fuese una sesión SSH exitosa, la misma será de mayor duración que una fallida. Tamaño del paquete: los servidores SSH han establecido respuestas para las autenticaciones exitosas o fallidas. Es posible observar el tamaño de los paquetes SSH e inferir que los de mayor tamaño, constituyen a sesiones exitosas. Tiempo del paquete: Aquellos paquetes que requieren interacción del usuario, si la autenticación fue exitosa, tendrán más tiempo que aquellos que son automatizados. Esto último se refiere a los paquetes con menor tiempo de vida debido a las autenticaciones fallidas. Además, te recomendamos revisar el número de intentos de inicio de sesión, si observas un número irregular es porque existe la posibilidad de haber sido víctimas de ataque de tipo Credential-Stuffing. Escaneos de accesos remotos Uno de los mayores inconvenientes y riesgos generados a partir del auge de tecnologías emergentes como el Internet de las Cosas es que los dispositivos habilitados cuentan con SSH habilitado en primera instancia. Normalmente, sus sistemas asociados acostumbran a utilizar las credenciales por defecto o con alguna modificación mínima. ¿Por qué esto es un riesgo? Cualquiera que tenga conocimiento acerca de esas contraseñas o la capacidad de adivinar las usuarios y contraseñas, puede fácilmente acceder remotamente a las máquinas. Así es, incluso SSH puede contar con sus particulares agujeros de seguridad. Sin embargo, es posible tener control de estas máquinas que actúan como servidores SSH inseguros. Sabiendo que las solicitudes y tráfico SSH legítimas, deberían tener como origen la propia red interna. Por ende, se tratan de direcciones de IP confiables. Filtrando en Wireshark las solicitudes y el tráfico SSH interno, además del proveniente de direcciones IP externas, ayudará a identificar situaciones sospechosas. Se puede entender que, en la mayoría de los casos, el tráfico SSH proveniente de direcciones IP desconocidas a nuestra red interna puede dar señal de que la red ha sido vulnerada. Ésto último no significa precisamente que todo lo que pueda provenir de fuera de la red sea sospechoso o peligroso. Una vez que un atacante consigue acceso remoto a una máquina, SSH se convierte en un aliado ideal para llevar a cabo otros tipos de ataques y expandirse rápidamente a otras máquinas, realizando más de un ataque a la vez si lo desea. ¿Cómo es posible detectar esto? Con Wireshark, analizando todo el tráfico SSH, puedes establecer patrones de acceso tanto usuales como los inusuales. Un caso de patrón inusual puede consistir en que se den evidencias de un alto nivel de tráfico proveniente de una sola máquina. Otro caso de patrón inusual puede ser que una máquina realice solicitudes a otros sistemas que normalmente no lo haría. Tanto a nivel de tu red local como una red corporativa, SSH puede convertirse en un gran aliado y a su vez, un gran enemigo. Lo que da lugar a un monitoreo muy cercano y un especial control si es que estamos con la responsabilidad de administrar de una red corporativa. Controlando e incluso bloqueando el tráfico SSH en la red resulta ser una buena idea, así también las comunicaciones y el tráfico en general que se da dentro de la red deben ser monitoreadas ante cualquier anormalidad. Pero Wireshark también puede ser muy útil en otros ámbitos, como puede ser la educación. Esto puede ayudar a estudiantes y profesores a comprender mejor cómo transcurren los paquetes por las redes, de forma que se pueden formar en diferentes aspectos. Desde técnicos de redes, administradores y sí, hackers éticos. Qué tener en cuenta Una vez que lo tenemos descargado y ya sabemos cómo utilizarlo, puede que tengamos que resolver algunas preguntas importantes que te hayas hecho llegado a este punto. Por ejemplo, ¿es legal? También hay una serie de peligros si usas Wireshark y hay precauciones que debes tomar. ¿Es legal utilizar Wireshark? Si bien el uso de Wireshark no es ilegal, sí lo son algunas tareas que se pueden llevar a cabo con la información que nos puede proporcionar. En este caso, todo está en el código penal, siendo un delito de descubrimiento y revelación de secretos, lo cual es un derecho fundamental de la Constitución Española. El delito en sí, se refiere a la filtración o en su defecto, difusión de la información o material de un usuario, que en este caso es la víctima. Siendo de especial importancia, la difusión, lo cual puede acarrear otro tipo de delitos, que ya no tienen que ver con la informática. Esto se puede dar si se difunde la información relativa al círculo íntimo de una víctima que puede ser una persona física o jurídica, en resumen, todo lo que no sea público. Por tanto, si vas a usar esta herramienta, lo mejor será que solo lo hagas con redes propias o de las cuales tienes permisos, pues si bien es complicado que detecten tu presencia, en caso de hacerlo, podrías enfrentarte a problemas innecesarios. Aclaraciones sobre Wireshark Como hemos visto, con Wireshark estamos ante una herramienta muy poderosa la cual nos puede arrojar mucha información sobre los paquetes que transcurren por una red. Pero con el tiempo se han ido generando dudas o inquietudes de muchos usuarios hacia este programa, las cuales algunas veces aciertan o no. Vamos a ver algunas de estas preguntas, pues puede que te sirva para decidir usarlo o no. Algo muy extendido, fue un virus llamado «Wireshark Antivirus», el cual era un malware que infectó a muchos equipos. Este mostraba un mensaje indicando que teníamos que pagar por un antivirus, el cual no existía, era falso. El equipo de CACE Technologies, desarrolladores de Wireshark, sacaron un comunicado donde indicaban que en ningún momento llegaron a crear virus alguno, e indicando que un tercero estaba usando su nombre con fines fraudulentos. Los piratas informáticos también están en el punto de mira, pues al tratarse de un programa dedicado a estos fines, puede utilizarse como tal para atacar a otros usuarios o robarles información. En este punto es donde debemos separar a los hackers éticos de los que tienen fines maliciosos, y recordar que el simple uso de este software no es ilegal, sino el fin con el que se puede utilizar. Existe un video en Internet en el que mostraban cómo realizar un robo de una contraseña en un aeropuerto utilizando Wireshark. Esto es real, pues con Wireshark se pueden capturar todo tipo de datos, siempre que se usen en los envíos de los paquetes en una red. Por lo cual, siempre que Wireshark esté capturando los datos, y el usuario que lo utiliza tenga conocimientos para conseguir contraseña, se puede hacer. Este también se puede utilizar para monitorizar hosts desconocidos, incluso extraer direcciones IP y aprender sobre los dispositivos conectados mediante IA. Precauciones para utilizar Wireshark Como puedes ver, Wireshark es una herramienta muy versátil. Sobre todo, cuando tratamos de buscar información en los paquetes que circulan por una red. Pero que sea muy útil no significa que no debas tener en cuenta que hay peligros. Es por ello que siempre se deben guardar algunas precauciones cuando lo utilizamos, buscando no caer en un uso incorrecto que pueda ser incluso ilegal. A su vez, esto nos ayudará a hacer que lo utilicemos de forma óptima, y siempre dentro de unos límites legales y totalmente recomendados. Los cuales pueden hacer que nuestra red mejore, que entendamos mejor cómo funciona u otros ámbitos. Algunos de estas precauciones que mencionamos son: Privacidad y cumplimiento: Siempre que capturamos los datos que circulan por una red, debemos tener presente que es obligatorio respetar la privacidad y cumplir con todas las leyes y regulaciones locales. Por otro lado, si vamos a monitorizar una red que no es nuestra o es utilizada por más usuarios, lo mejor es tener permiso explícito para poder llevar a cabo la tarea. Usar redes legales: Si seguimos un poco la explicación previa, podemos extenderla hasta las redes que se pueden analizar. Podemos poner el ejemplo de las redes abiertas o todas en las que no tengamos autorización. De hacerlo de todos modos, puede ser considerado un delito, por lo que como ya dijimos, será mejor no arriesgarse en estas. Segmentación de la red: Siempre y cuando sea posible, debemos segmentar la red para tratar de establecer unos límites al tráfico. Esto hará que el sistema no se sobrecargue en exceso, y también nos ayuda a minimizar los accesos a datos que tal vez no son tan relevantes. Filtros: Siempre debemos utilizar los filtros adecuados. Si utilizamos un filtro incorrecto, podemos llegar a tener acceso a información que no estamos autorizados a ver. Por lo cual, de nuevo, podemos estar incurriendo en un delito. O por la contra, de nuevo podríamos estar obteniendo más información de la que realmente necesitamos para nuestra tarea. Lo cual puede ralentizar el trabajo. Alternativas a Wireshark Como has visto, Wireshark es una herramienta muy completa y que puede resultar muy útil en muchos casos. Pero lo cierto es que nos podemos encontrar muchas otras opciones, las cuales tienen funciones diferentes. En algunos pasos puede que Wireshark no tenga la misma funcionalidad para algunas tareas, por lo cual será necesario buscar otra herramienta de análisis de red. Elegir una puede llegar a ser complicado. Y sobre todo si buscamos una que cubra todo el rango posible de posibilidades. Pero no es la única. Si no te convence, siempre se puede optar por buscas otras opciones en Internet. Y es que siempre puedes dar con otras herramientas que cumplan de manera significativa con lo que estabas buscando. Por lo tanto, es buena idea que eches un ojo a algunas de las mejores alternativas que tienes disponible: Cloudshark Es una herramienta basada en la web, y su función es realizar los análisis y compartir los archivos de paquetes que se han capturado. Con los datos capturados, podemos resolver problemas en la red a un ritmo mucho más alto. En todo caso, esta herramienta se basa en el análisis del navegador web. Nos permite funciones similares y, como la del tiburón, también podemos ver los archivos .pcap y visualizar los paquetes. Es gratis y con muy buenas características por lo que se ha convertido en una de las mejores alternativas a Wireshark. En muchos casos se pueden combinar, ya que una se instala en local y la otra no. SmartSniff Otra buena alternativa a Wireshark que puedes tener en cuenta si no te convence la anterior es SmartSniff. Está diseñada principalmente para entornos basados en Windows. Nos ayuda a realizar la captura de los datos, como si de una conversación entre servidores y clientes se tratara. Una de las desventajas, es que para poder recolectar los paquetes necesita instalarlos previamente bajo demanda. Pero cuenta con las facilidades que nos dan la opción de omitir los paquetes que sean necesarios, o la ayuda que da al controlador de red. Tcpdump Otra alternativa popular al uso de Wireshark para analizar el tráfico de red es Tcpdump, una herramienta de captura de paquetes de red en sistemas basados en Unix, como Linux. Adiferencia de Wireshark, esta aplicación no tiene una interfaz gráfica y opera únicamente en línea de comandos, lo que la hace más complicada de usar para usuarios inexpertos. Su funcionamiento es similar al resto, captura paquetes en una interfaz de red especificada. Puede filtrar la captura según criterios como protocolos o direcciones IP, por ejemplo. Además, la aplicación proporciona una salida legible en línea de comandos, detallando información como direcciones IP, puertos, protocolos y datos de los paquetes. En comparación con Wireshark, la principal diferencia radica en la ausencia de una interfaz gráfica. Mientras Wireshark ofrece una representación visual estructurada y herramientas interactivas, Tcpdump presenta la información directamente en la línea de comandos, lo que requiere un mayor conocimiento técnico para interpretar los datos. Como hemos dicho, la interfaz de Tcpdump es textual y ejecutable en línea de comandos. Aunque puede parecer más inaccesible para principiantes, Tcpdump es eficiente y esencial para administradores de sistemas y redes que prefieren trabajar en entornos de líneas de comando. Una opción bastante interesante si estás buscando una alternativa a Wireshark para analizar el tráfico de red. ColaSoft Capsa En este caso, estamos de nuevo ante un analizador de los paquetes que circulan por la red. Pero tenemos una peculiaridad, y es que esta aplicación nos presenta toda la información de forma compacta. Resulta muy sencilla de utilizar, siendo así más accesible que las opciones anteriores. Podemos hacer escaneo de puertos TCP, podemos exportar datos y es bastante completa y compatible con todo tipo de ordenadores descargándola desde su web. El programa puede usarse de forma gratuita y nos permite monitorizar 10 direcciones IP durante unas cuatro horas seguidas. Pero también podemos elegir usar una versión de pago que desbloquea todas las funciones posibles y que nos da muchas más opciones de uso. Aunque es de pago, podemos probarla durante 30 días gratis si quieres comprobar qué te ofrece o si quieres saber si es una buena alternativa a Wireshark en la que confiar. Wireshark en Android Pese a que actualmente esta aplicación en concreto no puede ser ejecutada en dispositivos móviles, si deseas realizar algo similar con un teléfono Android podrás hacerlo. Por aquí te dejamos algunas de las mejores alternativas: tPacketCapture: Es una aplicación para Android que permite capturar paquetes de red sin necesidad de acceso root ni ninguna modificación del propio sistema operativo para ello. Utiliza una VPN local para capturar el tráfico. Shark for Root: Los archivos de captura se pueden analizar posteriormente con Wireshark en un ordenador, sin embargo necesitaremos root para poder utilizar esta app, por lo que no será tan sencillo como la anterior. Packet Capture: Al igual que la primera, utiliza la API VPN para capturar tráfico de red sin necesidad de root, por lo que lo podremos hacer con cualquier dispositivo Android sin complicaciones. De todas formas, salvo que se puedan analizar redes y datos desde un Android, lo mejor será, si es posible, realizarlo desde un ordenador, donde podremos capturar más y mejores paquetes para poder revelar toda la información que busquemos. Las antenas de una tarjeta de red de un equipo como un PC no solo nos proporcionará mayor alcance, sino una velocidad de procesamiento y captación de datos mucho mayor, por lo que será más efectivo y fiable. Eso sí, siempre de forma legal y con permiso. Wireshark en iOS (iPhone) En caso de buscar el mismo método, pero en iPhone, la cosa cambia, y es que Wireshark, así como la mayoría de aplicaciones móviles, no están disponibles en iOS, debido a sus limitaciones y sistema más cerrado. Sin embargo, si hay herramientas que nos pueden ayudar, y pese a no tener todas las funciones, quizás contengan la que necesitas: iNetTools: Gracias a esta app podremos escanear redes, hacer PING a dispositivos y analizar tráfico de red capturado. No será la más completa de todas, pero nos ayudará a conocer el estado de la misma. Network Analyzer: Aquí sí podríamos hablar de algo más interesante, ya que no solo realizaría las funciones de la anterior, sino que también te permite analizar el tráfico de red capturado en tiempo real. HTTP Catcher: Permite interceptar y analizar el tráfico HTTP y HTTPS gracias a tu iPhone. Del mismo modo podremos modificar y reenviar solicitudes HTTP. Todas ellas son gratuitas, por lo que probarlas no nos costará nada, y aunque no es Wireshark, para ser iPhone no están nada mal, debido a las limitaciones que conocemos de su sistema operativo, aunque siempre recomendaremos antes Android en estos temas, y sobre todo, como ya dijimos, un ordenador, pues no tendrá ni punto de comparación.