Análise de pacotes de rede com Wireshark

Introdução

Este documento tem como objetivo demonstrar uma análise de pacotes dentro de uma rede, mostrando como é importante o monitoramento para mitigação de riscos e detecção de incidentes.

Fundamentos de Redes de Computadores

Em fundamentos de redes, os pacotes e protocolos são partes essenciais a serem entendidas. Os pacotes são conjuntos de dados de forma estruturada para transmissão de informações na rede. Já os protocolos são as regras das comunicações, desde como iniciar, as informações que devem conter e como finalizar.

A importância da captura de pacotes na segurança é crucial para análise e ação dos times, onde vão identificar padrões, possíveis ameaças e tomar atitudes necessárias.

Ferramenta utilizada

Para esta análise, utilizei o Wireshark, uma ferramenta de captura de pacotes. Utilizada também por times de segurança por ser uma ferramenta completa e de alta eficiência, onde captura e entrega os protocolos e informações dos pacotes que trafegam na rede.

Protocolos observados

Capturas feitas dos protocolos e qual sua utilidade na segurança:

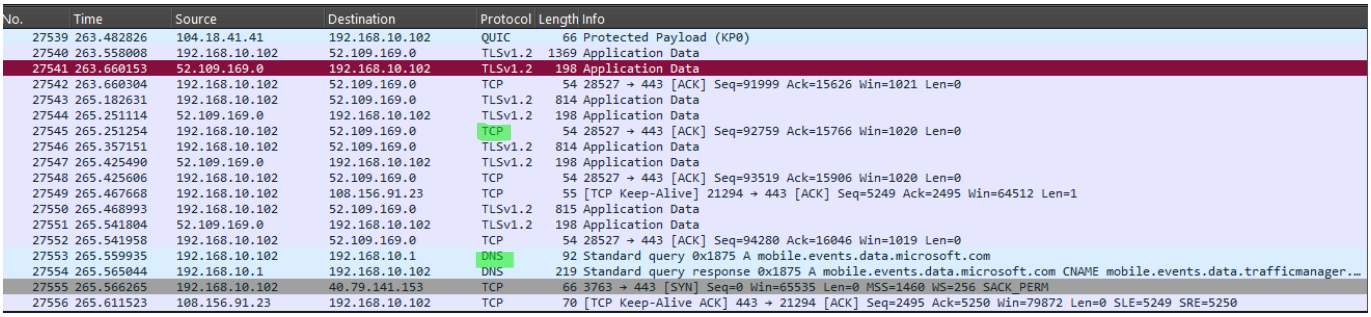
1. TCP(Transfer Control Protocol) – Protocolo importante para a confiabilidade da entrega e confirmação dos pacotes.
2. QUIC(Quic UDP Internet Connections) – Protocolo em substituição do TPC+TLS usado no HTTPS, utilizando de HTTP/3, para abordagem moderna e eficiente.
3. DNS(Domain Name System) – Protocolo utilizado para tradução de nomes de domínios (ex:os nomes dos sites que utilizamos), para endereços IP's.

Metodologia utilizada

1. Início da captura: Ligar a captura do Wireshark
2. Ação: Entrei em sites como: Cousera e Linkedin
3. Final: Desliguei a captura do Wireshark

Análise com foco em segurança

Com esta análise é possível compreender como é importante ter um tráfego criptografado, pois com uma ferramenta de captura, se tem acesso a todos os tipos de dados que estão em trânsito e em caso de configurações incorretas ou ausência de criptografia, a rede se torna vulnerável e as informações se tornam expostas.



No.	Time	Source	Destination	Protocol	Length	Info
27539	263.482826	104.18.41.41	192.168.10.102	QUIC	66	Protected Payload (KP0)
27540	263.558008	192.168.10.102	52.109.169.0	TLSv1.2	1369	Application Data
27541	263.660153	52.109.169.0	192.168.10.102	TLSv1.2	198	Application Data
27542	263.660304	192.168.10.102	52.109.169.0	TCP	54	28527 → 443 [ACK] Seq=91999 Ack=15626 Win=1021 Len=0
27543	265.182631	192.168.10.102	52.109.169.0	TLSv1.2	814	Application Data
27544	265.251114	52.109.169.0	192.168.10.102	TLSv1.2	198	Application Data
27545	265.251254	192.168.10.102	52.109.169.0	TCP	54	28527 → 443 [ACK] Seq=92759 Ack=15766 Win=1020 Len=0
27546	265.357151	192.168.10.102	52.109.169.0	TLSv1.2	814	Application Data
27547	265.425490	52.109.169.0	192.168.10.102	TLSv1.2	198	Application Data
27548	265.425606	192.168.10.102	52.109.169.0	TCP	54	28527 → 443 [ACK] Seq=93519 Ack=15906 Win=1020 Len=0
27549	265.467668	192.168.10.102	108.156.91.23	TCP	55	[TCP Keep-Alive] 21294 → 443 [ACK] Seq=5249 Ack=2495 Win=64512 Len=1
27550	265.468993	192.168.10.102	52.109.169.0	TLSv1.2	815	Application Data
27551	265.541804	52.109.169.0	192.168.10.102	TLSv1.2	198	Application Data
27552	265.541958	192.168.10.102	52.109.169.0	TCP	54	28527 → 443 [ACK] Seq=94280 Ack=16046 Win=1019 Len=0
27553	265.559935	192.168.10.102	192.168.10.1	DNS	92	Standard query 0x1875 A mobile.events.data.microsoft.com
27554	265.565044	192.168.10.1	192.168.10.102	DNS	219	Standard query response 0x1875 A mobile.events.data.microsoft.com CNAME mobile.events.data.trafficmanager.…
27555	265.566265	192.168.10.102	40.79.141.153	TCP	66	3763 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
27556	265.611523	108.156.91.23	192.168.10.102	TCP	70	[TCP Keep-Alive ACK] 443 → 21294 [ACK] Seq=2495 Ack=5250 Win=79872 Len=0 SLE=5249 SRE=5250

Conclusão

Este projeto permitiu compreender como a análise de pacotes contribui para o entendimento do tráfego de rede e para a identificação de possíveis riscos de segurança.