LAB 02 | Primeiros passos com Wireshark

Abra uma captura sintética e identifique DNS, handshakes TCP e HTTP sem capturar dados de terceiros.

Uso exclusivo em ambiente próprio, isolado ou expressamente autorizado. Materiais e endereços de teste são fictícios.

Objetivos de aprendizagem

- Abrir e preservar um arquivo PCAP de treinamento
- Aplicar filtros de exibição para DNS e TCP
- Interpretar indícios sem inferir autoria

Procedimento passo a passo

01 Obter a captura didática

Baixe o arquivo trafego_sintetico.pcap da biblioteca. Ele contém somente quadros artificiais com endereços reservados para documentação.

02 Abrir a captura

No Wireshark, selecione Arquivo > Abrir e escolha o PCAP. Confira a lista de pacotes e registre nome do arquivo e horário de análise.

03 Filtrar DNS

Aplique o filtro dns e observe consultas com nomes comuns e outros intencionalmente longos. Anote o contexto antes de avaliar qualquer suspeita.

04 Filtrar início de conexões TCP

Aplique tcp.flags.syn == 1 && tcp.flags.ack == 0. Observe destinos, portas e frequência relativa, distinguindo varredura, repetição e comunicações normais.

05 Examinar HTTP sem TLS

Aplique http e use Follow > TCP Stream quando apropriado. Identifique apenas as credenciais fictícias de teste contidas no arquivo e discuta o motivo de expô-las em claro ser um risco.

06 Produzir o registro

Capture as telas de filtros, documente hipótese, pacotes relacionados e limitações de interpretação.

Evidências esperadas

- Print de consulta DNS selecionada
- Print de filtro TCP com flags SYN
- Tabela com endereço/porta/hipótese e justificativa

Checklist de execução

[ ] PCAP de origem sintética baixado

[ ] Filtros DNS e SYN testados

[ ] Pelo menos dois fluxos TCP analisados

[ ] Dados fictícios tratados como tal

[ ] Evidências e limitações documentadas

Questões para discussão

1. Qual a diferença entre filtro de captura e filtro de exibição?

2. Que informações adicionais ajudam a distinguir anomalia de um serviço legítimo?

Filtros úteis - Wireshark (exibição)

Consultas DNS: dns

DNS da zona didática: dns.qry.name contains "lab.example.test"

Início de conexão TCP: tcp.flags.syn == 1 && tcp.flags.ack == 0

Tráfego HTTP: http

Requisições POST: http.request.method == "POST"

Host de simulação: ip.addr == 198.51.100.20

PCAP incluído: trafego_sintetico.pcap | SHA-256: 7031207d979d22ccd8722952d60756567a6286e9b503cb676564f39d3320650d

Registro final

Data: ____ / ____ / _____ Responsável: _____

Resultado, justificativa e limitações: