LAB 05 | Investigação de tráfego suspeito (PCAP)

Analise um PCAP sintético com varreduras, SYNs repetidos, subdomínios atípicos, beaconing simulado e credenciais de teste em HTTP.

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

Objetivos de aprendizagem

- Identificar padrões sintéticos de port scan e sequência de SYNs repetidos
- Examinar subdomínios longos e conexões periódicas simuladas
- Explicar o risco de credenciais fictícias em HTTP não criptografado

Procedimento passo a passo

01 Preparar a investigação

Baixe o PCAP sintético e registre seu SHA-256, horário de análise, ferramenta utilizada e escopo do exercício.

02 Localizar SYNs de uma varredura

Aplique tcp.flags.syn == 1 && tcp.flags.ack == 0. Agrupe por destino e porta para reconhecer múltiplas tentativas a portas diferentes. Não tente reproduzir varredura fora do laboratório.

03 Observar repetição de SYNs

Use o mesmo filtro e ordene por tempo. Uma série concentrada de SYNs para uma porta pode representar uma simulação de flood, mas a captura por si só não prova indisponibilidade.

04 Inspecionar DNS atípico

Aplique dns.qry.name contains "lab.example.test". Compare comprimento e diversidade dos nomes consultados. Explique por que nomes longos, isoladamente, não provam tunneling.

05 Analisar comunicação periódica

Filtre ip.addr == 198.51.100.20 e examine intervalos entre requisições HTTP de teste. Trata-se de beaconing C2 simulado, não de comunicação real com um controlador.

06 Localizar dados em HTTP

Aplique http.request.method == "POST" e inspecione o stream. A conta e senha do exercício são artificiais. Explique como TLS e outras salvaguardas evitariam exposição equivalente em redes reais.

07 Construir o relatório

Escreva cinco achados contendo filtro, pacote ou fluxo, hipótese, evidência, limitações e recomendação. Evite afirmar ataque real baseado em um único padrão.

Evidências esperadas

- Cinco filtros usados e respectivas capturas de tela
- Tabela de achados e seus números de pacote
- Explicação dos limites da inferência

Checklist de execução

[ ] Arquivo de treinamento identificado como sintético

[ ] Varredura de portas caracterizada

[ ] SYNs repetidos contextualizados

[ ] DNS atípico documentado sem suposição conclusiva

[ ] Beaconing simulado analisado

[ ] Credenciais fictícias em HTTP reconhecidas

[ ] Relatório com evidências e limitações elaborado

Questões para discussão

1. Por que uma sequência de SYNs não comprova por si só um incidente de indisponibilidade?

2. O que distingue evidência observável de hipótese de ataque?

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: