Trabalho Prático 2

Instruções

- O trabalho prático deverá ser feito em grupo de, no máximo, 3 membros;
- A submissão deverá ser feita por apenas um dos integrantes do grupo, exclusivamente, via *blackboard*;
- Para todas as questões propostas, inclua imagens que demonstrem a forma como chegou aos resultados obtidos;
- A entrega consistirá em um ficheiro *pdf* que inclua todas as análises propostas neste enunciado;
- O prazo de submissão será **23h59** do dia **20/04/2025**;
- Será marcada, posteriormente, uma sessão onde cada grupo discutirá os resultados obtidos com a equipa docente.

Objetivos

Este trabalho prático explora técnicas de *footprinting* de serviços conectados como um meio para a análise dos riscos relacionados com a superfície de exposição da infraestrutura de suporte. Para isso, serão usadas diferentes técnicas e ferramentas tipicamente adoptadas na identificação de vulnerabilidades e na proteção das propriedades da segurança da informação.
O trabalho é dividido em duas componentes diretamente mapeáveis na fase de *footprinting* dos testes de penetração: (*A*) fase de *reconhecimento*; e (*B*) fase de *varredura* e *enumeração* de vulnerabilidades e fraquezas.

Parte A

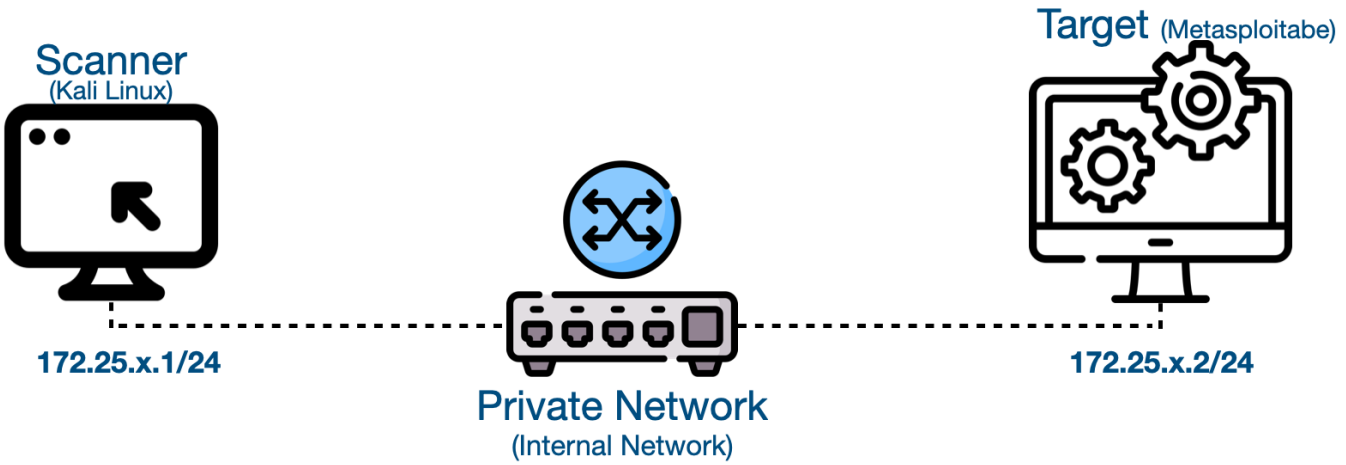
Selecione duas empresas que realizam suas operações comerciais por meio de serviços *online* — uma grande corporação e um negócio local — e aplique técnicas de coleta passiva (*i.e.,* de domínio público) de informações para descobrir detalhes sobre seus sistemas e infraestrutura. Relate as estratégias utilizadas, os resultados encontrados e as possíveis diferenças na forma como os administradores desses domínios gerenciam sua segurança e exposição. Por fim, apresente uma análise crítica sobre os riscos relacionados às práticas observadas.

Parte B

A Parte B deste trabalho explora a varredura e a identificação de vulnerabilidades em um sistema alvo dentro de um ambiente de testes controlado. O objetivo é compreender como diferentes técnicas podem revelar possíveis falhas de segurança e avaliar os riscos envolvidos. Esses testes são fundamentais para fortalecer a proteção de sistemas, ajudando a antecipar ameaças e aprimorar estratégias de defesa contra ataques.

Cenário de testes

Com o objetivo de manter o ambiente de testes isolado da rede local e, portanto, evitar riscos à segurança, sugerimos que usem uma rede privada através de um ambiente de virtualização da vossa preferência (*e.g.,* WMWare, VirtualBox, UTM). Os testes propostos na *Parte B* do trabalho exigem um sistema que funcionará como um *auditor* (*scanner*) e um segundo sistema *alvo* (*target*). O esquema arquitetural da imagem abaixo considera que cada sistema corresponde a uma máquina virtual (*VM*) independente, nomeadamente o Kali Linux (que atuará como *auditor*) e o Metasploitable 2 (que atuará como *alvo*).
Em alternativa, poderão optar por ter todas as ferramentas necessárias instaladas no sistema operativo principal e apenas o *sistema alvo* a correr em uma VM.
Em ambos os cenários, a rede entre os sistemas deverá ser configurada na gama de endereços IP *172.25.x.0/24*, onde ***x*** corresponde ao número do vosso grupo (ver exemplo na figura abaixo).



Se optarem por usar o Kali como *sistema auditor*, terão a maior parte das ferramentas necessárias já instaladas. Deverão, contudo, instalar também um *Network-Based Intrusion Detection System* (NIDS) e um *Scanner de Vulnerabilidades*. Para o NIDS, duas sugestões são o Snort e o Suricata. Já para o scanner de vulnerabilidades, podem escolher entre o openVAS e o Nessus. Em ambos os casos, as bases de dados de regras e de conhecimento de vulnerabilidades públicas são suficientes.

Questões

Durante os testes da *Parte B*, certifique-se que tem o NIDS e um analisador de tráfego (*e.g.,* Wireshark ou TCPdump) de sua escolha corretamente configurados no *sistema auditor*. Ambas as ferramentas deverão estar a analisar o tráfego entre o *sistema auditor* e o *sistema alvo* para, com os respetivos resultados, responderem as questões propostas.

⚠ Todas as varreduras (*scans*) propostas serão originadas do *sistema auditor* e direcionadas exclusivamente ao *sistema alvo*.

B1: Conecte-se ao *sistema alvo* usando o protocolo de rede telnet. Analise o tráfego capturado e discuta os potenciais problemas de segurança identificados. Qual seria a solução para os problemas identificados?

B2: Use a ferramenta Network Mapper (Nmap) para executar quatro varreduras distintas:

```
1: nmap -sV IP_alvo
2: nmap -sV -p 80 IP_alvo
3: nmap -sV --script vulners IP_alvo
4: nmap -A IP_alvo
```

- **B2.1:** Compare e discuta os resultados de cada varredura (*i.e., output* do *Nmap*).
- **B2.2:** Analise o tráfego capturado e discuta o impacto (*detectabilidade*) de cada um do ponto de vista de um NIDS.
- **B2.3:** Analise o relatório do NIDS e discuta os resultados considerando a sua resposta ao item B2.2.

B3: Discuta como os levantamentos efetuados na *Parte A* do trabalho podem otimizar a varredura de sistemas alvo, em particular, reduzindo a sua detectabilidade.

B4: O *sistema alvo* possui uma *firewall* instalada, *i.e.,* iptables. Adicione regras para bloquear tráfego externo TCP para os portos 513 e 6000.

```
iptables -A INPUT -p tcp --dport port_number -j DROP
```

Volte a executar as varreduras da questão B2, compare e discuta os resultados do *Nmap*.

B5: Ainda com os portos 513 e 600 bloqueados para tráfego TCP de entrada, execute as varreduras abaixo, analise, compare e discuta os resultados.

```
1: nmap -Pn -sA IP_alvo
2: nmap -Pn -sF IP_alvo
3: nmap -Pn -sN IP_alvo
4: nmap -Pn -sX IP_alvo
5: nmap -Pn -sU -p 513,6000 IP_alvo
```

B6: Use o *scanner* de vulnerabilidades Nikto para varrer os serviços *web* a correr no *sistema alvo*. Compare os resultados da varredura e do tráfego capturado com aqueles observados nos *comandos 3* e *4* da questão B2.

```
nikto -h IP_alvo
```

B7: Use o *openVAS* (ou *Nessus*) para uma nova varredura de vulnerabilidades do *sistema alvo*.

- **B7.1:** Compare os resultados desta ferramenta com os obtidos nas questões B5 e B2.
- **B7.2:** Observe que algumas notificações do NIDS não possuem vulnerabilidades correspondentes no relatório do *scanner de vulnerabilidades*. Discuta as possíveis razões para tais diferenças.
