****

**Segurança de Sistemas Informáticos**

**Ficha de Exercicios 4 – Network Security**

**Grupo 04**

**2022/2023**

|  |  |
| --- | --- |
| Uma imagem com pessoa, parede, interior, pose  Descrição gerada automaticamente | **Uma imagem com pessoa, parede, homem, interior  Descrição gerada automaticamente** |
| A91697 - Luís Filipe Fernandes Vilas | A91671 - João Manuel Novais da Silva |
|  |  |
|  |  |
|  | |
|  | |

**Prazo de submissão: 23:59 de 19/05/2023**

Índice

[Índice 2](#_Toc134642508)

[Objetivos 3](#_Toc134642509)

[Execução 4](#_Toc134642510)

[Port Scan 4](#_Toc134642511)

# Objetivos

Com o desenvolvimento desta ficha, é expectável que fiquemos a conhecer de um modo mais profundo, os modos de funcionamento de diversas ferramentas que nos permitem ter conhecimento acerca de outros dispositivos que se encontram em rede.

É tambem previsto ficar a conhecer o modo como essas ferramentas operam, ou seja, quando lhes é pedido alguma informação, no caso do *nmap* o que a mesma aplicação executa para poder devolver os resultados para o utilizador.

# Execução

## Port Scan

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Figura 1 - Port Scan para h4cker.orgUma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Figura 2 - Port Scan para scanme.nmap.org

Após interpretarmos estas imagens, conseguimos entender que foram encontradas duas portas abertas, tanto no *scanme.nmap.org* como em *h4cker.org*. Apesar disso, as portas não são as mesma. O *scanme.nmap.org* não dispõe de HTTPS (ou seja) HTTP seguro, na porta 443. Por outro lado, o outro servidor também não tem a porta de ssh aberta para o público.

Uma imagem com texto, Tipo de letra, número, captura de ecrã

Descrição gerada automaticamente

Figura 3 - Tramas enviadas pelo NMAP (1), h4cker.org

## 

Uma imagem com texto, captura de ecrã, Tipo de letra, número

Descrição gerada automaticamente

Figura 4 - Tramas enviadas, com recebida, h4cker.org

Nas figuras acima conseguimos perceber que o *nmap* inicialmente envia tramas TCP para todas as portas mais usuais. Deste modo, ele espera receber alguma resposta, caso essa porta esteja aberta, tal como acontece na trama 47 (Figura 4).

Tal como vimos acima, este host tinha as portas 80 (HTTP) e 443 (HTTPs) abertas, ou seja, é esperado existirem duas respostas às queries.­­



Figura 5 – Tramas para a porta 22, scanme.nmap.org



Figura 6 - Tramas para a porta 80, scanme.nmap.org

Neste ultimo host, recebemos resposta às duas portas que foram apresentadas como estando a escutar. A porta 22 (Figura 5) e a porta 80 (Figura 6) correspondem ao servidor SSH e Web, respetivamente.

## Vulnerability Scan

Uma imagem com texto, captura de ecrã, Tipo de letra, número

Descrição gerada automaticamente

Figura 7 - Tentativa de encontrar vulnerabilidades em h4cker.org

Uma imagem com texto, captura de ecrã, número, Tipo de letra

Descrição gerada automaticamente

Figura 8 - Tentativa de encontrar vulnerabilidades em scanme.nmap.org

Através destas duas figuras conseguimos perceber a forma como o *NMAP* tenta descobrir vulnerabilidades.

Inicialmente verifica se a porta está aberta e, posteriormente tenta descobrir qual é a versão e o software que corre nessa determinada porta. Com essa informação e com a lista de vulnerabilidades detalhadas e das listas de CVE, determina se existem ou não vulnerabilidades que possam ser exploradas.

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

Figura 9 - Vulnerabilidades encontradas no scanme.nmap.org, mas não encontradas em h4cker.org

## Cypher Scan

Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente

Figura 10 - Lista de Cifras aceites (apenas o h4cker.org permite)

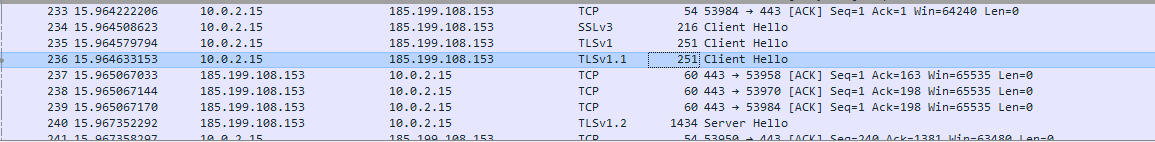


Figura 11 - Forma de Procura de Cifras

Através da Figura 11, conseguimos interpretar nas tramas 234,235,236 a forma como são procuradas as cifras disponíveis.

O *NMAP* experimenta conectar – se ao servidor utilizando as cifras por ele conhecidas e, caso uma resposta positiva seja recebida, essa cifra está disponível no servidor. Tal como podemos ver na trama 240 em que o servidor responde positivamente a uma pergunta do *NMAP,* utilizando o TLSv1.2.

# Conclusão

Através da realização deste trabalho, conseguimos perceber de que forma é que são feitos *scans* nos diferentes tipos de protocolos e, de que modo são encontradas diversas vulnerabilidades, mas também as cifras que os diferentes servidores utilizam.

Este tipo de procura é crucial pois, revelam o que pode existir de incorreto com um serviço e, deste modo, caso sejam encontradas previamente, os problemas poderão ser resolvidos. Este tipo de ferramentas são exaustivamente utilizados por Hackers para poderem ter mais informação acerca de qual dos potenciais serviços poderão atacar para poderem conseguir um trabalho positivo e ter controlo sobre a máquina em questão.