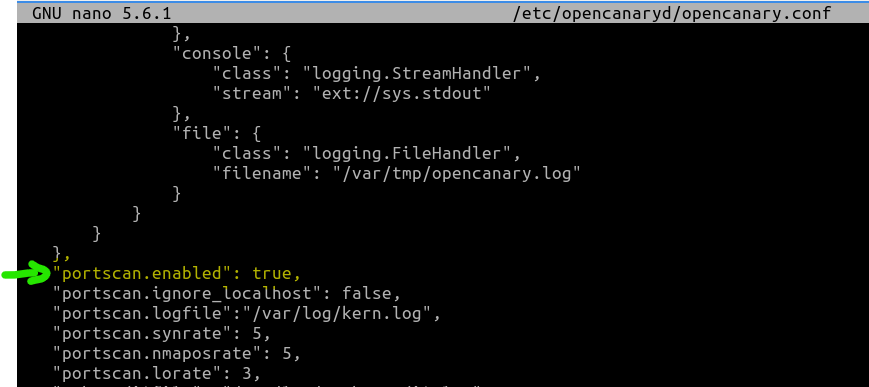
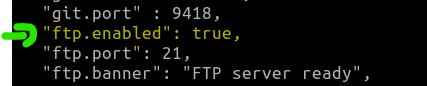
|  |  |  |  |
| --- | --- | --- | --- |
| **MODALIDADE:** | Curso de Especialização Tecnológica (CET) | **Ficha 4:**  ***Honeypot – Open Canary*** | |
| **CURSO:** | Técnico especialista em cibersegurança | | |
| **UFCD:** | Wargamming | **CÓDIGO UFCD:** | 9197 |
| **FORMADOR/A:** | Ricardo Lobo | **DATA:** | 17/03/2023 |
|  |  |  |  |
| **OBJETIVOS** | | | |
| * Continuação da exploração do *OpenCanary.* * Simulação de ataques ao *Honeypot*. | | | |

|  |
| --- |
| **A ficha de trabalho deverá ser realizada neste ficheiro** |

# Exercícios

1. Na VM onde instalou o *OpenCanary*, aceda ao ficheiro de configurações e ative as opções abaixo:





Grave as alterações e reinicie o *OpenCanary*.

opencanaryd –restart

1. Na VM do *OpenCanary*, **execute o comando abaixo**, para verificar quais as portas que se encontram abertas, **preencha a tabela** seguinte com as informações recolhidas, **faça um *print screen*** do resultado e cole na área disponível para o efeito.

netstat -tuln

-t: portas TCP

-u: portas UDP

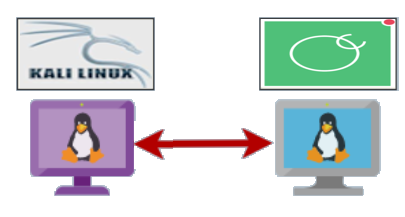
-l: *listenning* - apenas portas que se encontram “à escuta”

-n: número das portas abertas

|  |  |
| --- | --- |
| **NÚMERO DA PORTA** | **DESCRIÇÃO DA PORTA | SERVIÇO QUE SE ENCONTRA A CORRER** |
| 631 | IPP (Portscan) |
| 23 | telnet |
| 21 | FTP |
| 80 | HTTP |
| 53 | DNS |
| 38603 | ??? |
| 55849 | ??? |
| 5353 | Multicast DNS |

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

1. Interligue na mesma rede a VM onde instalou o *OpenCanary* e a VM do Kali Linux.



|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

1. Na VM do *Kali Linux*, faça um *scan* às portas abertas na VM do *OpenCanary*.

**Execute o comando** abaixo ou outro que julgue mais pertinente, **preencha a tabela** seguinte com as informações recolhidas, **faça um *print screen*** do resultado e cole na área disponível para o efeito.

nmap -sSU <IP>

|  |  |
| --- | --- |
| **NÚMERO DA PORTA** | **DESCRIÇÃO DA PORTA | SERVIÇO QUE SE ENCONTRA A CORRER** |
| 21 | FTP |
| 23 | Telnet |
| 80 | HTTP |
| 631 | IPP (Portscan) |
| 5353 | Multicast DNS |

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

1. Na VM do *OpenCanary*, consulte o log produzido pelo *honeypot* e obtenha os **últimos 5 registos** do ficheiro.

tail -n 5 /var/tmp/opencanary.log

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

1. No Kali Linux, efetue um novo *scan* às portas disponíveis na VM do *OpenCanary*, mas utilizando a ferramenta **MASSCAN**.

sudo masscan -p1-65535 <IP>

-p1-65535: o scan será feito desde a porta 1 até à porta 65535.

<IP>: endereço IP da máquina testada.

|  |
| --- |
|  |
| *PRINT SCREEN* COM O RESULTADO OBTIDO |
|  |

1. Após terminado o *scan* às portas, consulte o log do *OpenCanary* e obtenha os **últimos 5 registos** do ficheiro.

tail -n 5 /var/tmp/opencanary.log

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

1. No Kali Linux, aceda à pasta abaixo e obtenha as **primeiras 20 linhas** do ficheiro “**rockyou-75.txt**”.



head -n 20 rockyou-75.txt

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
| (caminho não existe, substitui para outro que tem a mesma lista de palavras) |

1. Obtenha o número de linhas do ficheiro “**rockyou-75.txt**”.

* **Dica:** Consulte a ajuda relativa ao comando **wc** (**wc --help**)

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
| (caminho não existe, substitui para outro que tem a mesma lista de palavras) |

1. Através do Kali Linux, execute o comando seguinte para simular um ataque ao FTP da VM do *OpenCanary*.

hydra -l admin -P ‘/pentest/password-recovery/dictionary/Passwords/Leaked-Databases/rockyou-75.txt’ ftp://<IP>

-l: *username* que vamos usar para a tentativa de ataque ao FTP.

-P: caminho para um ficheiro com *passwords* que serão utilizadas para o ataque.

ftp://<IP>: serviço que vai ser atacado e respetivo endereço IP.

Ajuda: **hydra --help**

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

1. Na VM do *OpenCanary*, obtenha o número de linhas do ficheiro de logs (/var/tmp/opencanary.log).

* **Dica:** Consulte a ajuda relativa ao comando wc (**wc --help**)

|  |
| --- |
| ***PRINT SCREEN* COM O RESULTADO OBTIDO** |
|  |

Depois de terminada a realização da ficha de trabalho, submeta este documento através da tarefa disponível no Moodle.

Bom trabalho.