10/07/2023 – TryHackMe – Juicy Details

Link: <https://tryhackme.com/room/juicydetails>

## Task 2  Reconnaissance

**What tools did the attacker use? (Order by the occurrence in the log)**

Comandos usados para a análise:

cat -n access.log // mostrar o número da linha

nl -b a access.log | grep -v GET // mostrar o número da linha e não mostrar as linhas que fazem “GET” na API

1. nmap

*2 ::ffff:192.168.10.5 - - [11/Apr/2021:09:08:34 +0000] "POST / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;* [*https://nmap.org/book/nse.html*](https://nmap.org/book/nse.html)*)"*

1. hydra

*224 ::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"*

1. sqlmap

*550 ::ffff:192.168.10.5 - - [11/Apr/2021:09:29:14 +0000] "GET /rest/products/search?q=1 HTTP/1.1" 200 - "-" "sqlmap/1.5.2#stable (*[*http://sqlmap.org*](http://sqlmap.org)*)"*

1. curl

631 ::ffff:192.168.10.5 - - [11/Apr/2021:09:32:51 +0000] "GET /rest/products/search?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 200 3742 "-" "curl/7.74.0"

1. feroxbuster

*632 ::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /a54372a1404141fe8842ae5c029a00e3 HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"*

RESPOSTA: nmap, hydra, sqlmap, curl, feroxbuster

**Outra alternativa:** utilizar o comando *cat access.log | cut -d '"' -f6 | uniq*

Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Mozilla/5.0 (Hydra)

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

sqlmap/1.5.2#stable (http://sqlmap.org)

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

curl/7.74.0

feroxbuster/2.2.1

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

**What endpoint was vulnerable to a brute-force attack?**

Sabendo que uma das ferramentas utilizadas pelo atacante que é utilizada para brute-force é o hydra, foi verificado qual endpoint foi atacado com o hydra:

*$ nl -b a access.log | grep hydra*

*208 ::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"*

RESPOSTA: /rest/user/login

**What endpoint was vulnerable to SQL injection?**

Sabendo que uma das ferramentas utilizadas pelo atacante que é utilizada para SQLi é o sqlmap, foi verificado qual endpoint foi atacado com o sqlmap:

*$ nl -b a access.log | grep sqlmap*

*550 ::ffff:192.168.10.5 - - [11/Apr/2021:09:29:14 +0000] "GET /rest/products/search?q=1 HTTP/1.1" 200 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"*

RESPOSTA: /rest/products/search

**What parameter was used for the SQL injection?**

Analisando a requisição escolhida acima (linha 550), verifica-se que o parâmetro é “q”

RESPOSTA: q

**What endpoint did the attacker try to use to retrieve files? (Include the /)**

Verificando a seguinte linha, encontra-se o endpoint “/ftp”. Sabendo que FTP é um protocolo de rede de transmissão de arquivos, esta é a flag correta

*640 ::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /ftp HTTP/1.1" 200 4852 "-" "feroxbuster/2.2.1"*

RESPOSTA: /ftp

## Task 3 Stolen data

**What section of the website did the attacker use to scrape user email addresses?**

Analisando as linhas que não se utilizaram de nenhuma ferramenta com o comando:

*$ cat -n access.log | grep "Firefox"*

Observando a seguinte linha:

*97 ::ffff:192.168.10.5 - - [11/Apr/2021:09:10:57 +0000] "GET /rest/products/37/reviews HTTP/1.1" 200 503 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0"*

Observa-se que foi feito no endpoint */rest/products/37/reviews*. Logo, a flag é: products reviews

RESPOSTA: products reviews

**Was their brute-force attack successful? If so, what is the timestamp of the successful login? (Yay/Nay, 11/Apr/2021:09:xx:xx +0000)**

Sabendo que o brute-force foi executado pelo “Hydra”, ao se utilizar o comando abaixo, verifica-se se houve sucesso no brute-force, assim como o seu timestamp se existe sucesso:

*$ cat access.log | grep "Hydra" | grep "200"*

*::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 200 831 "-" "Mozilla/5.0 (Hydra)"*

RESPOSTA: Yay, 11/Apr/2021:09:16:31 +0000

**What user information was the attacker able to retrieve from the endpoint vulnerable to SQL injection?**

Verificando a ferramenta “curl” (escolhida para ser analisada pois é utilizada logo após o sqlmap), encontra-se a seguinte requisição:

*631 ::ffff:192.168.10.5 - - [11/Apr/2021:09:32:51 +0000] "GET /rest/products/search?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 200 3742 "-" "curl/7.74.0"*

Com isso, verifica-se que os parâmetros “email” e “password” são requisitados pelo atacante.

RESPOSTA: email, password

**What files did they try to download from the vulnerable endpoint? (endpoint from the previous task, question #5)**

Verificando as últimas requisições, que foram as que o atacante buscou os arquivos no endpoint /ftp, encontram-se as seguintes linhas, que possuem a resposta para a pergunta a ser respondida:

*641 ::ffff:192.168.10.5 - - [11/Apr/2021:09:34:40 +0000] "GET /ftp/www-data.bak HTTP/1.1" 403 300 "-" "Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0"*

*642 ::ffff:192.168.10.5 - - [11/Apr/2021:09:34:43 +0000] "GET /ftp/coupons\_2013.md.bak HTTP/1.1" 403 78965 "-" ""Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0"*

RESPOSTA: coupons\_2013.md.bak, www-data.bak

**What service and account name were used to retrieve files from the previous question? (service, username)**

O nome do serviço foi encontrado no endpoint (ftp) enquanto o nome da conta foi encontrado observando o arquivo “vsftpd.log”:

*Sun Apr 11 08:15:33 2021 [pid 6482] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"*

*Sun Apr 11 08:15:55 2021 [pid 6529] CONNECT: Client "::ffff:127.0.0.1"*

*Sun Apr 11 08:15:58 2021 [pid 6526] [ftp] OK LOGIN: Client "::ffff:127.0.0.1", anon password "?"*

RESPOSTA: ftp, anonymous

What service and username were used to gain shell access to the server? (service, username)

Observando o outro arquivo (auth.log), verifica-se o serviço ssh, e nome de usuário www-data, ao observar as seguintes requisições repetidas diversas vezes:

*Apr 11 09:39:48 thunt sshd[8244]: Failed password for www-data from 192.168.10.5 port 40100 ssh2*

RESPOSTA: ssh, www-data