Practical Exam

Task 1:

In the digital realm, the waters can be treacherous. The currents are swift, and the winds are unpredictable. The machine you seek has already fallen victim to the tides, its shores washed away by the hacker's cunning. But like a castaway on a deserted island, there may be hope yet. The hacker has left a message, a message that could be the key to unlocking the secrets of the machine. But be warned, for the hacker is a master of deception, and the message is but a breadcrumb on a treacherous path. To navigate this path, you must master the art of the Docker, like a sailor mastering the art of the rigging. With Docker as your guide, you can traverse the perilous waters and uncover the secrets that lie hidden within. Are you ready to brave the digital tides and unlock the secrets of the machine left behind by the hacker?
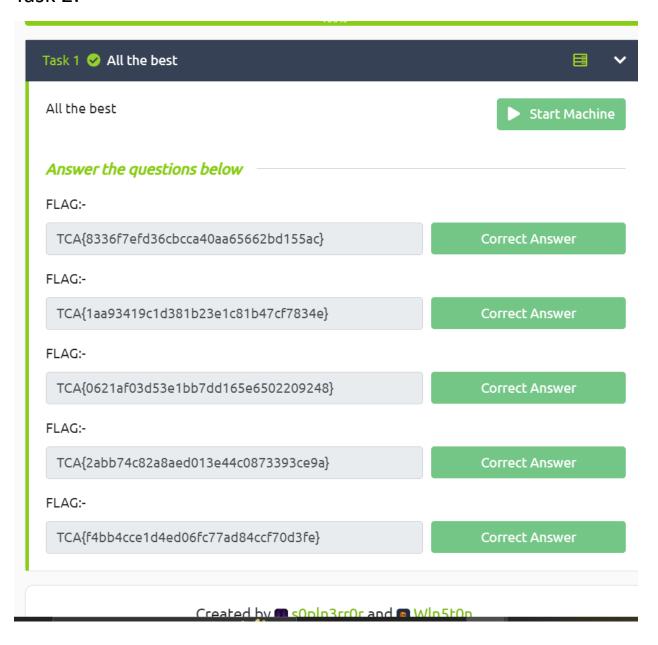
▶ Start Machine

Answer the questions below

FLAG:-

TCA{fa708492389368a73605155eabe48fa5}
Correct Answer

FLAG:-

TCA{a9904085a33ce938bccd7eba6e86f5b6}
Correct Answer

FLAG:-

TCA{e4a1c01309a5e49e4aa7376dd2170ce9}
Correct Answer

FLAG:-

TCA{e6101e8388ca49c410c04381ff5e8824}
Correct Answer

FLAG:-

TCA{5ee4238fa6363adfeaf6ae61911ffce6}
Correct Answer

```
root@ip-10-10-213-23:~/Desktop# rutscan -a 10.10.227.179
rutscan: command not found
root@ip-10-10-213-23:~/Desktop# rustscan -a 10.10.227.179
.-----. .-. .-. .----..----.   .-----. .----.   .--. .-. .-.
| {} }| { } |{ {__ {_   _}{ {_ / __}/ {} \|   `| |
| .-. \| {_} |.-._} } | |  .-._} }\  __}/ /\ \| |\  | |
`-' `-'`-----'`----'  `-'  `----' `----'`-'  `-'`-' `-'`-'
The Modern Day Port Scanner.
_____
: https://discord.gg/GFrQsGy         :
: https://github.com/RustScan/RustScan :
--------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/rustscan/.rustscan.toml"
[~] File limit higher than batch size. Can increase speed by increasing batch si
ze '-b 1048476'.
Open 10.10.227.179:22
Open 10.10.227.179:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-28 09:08 UTC
Initiating Ping Scan at 09:08
Scanning 10.10.227.179 [2 ports]
Completed Ping Scan at 09:08, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:08
Completed Parallel DNS resolution of 1 host. at 09:08, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0
```

```
root@ip-10-10-213-23:~/Desktop# sudo nmap -T4 -sC -sV -p- -oN nmap.log 10.10.213.
23

Starting Nmap 7.60 ( https://nmap.org ) at 2023-04-28 10:14 BST
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.59% done; ETC: 10:18 (0:01:46 remaining)
Stats: 0:02:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.66% done; ETC: 10:17 (0:00:05 remaining)
Stats: 0:04:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 10:19 (0:00:09 remaining)
Stats: 0:05:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 10:19 (0:00:00 remaining)
Stats: 0:05:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.79% done; ETC: 10:20 (0:00:00 remaining)
Nmap scan report for ip-10-10-213-23.eu-west-1.compute.internal (10.10.213.23)
Host is up (0.000011s latency).
Not shown: 65526 closed ports
PORT      STATE     SERVICE          VERSION
22/tcp    open      ssh              OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; pr
otocol 2.0)
| ssh-hostkey:
|   2048 5a:57:5f:81:a1:3c:1e:5f:8c:e1:ac:a2:2c:7c:85:d0 (RSA)
|   256 ed:a1:5b:b1:3a:36:c4:df:5d:68:3e:f1:71:99:83:30 (ECDSA)
|_  256 3d:e2:0d:f7:1b:3f:22:cc:90:a1:da:3f:73:a8:39:4d (EdDSA)
80/tcp    open      http             WebSockify Python/3.6.9
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 405 Method Not Allowed
|     Server: WebSockify Python/3.6.9
```

```
root@ip-10-10-213-23:~# ffuf -c -ic -r -u http://10.10.213.23/FUZZ -w /usr/share
seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -e .php,.html,.txt
ncountered error(s): 1 errors occured.
       * stat /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medi
m.txt: no such file or directory

uzz Faster U Fool - v1.3.1

TTP OPTIONS:
 -H                Header `"Name: Value"`, separated by colon. Multiple -H fl
gs are accepted.
 -X                HTTP method to use
 -b                Cookie data `"NAME1=VALUE1; NAME2=VALUE2"` for copy as cur
 functionality.
 -d                POST data
 -ignore-body      Do not fetch the response content. (default: false)
 -r                Follow redirects (default: false)
 -recursion        Scan recursively. Only FUZZ keyword is supported, and URL
-u) has to end in it. (default: false)
 -recursion-depth  Maximum recursion depth. (default: 0)
 -recursion-strategy Recursion strategy: "default" for a redirect based, and "g
```

Task 2:

Task 1 ✅ All the best

All the best

▶ Start Machine

Answer the questions below

FLAG:-

TCA{8336f7efd36cbcca40aa65662bd155ac}

Correct Answer

FLAG:-

TCA{1aa93419c1d381b23e1c81b47cf7834e}

Correct Answer

FLAG:-

TCA{0621af03d53e1bb7dd165e6502209248}

Correct Answer

FLAG:-

TCA{2abb74c82a8aed013e44c0873393ce9a}

Correct Answer

FLAG:-

TCA{f4bb4cce1d4ed06fc77ad84ccf70d3fe}

Correct Answer

Created by 🟪 s0pln3rr0r and 🟥 Wln5t0p

```
root@ip-10-10-213-23:~/Desktop# wget http://10.10.213.33/hidden_text/secret.dic
--2023-04-28 10:26:49--  http://10.10.213.33/hidden_text/secret.dic
Connecting to 10.10.213.33:80... failed: No route to host.
root@ip-10-10-213-23:~/Desktop#
```