

Proof of Concept- GPCSSI Buddy 52

Team Members :

Loveneesh Dhir-TEC-253

Parth Sikka TEC-153

KRISHNENDU SAMANTA SCH-046

Divyanshi Sharma Tec -054

Laksh Rawat NTE -066

Challenge 1(Mr. Robot) :

I am a so-called TOP MIDDLE EAST HACKER; I help people become MR. ROBOT

A simple Google search for “How to become Mr. Robot” lead us to a Quora page for this question :

The screenshot shows a Quora page with the following elements:

- Header:** Quora logo, navigation links (Home, Answer, Spaces, Notifications), and a search bar.
- Question:** "Looking for career options after 12th Commerce?" with a brief description: "Get a BBA degree from Jamia Hamdard, powered by upGrad. (Online + blended mode)." and a "Learn More" link.
- Answer by Abbas Naderi:** A user profile picture and name "Abbas Naderi, so-called Top Middle East Hacker" are shown. The answer text reads: "Usually by being stupid." followed by two paragraphs. The first paragraph states: "A high-profile hacker is like a high-profile spy. He probably won't live long if he's well known, he will be caught at any airport or other port, will have a good bounty on his head, and a much better chance of getting tortured for all the high-profile projects and information that he has." The second paragraph states: "All of the best hackers in the world, usually organized into APT teams, do everything in their power to remain anonymous. They even use a complete separate computer and network for hacking, never touch anything that related to their personal identity in a hacking project, and pay extra ... (more)". Below the text are icons for upvotes (81), downvotes (3), and comments (9).
- Comments:** A section labeled "9 comments" is visible.
- Related Spaces:** A section titled "Related Spaces (More Answers Below)" featuring four space cards: "Ethical Hacking Expert", "Cyber News & Threats", "Cyber Security", and "The Top 1000 Most Influential Hackers".

This question easily gives away the answer as **Abbas Naderi**, the so-called TOP MIDDLE EAST HACKER.

FLAG : CTF{Abbas Naderi}

Challenge 2(GOOGLECAN'T) :

But if you want to go here even Google Results cannot take you.

<https://chall.hackershala.com>

Knowing that “/robots.txt” is a file that cannot be indexed by Google, this was again a simple give-away and editing the url to :

<https://chall.hackershala.com/robots.txt>

Gave us the flag :



FLAG: CTF{YOUAREHACKER}

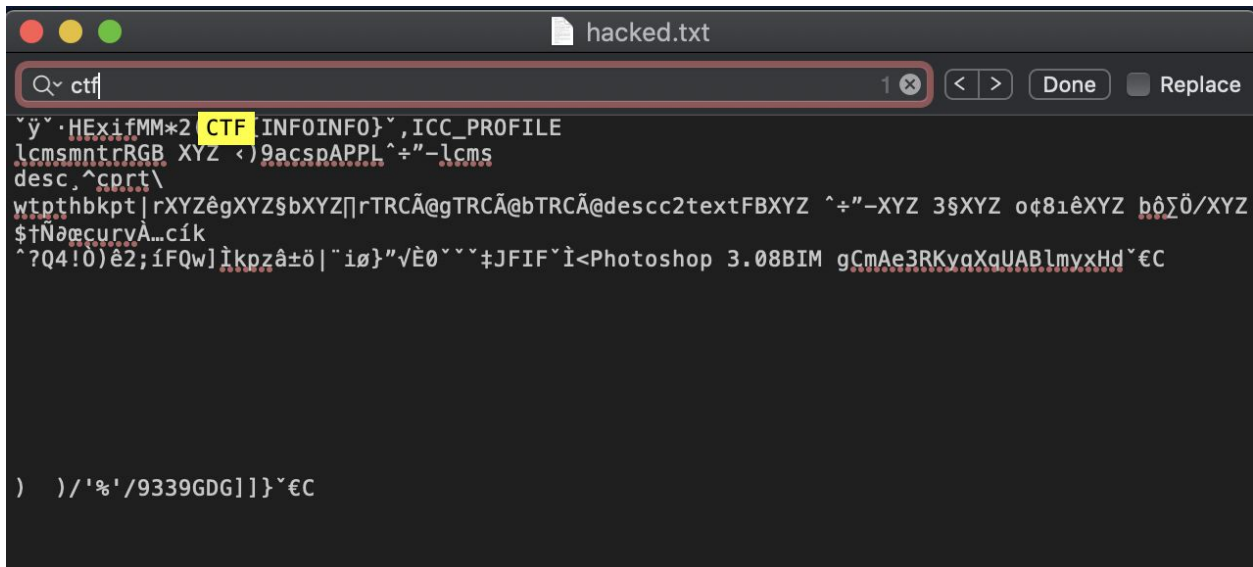
Challenge 4(HACKED) :

While investigating a cyber case you got Hacker's image. Images say a lot of information about a person.

The most common practice of cryptography is hiding the data inside the raw text of the image.

This was again done by renaming the file as ".txt" instead of a ".jpg"

The dump was then searched for the keyword "CTF" and voila! We got the flag!



```
Q~ ctf| 1 x < > Done Replace
y·HExiMM*2 CTF INFOINFO},ICC_PROFILE
lcmsmnrRGB XYZ <)9acspAPPL^÷"-lcms
desc,^cprt\
wtpthbkpt|rXYZêgXYZ$bXYZ[]rTRCÃ@gTRCÃ@bTRCÃ@descc2textFBXYZ ^÷"-XYZ 3$XYZ oq81êXYZ bôΣô/XYZ
$†NæcurvÅ...cík
^?Q4!0)é2;íFQw]îkpzâ±ö|"iø}"√È0~`~‡JFIF~î<Photoshop 3.08BIM gCmAe3RKyaXqUABlmyxHd~€C
) )/'%'/9339GDG[]}]~€C
```

FLAG : CTF{INFOINFO}

Challenge 5(SERVER ATTACKED):

In this challenge, we were supposed to go through the the network Dump of a server and look for an attacker :

This required us to go through all the files:

Observation :

The Network Dump consisted of three dates :

1. 30th July
2. 31st July
3. 3rd August

On observing the file for the date of 30th July, we observed an IP which tried to generate a reverse shell on its port 80 as shown in the image below :

```
125.63.105.227 - - [30/Jul/2019:07:25:28 -0400] "GET / HTTP/1.1" 200 5069
125.63.105.227 - - [30/Jul/2019:07:25:30 -0400] "GET /favicon.ico HTTP/1.1" 404 209
125.63.105.227 - - [30/Jul/2019:07:26:30 -0400] "GET / HTTP/1.1" 200 5069
125.63.105.227 - - [30/Jul/2019:07:26:31 -0400] "GET /favicon.ico HTTP/1.1" 404 209
165.225.106.90 - - [30/Jul/2019:07:31:16 -0400] "GET / HTTP/1.1" 200 5069
125.63.105.227 - - [30/Jul/2019:07:31:17 -0400] "GET / HTTP/1.1" 200 5069
125.63.105.227 - - [30/Jul/2019:07:31:18 -0400] "GET /favicon.ico HTTP/1.1" 404 209
165.225.106.90 - - [30/Jul/2019:07:31:21 -0400] "GET /favicon.ico HTTP/1.1" 404 209
34.77.49.52 - - [30/Jul/2019:08:22:28 -0400] "GET / HTTP/1.1" 200 5069

78.170.236.56 - - [30/Jul/2019:08:24:37 -0400] "GET / HTTP/1.1" 200 5069
125.63.105.227 - - [30/Jul/2019:08:37:50 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:08:59:55 -0400] "-" 408 -
136.243.12.147 - - [30/Jul/2019:09:15:24 -0400] "GET /phpinfo.php HTTP/1.0" 200 88886
125.63.105.227 - - [30/Jul/2019:09:15:58 -0400] "-" 408 -
157.44.83.1 - - [30/Jul/2019:09:26:36 -0400] "GET / HTTP/1.1" 200 5069

157.44.83.1 - - [30/Jul/2019:09:26:37 -0400] "GET /favicon.ico HTTP/1.1" 404 209
157.44.49.231 - - [30/Jul/2019:09:27:26 -0400] "GET / HTTP/1.1" 200 5069
157.44.49.231 - - [30/Jul/2019:09:27:26 -0400] "GET /favicon.ico HTTP/1.1" 404 209
125.63.105.227 - - [30/Jul/2019:09:46:34 -0400] "-" 408 -
203.194.101.95 - - [30/Jul/2019:09:57:52 -0400] "GET / HTTP/1.1" 200 5069
203.194.101.95 - - [30/Jul/2019:09:57:53 -0400] "GET /favicon.ico HTTP/1.1" 404 209
203.194.101.95 - - [30/Jul/2019:09:58:51 -0400] "-" 408 -
203.194.101.95 - - [30/Jul/2019:10:00:54 -0400] "-" 408 -
203.194.101.95 - - [30/Jul/2019:10:00:54 -0400] "-" 408 -
172.105.231.199 - - [30/Jul/2019:10:07:12 -0400] "GET / HTTP/1.0" 400 362
110.249.212.46 - - [30/Jul/2019:10:29:51 -0400] "GET http://110.249.212.46/testget?q=23333&port=80 HTTP/1.1" 400 226
110.249.212.46 - - [30/Jul/2019:10:29:51 -0400] "GET / HTTP/1.0" 400 362
91.92.81.192 - - [30/Jul/2019:10:30:23 -0400] "GET / HTTP/1.1" 200 5069
139.159.202.161 - - [30/Jul/2019:10:44:53 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:10:50:01 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:10:51:32 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:10:54:38 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:10:54:38 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:10:55:10 -0400] "-" 408 -
203.194.101.95 - - [30/Jul/2019:10:55:36 -0400] "GET /index.php?SELECT%20*%20FROM%20mysql.users HTTP/1.1" 404 207
203.194.101.95 - - [30/Jul/2019:10:55:42 -0400] "GET /favicon.ico HTTP/1.1" 404 209
125.63.105.227 - - [30/Jul/2019:11:06:25 -0400] "-" 408 -
45.83.66.237 - - [30/Jul/2019:11:20:25 -0400] "GET / HTTP/1.1" 200 5069
125.63.105.227 - - [30/Jul/2019:11:22:25 -0400] "-" 408 -
125.63.105.227 - - [30/Jul/2019:11:22:25 -0400] "-" 408 -
187.110.209.107 - - [30/Jul/2019:11:40:00 -0400] "GET / HTTP/1.1" 200 5069
```

Thus, the attacker IP was located!!

FLAG: 110.249.212.46

Challenge 6(BRAINSTORM):

The clue said “**A file may lie but brain will never.**”

Thinking in terms of the clue, the file must be deceptive in essence, it must not be a “.exe” file. So analysing the Raw Dump by converting the extension to “.txt”, I could make out that the file is infact a “PDF” and not an “.exe”

The file on being read came out to be blank, but again, the hint was our way to move forward.

It was indeed a Deception!

The File contained a flag in white color which is why it wasnt visible in the pdf.

Editing the PDF using Adobe Acrobat ProDC, we could select the text which said :

}tididuoy{ftc

Which when read in reverse :

Ctf{youdidit}.

FLAG : CTF{YOUIDIDIT}

Challenge 3(HASHTAG ALL AROUND):

This was a kind of OSINT challenge.

It mentioned that the social media platform must be the one that has a feature that twitter isn't capable of.

Searching google for #hackershalahackershala gave us a direct link to a facebook post.

Now, we couldn't ask the owner for the flag because of obvious reasons.

I tried viewing the post and the options in the post.

It struck to me immediately that Twitter doesn't let us view the EDIT History for any post, however, Facebook does.

On viewing the Edit history for the POST, I came across the flag.

FLAG: CTF{Wohoooo}