Category: Forensics
Challenge: Secure Password

Write-up:

We are given a .ad1 file. When we research it, we can understand that it is a file type associated with Forensic Toolkit by Accessdata. It is an image file!

One can download many tools, but I will be using the FTK Imager, which Accessdata provides.

Since it is an image file, we need to open this evidence item as an Image File in the program. When we open it, we can see some folder and files under the root directory.

After looking at some folders and files, one can notice the folder named "not important files', and in that folder, there is a rar file protected by a password!
Since we are given the information that riat3n is using his password everywhere, we may find his password if we can crack this archive file.

We can use some tools on Kali Linux to crack the file. I used the "john" tool to crack it. But first, we need to extract the hash from rar to crack it with john. For this specific step, I used a tool called "rar2john".

```
┌──(root💀kali)-[~/writeup/pw]
└─# rar2john readme.rar > riat3n_password.hash

┌──(root💀kali)-[~/writeup/pw]
└─# ls
readme.rar  riat3n_password.hash

┌──(root💀kali)-[~/writeup/pw]
└─# cat riat3n_password.hash
readme.rar:$rar5$16$6f46e878ed3817b6762284b679e2c4e3$15$ef3809eae68794f73faa15d38a4678e4$8$eed31b0f4e6dbd44
```

After extracting the hash, we can proceed to the cracking step. It might take time depending on the password.

```
┌──(root💀kali)-[~/writeup/pw]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt riat3n_password.hash
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
easypeasy        (readme.rar)
1g 0:00:01:59 DONE (2021-02-27 12:00) 0.008348g/s 2049p/s 2049c/s 2049C/s emosita..easypeasy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
┌──(root💀kali)-[~/writeup/pw]
└─# john --show riat3n_password.hash
readme.rar:easypeasy

1 password hash cracked, 0 left
```

Password is "**easypeasy**", therefore,
Flag is: SUCTF{easypeasy}