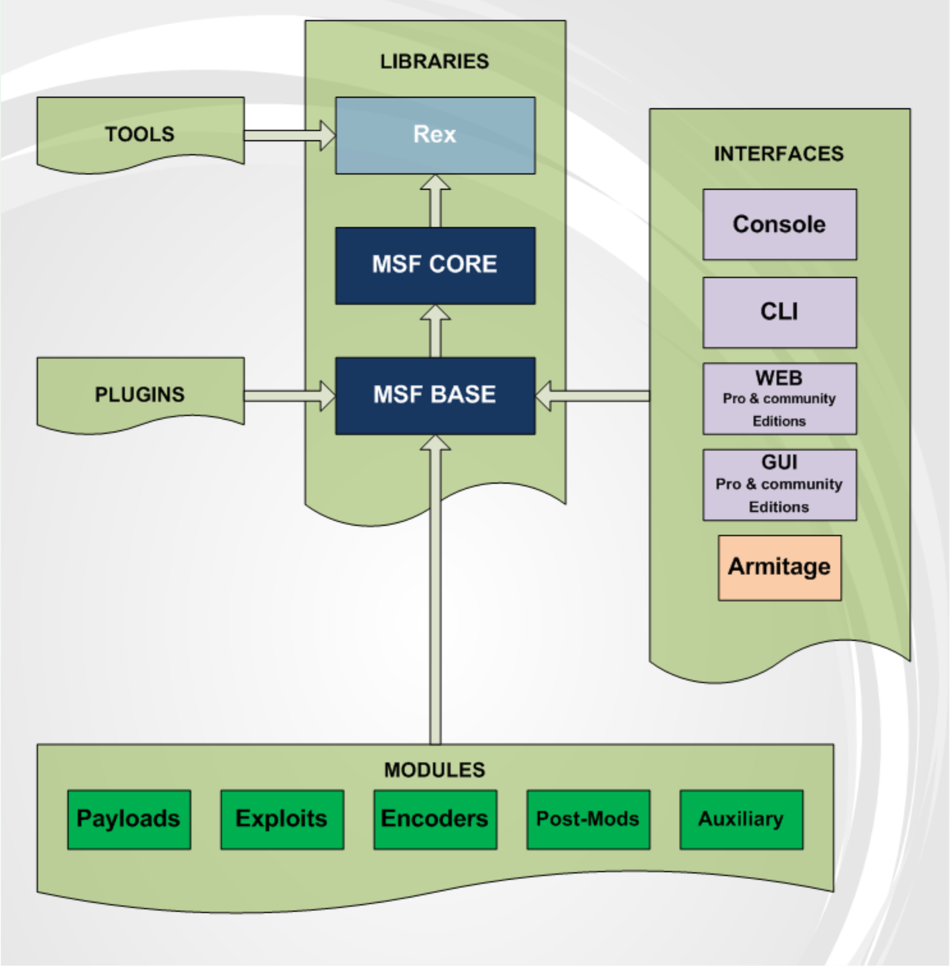
Introduction to Metasploit

NSSECU2 | ADVANCED AND OFFENSIVE SECURITY

INTRODUCTION TO METASPLOIT

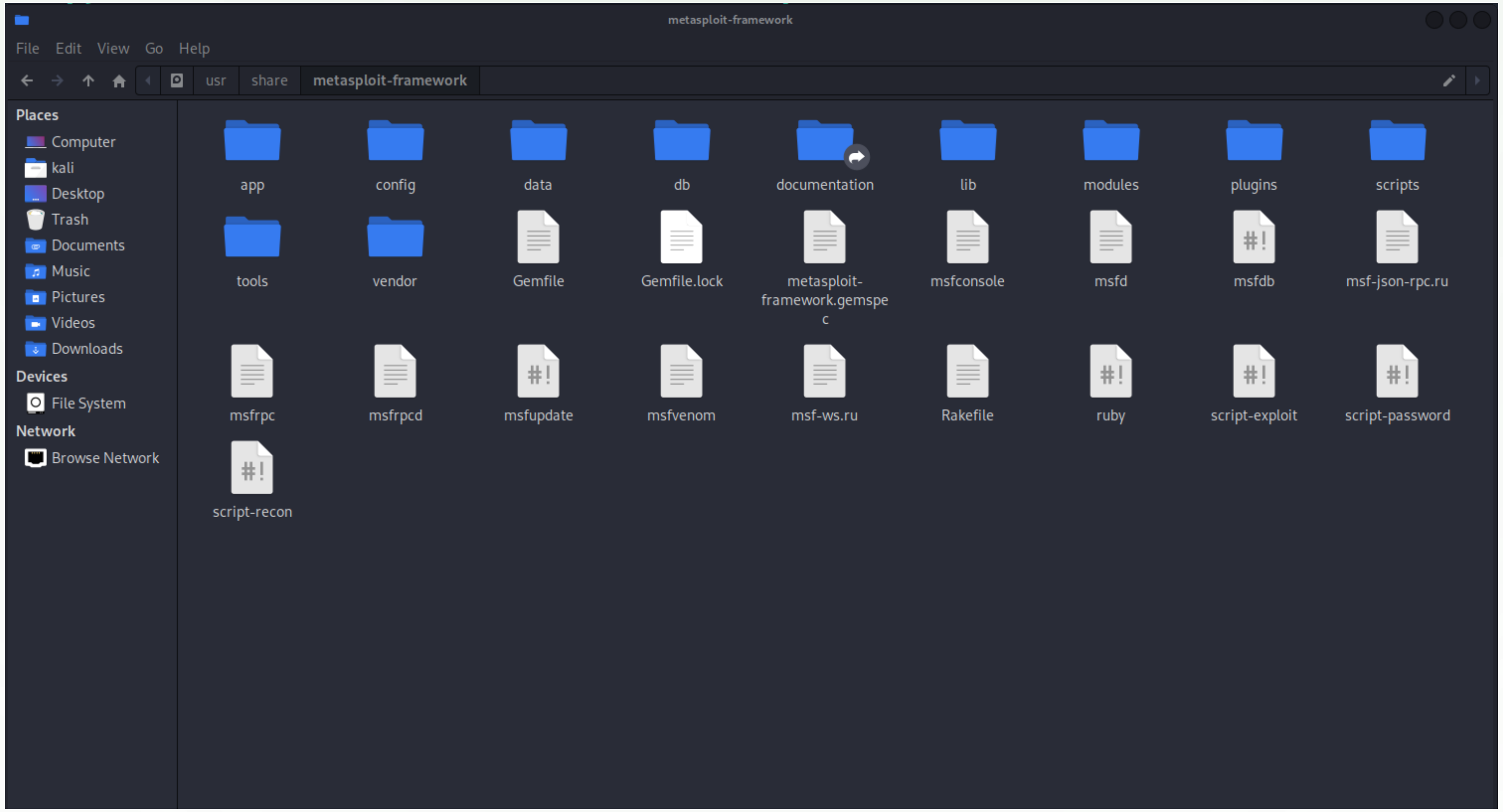
- It is an auditing tool freely available to security professionals
- Pre Installed on Kali Linux
- Has a collection of
  - Commercial grade exploits
  - Extensive exploit development environment
  - Network information gathering tools
  - Web vulnerability plugins

METASPLOIT ARCHITECTURE



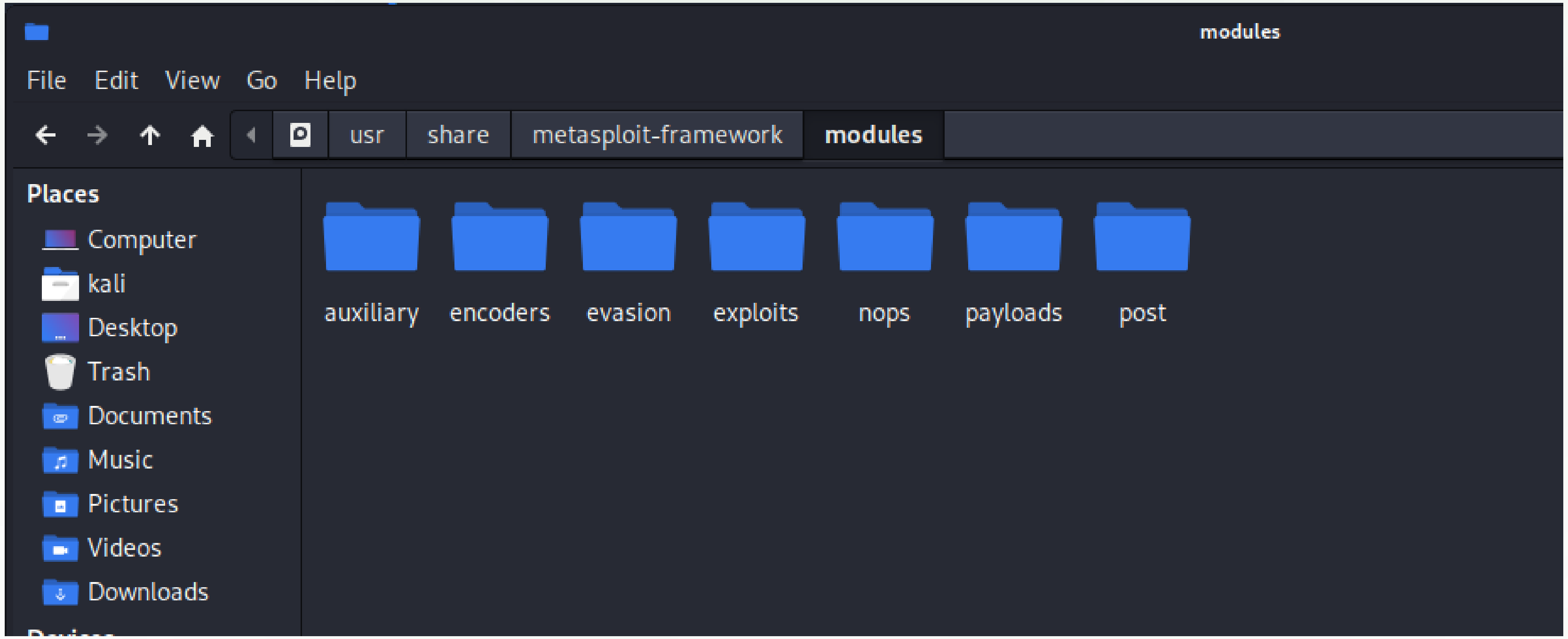
METASPLOIT FILESYSTEM AND LIBRARIES

- In Kali Linux, Metasploit is provided in the metasploit-framework package and is installed in the **/usr/share/metasploit-framework** directory



METASPLOIT MODULES AND LOCATIONS

- Metasploit primary modules are located under **/usr/share/metasploit-framework/modules/** and custom modules are located under **~/.msf4/modules/**



METASPLOIT MODULES AND LOCATIONS

Exploits - Modules for exploiting a vulnerability and delivering a payload. There are remote exploits, local exploits, privilege escalation exploits, client-side exploits, web application exploits and many others.

Payloads - Modules for performing an action during the exploitation, e.g. establishing meterpreter session, reverse shell, executing a command, downloading and executing a program etc. Payloads can be staged and non-staged.

Post - Modules for post exploitation action such as credential / hash dumping, local privilege escalation, backdoor installation, sensitive data extraction, network traffic tunneling (proxying), keylogging, screen capturing and many other actions.

Auxiliary - Modules for auxiliary actions such as network scanning, enumeration, vulnerability scanning, login brute force and cracking, fuzzing, spidering (traversal), data extraction and many others.

Encoders - Modules for payload encoding and encryption such as base64, XOR, shikata_ga_nai etc. This can help with obfuscation to evade defenses such as Antivirus or NIDS (network intrusion detection systems), EDR (endpoint detection and response) etc.

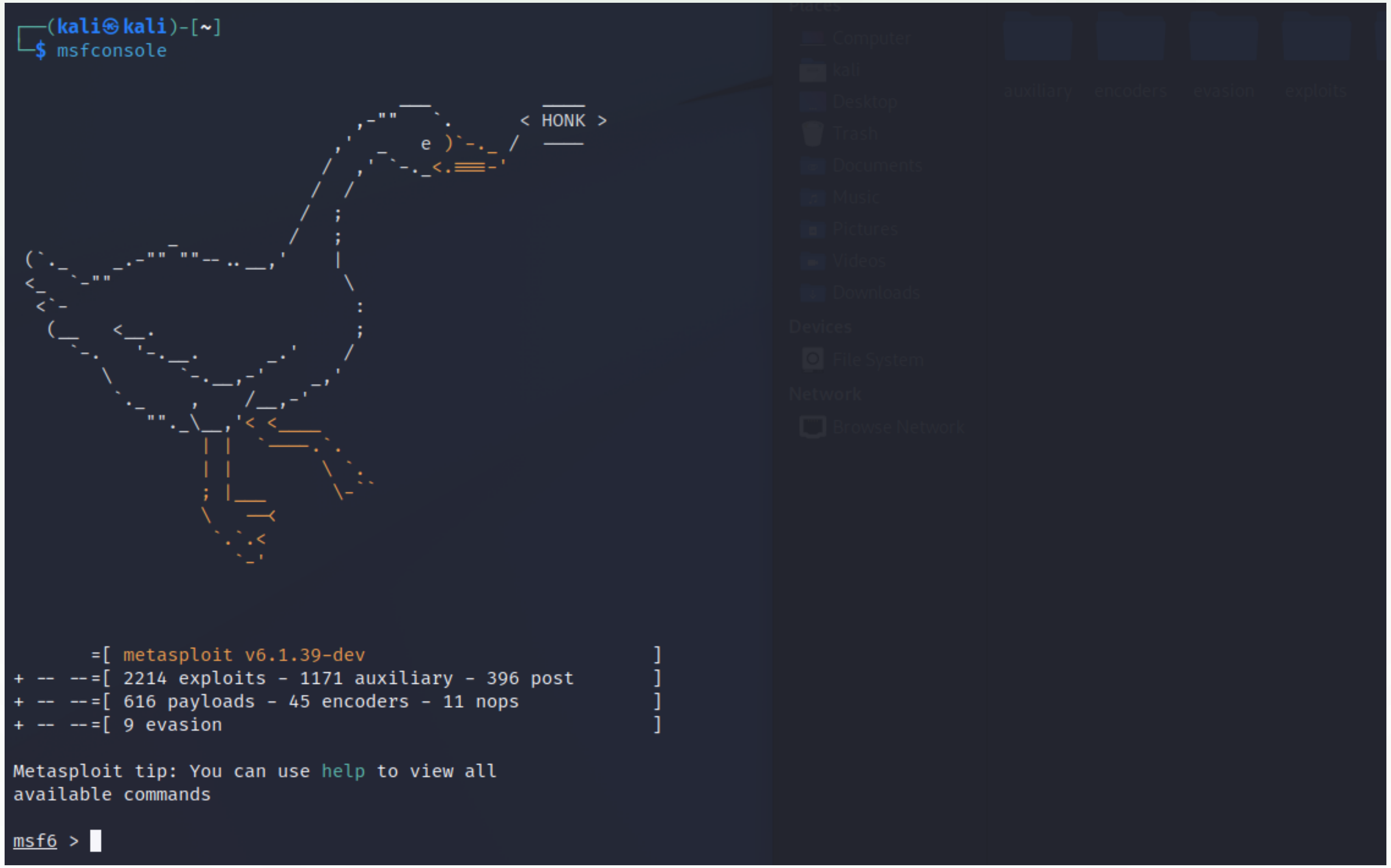
Evasions - Modules for evading defenses such as Antivirus evasion, AppLocker bypass, software restriction policies (SRP) bypass etc.

Nops - Modules for generating a harmless, benign "No Operation" instructions, e.g. for padding purposes, sliding in memory during exploitation etc.

Source - www.infosecmatter.com/metasploit-module-library/

METASPLOIT FUNDAMENTALS

MSFConsole is the only supported way to access most Metasploit commands



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

                                   ___          ____
                               ,-""   `.      < HONK >
                              ,' _   e )`-._ /  ----
                            /  ,' `-._<.===-'
                           /  /
                          /  ;
              _          /   ;
 (`._    _.-"" ""--..__,'    |
 <_   `-""                    \
  <`-                          :
   (__   <__.                  ;
     `-.   '-.__.      _.'    /
        \      `-.__,-'   _,'
         `._    ,    /__,-'
            ""._\__,'< <____
                 | |  `----.`.
                 | |        \ `.
                 ; |___      \-``
                 \   --<
                  `.`.<
                    `-'



       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands

msf6 > █
```