GETTING STARTED WITH METASPLOIT FRAMEWORK

-Deepanshu

d78ui98

OUR AGENDA

- What is metasploit?
- Its history
- Basic terminologies
- Architecture of metasploit
- Modules
- Few demos
- Conclusion

WHAT IS METASPLOIT FRAMEWORK?

METASPLOIT FRAMEWORK

- Its an open source exploitation framework.
- It is not just a single tool but collection of several.
- Used mostly for Penetration Testing, Research, Creating and Testing new exploits.
- It provides infrastructure to automate mundane and complex tasks.

LIL BIT HISTORY

- Created by HD Moore in 2003 in perl
- Follow up project came in 2004 Metasploit 2.0
- Metasploit 3.0 released in 2007
- In 2009 Metasploit was acquired by Rapid 7
- Then Metasploit pro and Metasploit Express were devloped

BASIC TERMINOLOGIES

#Vulnerability

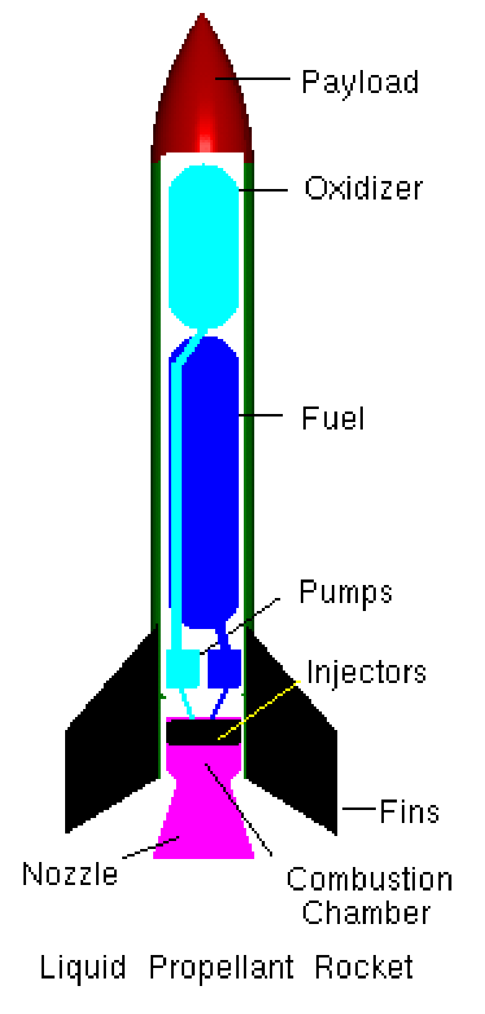
Weakness in a system, a bug which is to be exploited

#Exploit

- *Basically a piece of code to take advantage of a Vulnerability*

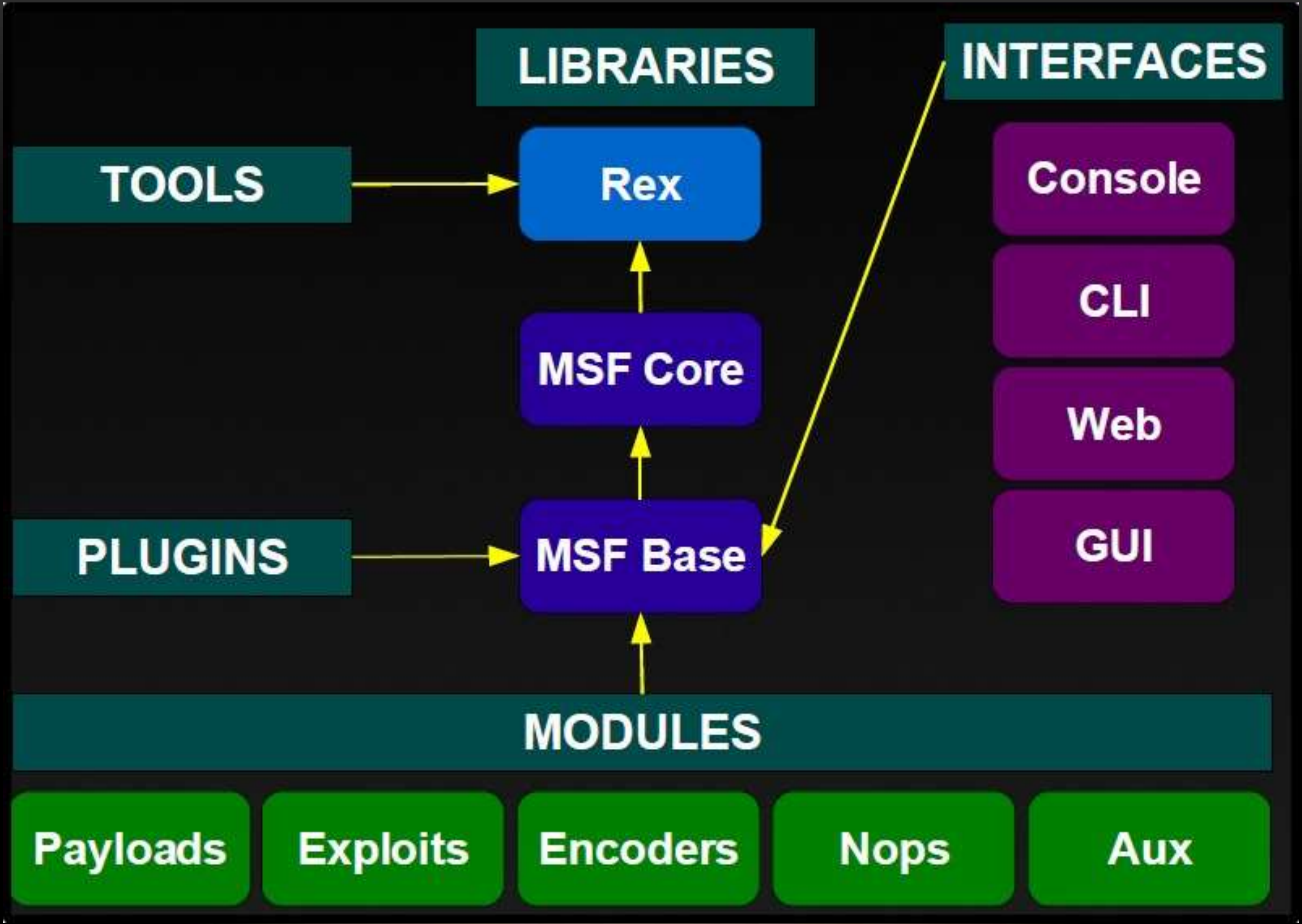
#PAYLOAD

- *Another piece of code that is executed through given exploit.*
- *lets us control a computer system after it's been exploited*



ARCHITECTURE OF METASPLOIT

- It is kind of Important to understand the basic structure of metasploit how is it designed. We should not directly start with the exploiting targets.


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux

MODULES

- Exploits
- Payloads
- Encoders
- Nops
- Auxiliary

#ENCODERS

- Encoders are used to evade the anti- virus Softwares and firewall
- However it has no effect on the functionality of out exploit
- Popular encoders are –
  1. shikata_ga_nai
  2. base64
  3. powershell_base64

#NOPS

- NOP is short for No OPeration
- NOPs keep the payload sizes consistent ensuring that validly executable by the processor.. Basically makes payload stable

#AUXILIARY

- Provides additional functionality like scanning, fuzzing, Information gathering

#PAYLOADS

- Singles

  Usually standalone. Fire and forget type.

- Stagers

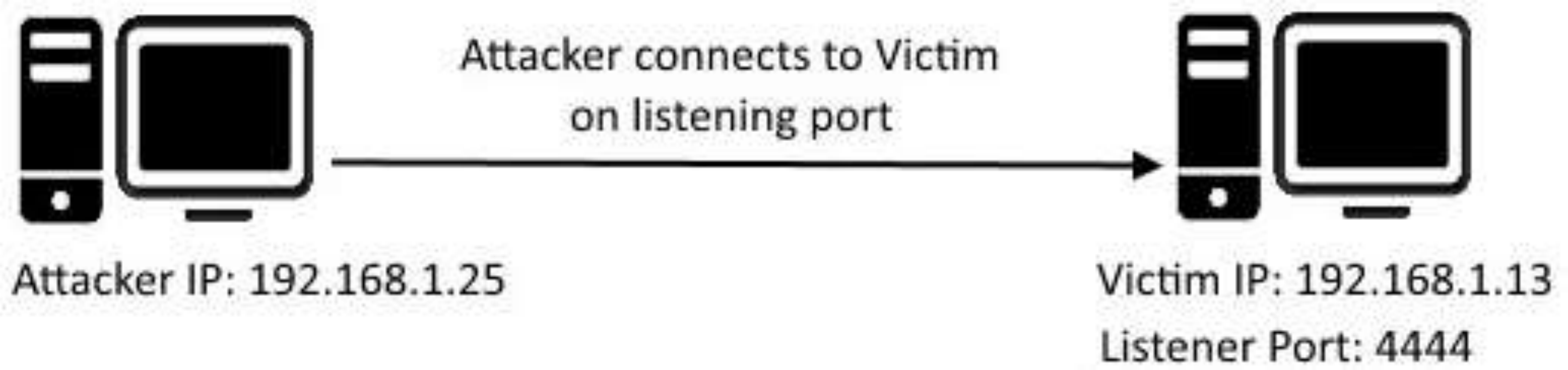
  Payload is divided into stages.

- Stages

  Components of stager module.

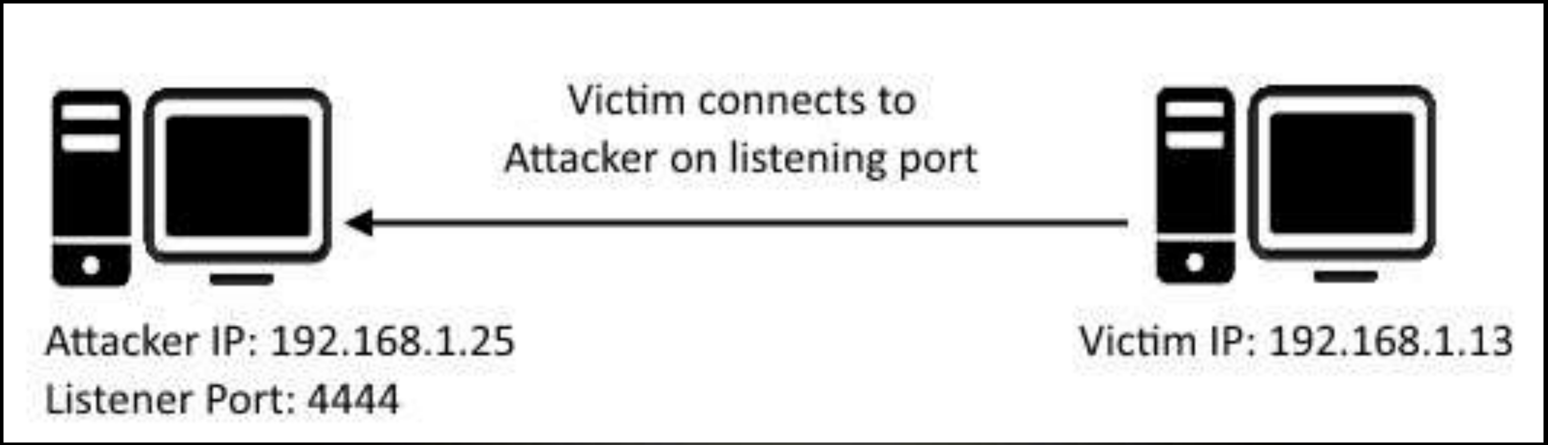
BIND TCP SHELL

- **In case of bind tcp an exploit opens a vulnerable port in victim machine. And then it waits for connection from attacker**


Attacker connects to Victim on listening port
Attacker IP: 192.168.1.25
Victim IP: 192.168.1.13
Listener Port: 4444

BIND REVERSE TCP

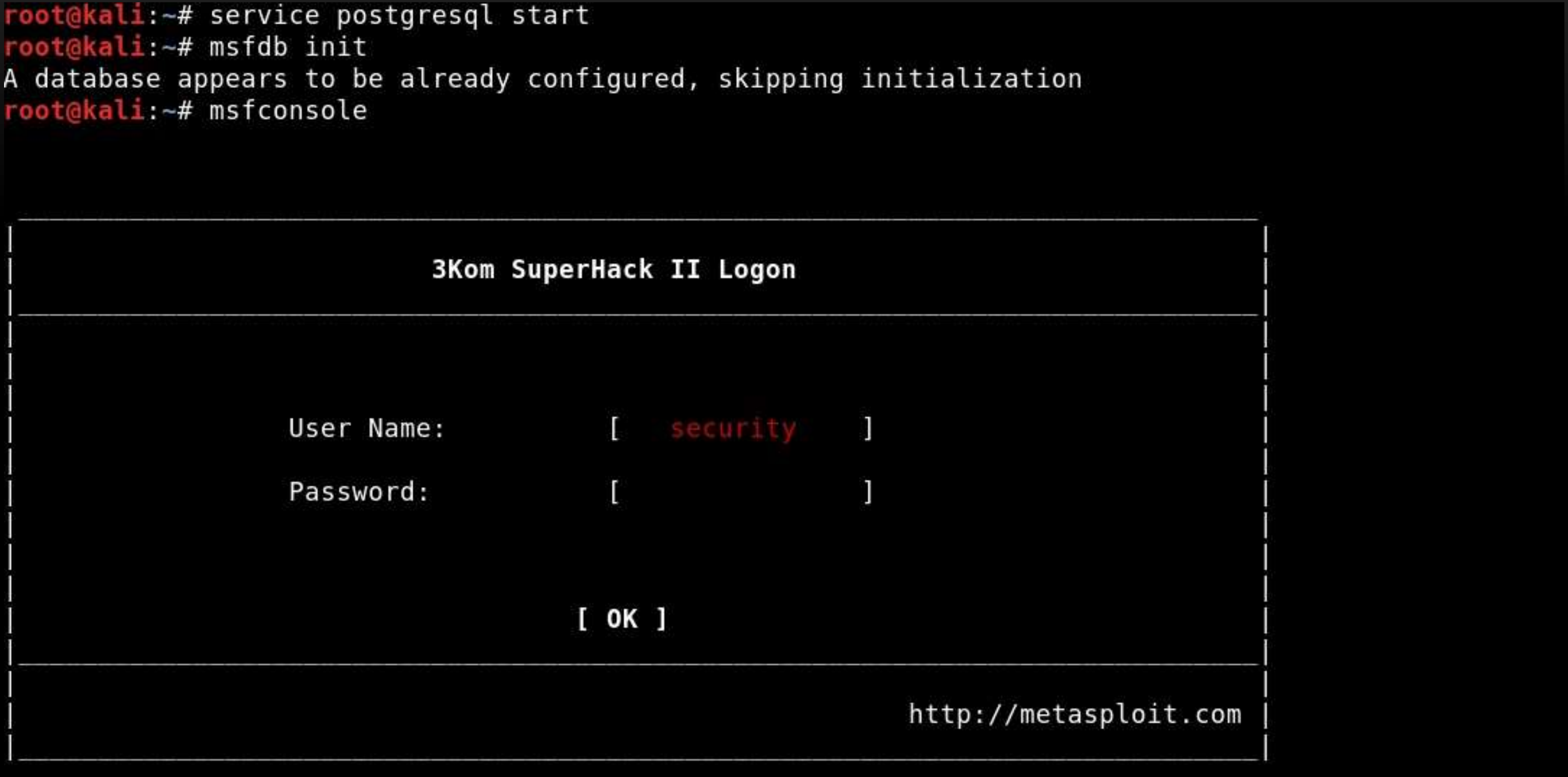
- In case of bind reverse tcp the target machine communicate back to attacker machine. Attacker machine has listening port open on which it receives connection.



NOW WE KNOW ENOUGH THEORY TO TRY OUT METASPLOIT FRAMEWORK

3 INITIAL STEPS

1. Start the postgresql service
2. Then make sure that msf database is running
3. Launch the metasploit framework by typing in msfconsole



```
root@kali:~# service postgresql start
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~# msfconsole


 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security   ]                         |
|                                                                              |
|                 Password:           [              ]                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       http://metasploit.com |
|______________________________________________________________________________|
```

SOME COMMANDS

- Show exploits
- Search
- Show info
- Show options
- Set

- Rhost
- Lhost
- Exploit or run
- Show advanced
- Back

DEMO 1

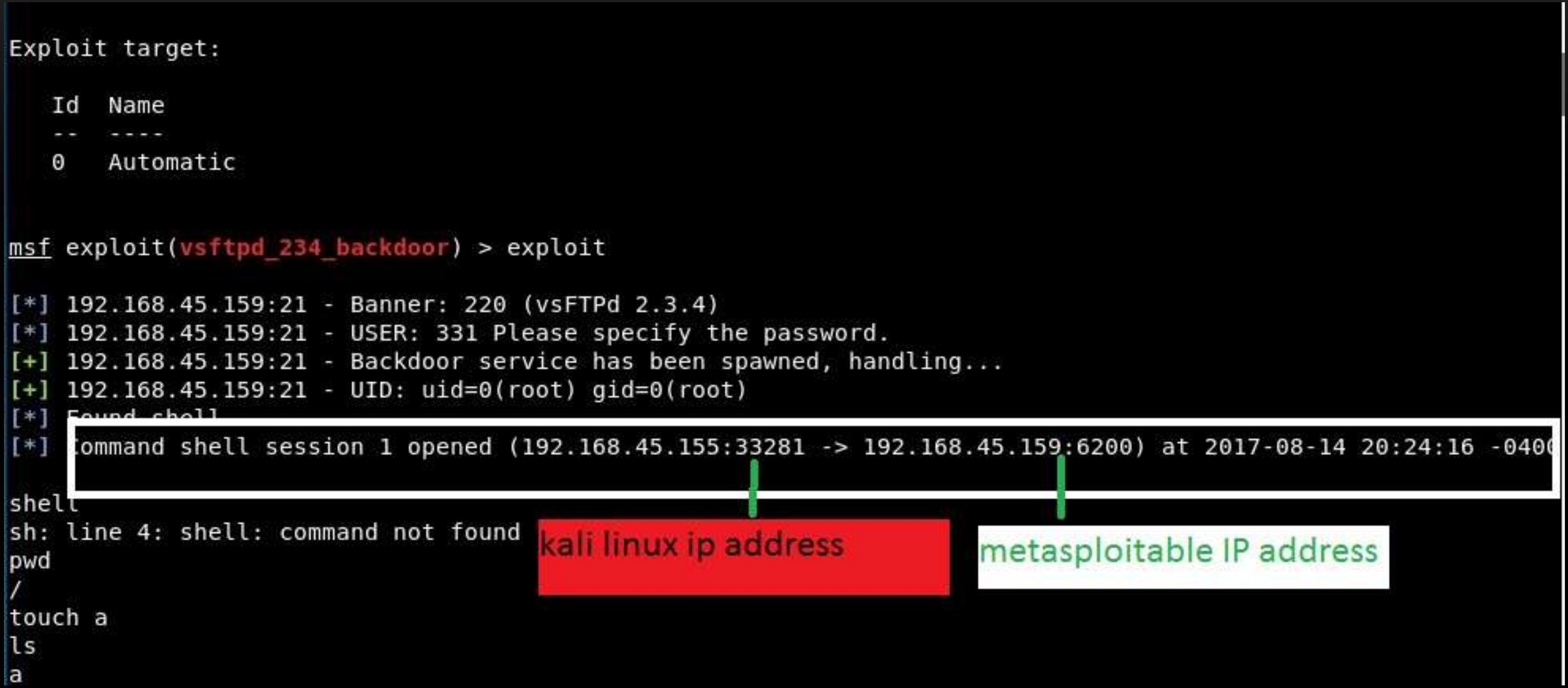
Using tcp scanner auxiliary

```
            ########                  #
        #################            #
     ######################         #
    #########################      #
  ############################
 ##############################
 ###############################
###############################
##############################
                #    ########    #
   ##       ###        ####   ##
                        ###   ###
                      ####   ###
 ####          ##########   ####
 #######################   ####
   ####################   ####
    ##################  ####
      ############      ##
         ########        ###
        #########        #####
      ############      ######
     ########     #########
       #####      ########
         ###      #########
        ######   ############
       #######################
       #   #   ###  #   #   ##
       ########################
        ##     ##   ##     ##
              http://metasploit.com
```

LETS START EXPLOITING

DEMO 2

Getting shell on Metasploitable VM



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.45.159:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.45.159:21 - USER: 331 Please specify the password.
[+] 192.168.45.159:21 - Backdoor service has been spawned, handling...
[+] 192.168.45.159:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.45.155:33281 -> 192.168.45.159:6200) at 2017-08-14 20:24:16 -0400

shell
sh: line 4: shell: command not found
pwd
/
touch a
ls
a
```

A SIMPLE COMMAND SHELL FROM ATTACKER TO VICTIM

#MSFVENOM

- It is a standalone payload generator and encoder
- Msfvenom replaced msfpayload and msfencoder in 2015.
- It allows use to create playloads in c, exe, python, java formats.
- Basically allow us to create mallicious files.

MSFVENOM STEPS

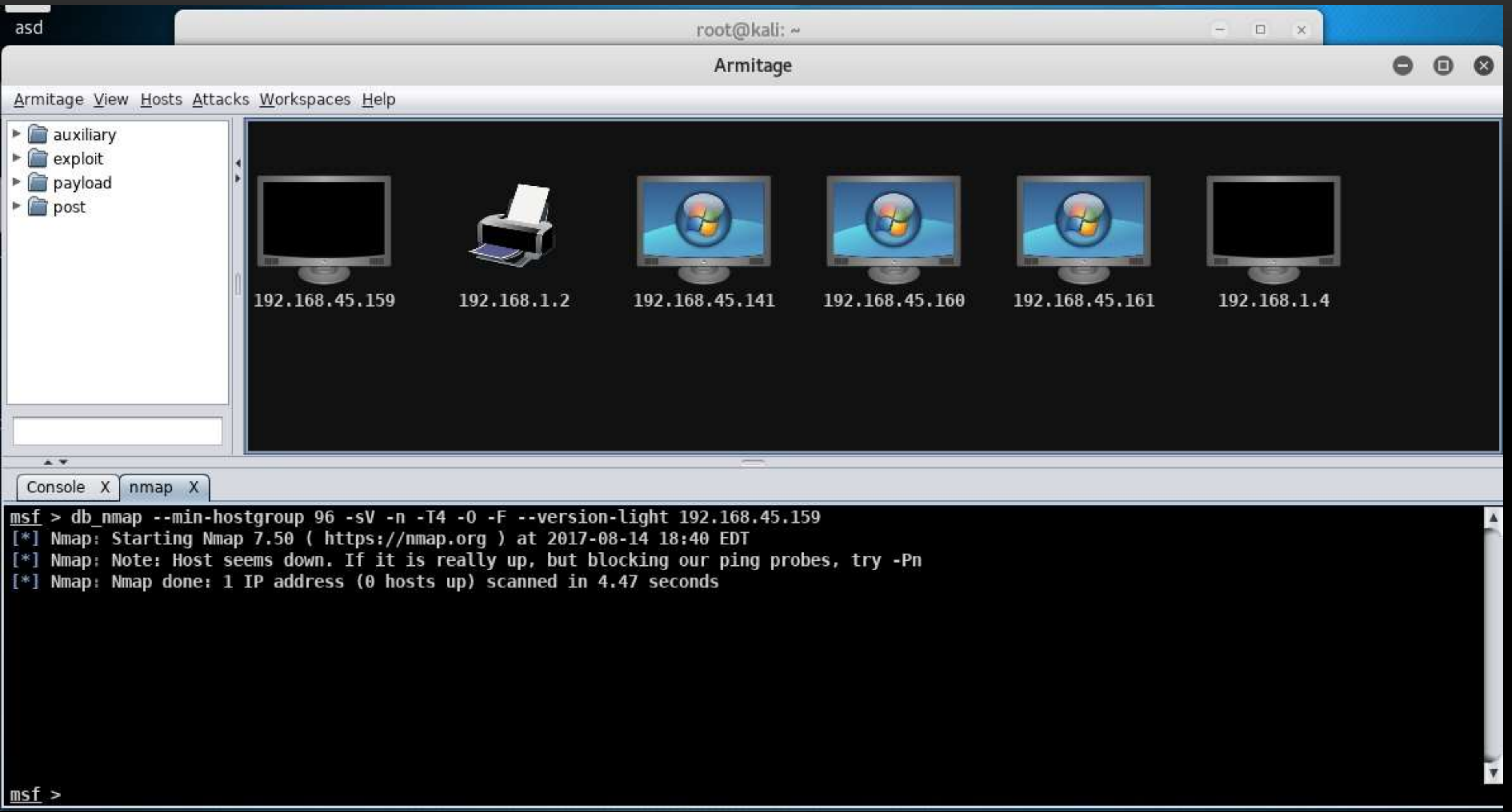
- Create a malicious file.
- Start the payload handler.
- Get victim to run the malicious file.

DEMO 3

Meterpreter shell on windows 7 machine via msfvenom

ARMITAGE

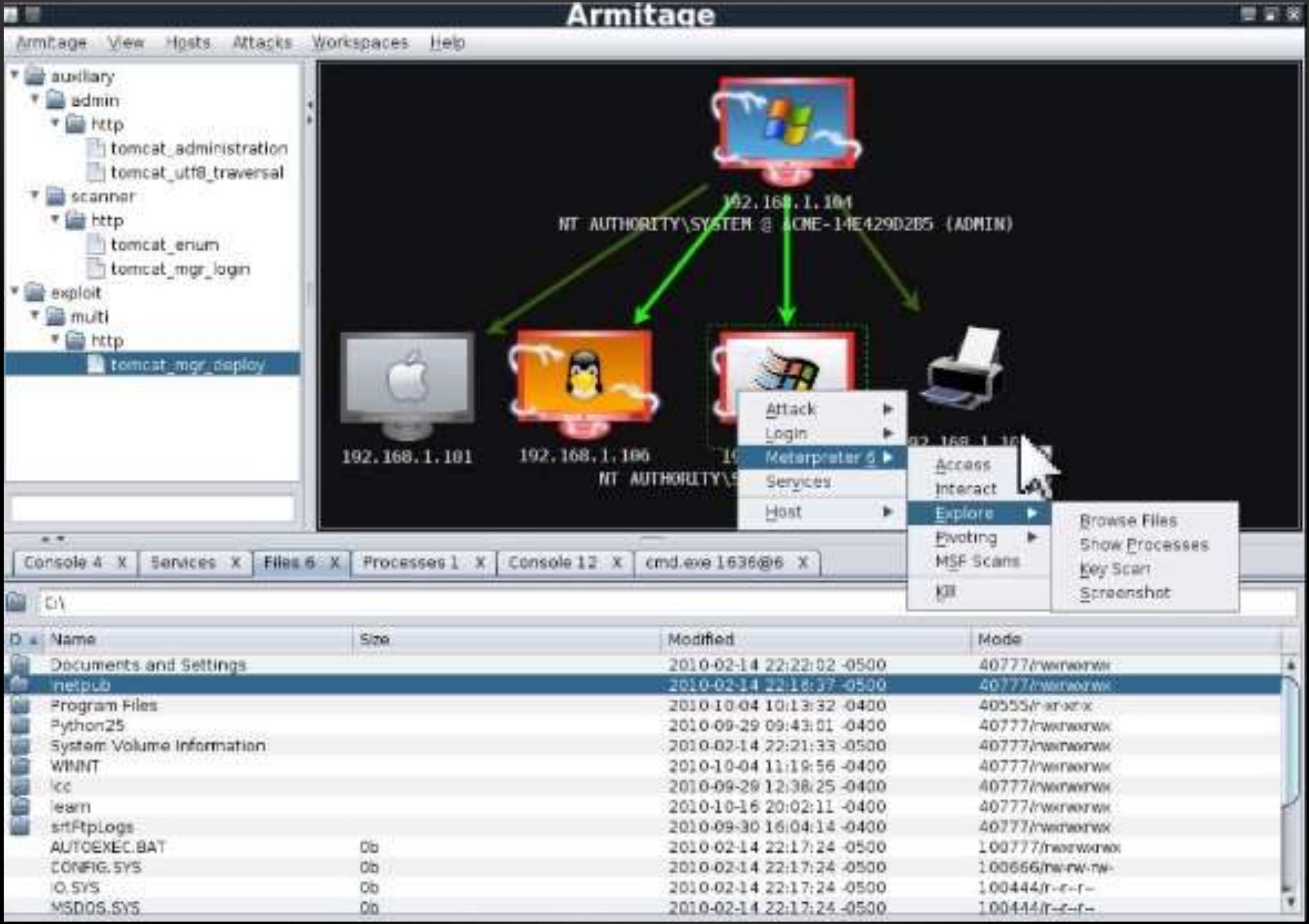
- Armitage is an attack manager tool that automates Metasploit in a graphical way.
- Created by Raphael Mudge
- Written in java



```
msf > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 192.168.45.159
[*] Nmap: Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-14 18:40 EDT
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 4.47 seconds

msf >
```

THIS IS HOW IT LOOKS LIKE



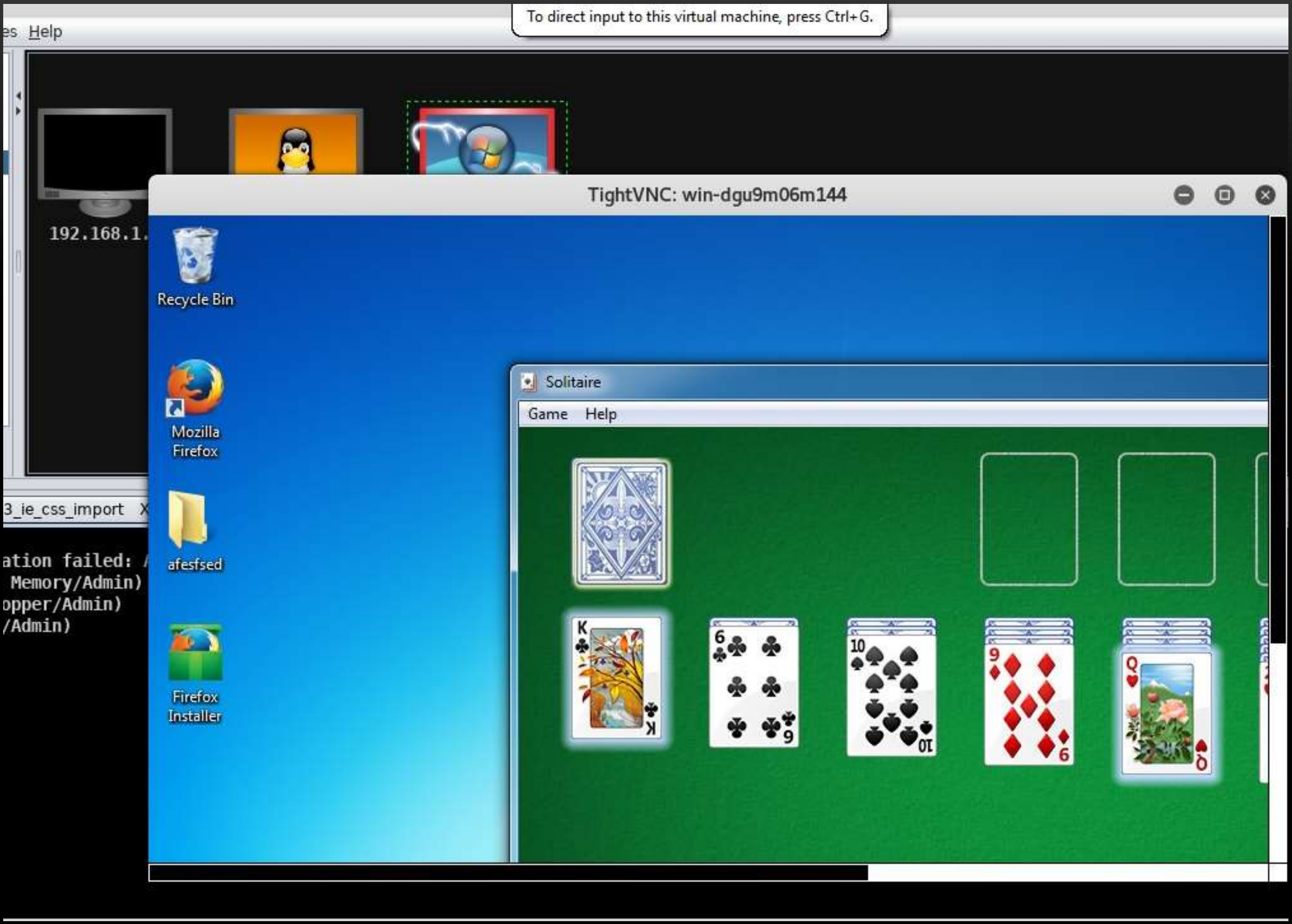
C:\

D	Name	Size	Modified	Mode
	Documents and Settings		2010-02-14 22:22:02 -0500	40777/rwxrwxrwx
	inetpub		2010-02-14 22:18:37 -0500	40777/rwxrwxrwx
	Program Files		2010-10-04 10:13:32 -0400	40555/r-xr-xr-x
	Python25		2010-09-29 09:43:01 -0400	40777/rwxrwxrwx
	System Volume Information		2010-02-14 22:21:33 -0500	40777/rwxrwxrwx
	WINNT		2010-10-04 11:19:56 -0400	40777/rwxrwxrwx
	icc		2010-09-29 12:38:25 -0400	40777/rwxrwxrwx
	learn		2010-10-16 20:02:11 -0400	40777/rwxrwxrwx
	srtFtpLogs		2010-09-30 16:04:14 -0400	40777/rwxrwxrwx
	AUTOEXEC.BAT	0b	2010-02-14 22:17:24 -0500	100777/rwxrwxrwx
	CONFIG.SYS	0b	2010-02-14 22:17:24 -0500	100666/rw-rw-rw-
	IO.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--
	MSDOS.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--

THIS IS HOW IT CAN LOOK LIKE AFTER ATTACK

DEMO 4

Internet explorer css exploit to get meterpreter shell



To direct input to this virtual machine, press Ctrl+G.

```
ation failed: /
 Memory/Admin)
opper/Admin)
/Admin)
```

PIVOTING

- Pivoting is a technique that allows attackers to use a compromised system to attack other machines in the same network
- Basically hack another machine through already compromised machine

DEMO 5

Pivoting an actual target

WAYS TO PREVENT THESE ATTACKS

- Don’t download files from unknown sources.
- Always run the latest version of software or Operating system.
- Don’t click on Random links on the internet.
- Lastly, Be smart don’t get social engineered by someone.

CONSLUSION

- These were some of the basic metasploit attacks.
- The point was not only to teach you that something like happens but also about how to prevent it.

QUESTIONS AND ANSWERS

Go ahead. Ask away

THANK

YOU

FOR JOINING

Hope you all had same amount of fun as I had while making this presentation

SRC

- https://github.com/rapid7/metasploit-framework/wiki
- https://www.offensive-security.com/metasploit-unleashed/
- https://www.slideshare.net/nullhyd/metasploit-42992322
- https://www.corelan.be/
- https://www.phillips321.co.uk/
- https://pentestn00b.wordpress.com/
- https://community.rapid7.com/community/metasploit
- http://www.hackingtutorials.org/metasploit-tutorials/
- http://metasploited.blogspot.in/2012/01/metasploit-tutorial-basics.html
- https://www.kali.org/
- https://developer.microsoft.com/en-us/microsoft-edge

IGNORE THE LAST SLIDE

- REX-- Handles almost all core functions such as setting up sockets, connections, formatting, and all other raw functions MSF CORE-- Provides the basic API and the actual core that describes the framework MSF BASE-- Provides friendly API support to modules
- run event_manger –c
- Pivoting refers to accessing the restricted system from the attacker's system through the compromised system
- netstat -anp|grep "port_number"
-