




Ethical Hacking Basics Course

By : Mohammad Askar
@Mohammadaskar2



Module 5

Exploitation

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the text area.

Definition of Exploitation

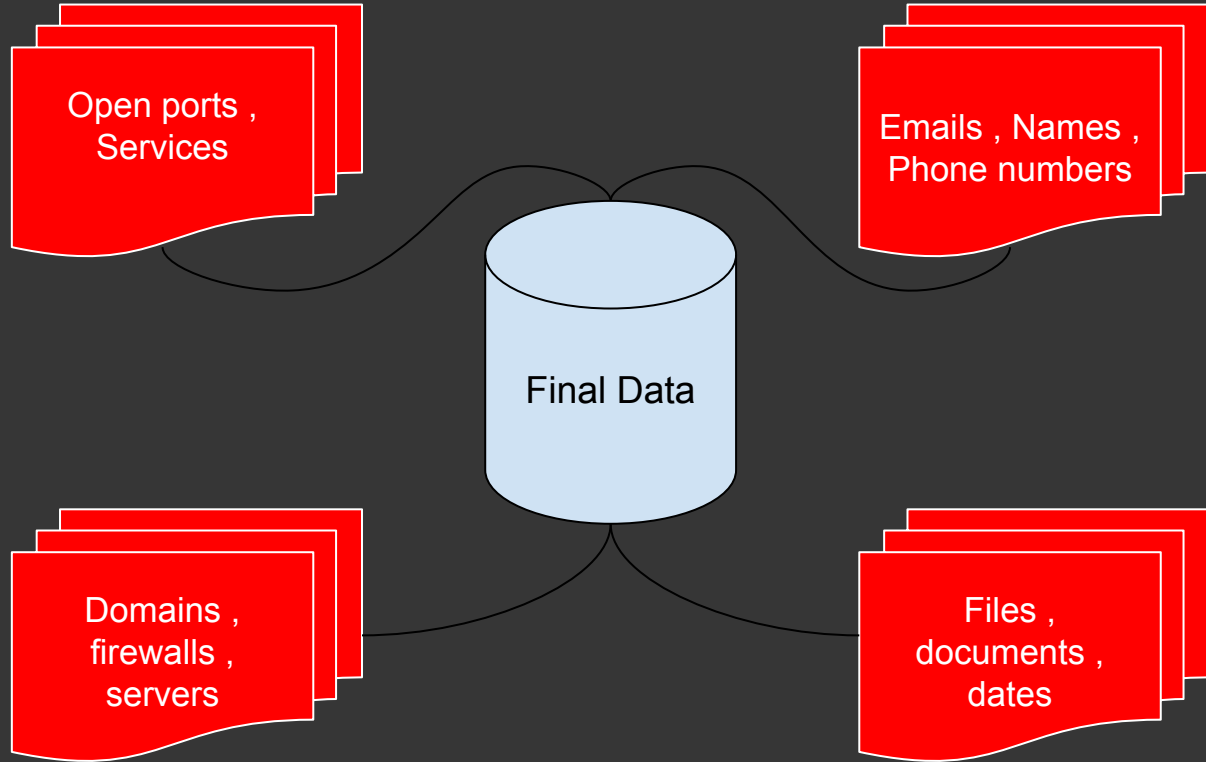
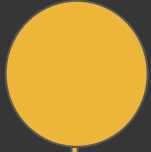
Exploitation focuses on establishing access to a computer system by take advantage of vulnerabilities or security weakness point (weak passwords, misconfiguration etc ..) that found on a computer system.

Also exploitation aims to proof that there is a “working vulnerabilities and weakness point”.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Putting all information together

- This is the Final step to gain access to the system.
- We need to know what we have to start the attack.
- Know your weapons , final targets and be ready for 100ts :D



A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Metasploit Framework

- Metasploit framework is a product from Rapid7
- Metasploit is the most popular pentesting framework ever.
- Metasploit has many tools and we can use it for various tasks.

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Metasploit Framework

- Metasploit provides +1524 exploits for a various applications , operating systems.
- The main purpose of metasploit is exploiting security Vulnerabilities.
- Metasploit is cross platfrom application that you could use it on various operating systems.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Metasploit Framework

- You can perform a full penetration testing using metasploit only.
- Metasploit provides a lot of users interfaces (msfconsole , web interface , armitage).
- There is a commercial version of metasploit.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

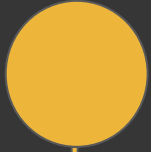
Metasploit Framework

- Metasploit is written on ruby.
- You can build your own modules and implement it to metasploit
- There are many modules that used to perform information gathering , exploit development , etc ..

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Metasploit Console

- AKA msfconsole
- This is one of metasploit UI and it is the most popular one.
- You can use it by this command :
`msfconsole`



Metasploit Exploits Modules

- AKA metasploit Exploits.
- There are many exploits that you can use it to gain access to vulnerable system affected by different vulnerabilities.
- You can list all metasploit exploits using :
`show exploits` command.



Metasploit Auxiliaries Modules

- AKA metasploit auxiliary.
- There are many auxiliaries that used to perform port scanning , fuzzing , sniffng , capturing data.
- You can list all metasploit auxiliaries using :
`show auxiliary command.`

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

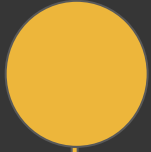
Metasploit Payloads

- Payload is the code or the procedure that we want to execute on the target system.
- You can list all metasploit payloads using :
`show payloads` command.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

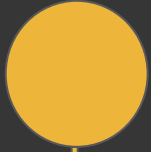
Metasploit Payloads

- **Staged Payload** : metasploit split the payload for two parts , the first part (stager) is the smaller part and his job to connect back to the attacker , after that ,metasploit will send the second part (stage) to the attacker and execute the full payload.
- **Non Staged Payload (Inline)** : when we send the whole payload in one time.



Metasploit Payloads types

- Meterpreter.
- Vnc.
- System shell.
- and many ..



Metasploit Database

- Using database with metasploit makes the work much easier.
- You can store a lot of data like hosts , ports , services.
- You can import scan results to a metasploit database using multiple methods.
- Searching process works faster.

Check Metasploit Database Status

- you can check database status by execute the following command :

* db_status

```
msf > db_status
[*] postgresql connected to msf3
msf > █
```



Importing Database

- We can import various database types (results scans) for Nessus , Nmap , NeXpose.
- Example : importing Nmap result scan.

```
msf > db_import /opt/scans/nmap-local-network-scan.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.7.2'
[*] Importing host 192.168.1.1
[*] Successfully imported /opt/scans/nmap-local-network-scan.xml
msf > █
```

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Using Metasploit Database

- `hosts` : list all hosts.
- `services` : list all services for all hosts.
- `vulns` : list all vulnerabilities that found on hosts.
- `creds` : show database connections credentials.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

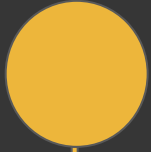
Remote system exploitation

- Remote system exploitation is a process that enables us to exploit a vulnerability on a remote system without send any files or do any action on the target machine.
- Remote system exploitation always exploit a vulnerability on some services on the remote system such as ftp services , telnet services , smb services or any service on the remote system.



Remote system exploitation

- After doing a VA , you should have a list of services and and possible vulnerabilities that could affect this system , here you have to take a move and try to exploit it.
- Exploitation proccess could be done by metasploit as we talked , or you can search manually for an exploit and setup the proccess.
- There are many sites that you could use to find an exploit.



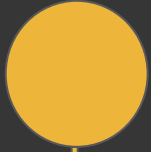
Remote system exploitation

- We can use this sites to search for exploits :
 - * exploit-db.com
 - * securityfocus.com

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Remote system exploitation

- Exploiting RDP DoS vulnerability on remote system (windows7) using metasploit and separated exploit.
- Exploiting FTP service vulnerability on remote system (windows xp).
- Exploiting multiple remote vulnerabilities on linux machine.

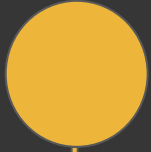


Getting The Shell :D

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.


Password Attacks

- Online Password Attacks.
- Offline Password Attacks (later on).
- Password Hash Attacks (later on).



Online Password Attack

- Trying to crack password using some attack techniques like :
 - * Brute Force Attack.
 - * Dictionary Attack
- we can perform those attacks using various tools.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running parallel to the left edge of the text area.

Difference between brute force and dictionary attack

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Dictionary Attack Tools

- THC Hydra.
- Medusa.
- Metasploit.
- Python scripts :D

A yellow circle is positioned at the top left of the slide, with a thin yellow vertical line extending downwards from its center.

THC Hydra

- THC Hydra is one of the most popular password cracking tools.
- we can install it on Debian-like by executing this command :

```
*apt-get install hydra
```
- <http://sectools.org/tool/hydra/>



THC Hydra

- **Example** : `Hydra -L users.txt -P password.txt ftp://127.0.0.1`
 - * `-L` path of usernames list.
 - * `-P` path of passwords list.
 - * `ftp://` the protocol type.
 - * We can also use `-vV` to display the results directly.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Metasploit

- We can perform dictionary attack using metasploit by several modules for several services such as :
 - * FTP.
 - * SSH.
 - * Telnet.
 - * Vnc.
 - * And More !!!

A yellow circle is positioned at the top left of the slide, with a thin yellow vertical line extending downwards from its center.

Metasploit

- **SSH Login Scanner :**
`auxiliary/scanner/ssh/ssh_login`
- **FTP Login Scanner :**
`auxiliary/scanner/ftp/ftp_login`
- **Telnet Login Scanner :**
`auxiliary/scanner/telnet/telnet_login`

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Metasploit

- `set RHOSTS 192.168.1.1.`
- `set RPORT 23.`
- `set USER_FILE /opt/wordlist/users.txt.`
- `set PASS_FILE /opt/wordlist/password.txt`
- `set USERNAME/PASSWORD.`



Client Side Attack

- Client Side Attack (CSA) is an attack that requires user-interaction to break into the system.
- Metasploit is the most popular platform used to perform this attack.
- There are multiple techniques we can use to perform this attack.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Client Side Attack

- Malicious File Attacks.
- Browsers Attacks.
- Social Engineering Attacks.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Malicious File Attacks

- Prepare the malicious file.
 - * Information gathering magic.
- Find a trusted method to send the file.
- Gain access to the system :D

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Malicious File Attacks

- PDF file attack scenario.
- Mp3 file attack scenario.
- EXE file attack scenario.
- Jar file attack scenario.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Browser Attacks

- Usually we exploit a vulnerability on the browser.
- Also java and flash player could be widely exploited.
- Metasploit browser autopwn.
- XSS to control the browser (Later).

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Browser Attacks

- Need to send a URL to the target.
- Once the target open it , you PWNed him :D

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Java Applet Attack

- We can use display a malicious java applet to the attacker.
- Once the target open it , you PWNed him :D
- Cross Platform Attack.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Browser Attacks

- IE exploit scenario - send the link.
- IE exploit scenario - spoof the link.
- IE exploit scenario - inject the link (Later).
- Java Applet attack scenario.

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Social Engineering Attacks

- Social Engineering - The Art of human hacking
- Social Engineering refers to psychological manipulation of people into performing actions or divulging confidential information.
- You can't patch the human's mind :D



Social Engineering Toolkit

- Social Engineering Toolkit AKA SET.
- Written in python.
- Developed by David Kennedy , founder of Trustedsec.
- We can perform a lot of attacks using it.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Social Engineering Toolkit

- Website Attack Vectors.
- Spear-Phishing Attack Vectors.
- Infectious Media Generator.



Website Attack Vectors

- Can perform various types of based-on web attacks.
- Create a “Mirror” from a website and trying to cheat the user.
- Very powerful Social Engineering attack method.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Website Attack Vectors

- Credential Harvester Attack Method.
- Java Applet Attack Method.
- Metasploit Browser Exploit Method.
- Multi-Attack Web Method.



Credential Harvester Attack Method

- Method Used to Steal the user credential.
- Very easy to setup.
- You can use it with various sites.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Java Applet Attack Method

- Display fake Java Applet to the user.
- This applet used to attack the user.
- This method is based-on Metasploit.



Metasploit Browser Exploit Method

The Same way used by metasploit , but SET use a website template with it.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Java Applet Attack Method

- Display fake Java Applet to the user.
- This applet used to attack the user.
- This method is based-on Metasploit.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Bypassing Antivirus softwares

- Antivirus software is a software used to detect and remove the viruses from The computer.
- Bypass Antivirus software always a big challenge for any pentester.
- There are various methods that we can use to bypass Antivirus software.

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Using Python to bypass anti-virus

- Rewrite the shellcode as python program.
- Using py2exe technique.
- The shellcode should be generated as python script.
- The final result is clean .exe file.



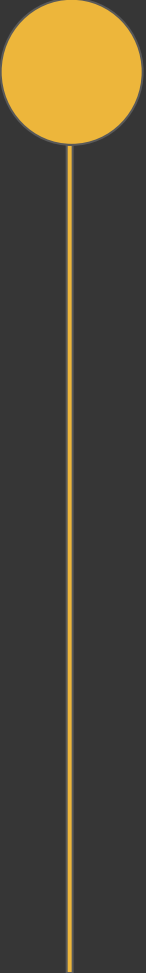
Web Application Attacks

- Web Application is a (Client - Side) application that mainly you can browse it from the internet browser.
- This Applications could be affected by a lot of security vulnerabilities.
- As a security guys , we have to figure out how we can exploit this security vulnerabilities.



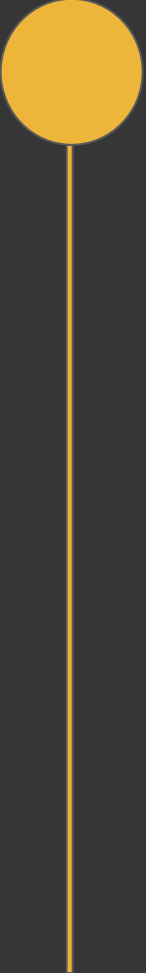
Web Application Attacks

- Most of this security vulnerabilities caused by a flaw in validating and filtering the user input.
- Studying the application and the way that the application works is the most important step.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

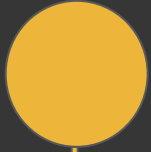
Web Application Vulnerabilities (Client Side)

- Cross Site Scripting (XSS).
 - * Reflected Cross Site Scripting.
 - * Stored Cross Site Scripting.
 - * Blind Cross Site Scripting
- Cross Site Request Forgery (CSRF).

A yellow circle is positioned at the top left of the slide, with a thin yellow vertical line extending downwards from its center.

Web Application Vulnerabilities (Server Side)

- SQL injection.
- Remote Command Execution.
- Unrestricted File Upload.
- Local File Include.
- And More !



HTTP Protocol

- Hypertext Transfer Protocol.
- Protocol That used for communicating with web servers and transferring web pages
- We can use HTTPS as safe way to transfer data over HTTP.

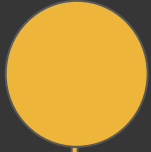
HTTP Protocol



A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Burp Suite

- Burp Suite is an integrated platform for performing security testing of web applications.
- Burp contents various tools work seamlessly together to support the entire testing process.
- The Web pentester assistant.



Burp Suite Spidering

- Use to map all files and folders that used by this web application.
- Very powerful way to gather information about the web application.



Cross Site Scripting - XSS

- XSS is a Security vulnerability enables the attacker to inject client-side scripts into web pages viewed by other users.
- Most of web applications developers know nothing about filtering the users inputs.
- XSS is the most prevalent web vulnerability.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

XSS types

- Reflected XSS.
- Stored XSS.
- Blind XSS.

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Reflected XSS

- Reflected XSS is kind of Cross Site Scripting vulnerability that could directly effect the user by sending a link that contents the xss payload.
- Example :
`http://www.example.com/a.php?id="><script>alert(2)</script>`

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Stored XSS

- Stored XSS is kind of Cross Site Scripting vulnerability that could effect all web applications users that browse specific web page , cause the payload is already stored on the database.
- After inject the payload to the database , the payload should appers on the effected web page.



Remote Command Execution - RCE

- RCE is a web security vulnerability that allows the attacker to execute OS command on the remote system.
- This flaw caused by unfiltering user inputs that passed to some functions like :
 - * `system()`
 - * `exec()`
 - * `passthru()`

A yellow circle is positioned at the top left of the slide. A vertical yellow line extends downwards from the bottom of the circle, running along the left edge of the slide.

Unrestricted File Upload

- RCE is a web security vulnerability that allows the attacker to upload a malicious file to the server by manipulating with the file extension.
- Example : change .jpg extension to .php extension and execute it.
- There are many ways to filter the file input.



SQL injection - SQLi

- SQLi is a web security vulnerability that allows the attacker to inject some SQL queries to application to extract unauthorized information from it.
- SQLi is one of the most powerful Server Side vulnerabilities cause you can extract the data directly from the server.



SQL injection - Manually Exploitation

- need to know database tables.
- need to know database columns.
- information schema provides information about all of the tables , views , columns in a database.



SQL injection - Manually Exploitation

- `id=-1 UNION SELECT 1,database(),3,4--`
- `id=-1 UNION SELECT 1,group_concat(table_name),3 FROM information_schema.tables WHERE table_schema = database()--`
- `id=-1 UNION SELECT 1,group_concat(column_name),3 FROM information_schema.columns WHETE table_name = CHAR(table_name)--`
- `id=-1 UNION SELECT 1,group_concat(column1,column2,column3),3 FROM database.table--`



SQLmap - automated SQLi exploitation Tool

- SQLmap written with python.
- SQLmap is very powerful tool to exploit SQLi.
- Can deal with most of SQLi types.
- Examples !

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

Read Files using SQLi

- Using `load_file()` function.
- this function should be enabled by the DBA to the current DB.
- Can read some system files that could help with gaining access to the system.

A yellow circle is positioned at the top left of the slide. A thin yellow vertical line extends downwards from the bottom of the circle, running along the left edge of the slide.

FROM SQLi to RCE

- Using “INTO” & “OUT FILE” Functions
- this functions should be enabled by the DBA to the current DB.
- requires a folder with write permission.