



渗透测试工程师技术实战课

Web渗透测试环境搭建

教学目标

★ 能够掌握web渗透平台的搭建流程



●准备实验环境

渗透非授权系统的弊端

搭建自己的实验环境



● 安装虚拟机

Windows虚拟机

- <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

安装自己的虚拟机

- xp
- 2003
- win7
- ...



● 安装虚拟机

Linux虚拟机

- Centos
- LAMP
- kali

Metasploitable2

- <http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip>
- 问题: /var/www/mutillidae/config.inc
- dbname=owasp10



基于服务器的环境搭建

- *SQL注入渗透测试*
- *上传验证绕过*
- *XSS跨站脚本*
- *文件包含漏洞*
- ...

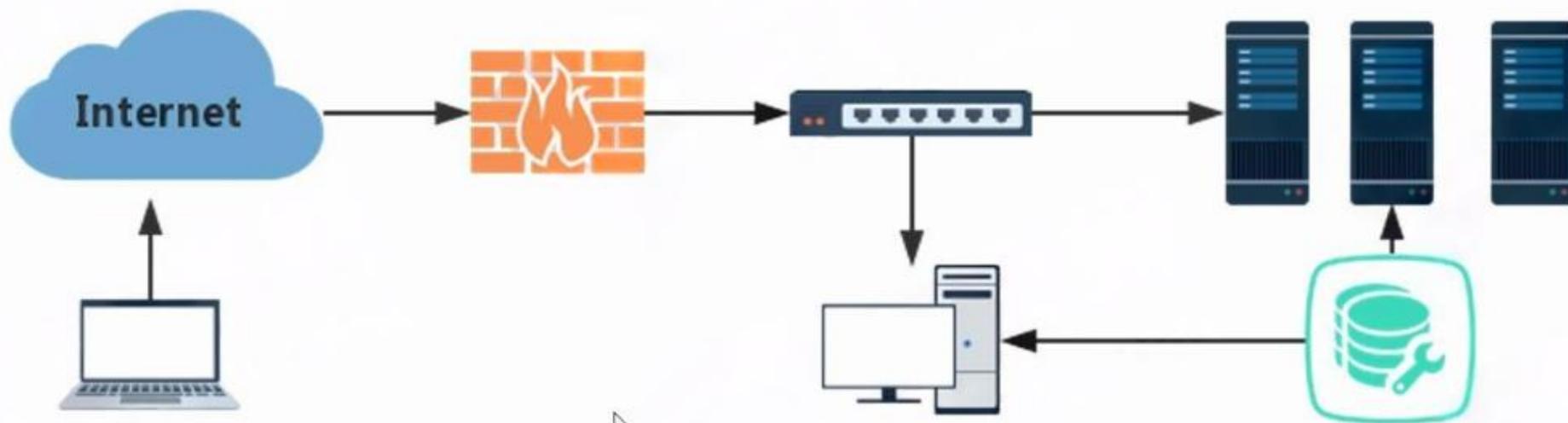


常见渗透测试靶场系统

- **OWASP Broken Web Apps**
- https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
- **ZVulDrill靶场二次开发**
- <https://github.com/redBu1l/ZVulDrill>
- **Hack This Site**
- <https://www.hackthissite.org/>



●环境搭建-模拟真实网络



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered across the scene, suggesting themes of cybersecurity, data protection, or digital privacy. The overall aesthetic is futuristic and high-tech.

谢谢观赏