



kali linux渗透测试

第8课 黑客如何通过网络侦察目标系统漏洞

漏洞扫描，是侦察阶段最为重要的一环

因为常用的操作系统版本有几十种，常用的软件大概有几千种，这些操作系统和软件包含的漏洞更是多到难以计数，所以想要人工完成漏洞的扫描极为不现实。漏洞的扫描离不开工具的使用。



扫描工具

Rapid7 Nexpose (商业)

Tenable Nessus (商业)

OpenVas (免费)



扫描的原理：和杀毒软件的工作方式类似，通过更新漏洞的特征库，去增强识别能力。

需要注意：不管采取何种扫描工具，都可能存在漏报或者误报的情况。



安装OpenVas

```
apt-get update
```

```
apt-get upgrade
```

```
apt-get install openvas
```

```
openvas-setup
```



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 throughout, suggesting themes of cybersecurity or digital privacy. A horizontal semi-transparent bar is positioned across the middle of the image, containing the text.

谢谢观赏