




kali linux 渗透测试



第7课 黑客是如何知道，你的电脑是什么操作系统，开启了哪些端口

诸神之眼--Nmap

跳过Ping扫描阶段（无ping扫描）

通常Nmap在进行其他扫描之前，都会对目标进行一个Ping扫描。

如果目标对Ping扫描没反应的话，就会直接结束整个扫描过程（服务器可以禁止Ping）

```
nmap -PN <ip>
```

仅使用Ping协议进行主机发现

有的时候，需要快速的大量的主机中去快速的发现主机，这个时候，仅使用Ping协议进行扫描，速度会非常快

```
nmap -sP <ip>
```



使用ARP协议进行主机发现

ARP协议扫描只适用于**局域网**内，使用ARP，不仅速度快，而且结果也会更加准确。

```
nmap -PR <ip>|
```



半开扫描和全开扫描

TCP协议三次握手

黑客



目标



3个过程全部完成叫全开扫描

最后一步不做，叫半开扫描

在实际过程中，半开扫描应用的最多，半开扫描不容易被目标电脑日志记录

半开扫描: `nmap -sS <ip>`

全开扫描: `nmap -sT <ip>`



I 识别操作系统

因为系统不一样，渗透的方法就不同，所以判断目标电脑使用的操作系统，非常重要

```
nmap -o <ip>
```

端口发现

在前面的视频中，我们提到nmap扫描的端口是1000个，实际上电脑的端口一共有65536个。nmap扫描的1000个只是常用的1000个端口。

扫描全部端口： `nmap -p "*" <ip>`

扫描指定的端口： `nmap -p 80 <ip>`



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, overlaid with a network of white and blue lines and dots. Scattered throughout the background are several padlock icons, some of which are open, symbolizing security or digital access. The overall aesthetic is high-tech and cybernetic.

谢谢观赏