“正着来难，那就试一下反过来”

比如给你一个sql injection 题，你发现php script中根本不展示任何结果，那么也许你可以试一下另一种思路，而不是纠结于到底如何才能看到exec的结果，又或者调试query语句。比如反过来的思路就是，我也许可以直接获得目标主机的remote shell，以root的权限去查看其内部内容。

攻击的目的

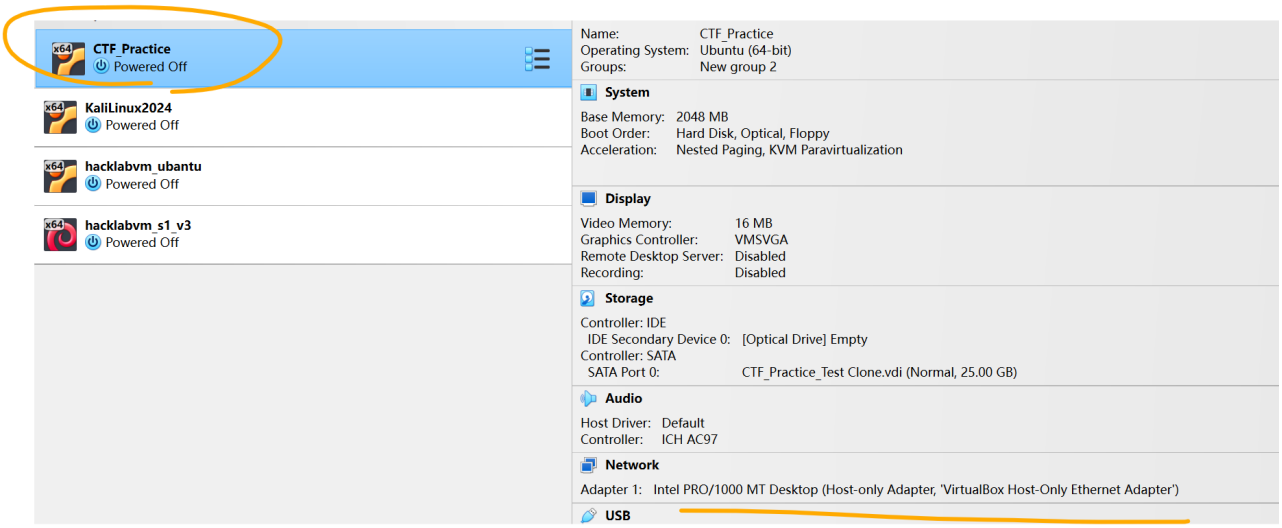
其真目的大都是经济目的，要么自己获益，要么对方利益受损。
要么是为了得到系统的最高权限

手段:

劫持信息（arpspoofing, DNS Spoofing... ）
获取信息(sql injection, command injection)
改变信息(buffer overflow)，比如获得系统root权限
代替victim发送恶意request执行特定操作，比如银行转账（XSS, CSRF...）
加密信息，以勒索用户，付钱解锁
使不可获取信息（DDOS...）
sudo -l 找到能够“越权”的script，去间接执行，来获得root权限。

完整的流程 与 对应的工具

你有一台靶机，和你的电脑，首先的第一步，就是要寻找对方的ip地址。前提是你们处于同一个网络中。
Host-Only adaptor
与你自己的kali机设置成同一个网络中。



使用Nmap去搜索网络中的设备，并判断哪一个是你的靶机，并去连接对方。

nmap

找到后，就去看target上都有什么服务（端口），这些端口就是你的突破口，比如ssh, ftp, http等。

接着就去做对应的事情。

看到文件夹，就看有没有隐藏信息

ls -la

看到script，就去看里面都有什么内容，看是否需要输入什么，或者能执行memory attack等。

C语言 和 x86 32bit指令集

看见图片，就去看有没有隐写的内容，file, binwalk stegonline等。

module10 隐写术 wireshark ghidra

既然是FTP，那么就用ftp就去访问，看有什么文件可以下载或上传等。

根据获得的新信息，来调整自己的策略，比如获得target上的某用户密码，相当于获得了特定权限，那就登入进去看能看到什么。