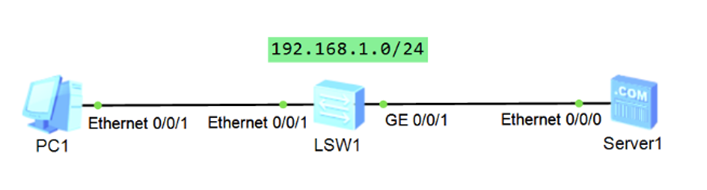
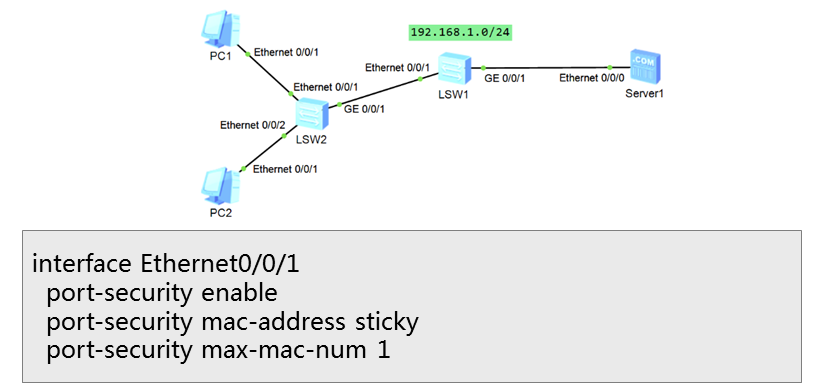
**端口安全**

控制交换机端口安全，禁止私接设备



端口安全配置（华为）



**勒索病毒及防护**

木马与病毒概述

计算机木马：向受害者系统中植入木马程序，用户很可能不知情

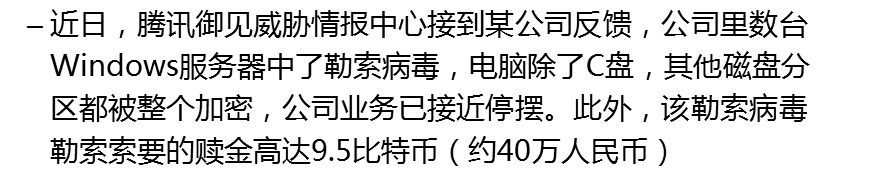
窃取敏感信息（如网游账号、银行账号、机密文件等）夺取计算机控制权

病毒：主要目的是破坏（如删除文件、破坏分区等），而不是窃取信息

病毒具有自我复制和传染能力，可以通过电子邮件、图片和视频、下载的软件、光盘等途径进行传播。

勒索病毒

安全事件：



比特币：是一种数字货币，可以用来兑现，可以兑现成大多数国家的货币。使用比特币可以购买一些虚拟物品。

中毒现象：



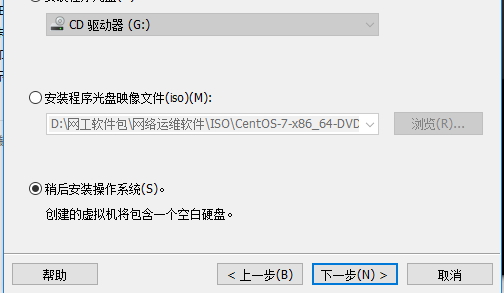
如何防范：

1. 先拔掉网线再开机，这样基本可以避免被病毒感染
2. 开机后尽快打上安全补丁，或者安上防御工具，才可以联网
3. 尽快备份电脑中的重要文件到可移动设备
4. 对于不明链接、文件和邮件要提高警惕
5. 利用系统防火墙高级设置阻止向445端口进行连接

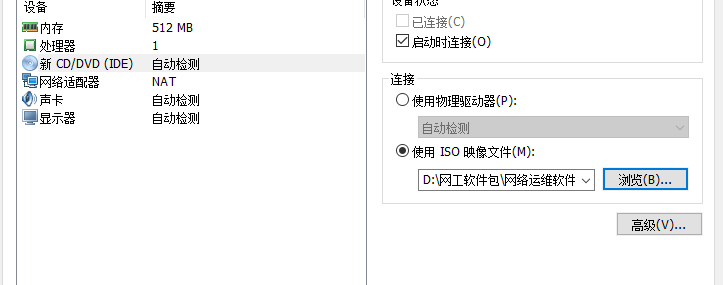
打开网络和共享中心-windows防火墙（确保启用）-高级设置-入站规则-新建规则-端口-特定本地端口-输入445-阻止连接-名称自定义

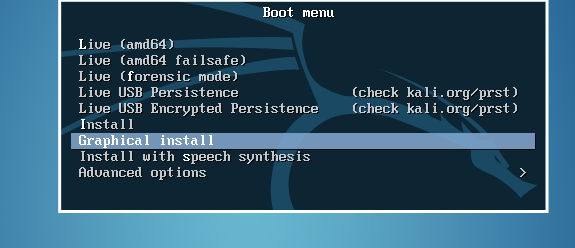
**NMAP扫描**

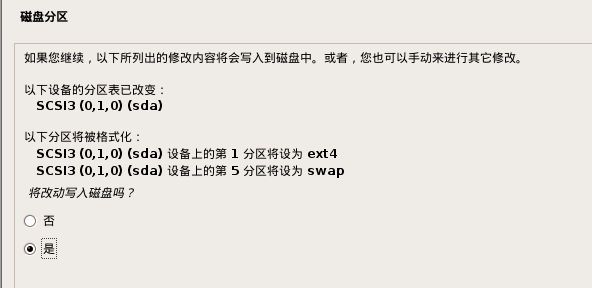
Kali（免费开源的，用来渗透测试和网络安全评估的一个系统）安装：

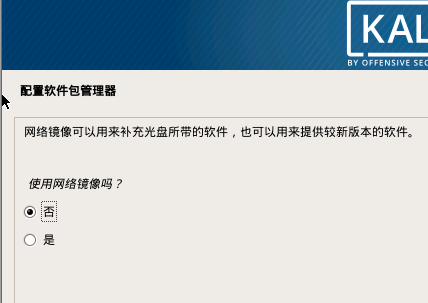














系统扫描概述

扫描指的是利用工具软件来探测目标网络或者主机的过程

通过扫描过程，可以获取目标的系统类型、软件版本、端口开放情况，发现已知或潜在的漏洞

攻击者可以根据扫描结果来决定下一步行动

选择哪种方式攻击

使用哪种软件

防护者可以根据扫描结果采取相应的安全策略

封堵系统漏洞

加固系统

完善访问控制

使用NMAP

NMAP：一款强大的网络扫描、安全检测工具

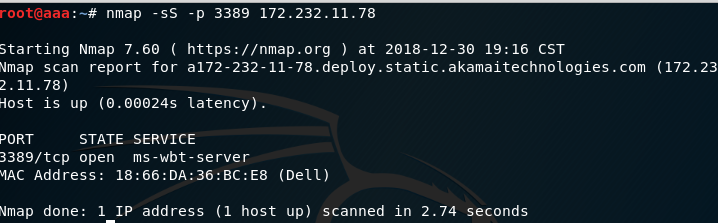
NMAP的扫描方法：nmap [扫描类型] [选项] <扫描目标…>

常用的扫描类型：-sS,TCP SYN扫描（半开）

-sT,TCP连接扫描（全开）

-sU,UDP扫描

-sP,ICMP扫描





**暴力破解**

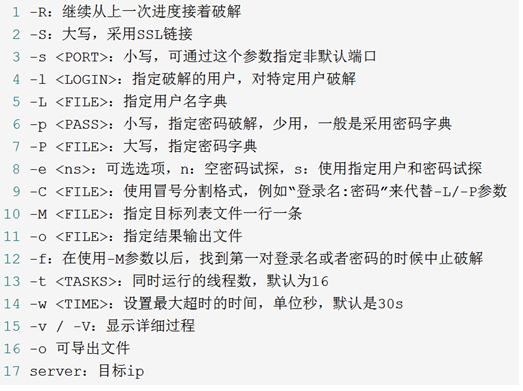
暴力破解概述

暴力破解多用于密码攻击领域，即是用各种不同的密码组合反复进行验证，直到找出正确密码

这种方式也称为“密码穷举”，用来尝试的所有密码集合称为“密码字典”

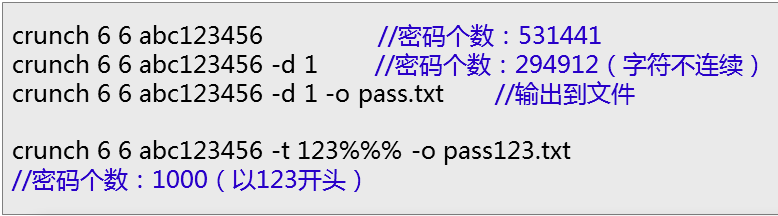
使用hydra

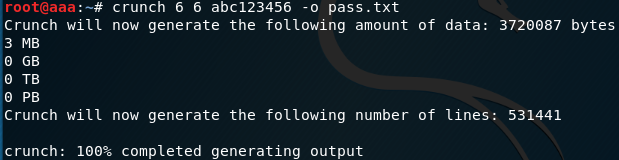
Hydra用法

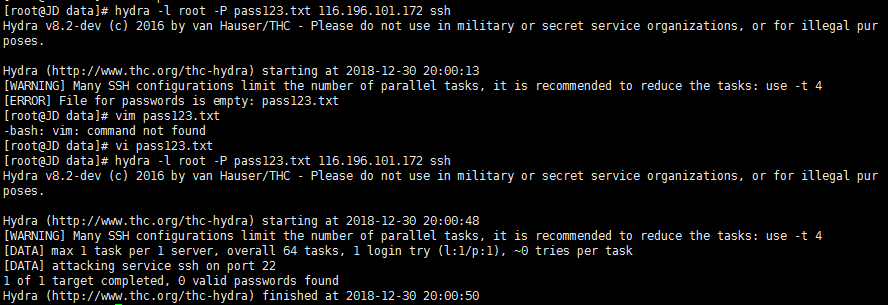


使用kali环境

生成密码字典工具crunch







WIN防爆破登陆

Gpupdate /force