HW7

PB17111614 王嵘晟

1~4

1. ①系统调查：收集目标主机相关信息的过程
②系统漏洞探测，寻找攻击目标系统内的安全漏洞
③实施攻击
④巩固攻击成果：重点是长期隐蔽潜伏
⑤痕迹清理：消除攻击过程的痕迹

2. 攻击者通过向目标程序的缓冲区写超出其长度的内容，造成缓冲区溢出，从而破坏程序的堆栈，使程序转而执行其他指令

利用网络协议的缺陷，采用耗尽目标主机的通信、存储或计算资源的方式来迫使目标主机暂停服务甚至系统崩溃

①登录目标主机，构建僵尸网络
②发布命令，控制僵尸程序
③展开攻击
④攻击者后，防止被跟踪溯源

5.

175