


第七次作业

PB19111708 杨云皓

HW.7



中国科学技术大学

University of Science and Technology of China

地址: 中国 安徽 合肥市金寨路96号 邮编: 230026
电话: 0551-63602184 传真: 0551-63631760 Http://www.ustc.edu.cn

1. (1) 系统调查: 通过网络收集目标主机相关信息的过程
(2) 系统安全缺陷检测: 寻找攻击目标系统内部的安全漏洞.
(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, 造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参量.
3. 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导致系统崩溃.
 - (1) SYN 泛洪攻击: 发送大量伪造的 TCP 连接请求, TCP 连接无法完成第三步握手
 4. (2) UDP 泛洪攻击: 通过伪造与某一主机的 chargen 服务之间的一次 UDP 连接, 回复地址向开着 Echo 服务的一台主机, 这样就在两台主机之间存在很多无用数据流
 - (3) Ping 泛洪攻击: 声称自己的尺寸超过 ICMP 上限自己, 出现内存分配错误
 - (4) 泪滴攻击: 利用在 TCP/IP 堆栈中实现信任 IP 碎片中的标题所给信息实现攻击
 - (5) Land 攻击: 设计一特殊的 SYN 包, 它由全被攻击的服务器每接收一个这样的连接都保留造成
 - (6) Smurf 攻击: 向一个局域网的广播地址发出 ICMP 回应请求, 导致目标主机被大量应答包淹没.
4. (1) 感染目标主机, 构建僵尸网络: 侵入主机, 植入僵尸程序
(2) 发布命令, 控制僵尸程序:
(3) 展开攻击
(4) 攻击善后: 隐藏攻击痕迹, 防止被追踪溯源

5.offset=135