主题：无线网络安全科普

时间： 7-15 周 周三晚 7:50

地点：一号学院楼 120

本周主题

- 我在悄悄地看着你
- 无线 D.O.S.
- CTF Center

我在悄悄地看着你

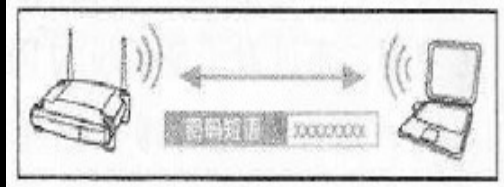
- 截获无线数据包
  - airodump
- 解密
  - airdecap-ng
  - airdecap-ng -l -e essid -p psk capfile
- 分析流量
  - Wireshark
    - http://blog.jobbole.com/70907/

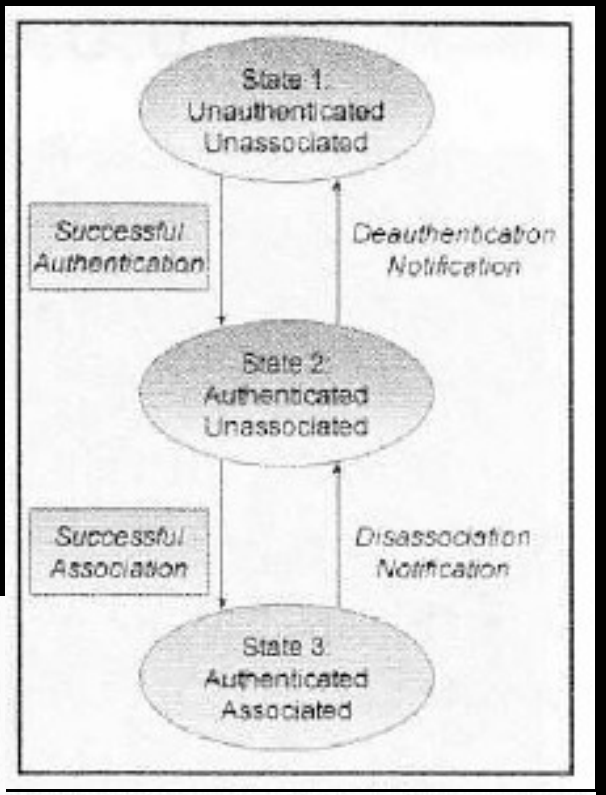
无线 D.O.S.

- WHAT
- MDK3
- Auth Flood
- Deauth Flood
- Association Flood
- Disassociation Flood
- RF Jamming

Deny of service

- D.O.S. 拒绝服务攻击
- 通过故意攻击网络协议的缺陷，或直接通过某种手段耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务停止响应甚至崩溃。
- MDK3
  - Linux shell 下运行的无线 D.O.S. 工具





状态机制	客户端状态	客户端具体表现	备注
State 1	Unauthenticated Unassociated	没有通过验证，没有和 AP 建立关联	无线客户端处于搜索及试图连接 AP 阶段
State 2	Authenticated Unassociated	通过验证，没有和 AP 建立关联	无线客户端已经输入正确的连接密码并等待
State 3	Authenticated Associated	通过验证，和 AP 建立关联	无线客户端被允许连接（AP 自动分配地址）

Auth Flood

- 验证洪水攻击 . 简称 Auth DOS 攻击

  国际上称为 Authentication Flood Attack
- 主要针对那些处于通过验证和 AP 建立关联的客户端，攻击者将向 AP 发送伪造的身份验证帧（即伪造的身份验证服务和状态代码），当收到大量伪造的身份验证请求超过所能承受的能力时， AP 将断开其他无线链接。
- mdk3 mon0 a -a ap_mac [-s speed]

Deauth Flood

- 取消验证洪水攻击，简称 Deauth 攻击
- 取消身份验证洪水攻击
- 旨在通过欺骗从 AP 到客户端单播地址的取消身份验证帧来将客户端转为未关联 / 未认证的状态

Association Flood

- 关联洪水攻击

Disassociation Flood

- 取消关联洪水攻击