实验2 网络信息搜集

网络信息搜集简介

- 攻防双方为了了解对方，都需要搜集对方的信息。
  - 攻击者需要了解攻击目标的域名、IP地址、网络拓扑、注册信息、地理位置等，为进一步的网络侦察做准备。
  - 防守者关注攻击者身份、网络位置、地理位置、攻击方法、造成的损失等，为进一步取证与追踪做准备。
- 信息搜集主要通过公开渠道完成，如Whois、DNS查询，搜索引擎搜索等。

1. 准备

- 选出位于不同国家/地区的3个Web站点和3个电子邮件服务器。

2. DNS查询

- 分别利用nslookup和dig软件，查询前面选出的Web站点和电子邮件服务器的IP地址。
- 根据这3个Web站点的IP地址，查询相近IP（比如同一网段）对应的主机名。思考这样的操作，对于攻击者有什么意义？

3. 网络路径分析

- 使用TraceRoute（*nix平台）或Tracert（Windows平台），列出从你的主机到那3个Web站点的网络通信路径。
- 分析路径中各节点的地理位置。
- 分析路径中哪些节点是你所在网络内的路由节点。
- 你是否能从中分析出你所在网络的ISP？

4. 网络状况分析

- 使用ping命令，了解访问这3个站点的数据包往返时间。
- 根据实际访问距离来评价各站点的访问速度。
- 你可能会发现，有些站点虽然可以访问，但却不响应ping请求，分析背后的原因。

5. 本机网络连接状态

- 通过netstat命令，了解本机上当前的网络连接状态，思考它有哪些安全用途。