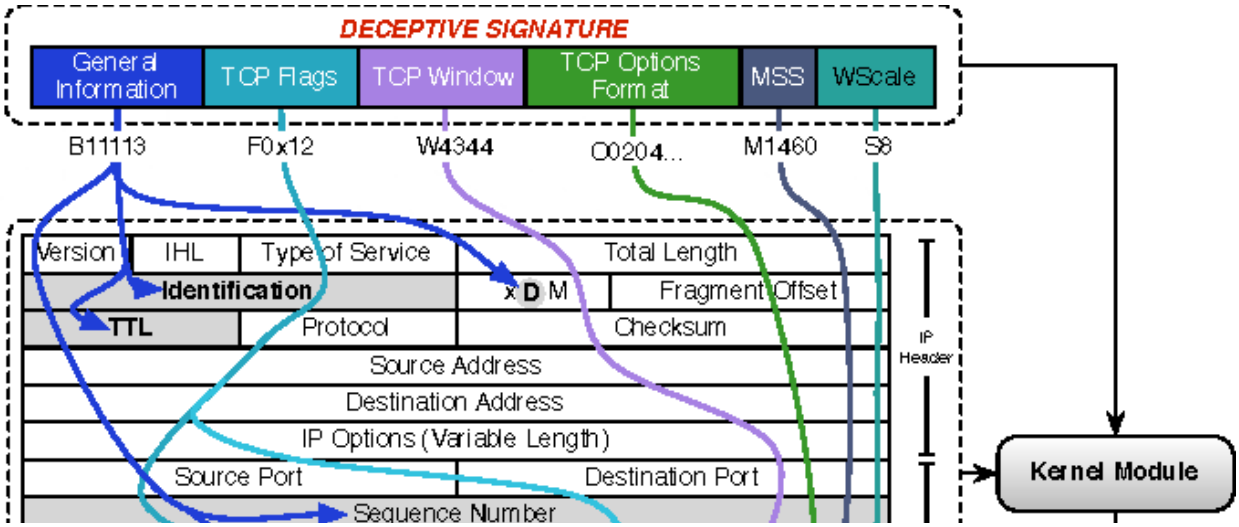


A Deception Based Approach for Defeating OS and Service Fingerprinting

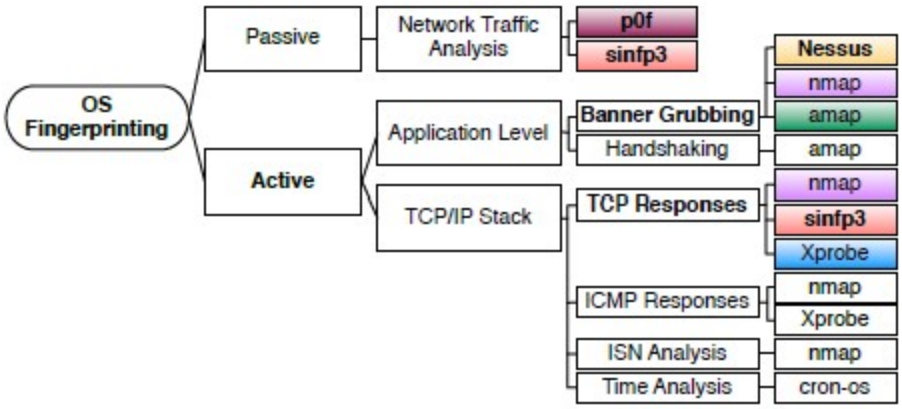
Writer	Massimiliano Albanese, Ermanno Battista, and Sushil Jajodia
Year of Publication	2015
Source	2015 IEEE Conference on Communications and Network Security
Link	https://ieeexplore.ieee.org/document/7346842

总结与摘录

1. 研究背景

- 操作系统指纹（OS Fingerprint）：记录主机的操作系统信息
  - 获取方式：
    - 静态：嗅探（sniffing）、流量分析（traffic analysis）
    - 动态：ICMP / TCP / UDP 探针（probing）

- 分类及工具



  - **Nmap**（按本文方法部分起作用）
    1. 原理：6 TCP probes → 2 ICMP echo request → 6 TCP tests → UDP test (closed port)
    2. 缺陷：包经不同主机传递后指纹可能会改变
- 服务指纹（Service Fingerprint）：记录主机上运行的服务信息

2. 操作系统指纹欺骗

- TCP Options（对大多数操作系统而言长度为**定值**）
  - 参数修改：IP 头长度域、TCP头 offset值
  - 重排序：调 sequence number
- 实现方法：Netfilter POST_ROUTING hook
  - deception module

```
if(ip->protocol == TCP && ip->len == 44 && tcp->ack == 1 &&
     tcp->syn == 1)
{
  //Probably 1st sinfp3's probe Response
  set_id();
  set_df_bit();
  set_ttl();

  set_tcp_window();
  set_tcp_flags();
  set_tcp_sequence();
  set_tcp_ack();

  if(new_option_len != option_len)
  {
    modify_packet_size(); //expands or shrinks
    //packet and updates IP Lenght and Offset
  }

  set_tcp_options(MSS, WScale, Option_Layout);
}
else if(ip->protocol == TCP && ip->len == 60 && tcp->ack ==
     1 && tcp->syn == 1)
{
  //Probably 2nd sinfp3's probe Response

  // Extract the timestamp value from the packet and save
  // it for re-injecting it in the right position later
  timestamp = get_tcp_timestamp();

  set_id();
  set_df_bit();
  set_ittl();
  set_tcp_window();
  set_tcp_flags();
  set_tcp_sequence();
  set_tcp_ack();

  if(new_option_len != option_len)
  {
    modify_packet_size(); //expands or shrinks
    //packet and updates IP Lenght and Offset
  }
  set_tcp_options(timestamp, MSS, WScale, Option_Layout);
}

if(tcpHeader_modified)
{
  tcp->check = 0;
  tcp->check = tcp_csum();
}

if(ipHeader_modified)
{
  ip->check = 0;
  ip->check = ip_csum();
}
```

    - extraction module
- 评价指标选择
    - 不同配置下服务器处理请求的能力（Apache Benchmark）：服务用户数量、服务器负荷
    - 工具软件：Nessus 漏洞扫描、OS 扫描工具误检率