Beijing Forest Studio
北京理工大学信息系统及安全对抗实验中心

Web中间人攻击简介

王逸洲　硕士研究生

2019年04月07日

内容提要

- 背景介绍
- 总体目标
- 预期收获
- 基本概念
- 成为中间人的方式
- 中间人攻击
- 中间人攻击的防范

背景介绍

- 提到安全攻击，往往会想到攻击来自于互联网，而内部的局域网安全问题被忽略。
- 在网络安全方面，中间人攻击很早就成为了常用的一种古老的攻击手段，并且一直到如今还具有极大的扩展空间。

总体目标

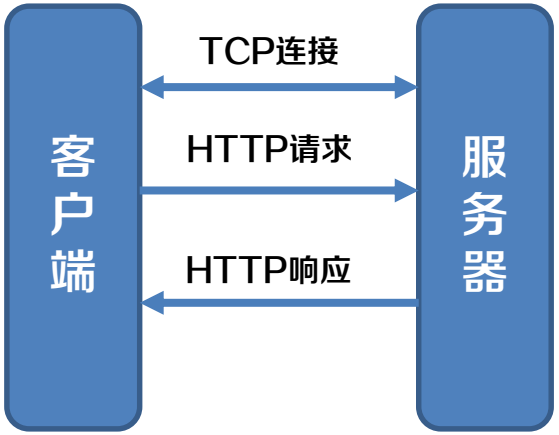
T	获取被攻击目标的网络通信数据
I	局域网内目标主机的IP地址
P	1.通过嗅探获取目标的MAC地址等信息 2.使用ARP欺骗攻击等手段成为中间人
O	目标提交的表单数据或会话COOKIE等

预期收获

- 了解Web中间人常见攻击方式
- 理解ARP欺骗攻击原理
- 了解ICMP重定向等攻击方式
- 了解中间人攻击防范方法

基本概念

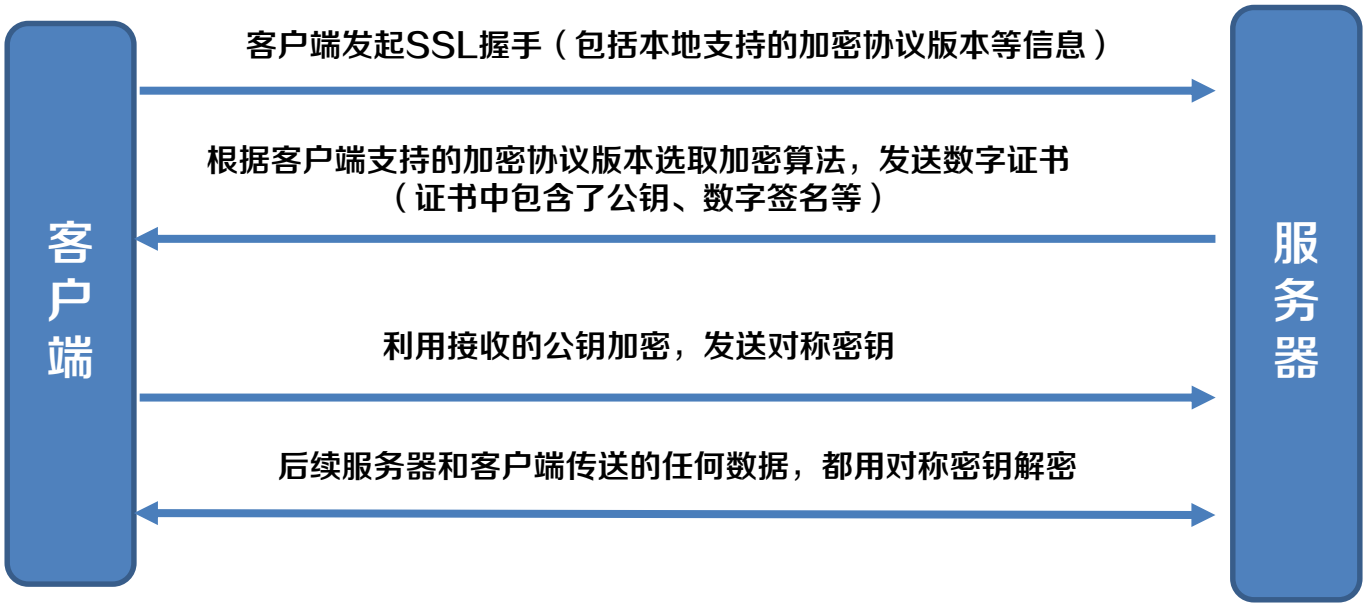
- HTTP、HTTPS
  - HTTP（ Hyper Text Transfer Protocol，超文本传输协议）是用于浏览器和服务器之间传输超文本的传输协议。



HTTP请求过程中，客户端和服务器无需身份验证。并且数据是以明文的方式传输的。

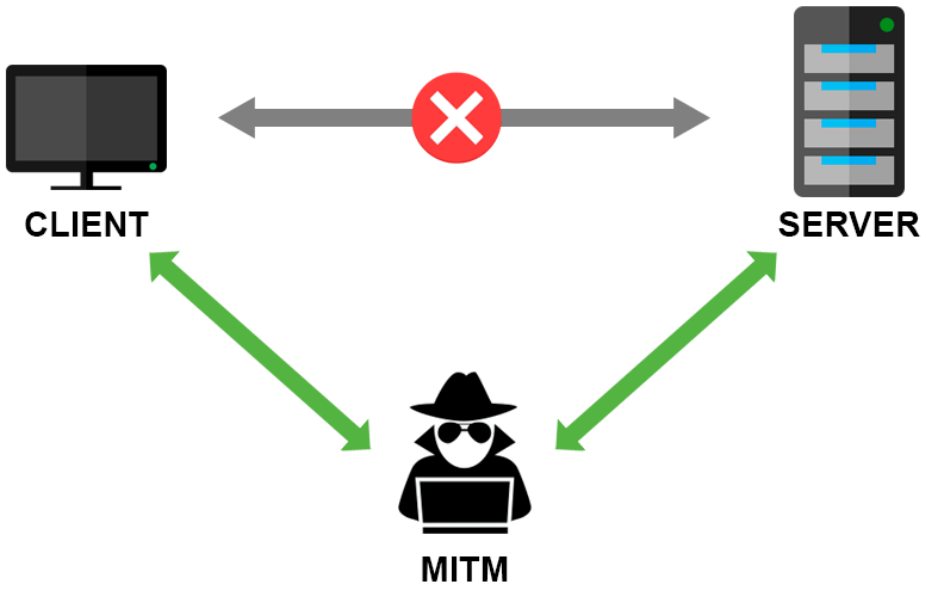
基本概念

- HTTP、HTTPS
  - HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，安全超文本传送协议）即HTTP+SSL/TLS，在HTTP 下加入 TLS 层，实现信息的加密传输



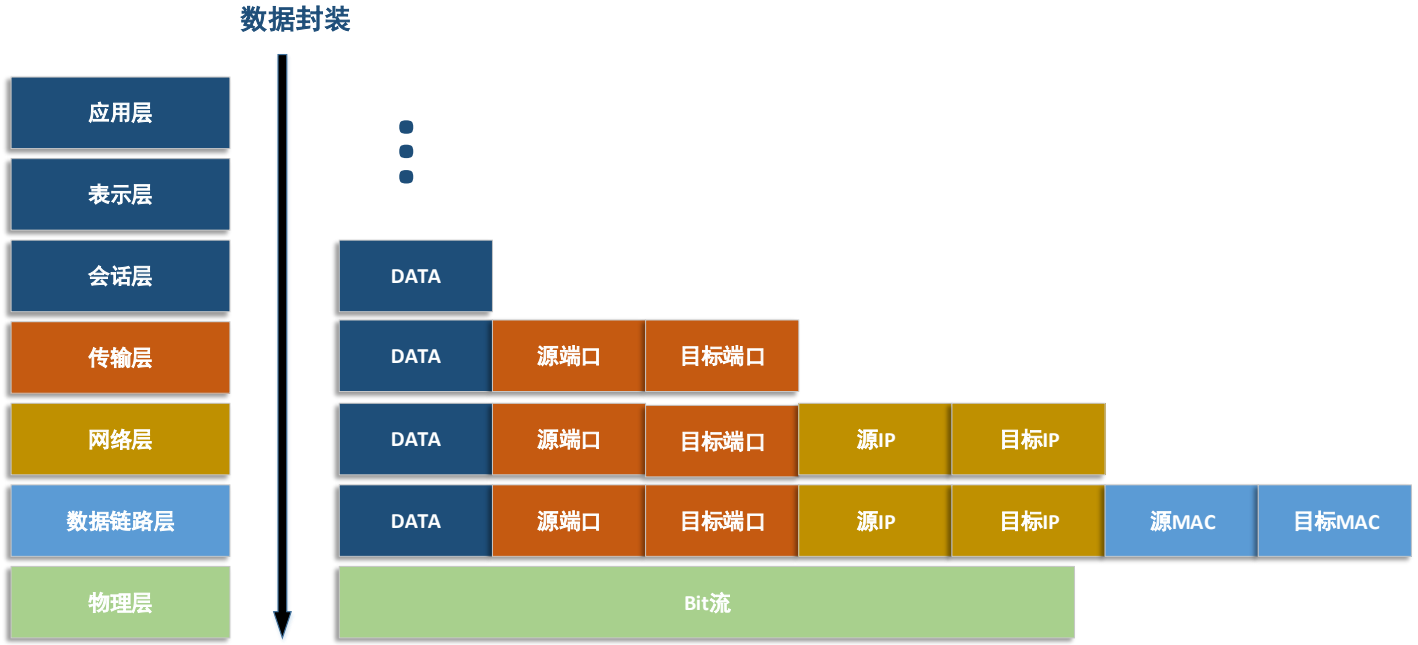
基本概念

- 中间人攻击（Man In The Middle, MITM）
  - 攻击者通过在通讯的两端创建独立连接，使两端的通讯者以为双方的连接是私密连接
  - 通过对数据进行拦截，篡改，伪造，达到攻击目标的效果



成为中间人——ARP欺骗

- ARP协议
  - ARP(Address Resolution Protocol, 地址解析协议)的基本功能是在主机发送数据之前将目标IP地址转换为MAC地址，完成网络地址到物理地址的映射，以保证两台主机能够正常通信。



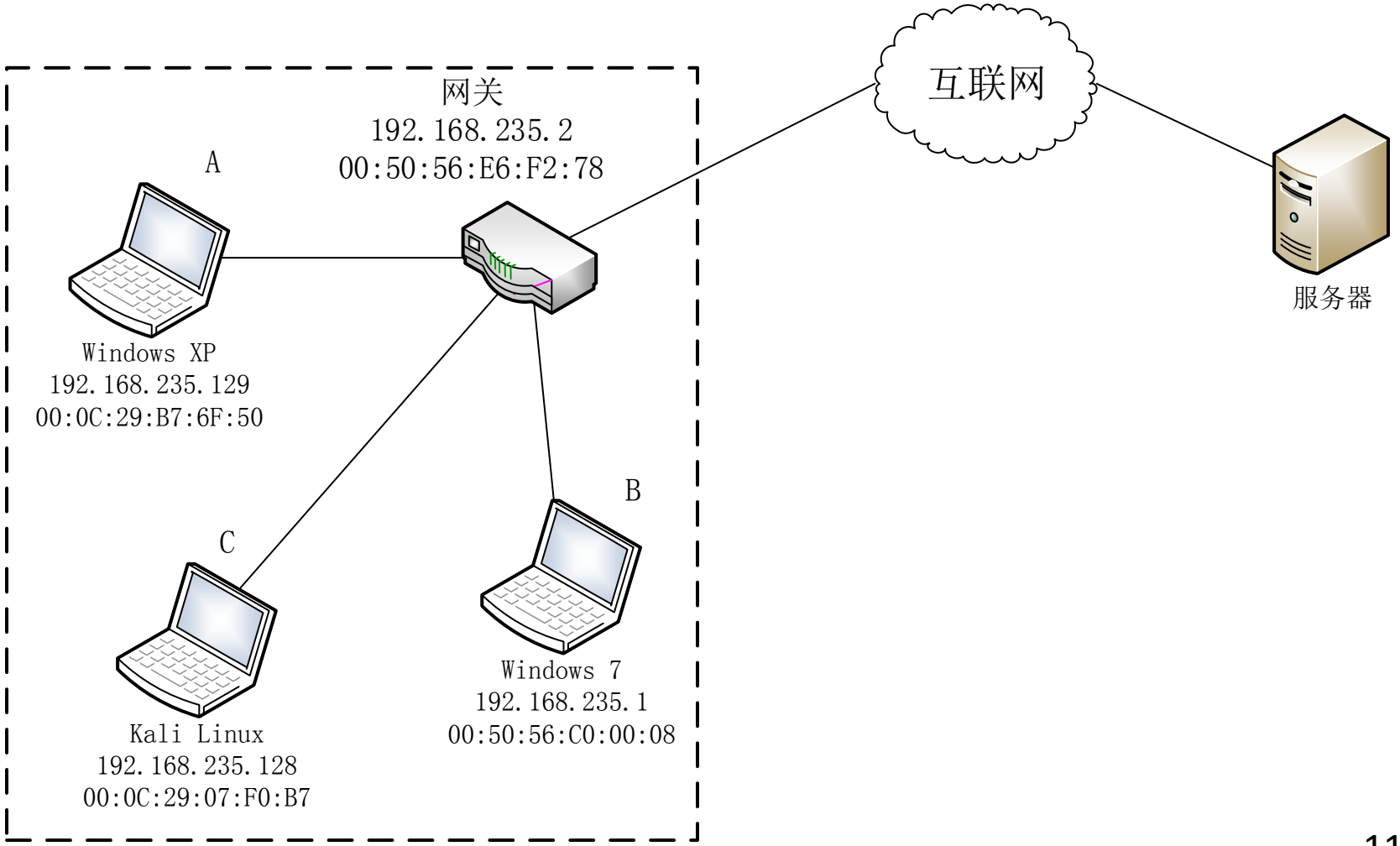
成为中间人——ARP欺骗

- ARP缓存表
  - 保存了当前局域网中各主机IP对应的MAC地址，保证数据传输的一对一特性
  - 静态ARP缓存永久储存
  - 动态ARP缓存在超过指定时间后将被删除

```
C:\Users\WYZ>arp -a

接口: 10.15.8.193 --- 0xc
  Internet 地址         物理地址              类型
  10.15.8.1             58-66-ba-82-82-41     动态
  10.15.8.115           b8-ca-3a-67-df-50     动态
  10.15.8.130           c0-3f-d5-02-38-bc     动态
  10.15.8.218           00-0c-29-65-99-09     动态
  10.15.8.255           dc-0c-5c-e6-ea-c2     静态
  10.15.9.255           ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
```

成为中间人——ARP欺骗

- 局域网主机通信



成为中间人——ARP欺骗

- ARP欺骗原理
  - 主机收到ARP应答信息后不会校验应答的准确性，直接将应答信息存入缓存

1514	1378.4677367…	Vmware_07:f0:b7	Vmware_c0:00:08	ARP	42	192.168.235.129 is at 00:0c:29:07:f0:b7
1515	1378.4681628…	Vmware_07:f0:b7	Vmware_b7:6f:50	ARP	42	192.168.235.1 is at 00:0c:29:07:f0:b7
1516	1380.2270460…	fe80::2021:776:d31a…	ff02::1:2	DHCPv6	146	Solicit XID: 0x4c8433 CID: 00010001229c63c528d244229205
1517	1388.4795962…	Vmware_07:f0:b7	Vmware_c0:00:08	ARP	42	192.168.235.129 is at 00:0c:29:07:f0:b7
1518	1388.4800562…	Vmware_07:f0:b7	Vmware_b7:6f:50	ARP	42	192.168.235.1 is at 00:0c:29:07:f0:b7
1519	1396.2274670…	fe80::2021:776:d31a…	ff02::1:2	DHCPv6	146	Solicit XID: 0x4c8433 CID: 00010001229c63c528d244229205
1520	1398.4908954…	Vmware_07:f0:b7	Vmware_c0:00:08	ARP	42	192.168.235.129 is at 00:0c:29:07:f0:b7
1521	1398.4911753…	Vmware_07:f0:b7	Vmware_b7:6f:50	ARP	42	192.168.235.1 is at 00:0c:29:07:f0:b7
1522	1408.5020791…	Vmware_07:f0:b7	Vmware_c0:00:08	ARP	42	192.168.235.129 is at 00:0c:29:07:f0:b7
1523	1408.5026689…	Vmware_07:f0:b7	Vmware_b7:6f:50	ARP	42	192.168.235.1 is at 00:0c:29:07:f0:b7
1524	1411.1079523…	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
1525	1413.7518490…	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
1526	1414.6074521…	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
1527	1415.6076734…	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1

```
▸ Frame 1521: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: Vmware_07:f0:b7 (00:0c:29:07:f0:b7), Dst: Vmware_b7:6f:50 (00:0c:29:b7:6f:50)
▸ [Duplicate IP address detected for 192.168.235.1 (00:0c:29:07:f0:b7) - also in use by 00:50:56:c0:00:08 (frame 1520)]
▸ Address Resolution Protocol (reply)
```

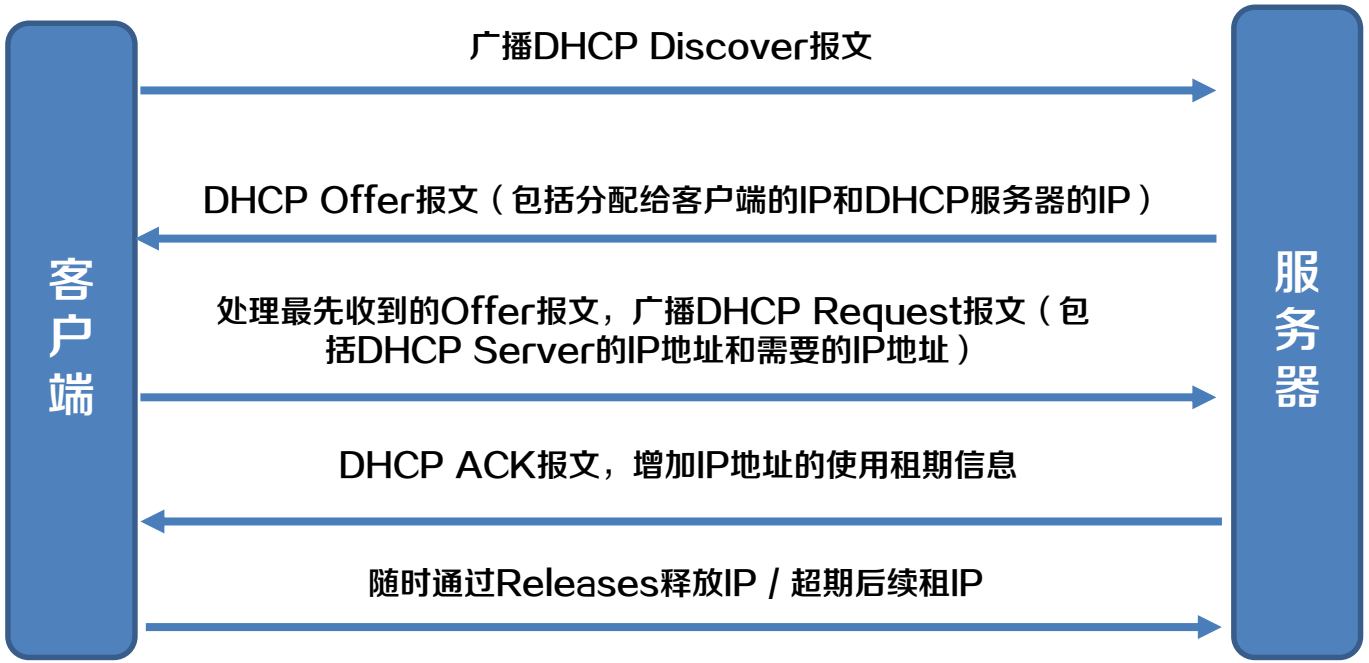
```
C:\Documents and Settings\WYZ>arp -a

Interface: 192.168.235.129 --- 0x2
  Internet Address      Physical Address      Type
  192.168.235.1         00-50-56-c0-00-08     dynamic
  192.168.235.2         00-50-56-f6-16-c2     dynamic
```

```
C:\Documents and Settings\WYZ>arp -a

Interface: 192.168.235.129 --- 0x2
  Internet Address      Physical Address      Type
  192.168.235.1         00-0c-29-07-f0-b7     dynamic
  192.168.235.2         00-50-56-f6-16-c2     dynamic
```

成为中间人

- ICMP重定向攻击
  - ICMP（Internet Control Message Protocol）是TCP/IP协议族的一个子集，用于在IP主机、路由器之间传递控制消息
  - ICMP重定向技术是用来提示主机改变自己的主机路由从而使路由路径最优化的一种ICMP报文

- DHCP攻击
  - DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）。作为局域网的一个网络协议，主要作用是给内网客户端自动分配IP地址。



成为中间人

- NDP攻击
  - NDP(Neighbor Discovery Protocol)是IPv6协议的一个重要组成，取代了IPv4的ARP，ICMP路由发现和重定向功能。
  - 在IPv6中使用NDP 来发现直接相连的邻居信息，包括邻接设备的设备名称、软/硬件版本、连接端口等，另外还可提供设备的ID、端口地址、硬件平台等信息。
  - 邻居信息表中的每一表项都是可以老化的，一旦老化时间到，NDP自动删除相应的邻居表项。

成为中间人

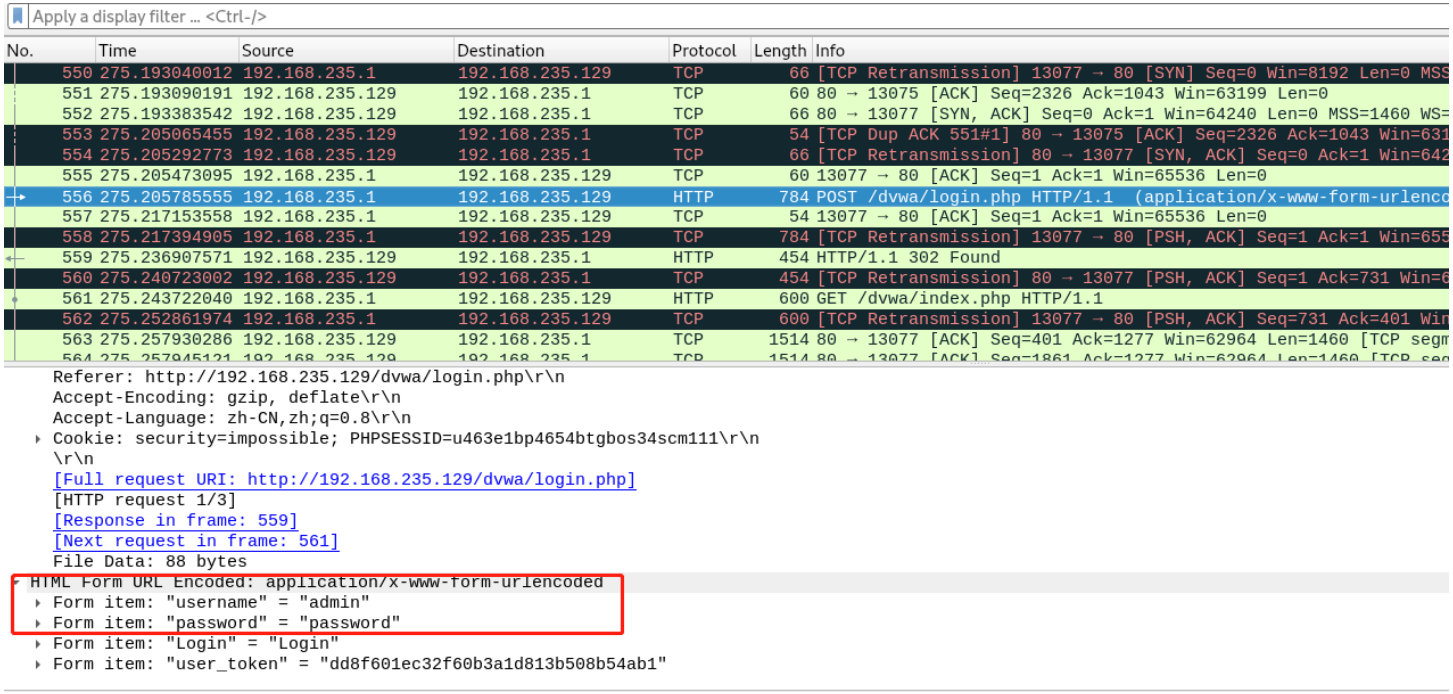
- 孪生AP攻击
  - AP的特征往往通过ESSID和加密方式来进行判断
  - 攻击者通过建立一个相同ESSID，相同MAC地址以及相同加密方式的AP，并且信号强度大于原AP，诱导目标设备自动连接攻击者的AP
  - 为目标主机分配IP和DNS服务器

基于HTTP协议的中间人攻击

- 断网攻击
- 信息窃取
- 会话劫持
- 会话修改
- DNS欺骗、钓鱼

基于HTTP协议的中间人攻击

- 信息窃取

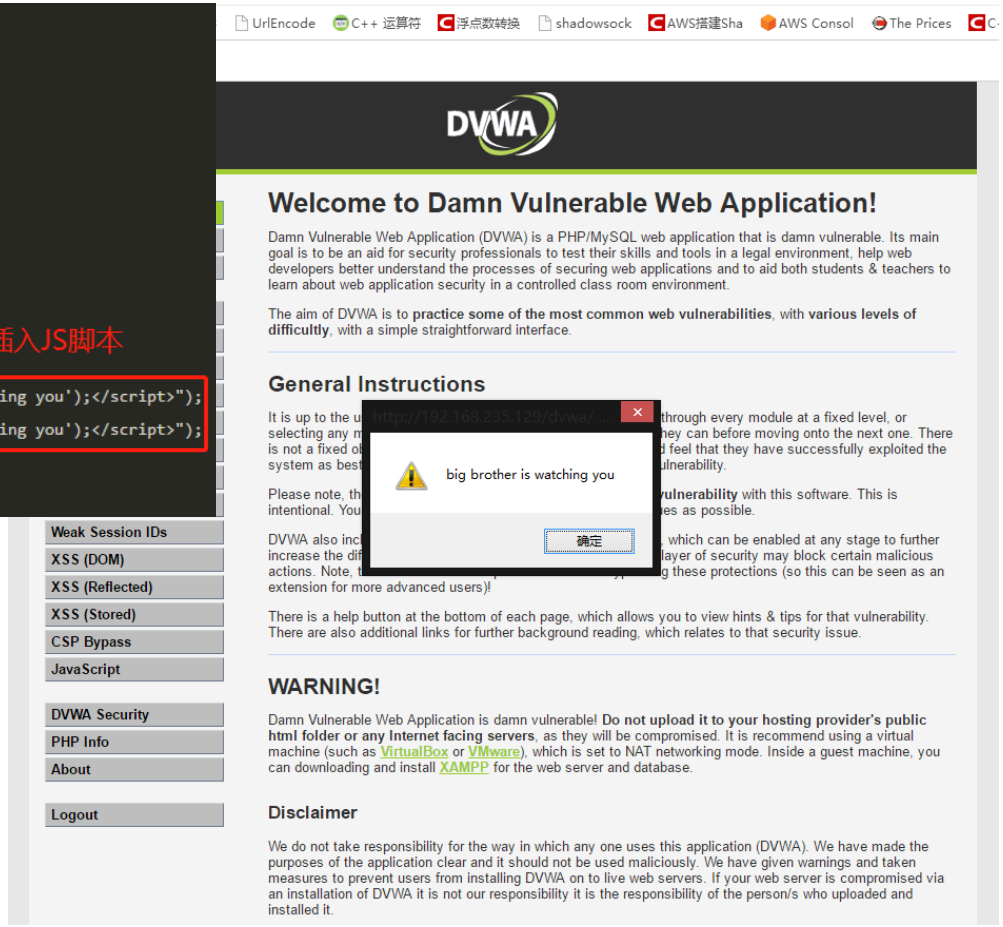


基于HTTP协议的中间人攻击

- 会话修改

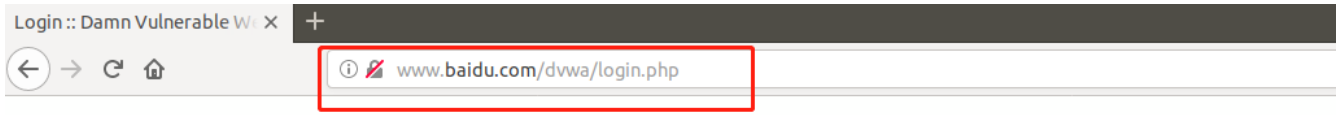
```
if (ip.proto == TCP && tcp.dst == 80)
{
    if (search(DATA.data, "Accept-Encoding"))
    {
        replace("Accept-Encoding", "Accept-Rubbish!");
        # note: replacement string is same length as original string
        msg("zapped Accept-Encoding!\n");
    }
}
if (ip.proto == TCP && tcp.src == 80)
{
    replace("<head>", "<head><script type="text/javascript">alert('big brother is watching you');</script>");
    replace("<HEAD>", "<HEAD><script type="text/javascript">alert('big brother is watching you');</script>");
    msg("Injecting OK!!\n");
}
```

在服务器返回的网页中插入JS脚本



基于HTTP协议的中间人攻击

- DNS欺骗
  - DNS为域名解析，即从url网址到ip地址的转换过程，通过DNS欺骗，把目标的请求重定向到指定的ip地址

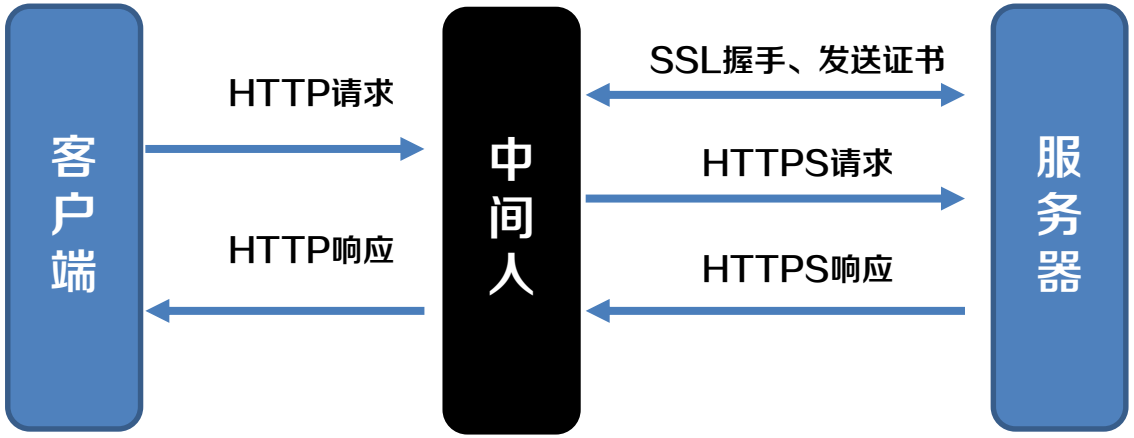



```
microsoft.com MX 2001:db8::1ce:c01d:bee3
##############################################
#TEST MY OWN SPOOF

www.baidu.com   A   192.168.235.129

##############################################
# This messes up NetBIOS clients using DNS
```

将baidu域名解析为恶意网站IP

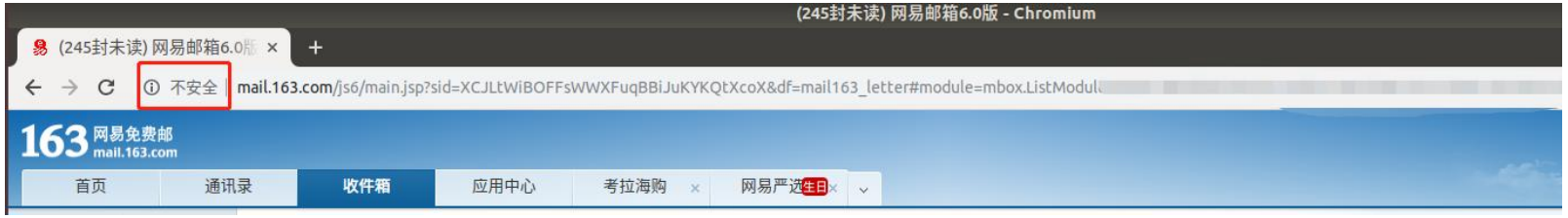
基于HTTPS的中间人攻击

- SSL卸载（HTTPS降级）



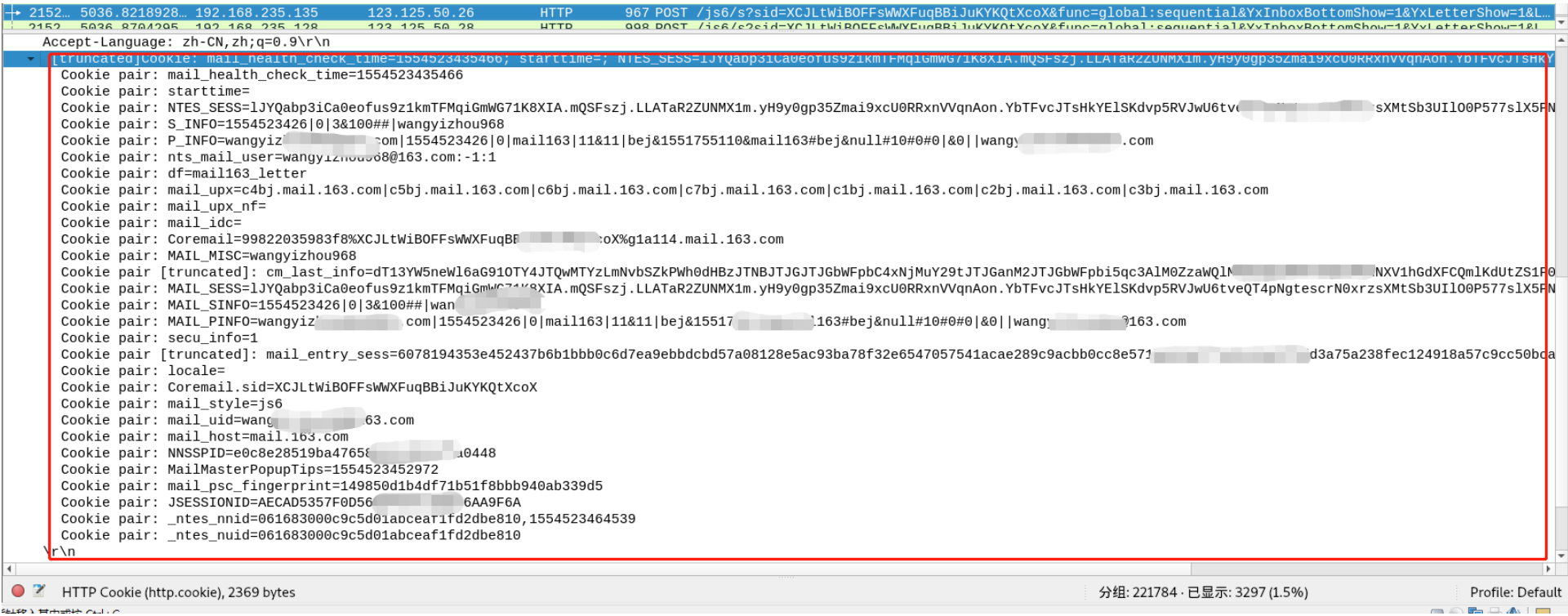
基于HTTPS的中间人攻击

- SSL卸载（HTTPS降级）



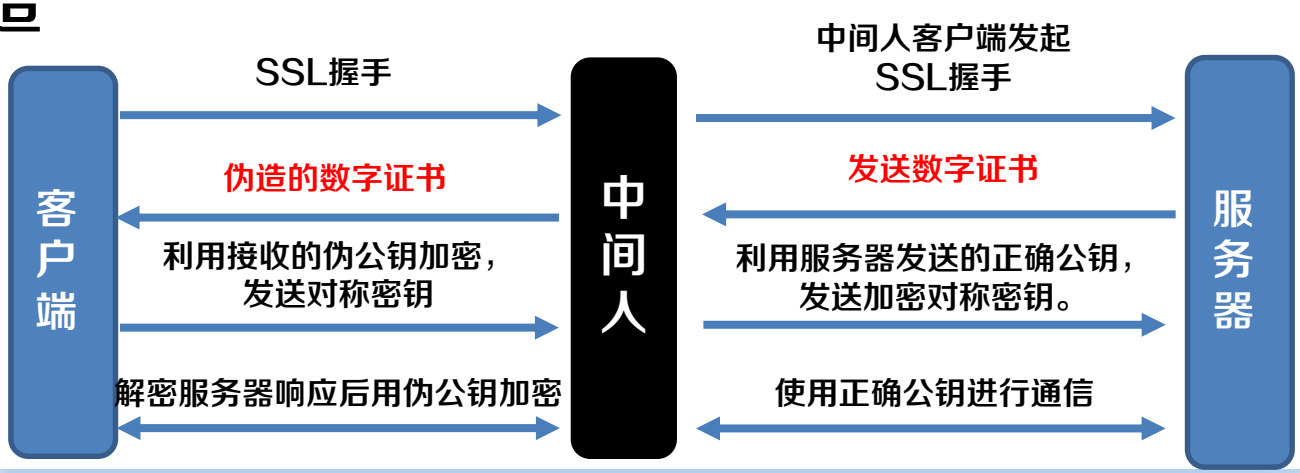
基于HTTPS的中间人攻击

- SSL卸载（HTTPS降级）



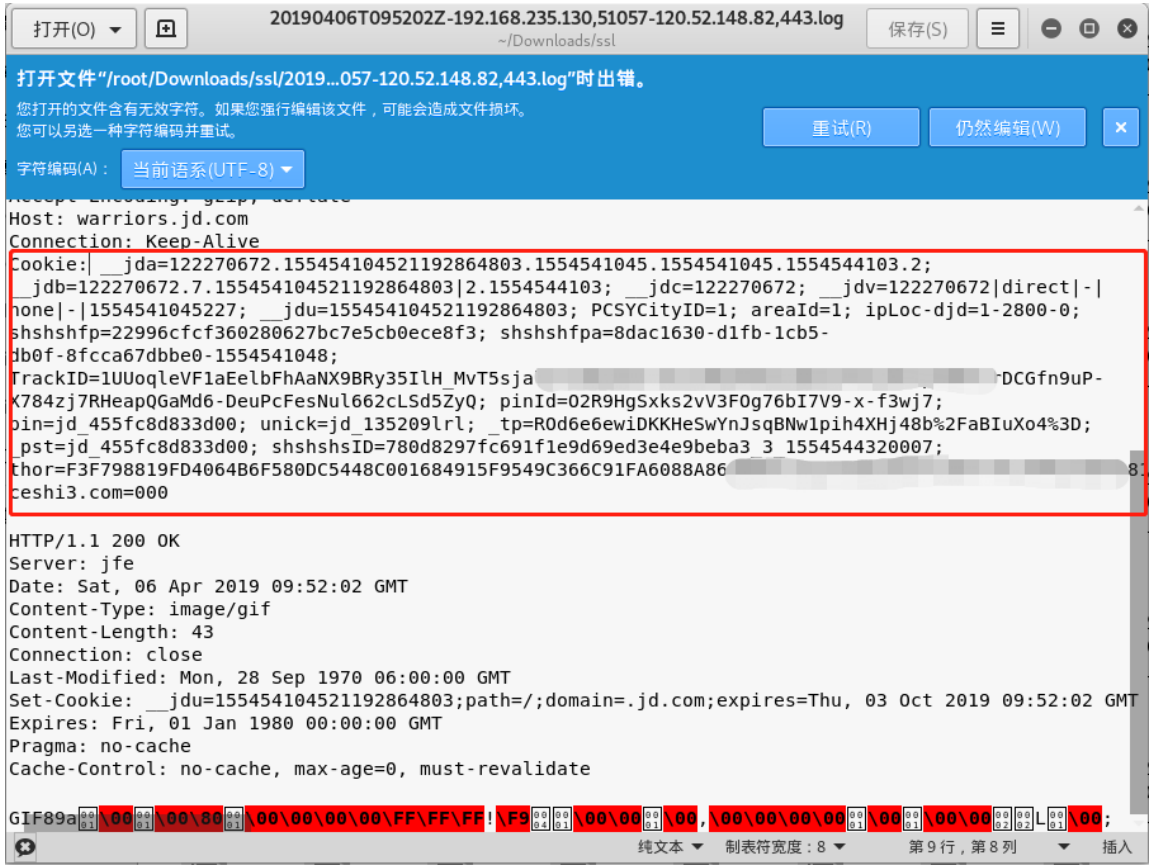
基于HTTPS的中间人攻击

- SSL伪造



基于HTTPS的中间人攻击

- SSL伪造



中间人攻击的防范

- 静态绑定IP和MAC地址
- 在交换机启用DHCP Snooping功能
- 拒绝接收ICMP重定向报文
- 访问有敏感信息的页面时使用HTTPS协议

参考文献

[1]张炳帅. Web安全深度剖析[M]. 电子工业出版社, 2015.
[2]https://cloud.tencent.com/developer/article/1197597
[3]https://evilpan.com/2015/11/28/how-to-become-mitm/
[4]https://evilpan.com/2015/11/01/mitm-detail-1/
[5]https://www.colabug.com/870868.html

知人者智，自知者明。胜人者有力，自胜者强。知足者富。强行者有志。不失其所者久。死而不亡者，寿。

谢谢！