利用流量分析还原攻击

指导老师：王美珍

实验内容

- 实验目的
- 实验环境
- 实验原理
- 实验任务
- 实验要求

1. 实验目的

- 利用wireshark监听网络流量信息并完整记录
- 通过实验了解使用wireshark进行恶意流量分析的基本流程及操作，同时能够配合互联网上其他公开的工具如在线分析引擎、搜索引擎、安全专家的技术博客等进行全方位的分析。
- 掌握wireshark流量分析的方法，还原现场

2. 实验环境

- 分析工具：wireshark（可以在windows下进行分析）
- 攻击还原环境：
  - 攻击机：kali-linux 2.0，靶机: metaploitable2

3 实验原理

- **什么是流量分析?**
  - 流量分析是网络取证中实时取证的重要内容，对原始数据进行网络还原、重现入侵现场具有重要意义
  - 实时取证，也称为动态取证，是指通过设备或软件实时捕获流经网络设备和终端应用的网络数据并分析网络数据的内容，来获取攻击者的企图和攻击者的行为证据
  - 利用分析采集后的数据，对网络入侵时间，网络犯罪活动进行证据获取、保存、和还原，流量分析能够真实、持续的捕获网络中发生的各种行为，能够完整的保存攻击者攻击过程中的数据，对保存的原始数据进行网络还原，重现入侵现场
- **不同的应用层，流量分析起到的作用不同**
  - 用户层：运营商通过分析用户网络流量，来计算网络消费。
  - 管理层：分析网络流量可以帮助政府、企业了解流量使用情况，通过添加网络防火墙等控制网络流量来减少资源损失。
  - 网站层：了解网站访客的数据，如ip地址、浏览器信息等；统计网站在线人数，了解用户所访问网站页面；通过分析出异常可以帮助网站管理员知道是否有滥用现象；可以了解网站使用情况，提前应对网站服务器系统的负载问题；了解网站对用户是否有足够的吸引能力。
  - 综合层：评价一个网站的权重；统计大多数用户上网习惯，从而进行有方向性的规划以更适应用户需求。

3. wireshark进行流量分析的基本操作

- 流量统计
- 获得主机信息：IP、域名、用户名等信息
- 流量过滤，去掉噪音
- 流量追踪
- 从数据包中导出数据到文件
- 结合其它信息一起分析

流量统计

- Wireshark加载之后，点击上方菜单统计-->ipv4 statistics-->all address
  - 确定IP地址范围

Wireshark · All Addresses · WLAN

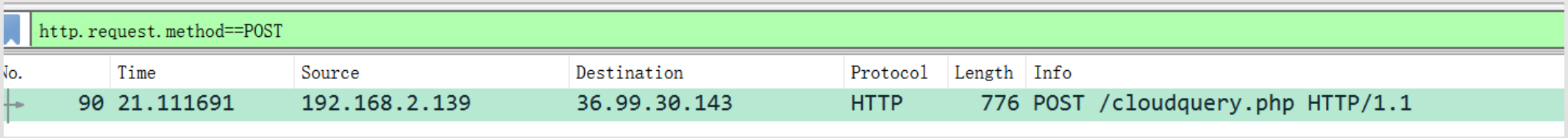
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	219				0.0086	100%	0.3100	8.967
58.49.138.26	23				0.0009	10.50%	0.1400	8.139
52.139.250.253	3				0.0001	1.37%	0.0200	17.717
239.255.255.250	26				0.0010	11.87%	0.1200	14.290
220.181.44.144	3				0.0001	1.37%	0.0300	8.169
203.119.169.109	52				0.0020	23.74%	0.0600	13.178
192.168.2.241	4				0.0002	1.83%	0.0100	14.290
192.168.2.139	193				0.0076	88.13%	0.3100	8.967
192.168.2.1	31				0.0012	14.16%	0.1100	14.290
183.3.224.144	29				0.0011	13.24%	0.1100	8.074
183.3.224.139	12				0.0005	5.48%	0.1100	4.262
180.163.26.115	18				0.0007	8.22%	0.1800	8.992
172.217.27.142	9				0.0004	4.11%	0.0200	2.001
172.217.24.14	4				0.0002	1.83%	0.0100	23.428
172.217.160.110	11				0.0004	5.02%	0.0300	20.014
123.151.78.31	7				0.0003	3.20%	0.0300	0.000
111.177.1.77	13				0.0005	5.94%	0.1300	8.307

获得主机信息：IP、域名、用户名等信息

- 主机名：过滤nbns信息，可以查看到查询域的报文信息（端口为137）
- IP：报文直接列出
- 用户名：通过某些应用数据可以获得用户名等信息，如FTP登录信息、HTTP表单提交的登录信息等

流量过滤

- 针对要分析的流量，通过设置过滤器，只保留感兴趣的流量，去除大量噪音流量
  - 比如：要分析http请求的流量，希望看到从服务器下载了什么文件或数据
    - http.request.method==GET
  - 向服务器上传了什么文件
    - http.request.method==POST



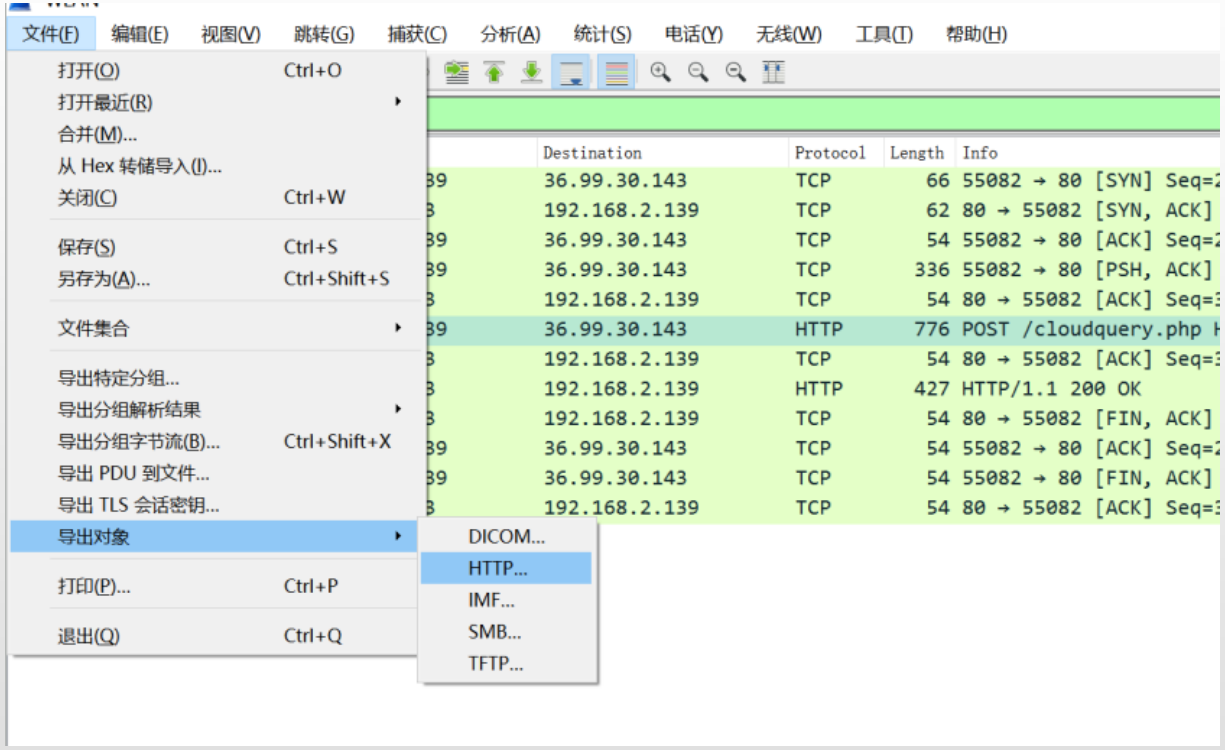
- 根据报文的协议、端口、报文的指定字段、标志等设定过滤器，进行比较精准的过滤

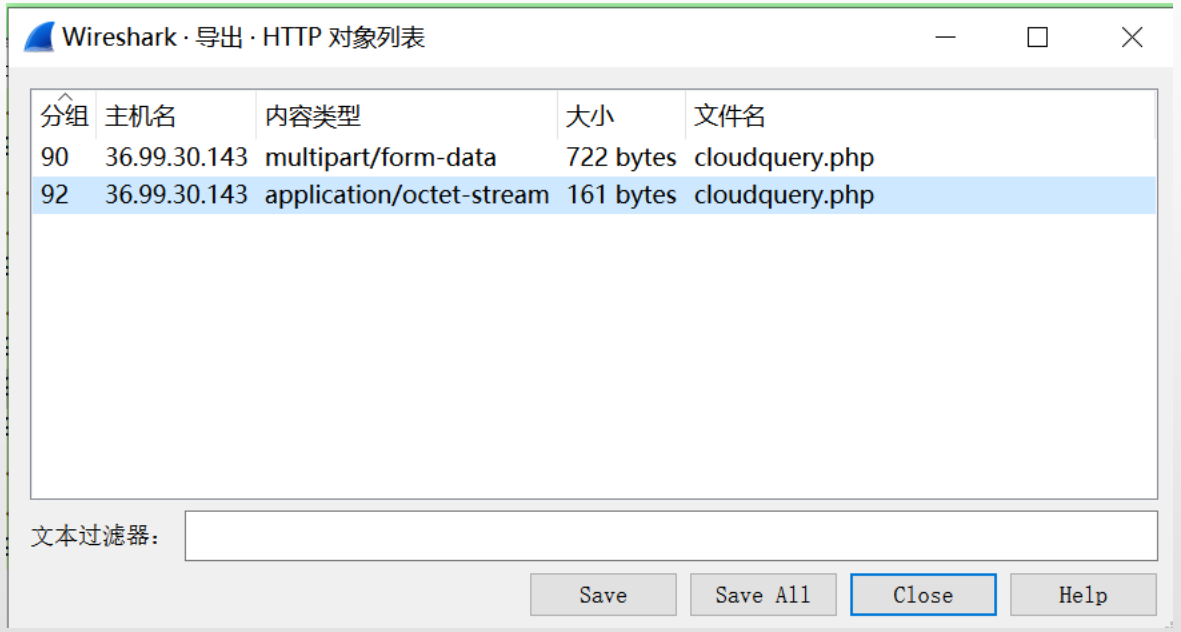
流量追踪

- 同一个会话的流量可以进行追踪


```
POST /cloudquery.php HTTP/1.1
User-Agent: Post_Multipart
Host: 36.99.30.143
Accept: */*
Pragma: no-cache
X-360-Cloud-Security-Desc: Scan Suspicious File
x-360-ver: 4
Content-Length: 722
Content-Type: multipart/form-data; boundary=----------------------------2ec67b9880fc

----------------------------2ec67b9880fc
Content-Disposition: form-data; name="m"


..@:@....i....-p..r.#...2A...K...]..@G........>1.),r9.0.D....Pg..
....f.}@"....-"..UGZ.:.l.....}.T.
.Uj~! 8?..qO.3z.t}....z..o.4sM........).!_Df....g....qO....
5....].G.zMvP..a.....;E.:....].v...k.)....c..E.,.-...'&ai'...7...5.......      Qb%^.....
4.4.a...0....../9....Y..!.M.....M.&..-.`]_...._.. .wk...T...&.Jz~....p.p!_...Ql%.(.....
..s)...^.p
Gc.,..*(....P,.}-1.0       ..
....0.M.:..sL.}...c..|...g..1.L...Y.......Aa-b.Ik.w..........X...../I..7...Q.~.....P..
5.F."..Z..s...P^..^Kz.).?.....blrZ...|.o....|f....e 7.)....F{(.^...ER6..K.b...V.
..,k..|.V..:....V..g.g
----------------------------2ec67b9880fc--
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 03 May 2020 08:19:42 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: close
Cache-Control: no-cache
pragma: no-cache

a1

...:@......P..E. B
...R..0...,..ve@.....7..d.;.>?1De/.w. .[..p.=[..m....'4L.4.,....y.
2.........<.R.....................................?.?.?.?.?.?.?.?.?.?.;.
0
```

从数据包中导出数据到文件





流量分析相关网络资源

- https://www.malware-traffic-analysis.net/ ,所有压缩包解压密码均为infected
- http://hetianlab.com ， 合天网安实验室，恶意代码流量分析系列课程，里面用的截包材料也是上面网站的资源

4. 实验任务

- 学习2个恶意流量分析的案例，了解流量分析的基本操作和过程（部分针对恶意代码、病毒名称的分析可以跳过去，主要学习分析的思路，以及wireshark的用法）；
  - 案例1文件：实验2 流量分析 案例1.rar
  - 案例2文件：实验2 流量分析 案例2.rar
  - 压缩包解压密码：infected
- 对提供的流量分析的截包，完成以下分析任务：
  - 1）数据包是在靶机192.168.2.222上截的包，请确认攻击主机的信息；
  - 2）还原攻击的步骤（利用了什么漏洞，整个攻击过程做了哪些操作）；
  - 3）还原从靶机获得的用户文件，并对用户文件进行密码破解，提交破解出来的root用户的口令；（提示：8个小写字符，以msf结尾）
  - 4）作业，把还原攻击和流量分析的过程记录下来。

5. 实验要求

- 按照实验任务要求独立完成实验，在规定时间内在线提交分析结果；
- 提交详细的实验报告（第三级课程结束时，跟课程其它实验一起提交）