实验二：网络攻击流量分析与溯源

一．目标

对网络攻击流量的分析可以对可疑安全事件进行定性分析，通过深入的数据关联、数据包解码分析和特征分析，真实的还原安全事件的发生过程，从而对各种异常网络事件进行精准的定性分析、追踪与溯源，以及提出后续处置方案。

（1）追踪问题源：包括涉及主机 IP 地址、地理位置、操作系统等；

（2）提取异常数据：包括攻击目标、是否使用 shellcode、是否涉及恶意软件等；

（3）为安全取证提供依据：包括还原攻击者实施攻击的整个过程等；

（4）安全响应与处置：包括提出应急处置方案和安全加固方案等。

二．要求

（1）6-7 人成一组，可沿用实验一的分组，也可重新调整。

（2）根据实验材料中提供的一段网络攻击数据包，数据包涉及到的简要网络信息如下：

网段:　10.10.10.0/24

（3）分析该数据包并回答以下问题。（注：流量包中的受害者的真实 IP 已被修改，请勿尝试进行重放）

- 攻击事件发生的时间和持续的时间，受攻击方涉及哪些系统信息（包含 IP 地址、MAC 地址、用户登录账户）？
- 受攻击主机的操作系统是什么？哪个服务？哪个漏洞？
- 在提供的流量文件中，包含多少个 TCP 会话？哪些应用层协议？

- 可以找到攻击主机的哪些信息？（如：IP 地址、MAC 地址、地理位置等）
- 详细描述攻击者实施攻击的整个过程。
- 攻击过程是否涉及到漏洞？如有，列出涉及到漏洞的 CVE 编号，并简要描述漏洞特点以及漏洞利用方式。
- 攻击过程是否涉及到恶意软件(Malware)？如有，列出恶意软件的名字和 MD5 值，所属恶意软件家族，并简要分析该恶意软件行为。
- 你认为这是一个人工实施攻击的过程，还是自动攻击的过程？为什么？该种攻击是否可以实现人工智能驱动的自动化攻击？设计一种自动化攻击的思路。
- 按照课堂讲授的方法，利用各类威胁情报平台，列出并分析本次攻击涉及到的攻击指示器，设计一套自动化利用威胁情报对该类攻击进行防御的机制。
- 假如你是该网络域的安全管理者，针对本次已发生攻击行为，对主机和网络作出详细的应急处置方案。在使用当前工业界已有产品前提下，对后续主机及网络的安全加固提出建议。

三．相关材料

- 实验分析对象：Exercise-II.pcap
- 推荐使用的工具：Wireshark、tshark、NetworkMiner、p0f、whois、nslookup、geoiplookup、dd、ollydbg、IDA 等。

四．交付物与截止时间

- 包含流量分析方法（分析思路、分析工具）、溯源结果（溯源步骤描述）等内容的 Word 版实验报告。注意列出参考文献。
- 实验报告 Word 版，按“溯源取证课-组长学号-组长姓名-流量分析与溯源”形式命名。在 2018 年 11 月 13 日前加密（密码约定 syqz2018!），发到**邮箱 yao_ye_peng@163.com**。
- **注意体现成员的分工/贡献。**