网络溯源取证实验二：网络攻击流量分析与溯源

注：要求每个组员必须完成累计15分以上的问题

|  |  |
| --- | --- |
| 组名： | |
| 组长姓名： | 研究室： |
| 邮箱： | 手机号： |
| 学号： | 答题情况：如问题1 |
|  | |
| 组员姓名： | 研究室： |
| 邮箱： | 手机号： |
| 学号 | 答题情况 |
|  | |
| 组员姓名： | 研究室： |
| 邮箱： | 手机号： |
| 学号 | 答题情况 |
|  | |
| 组员姓名： | 研究室： |
| 邮箱： | 手机号： |
| 学号 | 答题情况 |
|  | |
| 组员姓名： | 研究室： |
| 邮箱： | 手机号： |
| 学号 | 答题情况 |
|  | |
| 组员姓名： | 研究室： |
| 邮箱： | 手机号： |
| 学号 | 答题情况 |

|  |  |
| --- | --- |
| 问题1：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）？ | 5分 |
| 使用的工具： | 得分： |
| 答1： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题2：受攻击主机的操作系统是什么？哪个服务？哪个漏洞？ | 5分 |
| 使用的工具： | 得分： |
| 答2： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题3：在提供的流量文件中，包含多少个TCP会话？哪些应用层协议？ | 5分 |
| 使用的工具： | 得分： |
| 答3： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题4：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） | 5分 |
| 使用的工具： | 得分： |
| 答4： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题5：详细描述攻击者实施攻击的整个过程。 | 10分 |
| 使用的工具： | 得分： |
| 答5： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题6：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。 | 10分 |
| 使用的工具： | 得分： |
| 答6： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题7：攻击过程是否涉及到恶意软件？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。 | 15分 |
| 使用的工具： | 得分： |
| 答7： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题8：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。 | 15分 |
| 使用的工具： | 得分： |
| 答8： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题9：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。 | 20分 |
| 使用的工具： | 得分： |
| 答9： | |
| 评审意见： | |

|  |  |
| --- | --- |
| 问题10：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。 | 20分 |
| 使用的工具： | 得分： |
| 答10： | |
| 评审意见： | |

总分：