1. **确定分析对象**

通过对工控网络的分析确定我们测试对象。工业控制系统（ICS）是几种类型控制系统的总称，包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）和其它控制系统。对系统的核心控制元件和网络组件进行查验。

1. **分析过程和方法**
	1. **主机检测**

对处于关键节点的计算机进行检测

* + 1. **上位机**

上位机是一台计算机，我们可以用以下几种方法来分析

扫描端口：查看是否开放可疑端口

查看系统配置：查看系统的账户，是否存在隐藏账户，安全策略是否被改动

查找可疑进程和文件：使用杀毒软件对系统进行全盘扫描，查找是否存在后门木马以及病毒

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 扫描端口 | 查看是否开放可疑端口 | Nmap或者直接cmd运行命令netstat -an |
| 查看系统配置 | 查看系统的账户，是否存在隐藏账户，安全策略是否被改动 | 直接在系统上查看 |
| 查找可疑进程和文件 | 使用杀毒软件对系统进行全盘扫描，查找是否存在后门木马以及病毒 | 杀毒软件如mcafee，小红伞 |

* + 1. **应用服务器**

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 扫描端口 | 查看是否开放可疑端口 | Nmap或者直接cmd运行命令netstat -an |
| 查看系统配置 | 查看系统的账户，是否存在隐藏账户，安全策略是否被改动 | 直接在系统上查看 |
| 查找可疑进程和文件 | 使用杀毒软件对系统进行全盘扫描，查找是否存在后门木马以及病毒 | 杀毒软件如mcafee，小红伞 |
| Webshell查杀 | 使用专用的webshell查杀工具扫描，用来发现黑客留下的web后门 | D盾、360等 |

* 1. **网络检测**

网络监测：可以使用行为管控硬件进行监控，发现可以用户行为

流量监测：使用入侵检测系统进行监控

网络边界：在网络边界查找薄弱环节，查看边界完整性，是否存在不合理配置

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 网络监控 | 可以使用行为管控硬件进行监控，发现可以用户行为 | 上网行为管理 |
| 流量监控 | 使用入侵检测系统进行监控 | 如IDS |
| 网络边界完整性检查 | 在网络边界查找薄弱环节，查看边界完整性，是否存在不合理配置 | 手工查看 |

网络安全分析：

①病毒木马分析

②暴力破解分析

③垃圾邮件分析

④web服务器攻击分析

⑤ARP欺骗分析

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 收集网络流量 | 收集流量以便于分析 | 专用的流量收集设备 |
| 网络协议分析 | 使用相应的工具对收集到的流量包进行分析处理，找出流量较大、发包次数较大的节点ip | Wireshark、专业的分析工具 |
| 找出异常流量并对其分析 | 对流量较大的节点ip进行进一步的分析，找出对应的进程和端口 |  |

* 1. **漏洞**

**漏洞类型：**

①应用系统漏洞

②Windows系统漏洞

③Linux系统漏洞

④路由器及其他硬件设备漏洞

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 应用系统漏洞 | 找出系统薄弱容易被利用的环节 | 手工测试辅以工具 |
| 操作系统漏洞 | 找出系统薄弱容易被利用的环节 | 手工测试辅以工具 |
| 路由器及其他硬件设备漏洞 | 找出系统薄弱容易被利用的环节 | 手工测试辅以工具 |

* 1. **日志分析**

**收集对象及工具**：

①应用系统日志：可以使用

②数据库：

③应用服务器日志：

④路由器：

⑤防火墙：

⑥访问控制日志：

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 收集需要分析的日志 | 将所有需要分析的日志进行收集，如数据库日志、应用日志、应用系统日志、操作系统日志、路由器、防火墙等硬件设备日志 | 人工收集、审计系统收集 |
| 对日志进行分析 | 对所有收集到的日志进行初步分析，将疑似攻击痕迹进行记录 | 日志分析工具如360星图、人工编写匹配规则 |
| 上机检查 | 根据日志分析的初步结果，上机进行行为判断，推测入侵过程 | 人工测试 |
|  |  |  |

* 1. **渗透测试**

|  |  |  |
| --- | --- | --- |
| 方法 | 目的 | 工具 |
| 工具扫描 | 用工具找出常见的、易发现的漏洞 | 常见的扫描工具wvs、appscan、Nessus等等 |
| 手工测试 | 利用经验和不同的思路来找出系统不容易发现的威胁 | 手工测试 |
| 社会工程学 | 利用平时收集的数据库找出目标用户的信息，从而获取进入系统的钥匙 |  |
| 漏洞攻击 | 对发现漏洞的系统，用已经有利用的工具进行攻击 | Sqlmap、metasploit等 |
| 权限提升 | 利用权限提升的工具获取系统最高权限 |  |

| **测试项** | **测试子项** |
| --- | --- |
| 自动化扫描测试 | 专业工具扫描 |
| 信息收集 | Web服务器端口扫描 |
| 危险HTTP方法测试 |
| Web中间件版本 |
| 脚本语言 |
| 中间件安全 | 中间件安全漏洞 |
| 中间件管理后台 |
| 目录浏览 |
| 文件目录测试 | 程序遍历目录 |
| 任意文件修改 |
| 文件上传 |
| 文件下载 |
| 文件包含 |
| 注入测试 | SQL注入测试 |
| 命令执行测试 |
| 跨站脚本 | 反射型跨站脚本 |
| 存储型跨站脚本 |
| 权限管理测试 | 横向测试 |
| 纵向测试 |
| 口令测试 | 弱口令/默认口令 |
| 编辑器测试 | 编辑器漏洞测试 |
| 信息泄漏测试 | 测试、备份页面代码 |
| 备份压缩文件 |
| Robots接口信息泄露 |
| 异常处理信息泄露 |
| 管理后台是否可猜测 |
| 其他方式 |
| 开源代码检测 | 开源代码漏洞检查 |
| 逻辑测试 | 业务/程序逻辑测试 |
| 程序设计漏洞 |
| 入侵挂马检测 | 百度检测 |
| Google检测 |
| 安全联盟 |
| 旁路测试 | 旁路测试 |
| 漏洞危害性测试 | 漏洞危害性测试（通过对漏洞验证之后是否可以对内网以及其他服务进行渗透测试） |
| 其他漏洞 | 用户登录认证绕过重放攻击 |