2025《信息物理系统安全》PPT 展示题目

（从以下题目中任选一题准备每组 15-20 分钟 PPT 展示）

事件综述类

（从真实的信息物理系统安全事件分析，可以分析**行业背景、信息物理系统结构与特点、攻击原理、造成影响、防御措施**等，也可选择其他信息物理系统安全事件；**在展示中融入自己的思考**；标*问题相对更新颖，赋分高）

1. 从特斯拉 Model X 中继攻击看自动驾驶汽车信息物理系统安全
2. 从 SolarWinds 供应链攻击看信息物理系统安全
3. 从台积电事件看制造业信息物理系统安全
4. 从 colonial pipeline 公司被勒索事件分析信息物理系统安全
5. Vault7 等数据泄露事件与信息物理系统安全
6. 从乌克兰停电事件看电网信息物理系统安全
7. *CVE-2024-3094 Informational: Impact of Malicious Code in XZ Tools and Libraries 研究该事件的供应链攻击原理
8. *基于 2025 年 Black Hat Double Tap at the Blackbox Hacking a Car Remotely Twice with MiTM，分析未来电动汽车/共享电动汽车对智能电网的潜在威胁，可以结合交通网络建模、用户使用习惯等进行分析
9. *分析量子信息技术对信息物理系统安全带来的挑战与机遇，可以结合量子计算、量子通讯等技术的最新进展

创新实践类（动手实践，赋分高）

1. Modbus 协议是信息物理系统较为常用的一款网络协议。试分析 Modbus 协议的应用层格式和存在的安全性问题（例如机密性、完整性、实时性等），编写 Python 脚本实现支持 Modbus/TCP 通信的 Client 和 Server（可参考 github 上的开源项目）。

   Modscan：模拟 Modbus 主站

   Modsim：模拟 Modbus 从站

   Pymodbus：https://pymodbus.readthedocs.io/en/latest/

2. 了解模糊测试 Fuzzing 以及目前针对 IoT 设备的主流模糊测试方法，了解、介绍、测试开源工具 AFL Fuzz 或

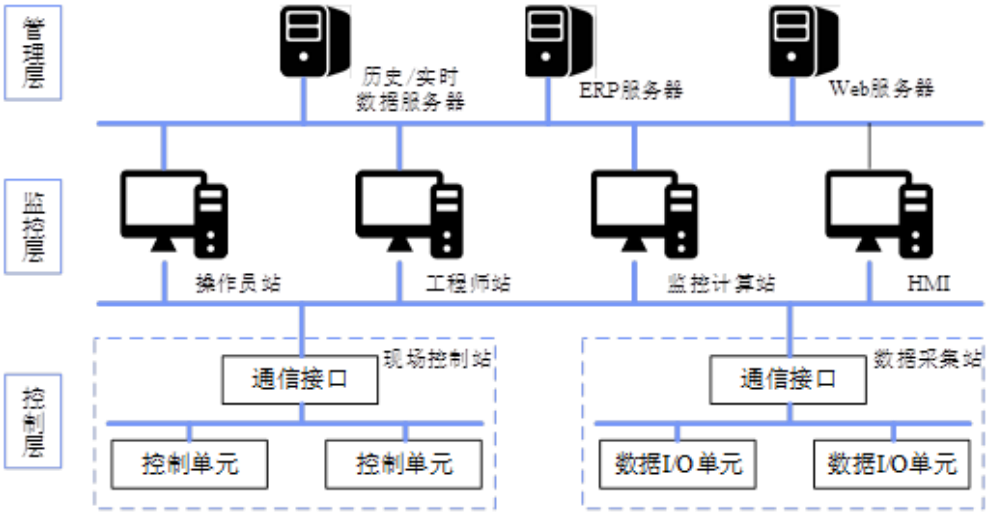
   AFL：https://github.com/google/AFL

   AFLNet：https://github.com/aflnet/aflnet

   BooFuzz：https://boofuzz.readthedocs.io/en/stable/index.html

3. 调研私有协议逆向的主流方法，选取现有的工具，如 Netzob 等进行介绍并针对工业控制系统典型协议进行分析。

4. 下图展示了某一工业控制信息物理系统网络结构，目前各层内和各层之间没有对信道传输的数据进行保护，尝试调研、设计各层内和各层之间的数据加密/解密算法，并使用 python 进行实现（提示：考虑控制层的实时性问题，其层内和与其他层的通信可采取完整性校验算法；python 的加密算法库可以直接调用）



5. 分析 Nmap、p0f、xprobe2、PLCscan（也可以是其他专用工具）等扫描工具对信息物理系统的识别方式，尝试扫描公网上的一些设备，给出设备信息。

（工具可自行选择**两种及以上**；设备 IP 可利用 Shodan 搜索引擎，请自行检索 Shodan 使用方法；扫描工具建议在 VMware 虚拟机中安装 Kali linux 系统，该系统有上百种已安装好的网络安全分析工具，包括题目中涉及到的扫描工具）

Shodan：https://www.shodan.io/

ZoomEye：https://www.zoomeye.org/

Nmap：https://github.com/nm0ap/nmap

p0f: https://github.com/p0f/p0f

PLCscan: https://github.com/yanlinlin82/plcscan

6. 选择一款针对信息物理系统进行攻击的开源项目，分析程序的攻击流程、攻击效果（例如 Stuxnet，TRITON 等，可在 github 上寻找其他项目）

   STUXNET：参考文献《W32. stuxnet dossier》

   TRITON：https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN

7. 分析 conpot、snap7 等蜜罐对工业控制器的模拟方式，尝试在云服务器上部署此类常见蜜罐，进行一定时间（一周以上）的捕获，分析捕获结果。（蜜罐可自行选择两种及以上，分析蜜罐主要交互功能的实现方法，并对捕获结果进行分类）

   Conpot：https://github.com/mushorg/conpot

   https://download.csdn.net/blog/column/12580050/135676385

   HFish：https://hfish.net/#/

   Snap7：https://github.com/gijzelaerr/python-snap7

8. 分析 ISF、msf 等工具以及 ClearEnergy、Flame、Trisis 等攻击事件的攻击脚本，分析其攻击路径及架构，实施攻击前是否考虑 PLC 运行状态、连接状态、密码保护等情况，有能力的话可以尝试对攻击脚本添加设备状态扫描功能。

   需要一定的 python 或 C 代码的基础

   攻击事件脚本：

   ClearEnergy：https://github.com/0xICF/ClearEnergy

   Flame：https://github.com/loneicewolf/flame-sourcecode

   TRISIS：https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN

   攻击工具（分析攻击施耐德、西门子 PLC 的 payload 即可）：

   ISF： https://github.com/dark-lbp/isf

   metasploit-framework：https://github.com/rapid7/metasploit-framework

9. 对现有的工业物联网（如 MQTT）或工控协议（如 Modbus）进行后量子安全增强，一种参考的方式是借助 TLS 部署量子安全的密钥交换机制，可能涉及的工具包括 OpenSSL、liboqs、OQS-Provider 等，也可使用其他方式。

   NIST 后量子安全标准：https://research.ibm.com/blog/nist-pqc-standards#-fn-1

附加类（CTF）

1. 逆向附件中的 exe 得到 flag，需要用到的知识：UPX 壳、TEA、逆向，可参考的学习网站：https://ctf-wiki.org/。（exe 见附件）

   静态分析工具 IDA Pro

   动态调试工具 x32dbg、ollydbg

   https://www.kanxue.com/

   https://www.52pojie.cn/portal.php?from=groupmessage&mobile=no