ISC Security Tools

hades / 2017-06-23 13:48:46 / 浏览数 10725 安全工具 工具 顶(0) 踩(0)

参考

https://github.com/ITI/ICS-Security-Tools

https://github.com/w3h/icsmaster

工控资产发现

- 被动工控资产发现-公网
- 主动工控资产发现

漏洞利用

- Siemens Simatic S7 Metasploit Modules

工控设备默认密码

- password

协议分析

- 协议fuzz方法及工具
- 协议测试包样例

工控入侵检测规则

- snortrules

漏洞库

- 工控漏洞库

目前抓取 http://ics.cnvd.org.cn

- 缓冲区溢出漏洞 197
- 拒绝服务漏洞 159
- 授权管理漏洞 111
- 信息泄露漏洞 75
- 身份认证漏洞 63
- 跨站脚本漏洞 62
- 代码执行漏洞 61
- 注入漏洞 55
- 目录遍历漏洞 48
- 文件权限漏洞 28
- 跨站请求伪造漏洞 21
- 访问控制漏洞 14
- 逻辑漏洞 11
- 会话管理漏洞 11
- 文件上传漏洞 7
- 命令执行漏洞 7
- 重定向漏洞 5
- 重放漏洞 3
- 搜索路径漏洞 3

其他工具

- 工具脑图

学习文档

- 工控安全评估标准+技术检测

感谢

- 灯塔实验室
- SCADA StrangeLove Research Team
- Digital Bond

Github：https://github.com/tanjiti/icstools

上一篇：getsploit - 命令行版本... 下一篇：【译】使用python检测和绕过w...
1. 0 条回复
   - 动动手指，沙发就是你的了！