Tips and trick from the ICS assessment and pen-testers

Intro – Søren Egede Knudsen

- Work experience
- 25+ Years in Network & Cybersikkerhed
- 11 Years with focus on SCADA cybersikkerhed
- 15+ Leadership and business managemnt

- Selected education and certification
- Master in Business Administration (MBA)
- GIAC-GRID
- CCIE
- Offensive Security & SANS trainings..

- Adminitrator of the OT security group on LinkedIN

- E-mail sek@egede.co – www.egede.co

Intro – Mikael Vingaard

- 15 years as "traditional" IT- Security consultant within pen-test, Blue-team, audit and BCP/preparedness.

- Last 6 years within Industrial infrastructure (primary energy + manufacturing)
- Build Deception technology (ICS Honeypots)

- GICSP, GRID, IACRB CSSA (Certified SCADA Security Architect) , CISSP ISO 27001 Lead Auditor, BeerISAC and much more..

- Member of ”I Am The Cavalry”

- Assisted with ”responsible disclosure” to vendors like; Huawei (router), Palo Alto (Firewall), MOXA, Honeywell, Ruggedcom and many others… (more in pipeline).

Agenda

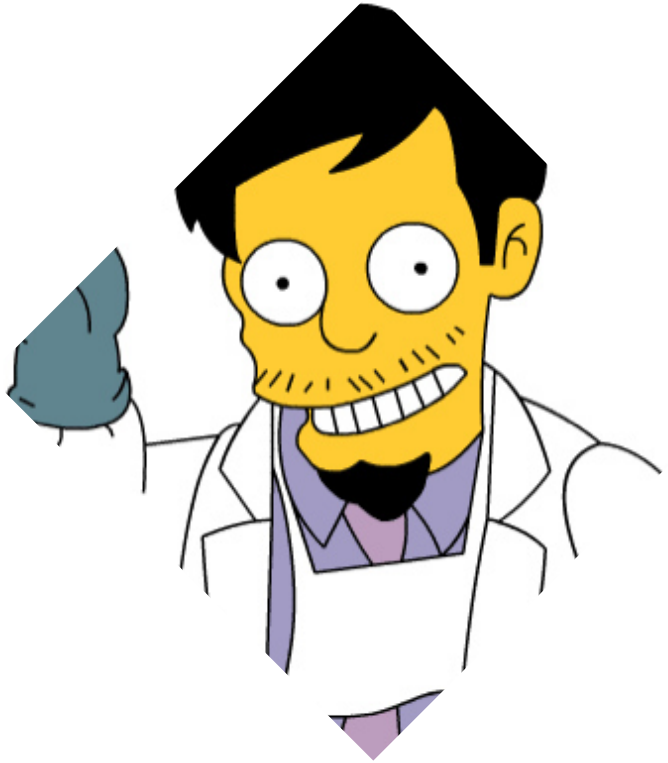
- Why Pen-testing the OT/ICS enviroment?
- IT vs OT pen-testers
- Experiances from the field
- What to ask and expect from the OT assessment & pen-test

Why Pen-testing the OT/ICS enviroment?

- Highly critical environments
- Increase of known vulnerabilities in the ICS environment
- Increasing attack surface
- Need for understanding the attack risk and possibilities

IT vs OT/ICS Pen-testers

- Specialists and understanding of environment
- Most time spent in a pen-test is research and understanding
  - “If I only had an hour to chop down a tree, I would spend the first 45 minutes sharpening my axe.” – **Abraham Lincoln**.
- If generalist are used higher risk of problems – need to understand the effect of what that is done - before



Traffic analysis

Every OT Pentest should always start with a passive network evaluation of the environment.

This phase will often provide a valuable insight to enable the testers to be more efficient.

-"Every device tells a story" - leverage the information provided & cross check with known Vulnerabilities. (Remember most firmware fixes "Reliability" rather than "Security")

- Have focus on the "reliability" angle.

- Your test scope would –often- no be to find "zero days", while that often happens :-)

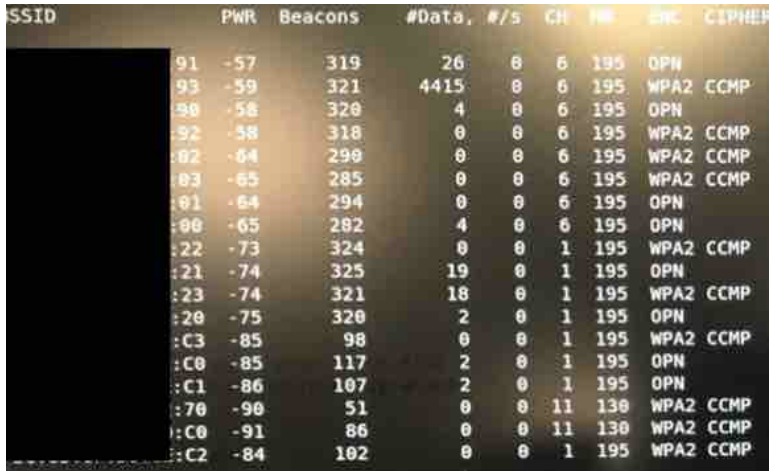
While looking for the "scope" part, one can get a lot extra "bonus" during this phase;

- Can catch various misconfigurations and unexpected traffic flow;
  - like Drop box connectivity from a sensible network segment.
  - unexpected cross-interconnected networks/routing … why has XX airgap'ed device access to the internet.
  - Equipment calling out to ghost equipment.

- **Finally – the documentation will be validated against the "real" life network**

Initial shell access

- Understand the target attack surface
- WIFI in the ICS or…
- Applications services (http or other)
- Office / Administration network access
- Use or modify exploit to your need



- Always do the active part in the LAB!
- Do not use tools that you do not know what is doing!

http://thetargetsite/layout.php?addr=../../../../../etc/passwd

The toolbox

- Big shout-out to the SANS ICS 612 Beta2 team (Tim, Jeff and Jason)
- *"One need to earn the access into such master class" :-)*
- Ask the pen tester(s) on the 3 initials tests she/he would perform in test/production environment.
- ("aka. what is in the toolbox?")

Ospf attack

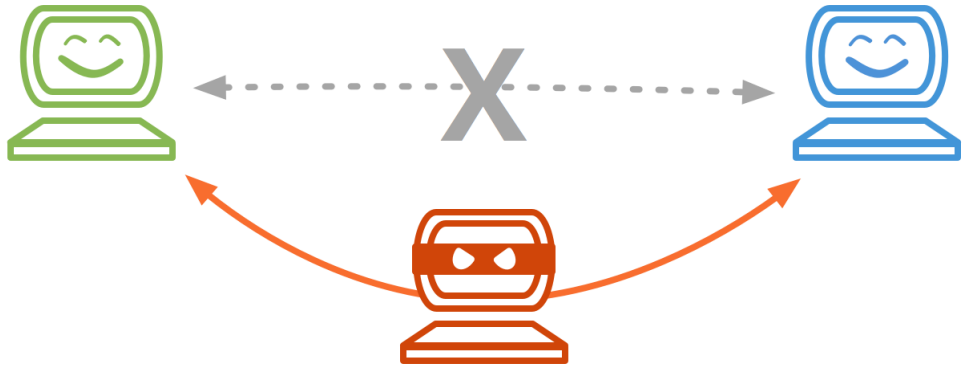
- Dynamic routing in the ICS
- Creating MiTM with OSPF
- Protect your network!

- Sample from the real life
  - Large organization
  - Gained wifi access
  - OSPF used in routers and firewall without md5 keys
  - Injecting OSPF routes to control traffic flow (MiTM)
  - Capturing password hashes / full control off traffic - ☺

```
R6#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           45  FULL/DR         00:00:39    192.168.1.1     FastEthernet0/0
2.2.2.2           1   2WAY/DROTHER    00:00:36    192.168.1.2     FastEthernet0/0
3.3.3.3           20  2WAY/DROTHER    00:00:30    192.168.1.3     FastEthernet0/0
4.4.4.4           100 2WAY/DROTHER    00:00:37    192.168.1.4     FastEthernet0/0
5.5.5.5           20  FULL/BDR        00:00:37    192.168.1.5     FastEthernet0/0
```

OSPF



- Not only OSPF many dynamic routing
- I bit of details ☺

- Inject routes with
  - Redistriute statics
  - Make you default gateway or other internal routes
- You have your MiTM

```
OSPF-100 ADJ   Fa0/0: DR/BDR election
OSPF-100 ADJ   Fa0/0: Elect BDR <IP>
OSPF-100 ADJ   Fa0/0: Elect DR <IP>
OSPF-100 ADJ   Fa0/0: Elect BDR 0.0.0.0
OSPF-100 ADJ   Fa0/0: Elect <IP>
OSPF-100 ADJ   Fa0/0: DR: <IP> (Id)   BDR: none
OSPF-100 ADJ   Fa0/0: No full nbrs to build Net LSA


OSPF-100 ADJ   Fa0/0: Rcv DBD from <IP> seq 0xA0770570 opt 0x52 flag 0x7 len 32  mtu 1500 s
OSPF-100 ADJ   Fa0/0: Nbr state is 2WAY
OSPF-100 ADJ   Fa0/0: end of Wait on interface
OSPF-100 ADJ   Fa0/0: DR/BDR election
OSPF-100 ADJ   Fa0/0: Elect BDR 255.255.255.255
OSPF-100 ADJ   Fa0/0: Elect DR <IP>
OSPF-100 ADJ   Fa0/0: Elect BDR 255.255.255.255
OSPF-100 ADJ   Fa0/0: Elect DR <IP>
OSPF-100 ADJ   Fa0/0: DR: <IP> (Id)   BDR: 255.255.255.255 (Id)
OSPF-100 ADJ   Fa0/0: Nbr <IP> Prepare dbase exchange
OSPF-100 ADJ   Fa0/0: Send DBD to <IP> seq 0x25E3 opt 0x52 flag 0x7 len 32
OSPF-100 ADJ   Fa0/1: end of Wait on interface
OSPF-100 ADJ   Fa0/1: DR/BDR election
OSPF-100 ADJ   Fa0/1: Elect BDR 255.255.255.255
OSPF-100 ADJ   Fa0/1: Elect DR 255.255.255.255
OSPF-100 ADJ   Fa0/1: Elect BDR 0.0.0.0
OSPF-100 ADJ   Fa0/1: Elect DR 255.255.255.255
OSPF-100 ADJ   Fa0/1: DR: 255.255.255.255 (Id)   BDR: none
OSPF-100 ADJ   Fa0/0: Rcv DBD from <IP> seq 0x25E3 opt 0x52 flag 0x2 len 72  mtu 1500 state
OSPF-100 ADJ   Fa0/0: NBR Negotiation Done. We are the MASTER
```

What to ask and expect from the OT assessment & pen-test

Suggested points to be assessed/asked, before sign-off:

- Show me your ability to do passive assessment (!) in our environment? – if they say Nmap … close the conversation fast...
- Tell me the first 3 points/areas, you will test in our OT test/production and why?
- Please document your contribution back to the community – have you done e.g. "responsible disclosure" to industrial vendors ? (ask for references /CVE-number).

As client, one should expect the tester(s), can demonstrate knowledge on OT, and will present two –very- different approaches in production/testing environments.

Questions