SCADA Security & Hacking Workshop

Yaniv Miron aka Lament
Security Researcher

FORTCONSULT
Straight talk on IT security

IL Hack

HACKTIVITY
Kelet-Közép-Európa legnagyobb hackerkonferenciája
2011. szeptember 17-18.

/ About Me

- **Yaniv Miron aka Lament**
- **Security Researcher and Consultant**
- **Found security vulnerabilities in IBM, Oracle, Microsoft and Apache products as in other products**
- **CISO Certified from the Technion (Israel Institute of Technology)**
- **Certified Locksmith**

Agenda

- Best be in this workshop after the SCADA Dismal talk
- Intro to the workshop
- Security Policies in SCADA
- Firewall architecture in SCADA
- Pentest in SCADA
- IDS/IPS signatures
- Q & A

Security Policies

- Intro to the workshop
- Security Policies in SCADA
- Firewall architecture in SCADA
- Pentest in SCADA
- IDS/IPS signatures
- Q & A

Security Policies

- **Policies are boring…but what you can do? We need them.**
- **Strong authentication? Probably user and password…PKI would be pretty hard in here.**
- **Install the latest security patches…Yeah right! Like I want to take the risk of installing patches on my nuclear reactor OS.**
- **Limitation of Administration…Think about it, Only one administrator? What will you do when he is in LalaLand and the water pipes are going crazy?**

Security Policies

- **Monitoring…YES, you HAVE TO MONITOR SCADA systems! ALL of them, ALL the time, or else…**

- **Backup…PLEASE BACKUP, what will you do when the definitions of the pressure in the water pipes will return to a default mode???**

- **Control your users, as in automatic logoff, as in only one user per username, as in…**

Firewall Architecture

- Intro to the workshop
- Security Policies in SCADA
- Firewall architecture in SCADA
- Pentest in SCADA
- IDS/IPS signatures
- Q & A

Firewall Architecture

- **"Divide et impera" - Divide and Conquer/Rule! Yes…Rules are very important.**
- **SCADA Historian (DB)**
- **SCADA report system**
- **SCADA eng. Work station**
- **SCADA HMI for operator**
- **SCADA internet PC**

Firewall Architecture

- **Probably would look like that (in the real world – not in the best scenario):**

Internet

SCADA internet PC → Access to DMZ

DMZ

SCADA report system → Access from the internet

Internal

SCADA Historian (DB) → Access from DMZ

SCADA eng. Work station → Access to DMZ

SCADA HMI for operator → Access to DMZ

Pentest in SCADA

- Intro to the workshop
- Security Policies in SCADA
- Firewall architecture in SCADA
- Pentest in SCADA
- IDS/IPS signatures
- Q & A

Pentest in SCADA

- **You should have been in the last talk about SCADA Dismal…Come on…So of course the SCADA DISMAL tool!**
- **MetaSploit**
- **Exploit-DB**
- **BoF**
- **Design Flaws**
- **Weak usernames and passwords**
- **Sniff! Sniff!**

IDS / IPS signatures

- Intro to the workshop
- Security Policies in SCADA
- Firewall architecture in SCADA
- Pentest in SCADA
- IDS/IPS signatures
- Q & A

IDS / IPS signatures

- **Don’t be lazy and don’t trust the IDS/IPS providers that much… if you see something that doesn’t look right sign it.**

- **If you can’t sign it because it’s a Off-The-Shelf IDS/IPS either you should**
  - **Immediately contact the provider so they will add a sign.**
  - **OR/AND you should add a snort based home build IDS/IPS just for your signatures.**

- **If your not an expert in that DO NOT USE Heuristic signatures, it will f*ck up a lot of stuff.**

To wrap it all up

This was only a short introduction to SCADA Security & Hacking training.

SCADA is not secure.

E [0] F

Thank you!

Questions?

>>

Yaniv Miron aka Lament
lament@ilhack.org
http://www.ilhack.org/lament

In god we trust, all others we monitor.