Scoville Hacking & Security

Yaniv Miron aka Lament
Senior Security Consultant @ FortConsult

Requested by: Shlomi Dolev, Professor @ BGU

FORTCONSULT
Straight talk on IT security

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev
COMPUTER SCIENCE
Ben Gurion University of the Negev

/ About Me

- Yaniv Miron aka Lament
- Security Researcher and Consultant
- Working as a Senior Security Consultant @ FortConsult
- Found security vulnerabilities in IBM, Oracle, Microsoft and Apache products as in other products
- Hacking & Security certifications
- Certified Locksmith

/ About FortConsult

- IT security company established in 2002 by Ulf Munkedal
- We provide unbiased straight talk on IT security

- We are specialized in
  - Vulnerability assessments and penetration tests
  - PCI compliance audits, consultancy
  - Ad hoc special consultancy

- 26 employees with more than 25 international IT security certifications
- HQ in Denmark, delivery centers in Denmark and Lithuania, and branch office in Russia
- Mix of projects: 60% International, 40% in Denmark

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

FORTCONSULT
Straight talk on IT security

Scoville

"The Scoville scale is a measurement of the spicy heat (or piquance) of a chili pepper."

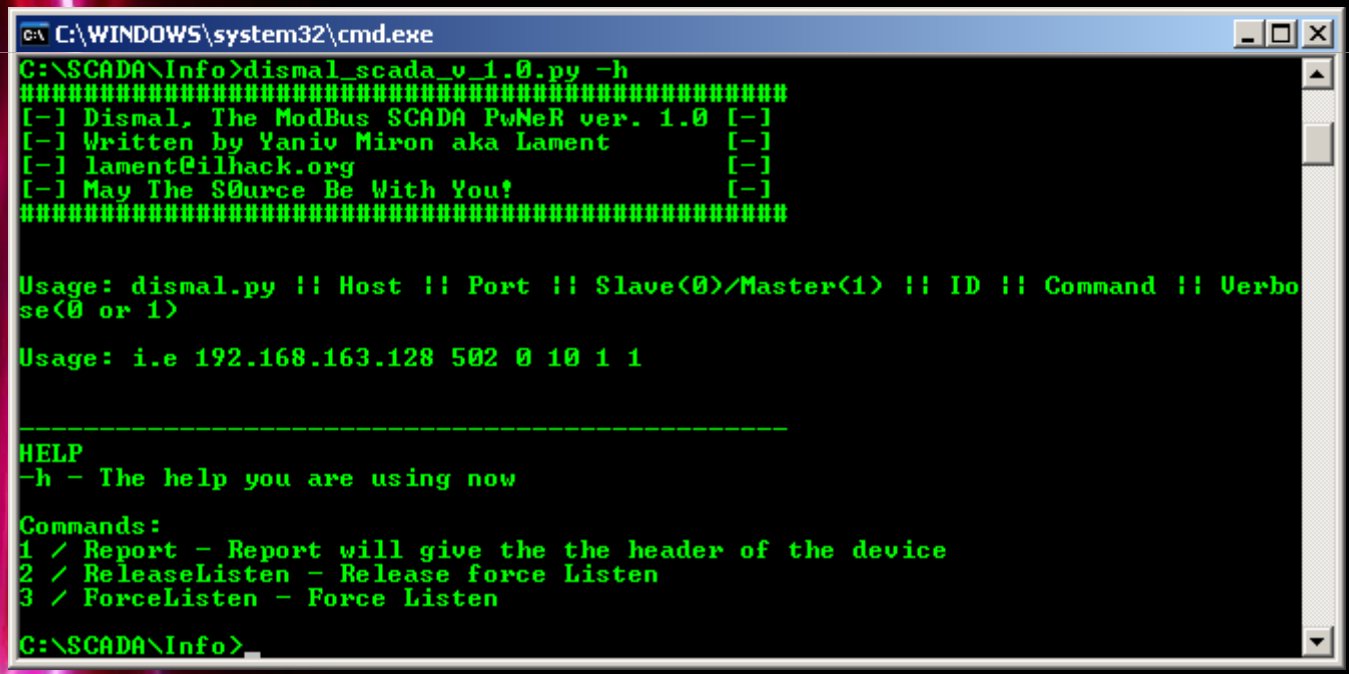
- Wikipedia (PwNz)

Agenda

- SCADA Hacking
- TV Cables Hacking (?)
- Hardware Hacking
- Top 4 ways to get infected from the net
- Cyber[x]
- 5 topic, ~10 minutes each

SCADA Hacking

- **Lets skip the talks and move to the demo…**
- **The Dismal Tool – PwnZ Modbus**



TV Cables Hacking (?)

- It’s a new project, might work, might not…
- Cable on my router?
- VoD on my router? Are you joking ?
- Is it encrypted ?

Hardware Hacking

- No, it's not moding a CPU to perform better, it's actual hacking (Cracking?).
- So what would you do with a fully encrypted laptop ? Fully hardened one ?

Top 4 net infection

- Four Horsemen of the Apocalypse
- Web Browsers
- Java
- Flash
- PDF
- USB (not)

Cyber [x]

- It's so cool to talk about cyber [something]
- Saudi Arabia hacking ?
- Credit card over the net ?
- The fingerprint database in Israel [BAD!]

E [0] F

Thank you!

Questions?

>>

Yaniv Miron aka Lament @ FortConsult
ymt@fortconsult.net
lament@ilhack.org (Private)

In god we trust, all others we monitor.

FORTCONSULT
Straight talk on IT security