INDUSTRIAL DEFENDER®

SCADA / DCS Penetration Testing

You don't know how strong your defenses are until you test them…

SANS SCADA SUMMIT, Jan 2008

Jonathan Pollet, CISSP, CAP, PCIP

INDUSTRIAL DEFENDER® Short Video Clip on SCADA as a Target

Outline for Brief Discussion

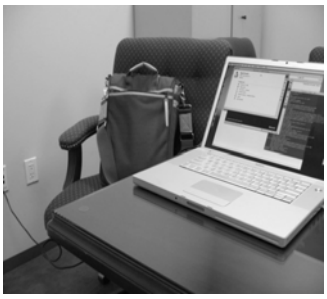
- Attack Vectors for SCADA / DCS Systems
  - Gaining Access
    - Remote
      - Internet > Corporate > SCADA / DCS
      - Dial-up Lines, Modems, VNC, etc..
        PCAnywhere = Hack.Me.Anywhere
    - Onsite
      - Physical Access to any Corporate PC / network port
      - Wireless Access
        *(WEP = **W**elcome **E**veryone to the **P**arty)*
      - Physical Access to any SCADA PC / network port
    - Lessons Learned from Red Team Exercises
  - What can you do once you're in?

Gaining Access to SCADA / DCS > Remote

- Remote Access - 50% Success Rate
  - Internet > Corporate > SCADA / DCS
    - Internet Border Usually Fairly Tight - Access made through Internet connect to Corporate IT about 50% of the time undetected
    - Corporate to SCADA border - Very Insecure
      - Data Historians, OPC Servers, Engineering Workstations, and other data connectors are often a bridge to SCADA
      - Firewall rules for Engineering access or Vendors almost always WIDE OPEN
      - Active X components used on a majority of SCADA and Web HMI systems - highly insecure and vulnerable to exploits available today
      - Default accounts and passwords sill a HUGE problem - just knowing the vendor of the system is often all we need to own the network
  - Dial-up Lines, Modems, VNC, etc..
    - Dial-up access still a very viable access - no IDS and often no passwords
    - Passwords are often easy to guess

INDUSTRIAL DEFENDER® Gaining Access to SCADA / DCS > Onsite

- Onsite Physical Access - 100% Success Rate
  - Physical Access to any Corporate PC / network port
    - Open RJ45 ports in publicly available areas make great targets
    - Printers are also excellent places for planting WiFi devices for remote access
    - Walk into any spare office and look like you belong there

INDUSTRIAL DEFENDER® Wireless and Physical Access

- Wireless Access (WEP = **W**elcome **E**veryone to the **P**arty)
  - WEP is practically useless as a security method
  - Wireless can be cracked from miles away, let alone from a nearby parking garage
- Physical Access to any SCADA PC / network port
  - Physical trumps Cyber every time
  - Doing your homework pays off - simply walk into the plant and find a place to plug in
  - Don't let this guy in your plant >

Lessons Learned from Red Team Exercises

- Remote Access
  - Internet-to-Corporate Border Fairly Secure
  - Corporate-to-SCADA Border Insecure
  - Firewall rules usually weak
    - Vendor connections are usually ANY-TO-ANY with all ports open
    - Some work put into INBOUND rules, but OUTBOUND rules usually wide open
    - Do some homework to lock down Corporate IT to SCADA connections
  - Very little of no use of IDS in SCADA perimeter or on the inside of SCADA environments
- Onsite Physical Access
  - Physical Trumps Cyber Every time
  - Social Engineering works 100% of the time
  - Recon, research, and doing your homework pays off
  - Look like them, talk like them, and have a good story backed up with work orders, contractor badges, and you're in
  - >> NEED MORE SECURITY AWARENESS FOR EMPLOYEES!!!

Thanks

- Credits
  - Video > YouTube
  - Content and Photos > Industrial Defender Security Services Team
- Web Site
  - www.industrialdefender.com
- Contact Information
  - Jonathan Pollet, CAP, CISSP, PCIP
  - jpollet@industrialdefender.com
  - jonathan.pollet@gmail.com
  - Office: +1.877.302.DATA EXT 211
  - Cell: +1.281.748.6401