Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Together. Free your energies

SANS Amsterdam, Netherlands – September 8, 2008

Penetration Testing of control systems, is it a good idea?

Roelof Klein

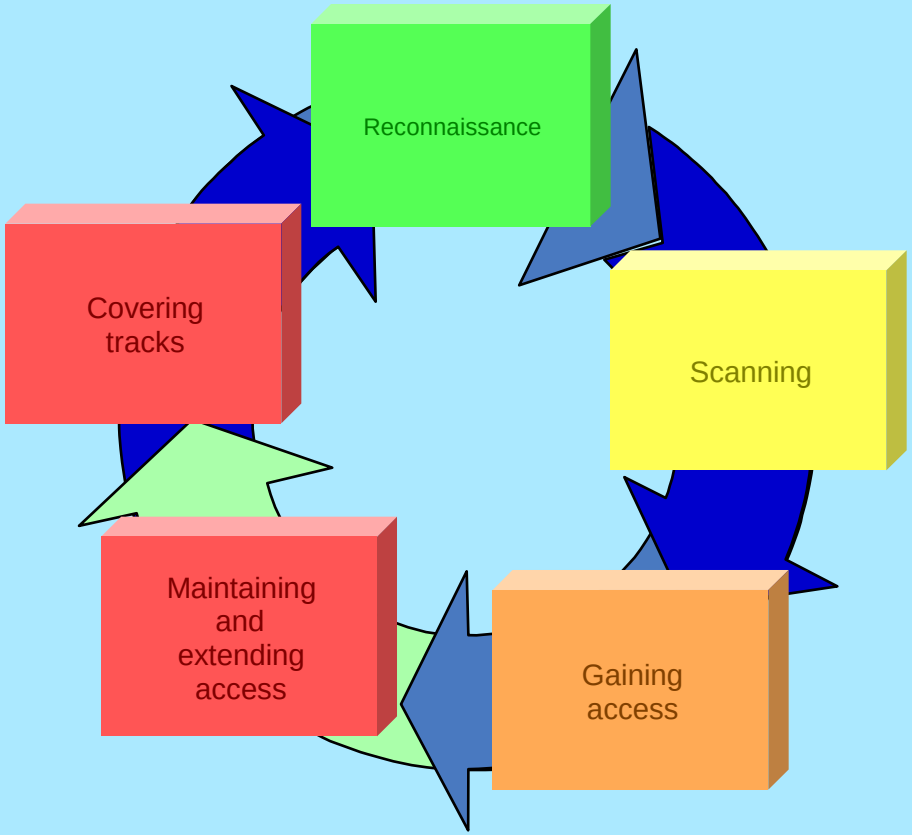
Managing Consultant

Roelof.Klein@capgemini.com
http://www.linkedin.com/in/roelofklein

Definition of Penetration Testing

A **penetration test** is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities.

(Wikipedia)



Reasons to perform a penetration test.

When initiated from IT

- I don't trust the control and automation community.
- I think that my (office IT) is sufficiently protected.
- I don't trust the boundaries of my network.

When initiated from Control and Automation (C&A)

- I want funding to improve / enhance my control system.
- The managers don't believe me.
- The managers don't understand me.
- I don't trust the IT people.
- I don't trust my vendor.

When initiated from an Audit team

- All systems must be compliant (SOX, OLF, BSI …..).

When initiated from the management

- I heard the news, cyber attacks are happening to other companies.

Possible negative impact of a penetration test.

Business

- Integration projects can be delayed for years.
- Missing opportunities (outsourcing, B2B connections).

Technical

- Back to the stone age, delays in continuous improvement.
- Securing the core business (stopping with remote access).

People

- Decrease in trust between staff (IT and C&A).
- Less interesting jobs (no room for remote engineering, innovation).
- More travel, more HSE risks.
- Emphasized fear factor.
- Tunnel vision on security.

Why you will find holes during penetration testing.

Products

- Not all the Microsoft patches can be installed.
- Add-on products like Tofino, Industrial defender, mGuard do not provide you defense-in-depth security.
- It is often not possible to upgrade a system without reboots, shutdowns or losing functionality (single OPC server, single historian, applications installed on one server ….).

Design

- The current design of Control and Automation systems are at least 3-years-old and are frozen during project execution.
- Currently none of DCS vendors sell a system capable of withstanding pen testing.
- Secure remote access is always a design challenge.

People

- In the past there was not a SCADA security course.
- The people who implement these systems don't have a security focus during the design, reviews and implementation.
- Ownership of equipment is always an issue.
- Technical people give too much information on resumes.
- C&A staff will always help you with technical issues.

What are you testing?

	Implementation of mitigation actions (Defence in Depth)								
Attack method	Layered architectural design (SP-99)	Updated Asset Management (CMDB) + network drawings	Regular security Patches installed	Anti virus software installed and maintained	Hardened system	Firewall between office and production	DMZ zone in firewall implemented (remote access & file transfer)	Firewalls between production units	Authorisation and Authentication in production implemented
Access to / from Office Networks	Known connections and risks mitigated Office security usage	IP addresses of equipment known & owners (users) equipment known	Less documented holes available to attack	Less risks for wide spread viruses	Smaller attack vector	Less ports to attack	No ports to attack. Protocol translation	Less large scale attacks, more time needed to attack	Only known users have access
Access to/ from Internet	Not needed access via office	Routable IP addresses known + connections to the Internet	Less documented holes available	Less risks for botnet attacks	Less chance for a day 0 attack	Access via Office, double layer	Access via office	Less risks to find weak spots, less devices visible	Less changes for password guessing
Modem connections	Not needed access via office	Modems + owners of equipment known	Less holes available	Less risks to install unwanted software	More protection in case of a modem	Possibilities to monitor attacks from production	More protection / separation office and production	Less possibilities for hopping to other units	Less risk for password guessing
USB / CD / DVD usage	Not needed, controlled distribution of updates, reports	USB connections known	Latest security patches implemented	Less risks, by infected USB sticks	Less usage / need to use USB sticks for software updates	When NOT good designed , risks can increase	Possibility for secure file transfer	Less risks for large scale virus outbreaks	No automatic installation of software
Disgruntled employees	Less possibilities, no single responsibilities, no access to not required areas.	When NOT properly managed this can be a risk	Less holes available	Less risk to install unwanted software	Less obscure tooling	Possibility to block users in the office	Multiple administrators involved & central managed.	Limiting damage	Disable of rights when leaving the company.

What might be the impact of a pen test at this moment?

Operators

- Operators could lose the confidence in their system, resulting in less effective operators.

DCS system administrators

- Administrators have systems where outages for updates are very rare, they will get frustrated to hear that they are vulnerable.

Managers

- Freezing of innovation, back to old proven methods (disconnecting systems, procedures on paper).

IT Staff

- They could get the impression that they can do it much better, but they don't always understand the business.

What should you do as Control & Automation engineer?

Contacts with Vendors / suppliers / integrators

- Demand from your SCADA / DCS / PLC supplier a secure system.
- Create a long detailed list (RFQ) how security should be implemented including governance.
- Request independent test reports about security from your supplier including blackbox, whitebox testing.
- Check if your vendor can provide support to continuously enhance the security of the system without downtime.

IT Staff

- Ask IT to help you to secure the system (you can not do it alone)
- Realize that Control and Automation makes use of standard equipment, but they use it in another way.
- C & A is a separate discipline, don't think that IT can implement security with proven IT methods.

Is penetration testing of control systems a good idea or maybe not?

Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

Together. Free your energies

www.capgemini.com