

Security assessment of critical infrastructure

Rikard Bodforss, Founding partner Bodforss Consulting AB

Who am I?

...I wasn't always an IT-manager...



Listen to Säkerhetspodcasten!



Securing human rights



Promised deliverables

- Preamble
- Passive test methods
- Active test methods
- Choosing method and approach
- Summary

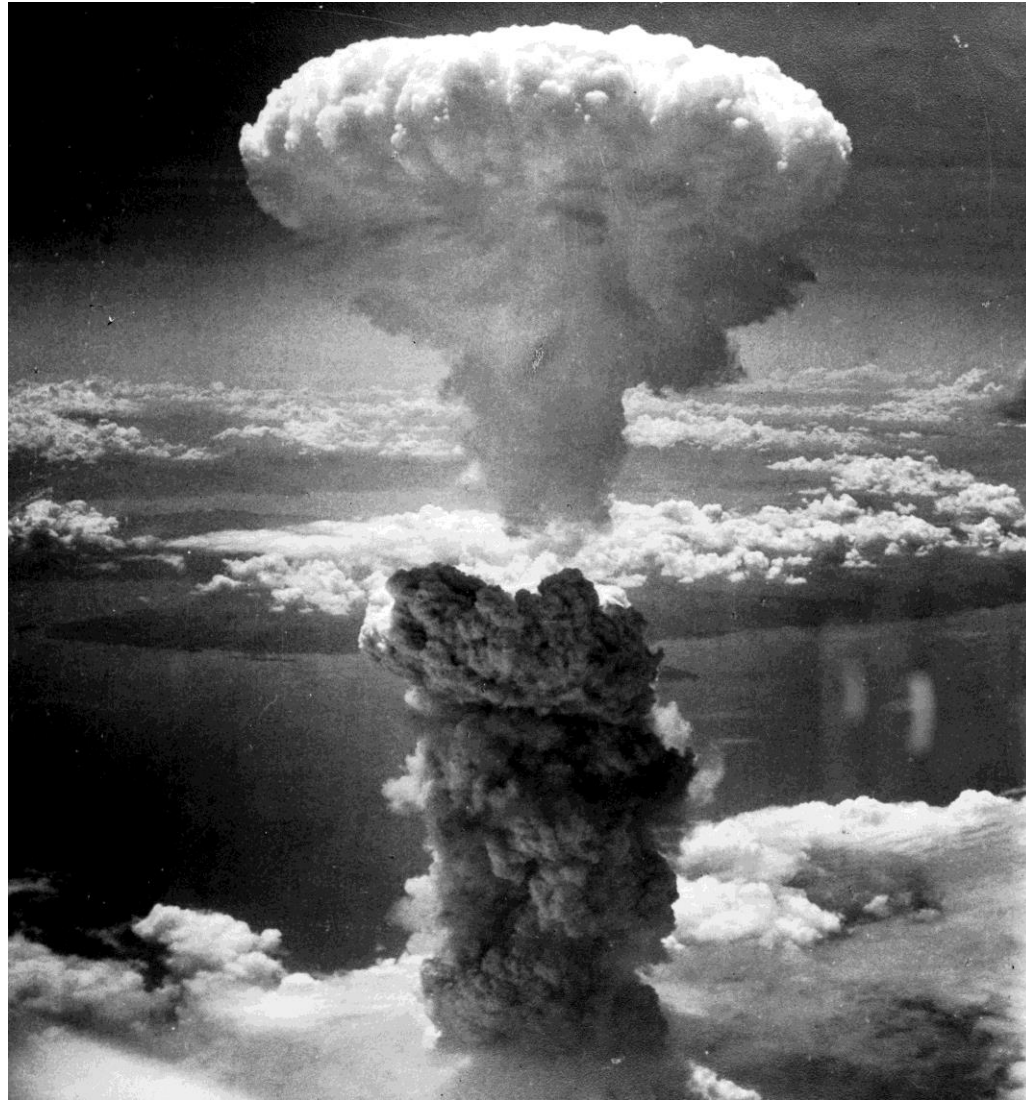
Preamble

Why do we test security?



What could possibly go wrong?





A brief summary of the state of academic research on the subject...

Activity	Usual Actions for IT	Preferred Actions for SCADA
Identification of hosts, nodes, and networks	Ping Sweep (e.g. nmap)	<ol style="list-style-type: none">1. Examine CAM tables on switches.2. Examine router config files or route tables.3. Physical verification (chasing wires).4. Passive listening or IDS (e.g. snort) on network.
Identification of services	Port Scan (e.g. nmap)	<ol style="list-style-type: none">1. Local port verification (e.g. netstat).2. Port scan of a duplicate, development, or test system.
Identification of vulnerabilities within a service	Vulnerability Scan (e.g. nessus, ISS, etc...)	<ol style="list-style-type: none">1. Local banner grabbing with version lookup in CVE.2. Scan of duplicate, development, or test system.

© 2005 Sandia National Laboratories, Duggan et.al.

Passive methods

Pen-test?



The map v/s the real world



Identify the weak links



Identify attack vectors

The screenshot displays the Threat Modeling Tool 2016 interface. The main diagram area shows a threat model with several components and attack vectors:

- Spoofer** (External Entity) is connected to the **Web Server** via **HTTP**.
- Human User** is connected to the **Browser** via **HTTPS**.
- Web Server** is connected to **Browser** via **HTTPS**.
- Web Server** is connected to **SQL Database** and **Binary** components.
- Applications Running on a non-Microsoft OS** is connected to **Binary** components.

Trust boundaries are shown as dashed red boxes:

- CorpNet Trust Boundary** encloses the **Web Server** and **SQL Database**.
- Sandbox Trust Boundary Border** encloses the **Applications Running on a non-Microsoft OS** and **Binary** components.

Attack vectors are labeled in red text:

- Elevation of privilege** (near Web Server)
- Spoofer** (near Spoofer)
- Repudiation** (near Human User)
- Denial of service** (near Browser)
- Tampering** (near Applications Running on a non-Microsoft OS)
- Information disclosure** (near Web Server)

The **Threat List** pane shows the following threats:

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Prio
0	Diagram 1		Generated	Not Started	Spoofer the B...	Spoofer	Browser may b...		HTTPS	Hig
1	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		HTTPS	Hig
2	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server ma...		HTTPS	Hig

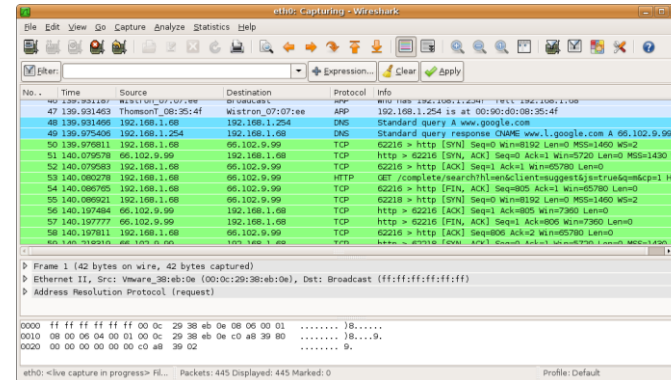
40 Threats Displayed, 40 Total

Threat Properties pane shows:

- ID: 0
- Diagram: Diagram 1
- Status: Not Started
- Last Modified: Generated
- Title: Spoofer the Browser External Entity
- Notes: no entries

More passive methods

- Log analysis
- Wireshark, Sniffer, etc.
- Monitor ports
- Passive wireless tools
- Config file analysis
- System charts
- Process inventory
- Protocol analyzers for I2C, RS232, RS485, etc.
- Etc....

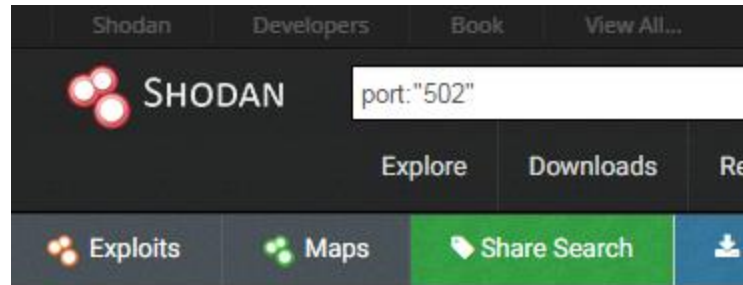


Drawbacks with passive methods

- Won't find everything
- False sense of security
- Demands skills, experience and competence
- Time consuming

Active test methods

Target analysis



TOP COUNTRIES



United States	2,563
France	834
Spain	621
Sweden	575
Poland	570


Total results: 11,210

128.125.31.1

fit-ph-508.usc.edu

University of Southern

Added on 2016-05-18:

 United States, Li

[Details](#)

Unit ID: 0

-- Slave ID D

b2c343232342d

Unit ID: 255

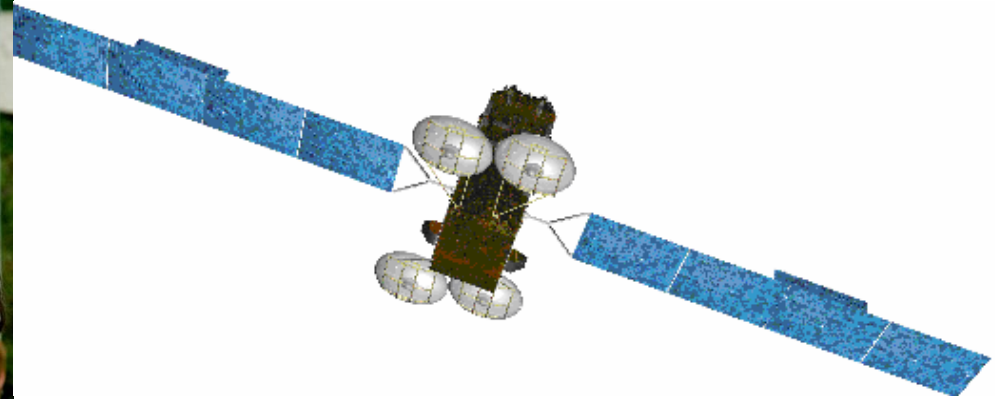
-- Slave ID D

b2c3432...

Test systems



FAT/SAT



Virtualization



Active methods

- Test systems (PHYSICALLY separated)
- Virtualization in lab environment (PHYSICALLY separated)
- FAT tests at supplier
- SAT tests on pre-production systems
- Shodan.io on your own networks
- Hack someone else (Just KIDDING!!!!!!)

Problems with active methods

- Lab is always a lab
- Real world and map don't match
- Oops... I thought those systems were running on separate environments...

Choosing methods

It all comes down to risk appetite

- Your mileage may vary...
- There are many ways to skin a cat....
- "It depends..."

Who should perform the tests?

- Internal or external
- If external, check for reference assignments
- Security clearance for sensitive infrastructure?
- Competence

Summary

And some final thoughts

Trust, but verify

**Доверяй
но проверяй**

Nobody is an expert on everything

- Share intel with colleagues in the business
- Hire help if you don't have all the pieces in the puzzle
- Become friends with the automation engineers
- Create teams and networks
- Cooperate with the suppliers
- Constant improvements (PDCA)
- Work strategically and proactively with risk management

Network and cooperate

- Learn from colleagues and peers in the business
- Form expert teams with specialists from both the business side and from the suppliers
- Attend conferences and network meetings
- Share knowledge and data

Further reading (and listening)

- http://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf
- <https://scadahacker.com/library/>
- <https://www.msb.se/scada>
- <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- <https://ics-cert.us-cert.gov/Standards-and-References>
- <https://www.microsoft.com/en-us/sdl/>
- <http://www.rics.se/>
- <http://www.sakerhetspodcasten.se/>

Thank you for listening!

Rikard Bodforss

Twitter: @rbodforss

Web: www.bodforss.se

www.sakerhetspodcasten.se

Email: rikard.bodforss@bodforss.se

Tel: +46-70 312 33 11

