The life of a security professional

Patrik Sternudd 2009

Agenda

Before break

- Introduction.
- What security is all about (my view)
- What I do, what others in the field do
- Common mistakes I see again and again (and again).

After break

- Case study – how to fix a really lousy infrastructure
- Open discussion and questions.

SANS/GIAC

The SANS (*SysAdmin, Audit, Network, Security*) Institute offers security training. They also are responsible for:

- ISC – Internet Storm Center (http://isc.sans.org)
- SCORE – Checklist development in cooperation with CIS
- ...and a lot of other initiatives. See http://www.sans.org for more information.

GIAC (*Global Information Assurance Certification*) is a certification organisation (accredited by ANSI). More information at http://www.giac.org

About me – *short intro*

- 3 GIAC Gold Certs
  - GCIA
  - GCFW
  - GSNA
- Authorized Grader for GCIA during 2004

- Working in IT since 1998
- Consultant since 1999
- Focus on
  - Information Security
  - Unix/Linux
  - Server consolidation
  - Project planning

Too pessimistic?

- You may get the impression that it is pretty awful to work in information security. Remember, I am talking about the *problems* here.

- There are a lot of advantages, too!
  - It's really exciting
  - Cool technology
  - Lots of challenges
  - You get to see (and work with) the whole picture
  - If you like secrets, it is the place for you!

Section 2

The Security Field

The goal of security

Why change a winning concept? CIA covers it all!

- *Good security ensures that the correct information is available at the right time, to the right persons.*

However...

- *Security not is a goal in itself, but rather an integrated part in every business aspect. Thus, it should support and simplify common operations, not hinder it.*

OK, we want/need security. How do we get it?

When I was young and naive, I wanted to

Secure Everything.

Well, security is nice, but...

- What if it's cheaper to recover from an incident that to ensure that it never happens?
- Protection is great, but there are other considerations too. Particularly, we need to detect and react to incidents.

Lots of disciplines!

- Security Audit
- Penetration Testing
- Policy & Organisation
- Cryptography
- System & Application Security
- Network Security
- Intrusion Detection
- Disaster Recovery
- Forensics

- It is possible to get very specialised in each of the given areas. Time is a limitation, though!

What colour is your hat?

- Black hats and White hats use the same tools.
- We also use the same techniques and do the same kind of attacks when we test a system.

There is *one* difference: **Permission**

- Get it in *writing*!
- Especially if you do penetration testing!
- If you do not, you might go to jail even through your intentions are good
- If your intentions are bad, you better keep away from my systems! :-)

My own focus

- Network security
  - Firewalls and their rulebases
  - Network design
  - NIDS
  - Traffic analysis

- ”System architecture” - the whole picture.
  - What about auxiliary systems such as backups?
  - Do you use your production systems for test?
  - Defense in Depth is critical.

Traffic analysis - example

Is this packet something we want to allow?

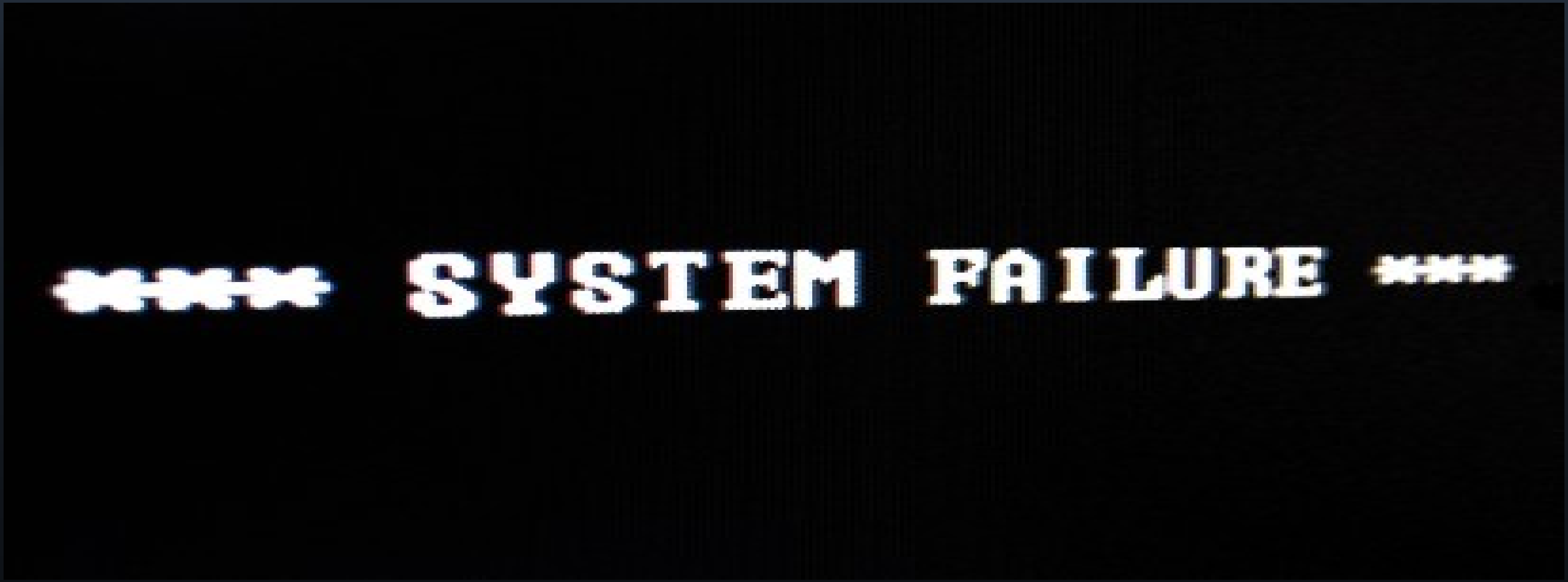
```
$ tcpdump -r 2003.12.15.7 -X -s 1514 -n -v "tcp and ip[0] & 0x0f > 5"

21:09:27.593273 IP (tos 0x0, ttl  64, id 31113, offset 0, flags [none],
length: 44, 10.10.10.141.35512 > 172.20.11.2.22: S  1749503129:1749503129(0)

      0x0000:  4600 002c 7989 0000 4006 ad92 0a0a 0a8d  F..,y...@.......
      0x0010:  ac14 0b02 8303 0400 8ab8 0016 6847 4c99  ............hGL.
      0x0020:  0000 0000 5002 0200 a286 0000 0000       ....P.........
```

- How do you know what is normal on YOUR network?

Section 3



***** SYSTEM FAILURE ****

Common problems and mistakes

Disclaimer

All similarities to any organisations and their networks are purely accidental.

However, many companies have similar set-ups (and problems), so even if you happen to recognise some parts, it does not mean I have been there.

After all, the ways you can design a network is rather limited.

#1: Lack of management support

- Everyone wants security, but no one wants to pay for it.
  - Until an incident occur. Then throw some money for quick fixes. Hire a consultant, install a firewall, etc.
  - The symptoms are fixed, but the problems remain.
- No security strategies or policies
  - If there is a policy, either it's stowed away and forgotten, or it cannot be used because the goals are unattainable.
- CISO/CSO reporting to CIO
  - Should be on the same level and report directly to CEO

#2 Unclear view of what security is

- ”We have a firewall, so we are 100% protected!”
  - In the same way a castle with moat and towers, but no guards is protected...
  - How do you know you are under attack if you are not watching?
  - How do you respond to the attack if you aren't aware of it?

- Security is not a product, it is a *process!*
  - Protect, Detect, React. Evaluate. Repeat.

#3 Insufficient security training

- I have lost count of how many times I have seen people without security training handling security devices.
  - Consider the firewall. Everyone needs one, and it will usually be managed by the network or system staff. However, both typically see security as something optional that steal time from their day to day operations.
- How is management supposed to be able to approve a change request for a firewall rule if they doesn't know what TCP is?
- End users need training too! Why bother penetrating multiple firewalls, if you can get an user to run a trojan for you?

#4 Security as an afterthought

It is uncommon that security requirements are found in specifications or product evaluation criteria.

- But security is very hard to add afterwards
- Even if you can, it will be much more expensive than if it had been added from start
- It can also affect the usability of the product

In a perfect world, developers would write secure products without being required to...Big chance for that.

Conclusion

Did you notice the pattern? My top problems doesn't have to do with technology at all, but rather the organisation:

> *”Technology is easy. The organisation is the hard bit.”*

- Unfortunately, the organisation is usually very difficult to change. You need a lot of time and patience for that. And a presentation tool such as Impress/Keynote/PowerPoint.

On the other hand, there are often a lot of technical security problems that you need to fix, too...and that quick!

Section 4

Case study: ”Just secure it, please”

Background

- MyRobot AB is a Swedish company specialising in robots for household purposes. They work with both hardware and software. There are 73 employees at the moment.
  - The company do a lot of research
  - All products are sold by resellers
  - They also cooperate with some competitors
- Recently, they suffered a virus/worm outbreak, which caused a lot of costs, both to clean it up and in lost work. This put some focus on security.
  - Their CIO just hired us to improve network security.

Scope reduction

- If it was an audit, I would be very interested in things like:
  - Patch level of systems
  - Patching routines
  - Change management
  - System hardening standards
  - How up to date documentation is

- However, due to political issues in the organisation, our mandate is restricted to the network design
  - Still, change control and management of the firewall ruleset is critical for the network security

What do we need to know?

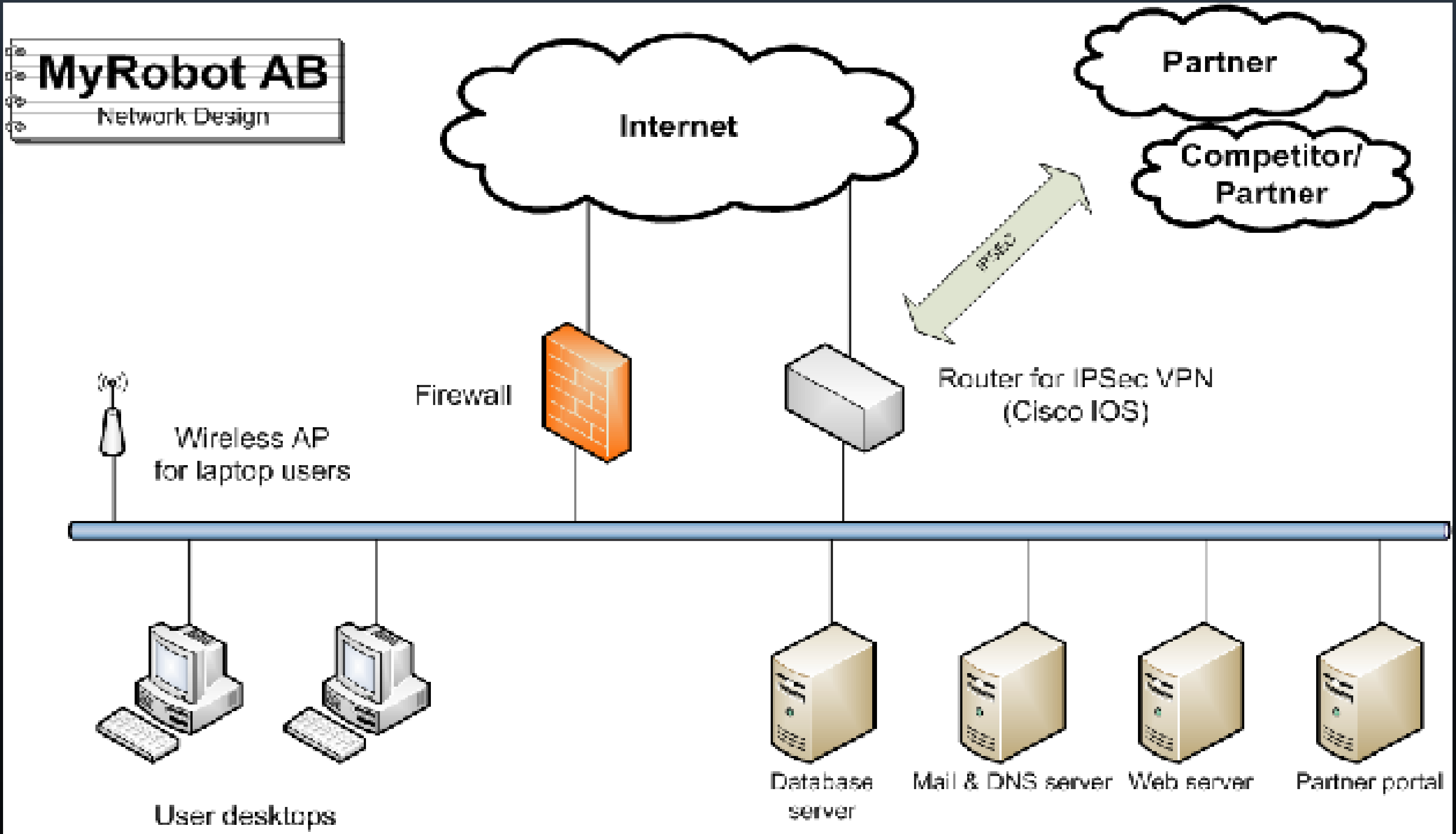
Suggestions?

Network diagrams

- Essential for getting the whole picture:
  - Important/sensitive systems
  - Entry points
  - Threats and obvious risks
  - Possibilities for improvement

- Sometimes, you have to create it yourself
  - If so, nmap is your friend. NB: get permission *first!*
- I like to have two diagrams: Today & The Bright Future

The network


MyRobot AB
Network Design
Internet
Partner
Competitor/ Partner
IPSec
Firewall
Router for IPSec VPN (Cisco IOS)
Wireless AP for laptop users
User desktops
Database server
Mail & DNS server
Web server
Partner portal

Problems with the design

The main issue: *no* defense in depth. There is only one layer of security (the firewall). If that fails, we are wide open.

- That IPSec VPN is scary. Do we trust everything at the other side?
- User networks should be separated from servers
- Public servers (Web, DNS, SMTP) should be placed on a separate screened subnet at the firewall
- Servers should be placed on different networks depending on how sensitive the data is
- No internal proxy server for outgoing traffic
- The wireless...oh my...

Thank you for listening!

Questions?