Security Infrastructure Management

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

10th March 2006

Security Infrastructure Management

- Often network/system security infrastructure are built without management
- Management is often a critical part of the network security infrastructure
  - but often forgotten
  - or worse... over-designed
- Security Infrastructure Management is a requirement to correctly manage, monitor and maintain the devices
- Keep the management infrastructure simple and very secure...

Out-of-Band (OOBI)

- In the 1950, OOBI was used as a "control path" to control phone services in case of failure or for maintaining them
- The same approach was used in the early IT networks to control via "other path" devices (e.g. IBM mainframe and modem)
  - The famous period of remote maintenance over modem...
  - but also the famous period of "wardialing"
- Out-of-Band Infrastructure is now part of data centers (e.g. IPMI, KVM-IP,...)
- In-Band versus Out-of-Band management is somewhat converging (e.g. Serial-Over-IP,...)

Security and Network Management

- Practical Management : "local-only" versus remote management
  - Disabling remote management is often the best way to eliminate the risk..
  - but this is not always practical.
- Hardening remote management is important but you have to find a balance between practical and secure approaches

Management of Security Devices

- Who is doing the management/monitoring of the security devices ? employee or external companies ?
- From where the management/monitoring of the security devices will be done ?
- What are the risks associated to use and build a management network ?
- What will be the protocols used ? Serial only ? IPs ?

Good Practises

- When building an IP Out-of-Band network, clearly separate production and management network (e.g. no IP routing between the two)
- Monitoring is important but the monitoring of management network is *more* important
- Availability of the management network is critical
- Strong authentication is mandatory (e.g. default password) and ... keep trace of every action done (e.g. TACAC+, rancid)
- Packet filtering must be applied on each management port
- For In-Band, you must keep a clear separation of network and IP used

Network Management - OpenSSH / jail-chroot TP

- You'll need to provide on a single system, two SSH access, one for network management (full access for an admin only) but another one used for file transfert with multiple customers. You must ensure a clear separation between the two access and only give scp access to the customers.

Q and A

- Thanks for listening.
- http://www.csrrt.org.lu/
- adulau@foo.be