

# Network Forensics

Thorsten Dahm  
t.dahm@resolution.de

# What is this talk about?

- high level (theoretical) overview of network forensics
- part of my daily work
- get other parties interested in this part of security
- make some of you aware of the topic

# and what is it not about?

- random commercial products and their shortcomings
- configuration guidelines and configlets
- a full, deep introduction into this topic

# Network Forensics ...what does it mean?

Network Forensics is the analysis of events in your network in order to discover the source of incidents and find out how bad the incident is/was.

# How an attack works - the stupid guys

- scan & exploit - still works :-)
- scanning an /8 takes ~ 32 hours
- DoS
- Malware attached to Emails / Phishing
- Files transferred via chat programs
- Vulnerabilities in Browsers and many other software
- attack all OS platforms - nobody is safe!

Scan for botnets by yourself - most are not well secured - and have fun :-)

# How an attack works - the smart guys

- abusing social network accounts with weak passwords or security weaknesses to infect friends
- remote holes in social networks
- Vulnerabilities in Browsers and many other software
- inconspicuous software like printer driver
- "Insider"
- attacks on DNS/BGP/...
- IPv6 (test) networks
- security equipment with radio like cameras
- weak access control to buildings
- attack all OS platforms - nobody is safe!

# Preventative measures

- be reasonable!
- ongoing reminders of physical security & social engineering
- regular training & penetration tests
- hire smart engineers and let them do their job
- spread your valuable information
- Read Sherlock Holmes books :-)

"Make my network 100 % secure" is rubbish!

# Preventative measures

- don't allow any machine to your network which is not under your control
- all other machines needs to go to guests networks
- lock down network access as much as possible
- separate infrastructure for "dirty" and "good" networks (e. g. DNS servers)
- secure DSL lines and similar entry points into your network

# You can only find what you are looking for

- Since infinite resources cannot be allocated to countermeasures, the goal should be the mitigation of risk to an acceptable level
- Risk is the probability that a bad guy using a certain vulnerability to negatively impact your network
- Countermeasures have practicable limits
- Incidents will occur, limit the damage and the cost
- You may have an incident response plan, but never tested it against real-world incident scenarios

# Design Principles

- Capture complete & correct evidence
- Accessibility of evidence
  - Captured evidence must be stored for a specified period of time
- Security & privacy of evidence
  - Integrity of collected evidence must be preserved
  - Privacy of users must also be preserved
- Incremental deployment
  - Design should be such that it can be seamlessly integrated into existing network components
- Modular and scalable design

# Detecting the incident

- malware using http/https/Twitter -> no IRC bots anymore
- increasingly encrypted & obfuscated connections
- many data sources available (syslog, netflow, ...)
- are they monitored?
- ability to detect DNS manipulations?
- Netflow - only used for traffic statistics?
- Syslog combined with AAA/netflow/...?
- Honey Token - simple watermarks on files or databases (invalid credit card number in a database)
- User logging in at unusual times
- and many more ...

The purpose of your analysis will drive your workflow.

# Detecting the incident

- watch netflow data (think on NAT!)
- upload/download volume of every single host
- exclude know top talkers like VPN gateways
- watch for strange / unusual behavior
- watch DNS
- watch syslog / traps
- watch event logs on your hosts
- watch for unusual events like new MAC address for router
- deploy a sniffer infrastructure
- quarantine VLAN
- normalize & combine the information you have!
- a good analyst is better than every software

# Sniffer infrastructure?

- Use SPAN/RSPAN/...
- mind the hardware limitations from your switch vendor
- prepare to sniffer user vlans, entry & exit points of your network, sensitive vlans like database vlan
- passive wire taps
- sniffer need to sniff at wirespeed
- do not silently drop any packets!
- in the worst case, use loadbalancers

After the detection:

**NO PANIC!**

# After the attack is discovered

- investigate deeper, contain/limit the damage
- Teamwork!
- limit access to (pre-)prepared services (DNS-Servers, quarantine vlan, ...)
- look into different layers (IP vs. Application)
- secure court-proof evidence
- inform co-workers as much as necessary, as less as possible
- investigate why/where your security management failed
- document the incident!

# Data analysis / root cause analysis

- Understanding the structure and meaning of protocol headers
- Understanding what occurs at each stage of the data communication process
- Being able to “decapsulate” a packet and identify the relevant headers
- Knowing what behaviour is expected at each point in the data transfer
- Being able to recognise when this behaviour is unusual
- Being able to identify what header information might be inconsistent and could be causing this behaviour to occur

# The End

Thorsten Dahm  
t.dahm@resolution.de