# Host-based Intrusion Detection Systems (HIDS)

Pieter de Boer
Martin Pels
09/02/2005

# Contents

- HIDS-types
- Example break-in
- Protection using HIDS
- Evasion possibilities
- Evasion prevention
- Conclusion

Contents

- *Types*
- Break-in
- Protection
- Evasion
- Prevention
- Conclusion

# HIDS-types

- Filesystem monitoring
  - ➔ AIDE, Mtree
- Logfile analysis
  - ➔ Swatch, Sec
- Connection analysis
  - ➔ Scanlogd, PortSentry
- Kernel-based IDS (process monitoring etc.)
  - ➔ IDSpbr, LIDS

Contents

- Types
- *Break-in*
- Protection
- Evasion
- Prevention
- Conclusion

# Example break-in

1) Bug in forum: uploading & executing PHP-code
2) Downloading netcat through PHP-file
3) Binding netcat to a port --> Shell
4) Executing root-exploit in the shell
5) Install rootkit, etc.

Contents

- Types
- Break-in
- *Protection*
- Evasion
- Prevention
- Conclusion

# Protection using HIDS

- Logfile analysis
  - Detection of PHP-file upload and netcat execution
- File monitoring
  - Detection files (PHP-file & netcat binary) and installed rootkit
- Connection Analysis
  - Detection of unauthorized daemons
- Kernel-based IDS
  - Detection of root-exploit execution

Contents

- Types
- Break-in
- Protection
- *Evasion*
- Prevention
- Conclusion

# Evasion possibilities

- Logfile analysis
  - ➔ Encoding of requests
- File monitoring
  - ➔ Deletion of files after use, modify file monitor
- Connection Analysis
  - ➔ Set up netcat connection to the outside
- Kernel-based IDS
  - ➔ Use of undetectable exploits

Contents

- Types
- Break-in
- Protection
- Evasion
- *Prevention*
- Conclusion

# Evasion prevention

- Logfile analysis
  - ➔ Anomaly detection
- File monitoring
  - ➔ Realtime monitoring,
    Placing monitor on read-only media
- Connection Analysis
  - ➔ Detection of connections to the outside
- Kernel-based IDS
  - ➔ Anomaly detection

Contents

- Types
- Break-in
- Protection
- Evasion
- Prevention
- *Conclusion*

# Conclusion

- HIDSs are not perfect
- Despite this they can certainly be useful