<< back | track 5

BY ZEE EICHEL

RAHARDJA - TANGGERANG
5 - 6 MEI 2012

WWW.INDONESIANBACKTRACK.OR.ID

"The quieter you become, the more you are able to hear."

<< back | track 5

WHY METASPLOIT

- SIMPLE & EASY
- TAB SUPORTTING
- METERPRETER MULTI-TASKING
- AUXILARY PLUGIN

"The quieter you become, the more you are able to hear."

<< back | track 5

PAYLOAD

- INLINE(NON - STAGED)
- STAGED
- METERPRETER
- PASSIVEX

"The quieter you become, the more you are able to hear."

<< back | track 5

PAYLOAD

- NONX
- ORD
- IPV6
- REFLECTIVE INJECTION

"The quieter you become, the more you are able to hear."

<< back | track 5

BACKDOORING

- Shell reverse tcp
- Shell bind tcp
- METERPRETER

"The quieter you become, the more you are able to hear."

<< back | track 5

DATABASE SUPPORTING

(POSTGRESSQL - MYSQL)

- INFORMATION GATHERING
- DB_CONNECT
- DB_NMAP

"The quieter you become, the more you are able to hear."

<< back | track 5

MSFCONSOLE

- SEARCH EXPLOIT
- USING EXPLOIT
- SHOW OPTIONS
- PLAY IN BACKGROUND

"The quieter you become, the more you are able to hear."

METERPRETER

- SESSIONS & MULTISESSIONS
- UNIX COMMAND SUPPORT
- MIGRATING
- EXECUTING FILE

"The quieter you become, the more you are able to hear."

METERPRETER

- DOWNLOAD & UPLOAD
- GETUID
- GET SHELL
- KEYLOGGER
- SCREENGRAB & ESPIA

"The quieter you become, the more you are able to hear."

<< back | track 5

METERPRETER

PRIVILAGE ESCALATION

- GETUID
- IDLETIME
- HASHDUMP
- USE PRIV
- GET SYSTEM

"The quieter you become, the more you are able to hear."

CLEARING LOG

- IRB SHELL
- CLEARING LOG
- LOGGING ASSESMENT

"The quieter you become, the more you are able to hear."

<< back | track 5

REMOTE

- SENT BACKDORING
- EXECUTING STAGGER

"The quieter you become, the more you are able to hear."

MAINTAINING

- UPDATE
- THIRD PARTY
- ATTACKING COMBINATION

"The quieter you become, the more you are able to hear."

THE END

"The quieter you become, the more you are able to hear."