CSIRT Training Material
Technical Issues

Klaus Möller
DFN-CERT
May 2001
Agenda

/ Goals of this module
/ Decisions and reasons
/ Programme
/ Whats been left out
/ Next steps
Goals of the module

Make new members of incident handling teams familiar with:

- Technical concepts behind incidents
- Incident technical terminology
- Goals of intruder activity
- Weaknesses exploited
Decisions and reasons

/ 1 ½ hour is much too short
  1 Concentrate on most common forms of incidents
  1 This way, new members can become productive
  1 Leave more advanced attacks for later

/ Programme follows intrusion cycle
  o Scan → Breakin → Hiding → Abuse
  1 Show full chain
  1 „Canonical“ structure?
Decisions and reasons (cont.)

Prerequisite skills:

- Basic UNIX administration
  - OS Structure: Kernel, (shared) libraries, programmes
  - Shell and environment variables
- Basic TCP/IP administration
  - Familiarity with IP/OSI stack model
  - Network interface
  - IP address
Programme

- Total length ~60 - 70 minutes
- How intruders work (~ 5 min)
- Information gathering (~ 20 min)
- Breaking into a system (~ 15 min)
- Hiding traces and digging in (~ 10 min)
- Abuses of systems (~ 10 min)
Programme (cont)

/ Information gathering

- Scans
  - ICMP Sweeps (Echo, Timestamp, Netmask)
  - TCP Scans (SYN, ACK, RST, XMAS, NULL)
  - UDP Scans

- Probes
  - DNS
    - Version information (banner grabbing, queries)

- Distinguishing scans and probes from normal activity
  - WINS
  - Load balancers
  - traceroute
Programme (cont)

// Breaking in
  o Buffer overflows
    : Program stack
    : When is a buffer vulnerable
    : Smashing the stack (overwriting return addresses)
  o Format string bugs
    : The unknown format chars of printf()
    : What functions are vulnerable
    : How it is done
    : How format bugs help buffer overruns
Programme (cont)

/ Hiding
  o Cleaning logfiles
  o Utmp, wtmp, lastlog
  o Other traces often overlooked by attackers
    : Shell history
    : Unsuccessful attacks

/ Digging in (rootkits)
  o Trojaned system commands
  o backdoors
Programme (cont)

/ Abuses (Denial-of-Service)
  o TCP SYN Flood
  o UDP Flood
  o Ping Flood
    o Smurf
/ Distinguishing between DoS and Scans
  o Backscatter
What's been left out

- Distributed attacks
  - Scans, Sniffing
  - Distributed Denial of Service
- Other attack forms
  - Heap corruption
  - Return to libc
- Kernel Mode rootkits
- Warez, SPAM
- Lots more
Next Steps

- Flesh out course material
  - Slides
  - Handouts
- Test materials
  - Incorporate critics
  - Document experiences