Common Scanning Tools

Antti Karessuo

Contents

- Small vs. Large Scanning Tools
- SATAN
- ISS
- COPS
- Nessus
- Nmap
- What else?

Small vs. Large Tools

- Small Tools
  - Dedicated
  - Best for some particular scan
- Large Tools
  - one tool for everything
  - make scanning automated and easy

Small dedicated tools

- Strobe -fast TCP port scanner, gives little info
- NSS -a Perl-based scanner, light
- IdentTCPScan - finds TCP UIDs
- CONNECT - TFTP scanner
- FSPScan -scans for FSP servers
- XSCAN -scans X-servers
- SafeSuit -scanner runing on NT

SATAN

- Security Administrator's Tool for Analyzing Networks, 1995
- Collects publicly given information from networks
- Runs on Unix, free
- Too old - Not effective anymore
- Many more advanced tools based on Satan (SAINT, etc)

ISS - Internet Security Scanner

- like SATAN, but scans better
- Internet Security Systems product
  - freeware for single user
  - expensive for corporate use
- Market leader (autumn 2002)
- Quite old, but still up-to-date

COPS- Computer Oracle and Password System

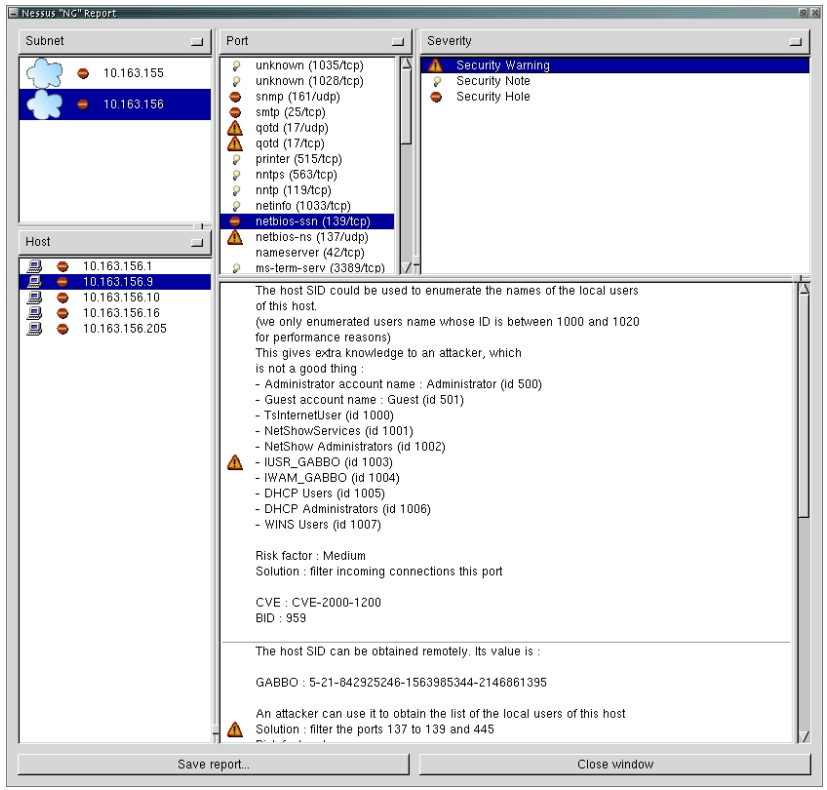
- Commonly used by Unix-admins
  - good for finding holes that give root rights
- Consists of many subprograms
  - permissions,passwords,SUID...
- Does not attempt to correct or exploit any found problems
- Not as easy to use as ISS or SATAN

Nessus (1)

- One of the best public scanners at the moment
- Free, powerful, up-to-date and easy to use
- Doesn’t take anything for granted
  - detects everything, no assumptions on for example default port numbers

Nessus (2)

- Produces nice and readable reports
  - What is wrong and how should you fix it
  - High or low risk
- Plug-in architecture
  - You can easily add own tests



NMAP (Network Mapper)

- A utility for port scanning large networks
  - various scanning techniques & protocols
  - powerful & scalable
- A "Stealth" scanner
  - Some features designed for crackers
  - Slow scanning, IP spoofing etc.
- Supports a number of performance and reliability features
- Flexible target and port specification
- Free, most platforms supported

What else?

- Distributed Vulnerability Scanners
  - Agents on various networks, controlled and reporting to a central location
  - Try to battle firewall and low bandwidth problems
  - Nessus can be used in Server-Client mode
- Non-public tools
  - We don’t know about the most evil tools
  - Rootkits etc.