

# Vulnerability Scans

## NETmind

Matthew R. Alderman, CISSP  
Alderman Consulting, LLC  
October 1, 2003

# Vulnerability Scanning

## Why?

- ◆ New vulnerabilities released daily
- ◆ Difficult to apply security patches
- ◆ Vulnerable systems can affect other systems
- ◆ Due diligence

# Vulnerability Scanning Traditional Methods

- ◆ Purchase a scanning tool
  - ISS
  - NetRecon
- ◆ Third Party scan
- ◆ Use freeware tool
  - Nessus
  - SARA
  - SATAN

# Vulnerability Scanning Problems

- ◆ Commercial tools are expensive
- ◆ Third Party scans are expensive
- ◆ Freeware tools reporting is lacking
- ◆ Resource requirements to perform scans

# NETmind

## ◆ Intrusion Detection

### – Security Audit

- NISSUS provides a security scanning utility that provides remote network security scanning.
- NMAP provides remote network security auditing.
- Combines freeware tools with scheduling and reporting interfaces.

## NETmind (cont.)

### ◆ Intrusion Detection (cont.)

#### – IDS Databases

- Snort is an open source network intrusion detection system, capable of performing realtime traffic analysis and packet logging on IP networks.

### ◆ Web Based Protocol Analyzer

- Ethereal allows network engineers the ability to remotely capture data from a live network and download it locally so that it can be examined.

## NETmind (cont.)

### ◆ Real Time Traffic Measurement

- NTOP tracks network usage, generating a series of statistics for each host in the local subnet and for the subnet as a whole.

### ◆ CACTI

- Cacti is a complete web based front-end to RRDTOOL, and a more powerful and configurable alternative to MRTG.

## NETmind (cont.)

### ◆ Web Based Syslog Reports

- The Web based Syslog report engine is an effective solution for central Syslog file monitoring and analysis.

### ◆ IP Address Management

- The IP address Management module provides a web based interface to managing the administration and support of IP addresses.

# NETmind Demo

# Questions & Answers

- ◆ Can the NESSUS reports be automatically emailed to predefined users? It appears the NMAP reports can be sent to an email address, but we did not see the feature for NESSUS.
  - In the current release NESSUS reports are not available for email, in the next minor release scheduled for late November this feature is added.
  
- ◆ Can the CACTI reports be exported or posted to another website? The DA Sites do not want remote users to access the box, so they would like to publish reports to another website for review.
  - Yes, the information can certainly be exported and published to another site. In addition, access to Cacti can be protected via username and password and only allow access to the report graphs. But either way, the requested functionality can be accomplished.
  
- ◆ If other products are added to the appliance, does this void the warranty? Many of these DA Sites have other LINUX applications that they may want to run on this box.
  - If the customer does buy Maintenance, then installing other apps will not void the warranty, but obviously Simbari & Associates will not support those applications. Additionally, if the situation is right, we will provide a custom build and integrate their predefined applications. There is also a Windows flavor of the NETmind appliance as well.
  
- ◆ Will you sell the code separately? If so, what is the price? Some DA Sites already have LINUX servers and may want to buy the code to install on their hardware.
  - We are currently working on this option, which will be covered in the next minor release which is scheduled for late November. A pricing model is still being finalized. Once it has been finalized, I will let you know.

# Thank You!

**Matthew R. Alderman, CISSP**

**Alderman Consulting, LLC**

**5725 Deer Creek Drive**

**Willoughby, OH 44094**

**Phone: (216) 210-3243**

**E-mail: [matthew@alderman-consulting.com](mailto:matthew@alderman-consulting.com)**

