Systems Management in an Untrusted Network

Dealing with backups, monitoring, administration, and logging in the DMZ

Introduction

Implementing systems management components in untrusted or semi-trusted networks is difficult…

…if you are concerned about security!

<u>Outline of today's talk:</u>

Example of threats

DMZ Network Architectures in the Real World™

Two core designs and advanced design issues

System and network configuration for systems management

The threat is out there…

- SNMP
  - Multiple Vendor SNMP World Writeable Community Vulnerability
  - NAI Sniffer Agent SNMP Buffer Overflow Vulnerability
- Sniffers
  - Microsoft Network Monitor Multiple Buffer Overflow Vulnerabilities
  - Solaris snoop (print_domain_name) Buffer Overflow Vulnerability

Specific Vulnerability Titles courtesy of SecurityFocus

The threat is out there…

- Remote Control Software (besides its intended functionality)
  - AT&T VNC Weak Authentication Vulnerability
  - PCAnywhere32 Denial of Service Vulnerability
- Administrative Interfaces (over intended functional protocols)
  - Allaire ColdFusion Server 4.5.1 Administrator Login Password DoS Vulnerability
  - Cisco 7xx Series Router DoS Vulnerability
  - Cisco 675 Web Administration Denial of Service Vulnerability

Specific Vulnerability Titles courtesy of SecurityFocus

The threat is out there...

- System logging
  - Age-old attacks:
    - log flood
    - log erase
    - selective log edit
  - Linux syslogd Denial of Service Vulnerability
  - Solaris syslogd Unresolvable Address Remote Denial of Service Vulnerability
- Backup
  - Unauthorized restore/delete, unencrypted backups
  - Veritas Backup Denial of Service Vulnerability

Specific Vulnerability Titles courtesy of SecurityFocus

The Purpose of the DMZ

- But… I'm filtering System Management Protocols at the perimeter! Isn't that enough?
- No.
- Why?
- Two words: Aggravated Penetration.
  Want two more? Privilege Escalation.
  More? Insider attack.

- DMZ hosts are bastion hosts or perimeter service hosts. Why do we spend all this time hardening our DNS servers and then leave a poor password on the ssh service listening on an untrusted interface?

The Purpose of the DMZ

- The DMZ exists to mitigate risk by isolating certain services and functions in a separate segment of the network.

- Segmentation by isolation is generally not enough. Ingress filtering is usually deployed, but typical designs need work past the “crunchy” outside layer. Defense in depth, along with proper protection of internal hosts from the DMZ, is required.

The Purpose of the DMZ

- Example 1. Bastion hosts in a DMZ Segment.

The Purpose of the DMZ

- Example 2. Perimeter service hosts in a flat network.

The Purpose of the DMZ

If it were only that simple...

The Purpose of the DMZ

- Example 3. Segmented DMZs.

The Purpose of the DMZ

- Example 4. Colocated DMZs.

The Purpose of the DMZ

- Example 5. Partner DMZs.

The Purpose of the DMZ

- Other problems in the DMZ
  - Constant change
  - Too many hands in the pot
  - Service protocols not designed with security in mind
  - Systems management protocols not designed with security in mind
  - Scalability mechanisms create additional separation and obfuscation of a clean network design
  - Collusion of disparate types of traffic going

System Management – Composite Sketch

- Common sighting – the status quo:
  - No centralized logging.
  - SSH inbound from the internal network; often from external network, too.
  - PCAnywhere, VNC, or SMS accessible from some management hosts or worse...
  - Backup system non-existent or backups batch copied to internal hosts.
  - Default administrative protocols and interfaces left accessible within the DMZ and from the internal network:
    - SNMP on routers, web interfaces on servers
    - Openview or other monitoring system “pinging” from the inside.