

Security Management Monitoring

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: security_management_monitoring.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Monitor for intruders

- **Intrusion detection is the process of monitoring the events occurring**
- **System for detecting attempts to break into a system or network**
- **System for detecting misuse of system or network**
- **DETECT intrusions - and react to them as well.**
- **Goals**
 - **Accountability**
 - **Response**
- **IDS can detect**
 - **Network scans,**
 - **Packet spoofing**
 - **DoS,**
 - **Script kiddie attacks,**
 - **Unauthorized attempts to connect**
 - **Improperly-structured TCP/IP packets,**
 - **Improper activity on a system.**
- **Type**
 - **Network-Based IDSs**
 - **Intro**
 - ◆ It is Passive
 - ◆ Provide Real Time information
 - ◆ Consist of a set of single-purpose sensors or hosts placed at various points in a network
 - **Advantages**
 - ◆ A few well-placed network-based IDSs can monitor a large network.
 - ◆ Deployment of network-based IDSs has little impact upon an existing network
 - ◆ Listen on a network wire without interfering with the operation of a network
 - ◆ Network-based IDSs can be made very secure against attack and even made invisible
 - **Disadvantages**
 - ◆ May have difficulty processing all packets in a large or busy network
 - ◆ May fail to recognize an attack launched during periods of high traffic
 - **Host-Based IDSs**
 - **Advantages**
 - ◆ Can detect attacks that cannot be seen by network-based IDS
 - ◆ Operate in an environment in which network traffic is encrypted
 - ◆ Analyze activities with great reliability and precision
 - ◆ Host-based IDSs are unaffected by switched networks
 - ◆ Host-based IDSs operate on OS audit trails
 - ◆ Detect Trojan horse or other attacks that involve software integrity breaches
 - ◆ Utilize information sources of two types, operating system audit trails, and system logs

- Disadvantages
 - ♦ Host-based IDSs are harder to manage
 - ♦ IDS may be attacked and disabled as part of the attack.
 - ♦ Host-based IDSs are not well suited for detecting network scans
 - ♦ Host-based IDSs can be disabled by certain denial-of-service attacks
 - ♦ The amount of information can be immense, requiring additional local storage
 - ♦ Limited by log capabilities

➤ **IDS Detection Methods**

- **Application-Based IDSs**

- Intro
 - ♦ Are a special subset of host-based IDSs
 - ♦ Detect suspicious behavior due to authorized users exceeding their authorization
- Advantages
 - ♦ Can monitor the interaction between user and application
 - ♦ Can often work in encrypted environments,
- Disadvantages
 - ♦ Vulnerable to attacks since the applications logs are not as well protected
 - ♦ Often monitor events at the user level of abstraction
 - ♦ They usually cannot detect Trojan horse or software tampering attacks
- Use an Application-based IDS + Host-based and/or Network-based IDSs

- **A signature Based ID**

- Signatures or attributes of known attacks are referenced and compared against
- Use a patterns corresponding to known attacks are called signatures
- Signatures of an attack are stored and referenced
- Must have signature stored to identify
- Advantages
 - ♦ Very effective at detecting attacks without alot of false alarms
 - ♦ Can quickly and reliably diagnose the use of a specific attack tool or technique
 - ♦ Can allow system managers, regardless of their level of security expertise
 - ♦ Most common form of misuse detection used in commercial products
- Disadvantages
 - ♦ Can only detect those attacks they know about
 - ♦ Use signatures that prevent them from detecting variants of common attacks

- **A statistical Anomaly Based ID**

- An IDS acquires data and defines a "normal" usage profile for the systems
- Anomaly detectors identify abnormal unusual behavior (anomalies) on a host or network
- Profiles are constructed from historical data collected over a period of normal operation.
- This level can be static or heuristic
- Observed data defines acceptable usage patterns,
- IDS determines "normal" usage profile using statistical samples
- Detects anomaly from the normal profile
- Advantages
 - ♦ Detect unusual behavior by detecting symptoms of attacks
 - ♦ Can produce information that can in turn be used to define signatures
- Disadvantages
 - ♦ Usually produce a large number of false alarms
 - ♦ Often require extensive "training sets " of system event records
 - ♦ Failure to recognize slow attacks

- **Type of Response**

- Active Responses

- ♦ Collect additional information
 - The most innocuous, but at times most productive
 - ♦ The additional information collected can help resolve the detection of the attack.
- **Passive Responses**
 - ♦ Provide information to system users, relying on humans to take action
 - ♦ Many commercial IDSs rely solely on passive responses.
- **Change the Environment**
 - ♦ Halt an attack in progress and then block subsequent access by the attacker
 - ♦ Actions
 - Injecting TCP reset packets into the attacker's connection
 - Re configuring routers and firewalls
 - Re configuring routers and firewalls to block the network ports
- **Take Action Against the Intruder**
 - ♦ The most aggressive form of this response involves launching attacks against
 - ♦ Attempting to actively gain information about the attacker's host or site
 - ♦ This response is not advised. Due to legal ambiguities about civil liability
- **Alarms and Notifications**
 - ♦ Alarms and notifications are generated by IDSs to inform users when attacks are detected
 - ♦ The most common form of alarm is an onscreen alert or popup window
 - ♦ Remote notification of alarms or alerts
 - ♦ Some products also offer email as another notification channel
- **Types of Intrusions**
 - Input Validation Error
 - Buffer Overflow
 - Boundary Condition
 - Access Validation Error
 - Exceptional Condition Handling error
 - Environmental Error
 - Configuration Error
 - Race Condition
- **3.4.3. Honey pots**
- **3.4.4. Incident Response**
- **2.3.3.3 Packet Sniffing**
 - **Network IDS (NIDS) can use packet sniffing**
 - to scan a network for known attack signatures

❖ **Auditing - Logging**

- **Involves monitoring a system or network**
- **Looking for potential security exposures or incidents**
- **Can be performed by**
 - Analyzing logs
 - System/network scanning
- **Logging is the process of recording interesting system and network events**
- **Classic Auditing**
 - Establish a baseline of "normal" activity
 - Monitor against the baseline for abnormal results
- **Services should be logged**
 - Bootp

- Tftp
- Sunrpc

❖ **Run vulnerability scans**

- **Monitoring your security infrastructure is an ongoing job**
- **Scan the system for vulnerabilities**
- **Patch the holes before the attackers find them.**
- **The process an attackers uses**

- **Footprinting**

- Sometimes called profiling,
- Chooses a target and begins to gather information.
- Determine the range of addresses assigned to the company
- Get names and titles of people
- Get Emails
- Get phone numbers
- Get physical address
- Visit to the company's dumpster
- Look inside the HTML code of a company's web site
- DNS servers are also a favorite target
- Social engineering
- Searching for Post-It notes

- **Scanning**

- The second step is scanning an organization's infrastructure
- Scan the target's border routers,
- Scan the Firewalls
- Scan the Web servers
- Scan other systems that are directly connected to the Internet
- Additionally, begin a wardialing
- Do some (Wardriving)

- **Enumerating**

- After determining network vulnerabilities and software exploits,
- Try to gain access to resources or other information.

- **Attacking**

- Once we have a clear picture of an organization's network
- All that's left is the actual attack.

- **Types of Security Scans**

- **General vulnerabilities**

- MBSA
- Nessus
- Security Analyst
- SAINT
- ISS
- NMap
- REALSecure
- LANGuard
- Cybercop

- **Man-in-the middle vulnerabilities**

- Smbrelay

- **Port vulnerabilities**
 - Superscan
 - ShieldsUP!
 - NMap
 - Netcat
- **Password vulnerabilities**
 - @stake LC4
 - LOphtCrack
 - John the Ripper
 - Pandora
- **TCP/IP vulnerabilities**
 - SATAN
- **Web-based vulnerabilities**
 - Whisker

➤ **Vulnerable TCP/UDP Ports**

- **7 echo Echo service**
- **19 chargen Character generator service**
- **20 ftp-data FTP data**
- **21 ftp FTP control**
- **23 telnet Telnet service**
- **25 SMTP Simple Mail Transfer Protocol**
- **42 nameserver Host name server use for WINS Replication**
- **53 DNS DNS server**
- **80 http Hypertext Transfer Protocol**
- **88 Kerberos Kerberos protocol**
- **110 POP3 Post Office Protocol 3 for email**
- **119 NNTP Newsgroups**
- **135 loc-srv/epmap RPC port mapper for initiating Communications**
- **137 NETBIOS-NS NetBIOS name service**
- **138 NETBIOS-DGM NetBIOS broadcasting**
- **139 NETBIOS-SSN NetBIOS Session service**
- **143 IMAP Internet Message Access Protocol**
- **389 ldap Lightweight Directory Access**
- **443 https HTTP over SSL**
- **445 MS-DS Microsoft-DS port**
- **464 kpassword For Kerberos authentication**
- **500 isakmp ISAKMP/Oakley key exchange Protocol**
- **563 nntps NNTP over SSL**
- **636 ldaps LDAP over SSL**
- **995 POP3s POP3 over SSL**
- **1701 L2TP Layer 2 Tunneling Protocol**
- **1723 PPTP Point-to-Point Tunneling Protocol**

❖ **Set up a honeypot**

- **Security tool that lures attackers away from legitimate network**
- **Lure individuals in and track their activities.**

- **Can be software emulation programs, or hardware**
- **Can be an entire dummy network**
- **Software-based honeypots**
 - Are elaborate emulations that mimic real network
 - Can be quite complex to create well
- **Hardware-based honeypots**
 - Systems comprised of hardware and software components
 - Partially disabled and improperly configured to entice attackers.
 - Relatively easy to build,
- **A composite or dummy network honeypot**
 - Uses software emulations, hardware and software
 - Create an entire honeypot network
 - Very expensive to build and maintain
- **Entrapment violate the code of ethics**

❖ **IDS Comparison**

- **Network-based IDS**
 - Primarily hardware sensors
 - Monitors traffic on specific network segment
 - Monitors protocol anomalies and known virus signatures
 - Can't analyze encrypted data
 - Passive
 - Use resources on network
 - Broad scope but very general
 - Management console or email messages
 - To secure a large area with noncritical data.
 - Generally not a problem installing on network
 - Hard to use as evidence in court
- **Host-based IDS**
 - Primarily software applications
 - Monitors traffic on the host it is installed on
 - Monitors Log files, inadvisable settings or passwords, and other policy violations
 - Can analyze encrypted data if it is decrypted before
 - Passive or active
 - Uses computing resources on host
 - Narrow scope but very specific
 - Management console or email messages
 - To secure a specific resource, e.g web server
 - May be service agreements or other policy restrictions
 - May be admissible as evidence in court