Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 13

INTRUSION DETECTION AND AUDIT ANALYSIS

Version 1.0

Objectives

1301. Intrusion detection techniques for information systems may have some or all of the following objectives:

a. To protect the confidentiality of identified information by detecting access by those users that do not have a need to know.

b. To detect attempts to impact the availability of a system.

c. To protect the integrity of information by detecting unauthorised attempts to alter system data or configurations

Overview and Terminology

1302. Intrusion detection is the process by which inappropriate, incorrect or anomalous activity on an information technology based system is detected. An intrusion can be categorised as one of:

a. Physical Intrusion, which is beyond the scope of this handbook.

b. System Intrusion, where an attacker already has low privileged access to a protected information system.

c. Remote intrusion, where an attacker exploits remote vulnerabilities to gain

access to an information system.

1303. Intrusion detection techniques can be broadly divided into the following categories:

a. Network and Host Intrusion Detection Systems. This technique relies on attack signature recognition, and is commonly found in emerging commercial intrusion detection systems.

b. System Integrity Verification. This technique is used to detect changes to critical system components, such as files, directories or services. These changes may alert an administrator to unauthorised changes that may signify an attack on the system. Alternatively, they may also alert the administrator to inadvertent system changes that render the system open to attack.

c. Audit and Log Analysis. This technique involves collecting and analysing audit logs using pattern recognition to detect anomalous activities, and is used to monitor critical assets.

d. Intrusion Repulsion. Some intrusion detection systems are combined with functionality to repel detected attacks, but Security administrator vigilance is still the most effective method. Caution and assessment of the potential impact should be exercised if this capability is to be used.

1304. Some of the common terms that are used in this handbook follow:

a. A firewall is a network device that filters incoming and outgoing network data, based on a series of rules set by the firewall administrator.

b. A bastion host (often referred to as either a 'demilitarised zone' machine, or part of a firewall configuration) is a server that sits outside an organisation's core network, either on the outside of the organisational firewall, or as a separate network controlled by the organisational firewall. Bastion hosts usually provide public information to networks of lower classification, or trust.

c. An intrusion is defined by different organisations in different ways, and therefore only the most generic goals can be satisfied by an 'off the shelf' intrusion detection system without significant configuration and modification.

1305. Implementation of intrusion detection tools and techniques should always flow from the goals laid out in the security policy or plan, which are derived from a risk assessment. Intrusion detection tools and techniques are important to organisations in much the same way as virus checking software. It is difficult for a security administrator to keep pace with all current and potential threats to information systems. An appropriately configured and managed intrusion detection

system will present a security administrator with more options to mitigate identified risks.

Network and Host Intrusion Detection Systems

1306. A network intrusion detection system monitors all traffic that passes through its network connection. Network intrusion detection systems are most often coupled with a firewall or screening router at the border of an organisation's network, but may also be installed at critical junctions within the network, such as the gateway to a network, between organisational networks, or the gateway from LAN to WAN. The placement of network intrusion detection sensors is critical in mitigating identified risks. A sensor that is placed on the outside of a network will (generally) report more than one that is placed on the inside of a network, especially if a security access control device such as a firewall or router exists to protect the network. An internal sensor, however, will usually only report those events that are critical to security, and may therefore indicate a serious security breach. The choice of security sensor, and indeed the reporting tools, can be important to an intrusion detection strategy.

1307. A host intrusion detection system monitors network traffic that is destined for a particular host, and some system events on the host itself. Host intrusion detection systems may be installed on critical infrastructure components within an organisation, or can be pervasively distributed on all information systems within an organisation.

1308. Network or Host intrusion detection systems scan the information for particular patterns that match the signatures of known attacks. Examples may be:

a. Report any port sweeps of hosts on the internal network in the range 10.0.0.1 to 10.0.0.255;

b. Report any packets which include a signature of a particular virus; and

c. Report any attempts to consume more than 64 HTTP connections to a single internal destination server within 30 seconds.

1309. More advanced systems can use heuristic analysis of traffic patterns, or user usage, to alert security administrators to potential security risks. Some examples of such patterns may include significant deviation from normal network traffic quantities, significant user deviation from normal file system usage patterns, or attempts to access previously unknown network services. Some intrusion detection systems can also be configured by the security administrator to perform custom operations when triggered by custom rules. Examples may include mail security@organisation.gov.au when a packet from IP address 10.0.0.2 is detected on the network, or play a sound whenever the Windows NT registry is opened for write access.

1310. Intrusion detection systems are rarely "plug-and-play". Inappropriate initial configuration can lead to a flood of irrelevant information that requires follow-up

action by administrative staff, or alternatively, may result in a poorly focused system that does not report on organisational security objectives. Tailoring the initial configuration of an intrusion detection system based on the organisational risk assessment, and performing regular maintenance and upgrades to the system are therefore essential to the ongoing viability of any intrusion detection system. Like virus checking software, an intrusion detection device should be updated regularly to ensure that the latest vulnerabilities and signatures are recognised by the detection software.

System Integrity Verification

1311. In order for a host intrusion to be effective, an intruder will usually need to modify a critical security component of the operating system. One of the more effective ways to detect such an intrusion is to use a system integrity verification tool. A system integrity verification tool generally uses cryptographic checksums to verify the integrity of a defined group of files, assessed by the security administrator to be critical to the security of the system. Any modifications to the files in question will be tagged and notified to the security administrator. The list of critical files will be organisationally and therefore risk dependant, though some common critical operating system files may be similar across organisations. The list of files presented to the integrity verification software needs to be critically examined in light of available security resources, and the regularity of normal authorised modifications to selected systems.

1312. The integrity of the list of files, and the associated database of cryptographic checksums is obviously critical to the secure operation of an integrity checking process. Administrators may therefore wish to consider storing the files on some form of write-only media, or on another host, if the risk warrants it and it is operationally viable. Those with particularly sensitive systems that consider the potential risk significant, may wish to use a one way data-diode that sends file and time encoded checksums, along with a regular 'data heartbeat' to a central integrity verification system that is not otherwise network connected or controlled.

Audit and Log Analysis

1313. Whereas a network or host intrusion detection tool relies primarily on signature analysis, analysis of audit log is targeted at anomaly detection. Audit and log file analysis can be one of the most difficult intrusion detection methods to configure effectively. A security administrator needs to contend with:

a. Collection - retrieving information of interest from operating systems, applications or network devices.

b. Rotation - breaking down audit information into date-based chunks.

c. Reduction - removing events or components that are of no interest for follow-on processing.

d. Analysis - examination of audit information for events of interest.

e. Correlation - examining trends taken from past audit events.

f. Migration - transfer of files to an appropriate central location for archival.

g. Archival - storage of audit logs for possible followup analysis.

h. Reporting - informing information managers of associated security issues.

1314. Each of these steps can imply significant effort for a security administrator, either in initial installation, or ongoing maintenance. However, an effectively configured auditing system can be one of the most powerful and flexible intrusion detection devices available in the security toolkit, allowing an organisation to implement those intrusion detection goals that may not be generic enough to be included in a commercial intrusion detection capability. Some security objective examples, where audit analysis may be useful, include:

a. To scan through web access logs to see if anyone has attempted a Common Gateway Interface (CGI) script attack.

b. To examine sendmail logs for incorrect commands, which may imply attempts to forge mail.

c. To search through firewall logs for attempts to access a secure internal web server, not normally available to extranet users.

d. To list all users that accessed privileged accounts that are not included in a list of authorised users.

e. To list any user that executed a particular application.

f. To scan for attempts to execute a buffer overflow command.

g. To list any users outside an authorised list who attempted to access a particular area of a file system.

h. To examine of web proxy logs to verify the site acceptable use policy is being followed.

1315. Enabling audit on network devices and servers is not worthwhile unless there is a tangible plan for the data that is produced. Managing audit logs is a non-trivial task that usually requires ongoing maintenance and monitoring. File systems need to be watched to ensure that disk space does not fill, and therefore contribute to a denial of service situation. Audit information needs to be protected by access controls so that it cannot be easily modified or deleted. Audit information needs to be archived to offline storage, or removed from the file system when no longer required. Audit analysis software needs to be written, installed, and run according to an agreed schedule. The results of the audit analysis need to be distributed to those who have a need to know, and examined by staff with the capability to recognise anomalous events. Anomalous events need to be followed up.

1316. The auditing of network devices and servers can result in significant benefits

to the organisation, including:

a. Logs can identify the source of some hacking attempts, or denial of service attacks;

b. Logs can pinpoint problems with server configurations;

c. Usage statistics can identify when an upgrade of network bandwidth is likely to be required; and

d. Audit logs can be distributed to owners of sensitive data, in order to distribute the audit analysis capability, and potentially identify situations where unauthorised users have access to sensitive data.

1317. A poorly considered audit configuration can lead to information overload due to excessive amounts of information being collected. Audit events to be collected should be critically examined in light of available security resources, the organisational risk assessment and any associated security goals. Information owners should be given the opportunity to be involved in the formulation of broad security goals, which are then implemented if technically and operationally feasible. **Annex A** to this Handbook details a methodology for undertaking audit analysis.

Intrusion Repulsion

1318. Some modern intrusion detection systems offer integration with operating systems and network devices to repulse an active attack once it has been identified by signature analysis. Firewall rules can be rewritten to lock out the source network address, accounts can be locked out, or routes can be changed after an attack has been identified. This form of repulsion can sometimes produce harmful effects for legitimate users when false positives are acted upon by the system. It may also introduce extra risk into the equation - generally, the intrusion detection device will require appropriate authentication credentials in order to modify router or firewall rules. The credentials may be stored in plain text depending upon the implementation of the device in question, and may also need to be outside the protection of the firewall system in order to receive an accurate attack profile.

1319. Intrusion detection tools and audit capabilities can scan for attack signatures, perform limited heuristic analysis of logs, and look for significant exceptions to normal system or network behaviour. Such tools are of limited value when new vulnerabilities crop up, or a sophisticated, cautious attack is under way.

1320. One of the most effective intrusion detection and repulsion assets an organisation can have is an active and dynamic security administration team, skilled in the process of intrusion research, risk assessment and management, and with close ties to the system administration and user community. Unusual activities, mentioned by a staff member, combined with a surge in network activity noticed by a network administrator, coupled with some 'bounced' email messages received by the email team, and all correlated with some data from audit logs, can be drawn together by an experienced security administrator to outline a potential attack profile. The

security administrator may then use other security assets, such as firewalls, network intrusion detection systems, and 'honey pot' servers to contain the potential attack, and gather information for further analysis.

Incident Handling and Response

1321. Procedures for establishing the cause of any security incident, whether accidental or deliberate, the action to be taken to recover and minimise the exposure to a compromise, and any recommendations on preventing a recurrence should be documented and maintained. Indeed, the reporting and handling of security incidents is one of the Ten Key Controls addressed in the Australian Standard on Information Security Management (see **Handbook 4 - Security Management**). An Agency should develop a documented Incident Response Plan which should, as a minimum, detail the following issues:

a. Broad guidelines on what constitutes an incident, and some examples of how incidents may be detected. This section should be based on the intrusion detection objectives of the organisation.

b. The plan should include the minimum level of training to be provided to users and system administrators on how to detect possible system compromises, and to whom a suspected event should be reported. System administrators should be specifically instructed not to reconfigure or access any systems until management have authorised such changes, and all events are recorded (see below).

c. The authority within the agency responsible for initiating a formal (administrative) investigation and police investigation of an incident. It may be prudent to outline the criteria by which the responsible authority would initiate a formal or police investigation of an incident. There should be a link here to other related agency policies such as the Fraud Control Plan. The authority may decide to allow an "attacker" to continue some actions under controlled conditions for purpose of seeking further information/evidence. Agencies considering this approach should seek appropriate legal advice.

d. The steps necessary to ensure the integrity of information supporting a compromise, together with the steps needed to ensure critical systems remain operational, should be detailed. Although in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected. It may therefore be prudent, for example, to transfer a copy of raw audit trails onto CD-ROM for secure archiving, as well as securing manual log records for retention. It would also be advisable to ensure all personnel involved in the investigation maintain a record of actions undertaken to support the investigation. A good discussion paper on "forensic computing" can be found at the Australian Institute of Criminology website at **http://www.aic.gov.au/publications/tandi/tandi118.html**.

1322. The PSM states that DSD should be notified of any incident involving a breach in the security of a Commonwealth Government computer system. DSD may then be able to assist in the analysis of the incident, identification of remedial measures to remove the exploited vulnerability and minimise the likelihood of compromise, and an overall assessment of the organisation's system security safeguards. Formal reporting of incidents should be undertaken using the established Information Security Incident Detection, Reporting, and Analysis Scheme (**ISIDRAS**). details of which are available from **http://www.dsd.gov.au/infosec**. ISIDRAS has been established to collect information on security incidents that affect the security or functionality of Australian Commonwealth Government computer and communications systems.

1323. ISIDRAS is not a substitute for a referral to the AFP in the case of criminal activity. Unauthorised access to a Commonwealth computing system is an offence under the Crimes Act, as is using a Commonwealth facility to obtain unauthorised access to any computing system. It would, therefore, seem that agencies that are subjected to a compromise have a duty to report the matter and to assist the police in their enquiries. Policy decisions on assistance to the AFP and its implications will undoubtedly fall to the senior management, and may be part of the agency's Fraud Control Plan. Details on the **Fraud Control Policy of the Commonwealth** can be found at **http://www.law.gov.au/aghome/commprot/olec/FCP/fcp3.html**. Fraud Investigation Standards can be found at **http://www.law.gov.au/aghome/commprot/olec/Standards/stndcnt.html**.

Grades of Intrusion Detection

1324. The following grades of intrusion detection system implementation have been included to assist in determining the level of effort that should be allocated to such a task. They are not definitive, and when implementing intrusion detection should be used as a guide only.

a. **Grade 0**

i. Perform regular integrity verification examinations of critical systems, as determined by the risk assessment.

b. **Grade 1**

i. Perform regular integrity verification examinations of critical systems, as determined by the risk assessment.

ii. Install and configure network intrusion detection systems at critical gateways. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures.

iii. Install and configure auditing for critical system hosts. Archive audit information to offline storage capable of retaining information for a period as directed by the security policy.

c. **Grade 2**

i. Perform regular integrity verification examinations of critical systems, as determined by the risk assessment.

ii. Install and configure network intrusion detection systems at critical gateways. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures.

iii. Install and configure host intrusion detection agents on critical bastion (or DMZ) systems. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures.

iv. Install and configure auditing for critical system, network and application assets as directed by security goals set by information owners. Archive identified audit information to offline storage capable of retaining information for a period as directed by the security policy.

d. **Grade 3**

i. Perform regular integrity verification examinations of critical systems, as determined by the risk assessment. System integrity verification signatures/checksums should be stored on append-only media or systems.

ii. Install and configure network intrusion detection systems at critical gateways. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures. Configure organisational gateway network intrusion detection systems to interact with firewall or screening router assets to automatically deny service to source machines from which an attack is detected.

iii. Install and configure host intrusion detection agents on critical bastion (or DMZ) systems. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures.

iv. Install and configure auditing for critical system, network and application assets as directed by security goals set by information owners. Regularly archive identified audit information to offline storage capable of retaining information for a period as directed by the security policy, and to guard against denial of service through audit overflow.

e. **Grade 4**

i. Perform regular integrity verification examinations of critical systems, as determined by the risk assessment. System integrity verification

signatures/checksums should be stored on append-only media or systems.

ii. Install and configure network intrusion detection systems at critical gateways, and network junctions within the organisation. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures. Configure organisational gateway network intrusion detection systems to interact with firewall or screening router assets to automatically deny service to source machines from which an attack is detected.

iii. Install and configure host intrusion detection agents on critical bastion (or DMZ) systems, and key server hosts within the organisation. Ensure regular upgrades for the intrusion detection systems in order to gain access to new attack signatures. Configure host intrusion detection systems to interact with the host operating system to automatically deny service to source machines from which an attack is detected.

iv. Install and configure auditing for critical system, network and application assets as directed by security goals set by information owners. Regularly archive identified audit information to offline storage capable of retaining information for a period as directed by the security policy, and to guard against denial of service through audit overflow.

v. Provide a distributed audit analysis capability to information owners for appropriate application, system or network assets.

ANNEX A

AUDIT ANALYSIS DEVELOPMENT

Audit Objectives and Requirements

A1. It is important that clear, unambiguous audit objectives be established and agreed. These objectives should be system independent and relate directly to mitigating those high security risks identified in a risk assessment. Examples of audit objectives may include:

a. List all users who have attempted, and failed, to access files in directory X.

b. List all users who have attempted to gain superuser privileges.

c. List the top ten users who have accessed documents/files within a specified directory/volume.

A2. Successful implementation of an audit strategy is critically dependent on defining those audit objectives that will be of benefit in mitigating risk. Audit storage, processing and archival can be a **very** resource intensive task, and it is important that the audit tasks be limited to those agreed objectives. Note that some audit objectives **do not** necessarily require processing at regular intervals or in real time, but are designed to collect audit information in event of an incident or investigation. Whilst regular review may not be required in this instance, the audit objective should reflect this requirement and archiving & forensic requirements. Since management is usually sensitive about "auditing staff actions" it is a wise idea to ensure appropriate management agreement or approval is granted before an audit strategy is implemented.

A3. The requirements for reporting should also be ascertained at this stage, including issues such as:

a. Who should receive audit reports?

b. Should the reports be sent automatically via email, or are they too sensitive; should they be sent by conventional mail?

c. Should audit trail files be manually or automatically sent to another processing/storage host?

d. How long should raw and processed audit logs and reports be retained?

Audit Trail Configuration, Processing and Storage

A4. Based on the audit objectives, the host or system audit trails should be configured so that the agreed objectives can be achieved. Care should exercised to ensure that only the minimum audit trails are activated, so as to prevent the system from being flooded with logs. Consideration should be given to automatically sending audit information directly to a secured host(s) (eg via a SYSLOG function if it exists). This will not only alleviate the storage load on individual hosts, but (equally important) provide a greater degree of protection to sensitive audit data. The audit configuration should be documented and regularly checked to ensure integrity.

A5. Development of appropriate processing tools can be difficult and time

consuming. It is therefore recommended that the **minimum** programming effort be expended to meet only the required audit objectives. On UNIX environments consideration should be given to using common search tools such as PERL, or SAS for Mainframe. These tools are also available on the PC environment. Note that the tools are required only for the processing environment and need not run on all hosts. In other words, if audit logs are sent to a UNIX audit server, then PERL could be used to process Netware, NT, UNIX or any other audit trails.

A6. There should be enough storage on the host(s) to store audit trail information. The actual amount of storage required will depend on:

a. The amount of audit trail records that are collected.

b. The extent of information contained within the audit trail records.

c. The regularity by which the information is deposited on the storage media.

d. The rate at which the information is archived and deleted from the storage media.

A7. Consideration should be given to archiving raw and processed audit trail data regularly onto CD ROM to ensure that archived data is retained in a reasonably secure fashion.

ANNEX B

Vulnerability Analysis

B1. An intrusion detection strategy should be complemented by a vulnerability analysis strategy. Vulnerability analysis means the detection of changes in the level of system vulnerabilities from an established security baseline.

B2. Vulnerability analysis can be conducted in a number of ways:

a. Monitoring and awareness of public domain information regarding new vulnerabilities in operating systems and application software

b. Running commercial/public domain tools to assess vulnerabilities

c. Running manual checks against system configurations to ensure disallowed services are prevented. Eg. "*netstat"* commands to check the status of open sessions against the configuration parameters

B3. It is recommended that a vulnerability strategy include one or more of the above techniques. All three would be preferable. A vulnerability analysis strategy also needs to identify when the analysis needs to occur eg. should occur as part of change control process. The determination should be based on a risk assessment allowing for focus on the areas of highest risk.

B4. Another point to note in the use of automated tools is that they are only as good as the level of analysis that they perform. For example, if they are not configured to assess the areas of high risk in a system configuration, then it will not be evident that a weakness may have emerged. Also if the software is not regularly updated to include new vulnerabilities, use of the tools will not necessarily uncover all weaknesses in a system.