

OPERATIONS MANUAL Stage One: Active Detection Phase

Hal Flynn 2000-05-11

OPERATIONS MANUAL Information Protection Centre

Stage 1 - Active: Detection Phase

Incidents: The IPC acts as a Point of Contact for security reporting and assistance. If someone detects some unusual or suspicious event related to the organisation's networks, computers or information, they can relay the details of the incident to the IPC for investigation. The results of the investigation will be provided back to the originator and, in most cases, will be posted to the IPC's intranet web site. It is often difficult to determine if the unusual or suspicious event is symptomatic of an incident because apparent evidence of security incidents often indicates a problem with system configuration, untested application program, hardware failure, or frequently user errors. Typical indications of security incidents include any or all of the following:

- A system alarm or similar indication set off by an intrusion detection tool.
- Suspicious entries in system or network accounting (e.g., a UNIX user obtaining root access without going through the normal sequence of events necessary to obtain this access).
- Accounting discrepancies such as a gap where there is a complete lack of activity.
- Unsuccessful login attempts.
- attempts (either failed or successful) to gain unauthorized access to a system or it's data.
- Unexplained new user accounts.
- Unexplained new files or unfamiliar file name.
- Unexplained modifications to file lengths and/or dates, especially in system executable files.
- Unexplained attempts to write to systems files or changes in system files.
- Unexplained modification or deletion of data.
- the unauthorized use of a system for the processing or storage of data .
- Denial of service or inability of one or more users to login to their account.
- System crashes.
- Poor system performance.

- Unauthorized operation of a program or sniffer device to monitor network traffic.
- "Door knob rattling" (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts).
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- Unusual time of usage - more security incidents occur in other than prime time.
- An indicated last time of usage for a user does not agree with the actual time of prior usage for that user.
- Unusual usage patterns - programs being compiled under a user's account who does not have any programming responsibility.

Intrusion Detection: The IPC will deploy Intrusion Detection Systems (IDS) at strategic points throughout the organisation's IT architecture. This is required to meet the "detect" phase of active security measures. The IDS look for known patterns of misuse or suspected attack and automatically notify the IPC via email, pager or cell phone.

- the IDS(s) passively monitor ethernet LAN and looks for known signatures:
 - 24/7 monitoring and logging by the monitoring engines
 - alarms relayed to central console at IPC
 - console can be set to email or page an any particular type of alarm
- IDSs don't catch everything:
 - the logs need to be reviewed in more detail at least bi-weekly to see if something was missed by the automated tools
 - this takes someone patient and who has good knowledge of known vulnerabilities and can detect unusual patterns of activities

Decoys: The IPC can optionally deploy decoys or "honey pots" to distract any potential attackers until their activities can be detected. Such a decoy must not be advertised as a lure but rather act as a tethered lamb to lure attackers away from more sensitive hosts. These are heavily instrumented hosts so they provide a lot of alarms and logs of activities that touch them.

Tripwires: File integrity can be established by applying calculations to file contents and deriving coded values which are stored separately. If in doubt about whether someone has altered your critical system files then pull out these stored check values and compare them to newly calculated values for the files.

Viral Scanning: Viral scanning is now a mature detective technology. Of course the possible variations of viral attacks make it a challenge to minimize the window of exposure between release of new variant to installation of latest detective database.

Net Mapping: The task of assessing incidents is made less difficult when there is an up to date map of the networks and their attached devices. Without this it is hard to determine where an attack may have come from, what systems it may impact, etc. An automated network mapping capability can also reveal changes which may themselves be security incidents (e.g., addition of unauthorized hosts, unprotected attachment to Internet). < p>**Sandboxes:** Desktop technologies have developed to deal with the downloading of active, malicious code. Web servers can ship a variety of nasties at you. Trojan code imbedded within useful applications can access and pass information about you or your system back to some collection site. Sandboxes try to impose restrictive controls on suspect code by detecting and stopping improper activities.

URL/Content Blocking: Organisations are often concerned that their users are wasting time or Internet bandwidth by carrying on non-business related activities in their web surfing. Some management feels they could be sued successfully should an employee be found violating policy or the law and there were no active attempts to prevent this. The content of outgoing web requests can be matched against prohibited sites. Incoming web content can be matched for improper text strings or prohibited graphical formats.

[Admin](#) [Passive](#) [Protective](#) [Assessive](#) [Responsive](#) [Integrative](#)

Original development of these pages was supported by
the Province of Manitoba

The content is maintained by [Andrew Mackie](#)

Last modified: April 28, 2000

[Privacy Statement](#)

Copyright 2006, SecurityFocus