Chapter 6

Detecting Signs of Intrusion

Intruders are always looking for new ways to break into networked computer systems. They may attempt to breach your network's perimeter defenses from remote locations or try to infiltrate your organization physically to gain access to information resources. Intruders seek old, unpatched vulnerabilities as well as newly discovered vulnerabilities in operating systems, network services, and protocols; and they take advantage of both. They develop and use sophisticated programs to penetrate systems rapidly. As a result, intrusions and the damage they cause can be achieved in seconds.

Even if your organization has implemented a number of the more popular information security protection measures, such as firewalls and intrusion detection systems, it is essential that you closely monitor your information assets and transactions involving these assets for signs of intrusion. Monitoring may be complicated, because intruder attack methods are constantly changing, and intruders often hide their activities by changing the systems they break into. An intrusion may have already happened without your noticing because everything seemed to be operating normally.

The practices contained in this chapter are designed to help you detect intrusions by looking for unexpected or suspicious behavior and "fingerprints" of known intrusion methods.

6.1 Overview

These practices are intended primarily for system and network administrators, managers of information systems, and security personnel responsible for networked information resources.

The practices are applicable to your organization if its networked systems infrastructure includes any of the following:

- Host systems providing services to multiple users (file servers, time-sharing systems, database servers, web servers, etc.)
- Local area or wide area networks
- Direct connections, gateways, or modem access to and from external networks, such as the Internet

The practices do not address the following issues:

- Protecting user privacy while in the process of detecting signs of intrusion
- Using security monitoring and reporting services provided by outside (third-party) organizations

6.1.1 The Need for Detecting Signs of Intrusion

If you do not know that an intrusion or an intrusion attempt has occurred, it is difficult, if not impossible, to determine later if your systems have been compromised. If the information necessary to detect an intrusion is not being collected and reviewed, you cannot determine what sensitive data, systems, and networks are being attacked and what breaches in confidentiality, integrity, or availability have occurred. As a result of an inadequate ability to detect signs of intrusion, your organization may face the following problems:

- Inability to determine either the full extent of the intrusion and the damage it has caused, or whether or not you have completely removed the intruder from your systems and networks. This will significantly increase your time to recover.
- Legal action. Intruders make use of systems they have compromised to launch attacks against others. If one of your systems is used in this way, you may be held liable for not exercising adequate due care with respect to security.
- Lost business opportunities, coupled with loss of reputation.

If you are adequately prepared and have the necessary policies and procedures in place to detect signs of intrusion, you can mitigate your risk of exposure to such problems.

6.1.2 An Approach for Detecting Signs of Intrusion

The practices in this chapter assume that you have implemented the detection preparation practices described in Chapter 5. The general approach to detecting intrusions is threefold:

1. Observe your systems for anything unexpected or suspicious.
2. Investigate anything you find to be unusual.
3. If your investigation finds something that isn't explained by authorized activity, immediately initiate your intrusion response procedures as described in Chapter 7.

While this process sounds simple enough, implementing it is a resource-intensive activity that requires continuous, automated support and daily administrative effort. Furthermore, the scale of intrusion detection practices may need to change as threats, system configurations, or security requirements change. In all cases, however, four areas must be addressed:

1. The integrity of the software you use to detect intrusions
2. Monitoring of the behavior of your systems and the traffic on your networks
3. Physical forms of intrusion to your computer systems, offline data storage media, and output devices
4. Follow through, including the investigation of reports by users and other reliable sources (such as incident response teams) and action following unexpected activities

As you look for signs of intrusion, keep in mind that information from one source may not appear suspicious by itself. Inconsistencies among several sources can sometimes be the best indication of suspicious behavior or intrusions.

Table 6.1 Detecting Signs of Intrusion Practice Summary

Approach	Practice	Reference
Integrity of intrusion detection software	Ensure that the Software Used to Examine Systems Has Not Been Compromised	Section 6.2; page 234
Behavior of networks and systems	Monitor and Inspect Network Activities	Section 6.3; page 237
	Monitor and Inspect System Activities	Section 6.4; page 243
	Inspect Files and Directories for Unexpected Changes	Section 6.5; page 251

(*continued*)

Table 6.1 Detecting Signs of Intrusion Practice Summary (*cont.*)

Approach	Practice	Reference
Physical forms of intrusion	Investigate Unauthorized Hardware Attached to the Network	Section 6.6; page 254
	Look for Signs of Unauthorized Access to Physical Resources	Section 6.7; page 257
Follow through	Review Reports of Suspicious System and Network Behavior and Events	Section 6.8; page 258
	Take Appropriate Actions	Section 6.9; page 261

6.2 Ensure That the Software Used to Examine Systems Has Not Been Compromised

When you look for signs of intrusions on your systems, and when you examine your systems in general, you should use a verified, reference set of software—one that contains only trusted copies of software that have not been modified—and perform a clean boot (start the system from a known, virus-free image of the operating system). In addition to executable programs, the verified set of software must include all the operating system kernel, system libraries, configuration and data files, and system utilities on which the programs depend. You should avoid relying on software that resides on systems being examined (unless you can verify that the software and its supporting libraries, configuration files, and data files have not been modified).

Intrusion detection depends heavily on the reliability of the information you gather about the state and behavior of your systems. Therefore, it is essential that you use only software that you know to be reliable and accurate in its reporting of such information.

Intruders often replace software that would reveal their presence with substitutes that obscure or remove such information. Intruders are known to have replaced programs, libraries, and other utilities called by the programs. If a program used in detecting intrusions has been tampered with or replaced with a substitute, obviously you cannot rely on its output.

Ensuring that you are using only verified software may be very difficult. Intruders can make extremely devious system modifications that make things appear normal when in fact they are not. They can create, substitute, modify, and damage files on systems to

which they have gained access. For example an intruder can use the rootkit tool set[1] to replace the *ps* command on a UNIX system with one that does not display the intruder's process; similarly, an editor can be replaced with one that reads a file other than the one specified, which the intruder may have hidden and replaced with another version. Intruders modify system log files to remove traces of their activities and may modify software that is executed at system boot and shutdown, complicating your ability to take a system safely offline for more detailed analysis. Viruses often do this. By masking their presence on a compromised system, intruders prolong the time they have to use that system for their purposes. In several notable cases, the presence of intruders on compromised systems was not discovered until many months after the initial intrusion occurred.

> Any examination or alteration of a suspect system could destroy data that may be useful during any legal investigation or proceedings. However, to determine the cause of the problem and return a system to operations as soon as possible, the system administrator may have no choice but to destroy such data. If you require legal evidence to be preserved, we recommend that you initiate your intrusion response procedures immediately, as described in Chapter 7.

The guiding principle for this practice is that you maintain a certain level of suspicion. Question everything you observe, and be able to answer these questions:

- What software is producing this output?
- What other software does it rely on?
- What software can I trust?

You can use five different approaches to achieve the goal of using a verified set of software. In all cases, the verified software should be located on physically write-protected media (e.g., CD-ROM or write-protected disk), so that it cannot be modified by a user or by software running on the system being examined. Each approach listed below has advantages and disadvantages, so you should choose a method appropriate to your current circumstances.

---

1. For Windows NT, refer to *http://www.rootkit.com.* For Linux, refer to *http://www.securityfocus.com/tools/1489.* To check for signs of the presence of rootkit, refer to *http://www.securityfocus.com/tools/1646.*

1. Move the disk from the system suspected of having been compromised to a write-protected, verified system, and examine the disk's contents using the software on the verified system.

The advantage of this method is that you do not need to rely on the integrity of any part of the operating system or the hardware on the suspect system. The method is effective and reasonable when you suspect that a particular system has been compromised and you want to analyze it. However, it may not be practical for automated procedures or for checking a large number of systems.

Be careful when shutting down the suspect system, since this act may in and of itself cause the evidence you are seeking to be hidden or lost. Before shutting down the suspect system, look at any programs that will run at shutdown for signs that they were modified (for example in some UNIX operating systems, the */etc/shutdown* program should be examined). However, be aware that just looking at the file may be misleading, since you are relying on the suspect system's software. You may want to execute verified copies of shutdown programs and their data files (taking care to save the original files for later analysis). Other alternatives are to execute the shutdown from external media, force the system to halt immediately, or just pull the plug.

2. Attach to the suspect system a write-protected, verified system disk that contains the operating system and all necessary software, and then reboot the system using the verified operating system. This method has advantages and disadvantages similar to those of method 1 but relies on the trustworthiness of the suspect system's hardware.

3. Generate an image of the suspect system disk, mount it on a verified system, and examine it there. This method is acceptable if you have a verified system that you can use to examine the suspect system disk. This approach has the advantage of not affecting the operational environment of the suspect system (because what you're examining is an image of it on another system) and preserving the original evidence for subsequent legal proceedings.

4. Use external media containing a verified set of software to examine the suspect system.

To use this method, you need to use a CD-ROM or a write-protected disk containing verified software when examining the suspect system. A significant concern with this approach is that you will still be using the suspect system's operating system (e.g., the UNIX kernel), and it is highly unlikely that you have provided every needed operating system program, utility, and library on the CD-ROM or write-protected disk. As a result, the outcome of such analysis is suspect.

5. Verify the software on the suspect system first, then use the verified software to examine the suspect system.

This method requires you to compare the software on the suspect system with a reference copy (either complete files or cryptographic checksums as described in Section 5.3). However, take care to use a verified comparison program or cryptographic checksumming program. The program used to verify the software should be located on physically write-protected media. This approach has the same problem as that noted in method 4 with respect to using the suspect system's operating system.

6.2.1 Policy Considerations

Your organization's networked systems security policy should specify the level of verification that is required when examining each class of data and service provided by the organization's systems.

6.2.2 Additional Information

Some operating systems have the ability to make files immutable, that is, unchangeable by any process on the system, including system and administrative processes. All operating system files that don't need to be modified when a system is running should be made immutable wherever possible.

When you are examining your system through a remote access connection, make sure that you have established a secure channel to the system (as described in Section 2.13). Configure servers for secure remote administration and use of SSH (as described in Section A.3), so that only authorized personnel use the channel and nothing is changed or revealed in transit.

6.3 Monitor and Inspect Network Activities

Data about network activities (traffic, performance, etc.) can be collected from a variety of sources, including the following:

- Administrator probes (Internet control message protocol [ICMP] pings, port probes, simple network management protocol [SNMP] queries)
- Log files (routers, firewalls, other network hosts and devices)
- Alert reports
- Error reports

- Network performance statistics reports
- The outputs of tools used to support in-depth analysis

You should watch for unexpected network behavior, such as the following:

- Unexpected changes in network performance such as variations in traffic load at specified times
- Traffic coming from or going to unexpected locations
- Connections made at unusual times
- Repeated, failed connection attempts
- Unauthorized scans and probes
- Nonstandard or malformed packets (protocol violations)

Monitoring messages as they traverse your network gives you the ability to identify intrusive activity as it is occurring or soon afterwards. By catching suspicious activity as early as possible, you can immediately begin to investigate the activity and hopefully minimize and contain any damage.

Logs of network traffic may contain evidence of unusual, suspicious, or unexpected activities, indicating that someone has compromised or tried to compromise a system on your network. By inspecting log files on a regular basis, you may be able to identify intruder reconnaissance in advance of an intrusion. You may also identify attempted or successful intrusions soon after they occur. However, if an intruder has altered log files, the data may no longer be present.

If you permit access to your systems and networks by third parties (vendors, contractors, suppliers, partners, customers, etc.), you must monitor their access to ensure that all their actions are authentic and authorized. This step includes monitoring and inspecting their network activities.

6.3.1 Notify Users

Inform authorized users of your systems about the scope and kinds of monitoring you will be doing and the consequences of unauthorized behavior.

A common method for communicating this message is the presentation of a banner message immediately before user login.

Without the presentation of a banner message or other warning, you probably cannot use log files and other collected data in any action you may choose to take against a user.

For further information on setting up monitoring banners for Windows NT, refer to the implementation *Setting Up a Logon Banner on Windows NT 4.0.*[2] Here's one example of banner language taken from this implementation:

> *This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.*

6.3.2 Review Network Alerts

Review and investigate notification from network-specific alert mechanisms (such as e-mail, voice mail, or pager messages), for example:

- Users and other administrators, via e-mail or in person
- Operating system alert mechanisms
- Network and system management software traps, such as those that can be set via SNMP (simple network management protocol)
- Intrusion detection systems
- Custom alert mechanisms from service or application programs (including tools)

6.3.3 Review Network Error Reports

These types of notifications are typically produced by one of the following devices:

- Operating system error reporting mechanisms
- Log file filtering tools

2. Available at *http://www.cert.org/security-improvement* under Windows NT implementations.

- Vendor or custom-developed management software
- Custom error-reporting mechanisms from service or application programs (including tools)

Often an administrator will be able to configure error reporting at a number of criticality, severity, or priority levels when installing the network system, service and application programs, and supporting tools.

6.3.4 Review Network Performance

Statistics are generally produced by vendor or custom performance-monitoring tools. Typical statistics include the following (refer to Section 5.3, Table 5.2):

- Total traffic load in and out over time (packet, byte, and connection counts) and by event (such as new product or service release)
- Traffic load (percentage of packets, bytes, connections) in and out over time sorted by protocol, source address, destination address, other packet header data
- Error counts on all network interfaces
- Comparison of previous network performance statistics with current statistics for the same time frame

Look for the following extraordinary occurrences:

- Unexpected changes in performance between current and previously captured statistics, for example, unusually high or low network traffic compared with expected levels for the day of the week and time of day
- Unexpected deviations from authoritative network traffic characterization information, for example (refer to Section 5.3):

  traffic coming from unexpected source addresses or using unexpected ports or protocols

  traffic going to unexpected destination addresses or using unexpected ports or protocols

  excessively high or low traffic volume for the day of the week and time of day

- Unexpected loss of connectivity
- Unusual modem activity or availability, which can indicate intruder access through overlooked entry points (ports) or intruder use of daemon dialers

6.3.5 Review Network Traffic

Identify any unexpected, unusual, or suspicious network traffic and the possible implications. From network log files and other network traffic collection mechanisms, look for the following extraordinary occurrences:

- Reconnaissance (probes, scans, use of mapping tools) in advance of an attack. These activities can indicate attempts to identify your configuration (hosts, operating systems, network topology, externally accessible paths into your systems, etc.) and your Internet service provider(s) (ISP), along with their configuration.
- Connections to or from unusual locations. For example, if a server host is dedicated to a single service (such as serving a public web site), any requests it makes for outbound connections are suspicious. Such requests may indicate that an intruder has compromised the server and that it is being used to launch an attack on another host.
- Protocol violations. These include, but are not limited to, invalid option bits in a transmission control protocol (TCP) packet, invalid sequence numbers in a TCP packet, invalid flags in a TCP packet (ACK before SYN), and invalid fragments. There is no good reason to violate the Internet protocol (IP), TCP, ICMP, and user datagram protocol (UDP) specifications. These types of protocol violations often result when an intruder uses a network scanner in an attempt to bypass your firewall (that may just check for an established bit set on a packet) and to identify the type of systems on your networks (since different host IP stacks will respond to the error in different ways). A DoS condition can occur, for example, when an intruder's host creates TCP half-open connections by sending a flood of SYN packets with no corresponding ACK packets.[3]
- Packets with source and destination addresses external to your network. Your firewall should always be configured to prevent this. If it occurs, it may indicate that an intruder has bypassed the firewall, possibly by compromising the firewall host, and is routing his or her traffic through your network, perhaps to take advantage of a network-level trust relationship. It may also indicate the presence of an inside intruder.
- Packets with an internal source address that actually originate from an external source. This can indicate an IP spoofing attack that may have bypassed your firewall.

---

3. Refer to CERT advisories CA-2000-21, *Denial-of-Service Vulnerabilities in TCP/IP Stacks* and CA-1996-21, *TCP SYN Flooding and IP Spoofing Attacks,* available at *http://www.cert.org/advisories.*

- Unusual port combinations in TCP and UDP packets. This type of traffic could indicate an unexpected service running on the network (such as a backdoor program). It could also indicate that the intruder has bypassed your firewall. Packets with the same source address and a sequence of destination ports often indicate that an intruder is trying to discover both the firewall policy and what services are available on your systems.
- Unusual address resolution protocol (ARP) traffic. In a switched network, an intruder can alter the ARP cache on one or more hosts so that any host on the same segment can see traffic on that segment (similar to a network interface card in promiscuous mode on a shared Ethernet segment). The intruder can then gain access to passwords and other unencrypted information sent over the network.
- Unusual dynamic host configuration protocol/boot protocol (DHCP/BOOTP) traffic. An intruder can cause a host to send bogus DHCP replies and convince other hosts that it is their default gateway. The compromised host will then receive all of the traffic for outbound networks and gain access to unencrypted information sent over the network.
- Packets with unusual protocol or port numbers sent to broadcast addresses. This type of traffic can indicate a DoS attack.
- An unusually high number of ICMP port unreachable packets from a single host. This indicates that an intruder is scanning the host looking for available services.
- Connections made at unusual times
- Unusual use of Internet Relay Chat (IRC), a common means of communication used by intruders

If you are reviewing network traffic on a system other than the one being monitored, ensure that the connection between them is secure, as described in Section 2.13.

6.3.6 Policy Considerations

Your organization's networked systems security policy should specify the following:

- The need for users to be notified that you will monitor network activities
- Your objectives for monitoring
- Which data streams will be monitored and for what purposes
- The responsibilities and authority of system administrators for handling notifications generated by monitoring and logging software

- What forms of unexpected network behavior users should watch for and the need to report any such behavior to their designated security officials and system administrators

6.3.7 Additional Information

1. For further UNIX- and NT-specific network monitoring and network data collection guidance, refer to CERT tech tips at the CERT web site, including the *Intruder Detection Checklist* and *Steps for Recovering from a UNIX or NT System Compromise.* A list of network-monitoring tools is presented in Section 5.3.15, and Table 5.3.
2. When possible, analyze and correlate data collected from multiple sources (as described in the other practices of this chapter). Performing some level of correlation analysis during the intrusion detection process, such as determining when suspicious activity occurring in one part of your infrastructure may be related to suspicious activity in another part, will assist you in determining the full extent of any compromise and its characteristics. Refer to Section 7.2 for further guidance.

6.4 Monitor and Inspect System Activities

System activities include those associated with system performance, processes, and users. Programs executing on your networked systems typically include a variety of operating system and network services, user-initiated programs, and special-purpose applications such as database services. Every program executing on a system is represented by one or more processes. Each process executes with specific privileges that govern what system resources, programs, and data files it can access, and what it is permitted to do with them. The execution behavior of a process is demonstrated by the operations it performs while running, the manner in which those operations execute, and the system resources it uses while executing. Operations include computations; transactions with files, devices, and other processes; and communications with processes on other systems via your network. User activities include login/logout, authentication and other identification transactions, the processes they execute, and the files they access.

If you are reviewing system activities on a host other than the one being monitored, ensure that the connection between them is secure, as described in Section 2.13

You need to verify that your systems are behaving as expected and that the processes executing on your systems are attributed only to authorized activities by users, administrators, and system functions. Unexpected or anomalous system performance may indicate that an intruder is using the system covertly for unauthorized purposes. The intruder may be attempting to attack other systems within (or external to) your network, or running network sniffer programs. A process that exhibits unexpected behavior may indicate that an intrusion has occurred. Intruders may have disrupted the execution of a program or service, causing it either to fail or to operate in a way other than the user or administrator intended. For example, if intruders successfully disrupt the execution of access-control processes running on a firewall system, they may access your organization's internal network in ways that would normally be blocked by the firewall.

If you permit access to your systems and networks by third parties (vendors, contractors, suppliers, partners, customers, etc.), you must monitor their access to ensure that all their actions are authentic and authorized. This step includes monitoring and inspecting their system activities.

6.4.1 Notify Users

Inform authorized users of your systems about the scope and kinds of monitoring you will be doing and the consequences of unauthorized behavior.

A common method for communicating this message is to present a banner message immediately before user login, as described in Section 6.3.1.

Without the presentation of a banner message or other warning, you probably cannot use log files and other collected data in any action you may choose to take against a user.

6.4.2 Review System Alerts

Review and investigate notifications from system-specific alert mechanisms (such as e-mail, voice mail, or pager messages), including the following:

- Users and other administrators, via e-mail or in person
- Operating system alert mechanisms
- System management software traps
- Intrusion detection systems
- Custom alert mechanisms from service or application programs (including tools)

6.4.3 Review System Error Reports

These types of notifications are typically produced by the following devices:

- Operating system error-reporting mechanisms
- Log file filtering tools
- Vendor or custom-developed management software
- Custom error-reporting mechanisms from service or application programs (including tools)

Often an administrator will be able to configure error reporting at a number of criticality, severity, or priority levels when installing the system, service and application programs, and supporting tools.

6.4.4 Review System Performance Statistics

Statistics are generally produced by vendor or custom performance-monitoring tools. Typical statistics include the following (refer to Section 5.3, Table 5.2):

- Total resource use over time—CPU, memory (used, free), disk (used, free)
- Status reported by systems and hardware devices such as print queues
- Changes in system status, including shutdowns and restarts
- File system status (where mounted, free space by partition, open files, biggest file) over time and at specific times
- File system warnings (low free space, too many open files, file exceeding allocated size)
- Disk counters (input/output, queue lengths) over time and at specific times
- Hardware availability (modems, network interface cards, memory)
- Performance statistics meaningful for a specific server or host[4]
- Comparison of previous system performance statistics with current statistics

Unexpected shutdowns, reboots, and restarts can indicate the presence of a Trojan horse program that requires a shutdown or restart of a system or service.

Investigate anything that appears anomalous.

---

4. For example, for a web server, these statistics include pages accessed, connection statistics, user requests over time, which pages are most requested, and who is requesting the pages.

6.4.5 Monitor Process Activity and Behavior

The examination of processes is complex, time-consuming, and resource-intensive. The degree to which you are able to identify suspicious processes depends on your knowledge of what processes you normally expect to be executing on a given system and how they should behave.

Due to the large number of processes and their rapidly changing natures, it is impractical for you to monitor them continually yourself. In addition, the amount and value of information that you can gather from a snapshot of currently executing processes may be very limited. This means that you must employ a variety of information-gathering and monitoring mechanisms to help you collect and analyze data associated with processes, and to alert you to suspicious activity.

One common approach with multi-user systems is to set up consoles (or separate terminal windows on workstations) that display the current status of processes and are updated at short intervals. Ideally, these consoles should be hard-wired to the systems for which they are displaying information. With strategic placement of these displays, you can take advantage of the experience of system administrators to notice unexpected activity that may not be picked up by your more immediate alert mechanisms.

Identify any unexpected, unusual, or suspicious process behavior and the possible implications. As a general guideline, you should look for the following:

- Missing processes
- Extra processes
- Unusual process behavior or resource utilization
- Processes that have unusual user identification associated with them

Data from log files and other data collection mechanisms will help you to analyze the process behavior, for example (refer to Section 5.3, Table 5.2):

- User executing the process
- Process start-up time, arguments, file names
- Process exit status, time duration, resources consumed
- The amount of resources used (CPU, memory, disk, time) by specific processes over time; top "x" resource-consuming processes
- System and user processes and services executing at any given time
- The means by which each process is normally initiated (administrator, other users, other programs or processes), with what authorization and privileges
- Devices used by specific processes
- Files currently open by specific processes

Look for processes that are operating in one of the following ways:

- Running at unexpected times
- Terminating prematurely
- Consuming excessive resources (wall clock time, CPU time, memory, disk), which may warn you of an impending DoS condition or the use of a network sniffer
- Password cracking, network packet sniffing or any other process not due to normal, authorized activities
- Unusually formatted in their output or arguments (for example, on UNIX systems, a process running as `./telnetd` instead of `/usr/sbin/telnetd`)
- New, unexpected, or previously disabled, possibly indicating that intruders have installed their own version of a process or service or are running IRC services, web services, FTP services, and so forth to allow them to distribute tools and files they have stolen (such as password files) to other compromised hosts.
- Being spawned by inactive user accounts using CPU resources
- A terminal process exhibiting abnormal input/output behavior
- Without a controlling terminal and executing unusual programs
- Unusually large in number

Pay close attention to the processes associated with intrusion detection and other security tools. Intruders regularly compromise these tools to gain greater leverage and information and to generate decoy alerts to distract and waste the time of system administrators.

6.4.6 Monitor User Behavior

Identify any unexpected, unusual, or suspicious user behavior and the possible implications.

Data from log files and other data collection mechanisms will help you to analyze user behavior, for example (refer to Section 5.3, Table 5.2):

- Login/logout information (location, time): successful, failed attempts, attempted logins to privileged accounts
- Login/logout information on remote access servers that appears in modem logs
- Changes in user identity
- Changes in authentication status, such as enabling privileges

- Failed attempts to access restricted information (such as password files)
- Keystroke-monitoring logs
- Violations of user quotas

Look for the following types of intrusions and intrusion attempts:

- Repeated failed login attempts, including those to privileged accounts
- Logins from unusual locations or at unusual times, including unusual or unauthorized attempts to log in via a remote access server
- Unusual attempts to change user identity
- Unusual processes run by users
- Unusual file accesses, including unauthorized attempts to access restricted files
- Users logged in for an abnormal length of time (both short and long)
- A user executing an unexpected command
- A user working from an unusual terminal

If you notice unusual activity associated with particular users, initiate supplemental data collection mechanisms to gather detailed information about their activities. Many multiuser systems provide mechanisms to audit all processes associated with a particular user. Since process accounting logs tend to generate a great deal of information rapidly, you will need to allocate sufficient resources to store the data collected. Similarly, detailed network logging of all activity associated with all the systems accessed by a specific user can be voluminous, and you will need to allocate resources accordingly. Review the newly collected data often (at least daily) and rotate files regularly to minimize the amount of information that you have to analyze at any given time (as described in Section 5.4).

6.4.7 Monitor for the Presence of Network Sniffers

One thing intruders commonly do is to gather information from the traffic on your networks to find user account names, passwords, and other information that may facilitate their ability to gain access to your systems. They do this by breaking into one system on your network and installing and executing a sniffer program. This program collects information about connections established between systems from network data packets as they arrive at or pass by the compromised system. To hide this illicit activity on compromised systems, intruders typically modify log files and replace programs that would reveal the presence of the sniffer program with Trojan horse versions. The substitute

programs appear to perform the same functions but exclude information associated with the intruders and their activities. In many documented cases of this type of intrusion, the intruders' activities went unnoticed for a considerable amount of time, during which they collected enough information to gain privileged access to several other systems.

Detecting the presence of distributed network sniffers may not be possible. Some operating systems (but not all, or even most) respond differently to an ICMP echo request when the interface is in promiscuous mode than when it is not, thus providing some indication that something is amiss. Even when this indication is present, however, the computer is under intruder control and will behave as the intruder directs. Without sophisticated analog electronic signaling techniques, it's probably impossible to detect a distributed sniffer externally.

This reality underscores the importance of using verified software to examine your systems (as described in Section 6.2) and the need to verify the integrity of your files (as described in Section 6.5). Unfortunately, intruders can use several sophisticated collections of programs to gain rapid access to systems and "set up shop" to install and execute a sniffer. In such cases the only way you may be able to catch such activity is to use verified software to examine processes on your systems for unexpected behavior (as described in Section 6.4), although this method is not effective against kernel modifications.

Processes associated with a sniffer will typically have transactions with a network interface that has been placed in promiscuous mode, as well as a file or network connection to which the information gathered from network packets is being sent. However, keep in mind that legitimate network monitors and protocol analyzers will set a network interface in promiscuous mode as well.

> Network interfaces on most systems normally operate in nonpromiscuous mode, which means that they ignore network packets not explicitly addressed to them. In promiscuous mode, no packets are ignored, that is, all packets that traverse the network segment to which the system is attached are read by its network interface and are accessible to processes executing on that system.

Refer to CERT advisory CA-1994.01, *Ongoing Network Monitoring Attacks,* at the CERT web site.

6.4.8 Run Network Mapping and Scanning Tools

The purpose of running network mapping and scanning tools is to understand what intruders who use such tools can learn about your networks and systems. We recommend carrying out this task periodically during nonbusiness hours and when you are physically present, because mapping tools can sometimes affect systems in unexpected ways. Eliminate or make invisible (if possible) any aspect of your network topology and system characteristics that you do not want to be known by intruders who use mapping tools.

6.4.9 Run Vulnerability Scanning Tools on All Systems

The purpose of running vulnerability scanning tools on all systems is to check for the presence of known vulnerabilities. We recommend running such tools periodically during nonbusiness hours and when you are physically present, because scanning tools can sometimes affect systems in unexpected ways. Eliminate all vulnerabilities identified by these tools wherever possible. Many of these can be dealt with by updating configuration file settings and installing vendor-provided patches as described in Section 2.4.

Consider using scanning tools that include password analysis as part of their vulnerability assessment. Such analysis may include the identification of weak, nonexistent, or otherwise flawed passwords, such as those that can be determined using brute force or dictionary-based attacks.

Refer to CERT vulnerability notes at the CERT web site and *How to Eliminate the Ten Most Critical Internet Security Threats: The Experts' Consensus, Version 1.25* (SANS 00) for a description of some of the more prevalent vulnerabilities.

6.4.10 Policy Considerations

Your organization's networked systems security policy should specify the following:

- The need for users to be notified that process and user activities will be monitored and state the objective of such monitoring
- The responsibilities and authority of designated systems administrators and security personnel to examine systems, processes, and user activity for unexpected behavior

- What forms of unexpected behavior users should watch for and require users to report any such behavior to their designated security officials and system administrators.
- What software and data users and administrators are permitted to install, collect, and use, with explicit procedures and conditions for doing so
- What programs users and administrators are permitted to execute and under what conditions

6.4.11 Additional Information

1. If you are reviewing system activities on a host other than the one being monitored, ensure that the connection between them is secure, as described in Section 2.13.
2. Whenever possible, analyze and correlate data collected from multiple sources, as recommended in the other practices of this chapter. Performing some level of correlation analysis during the intrusion detection process, such as determining when intrusion activity occurring in one part of your systems may be related to activity in another part, will assist you in determining the full extent of any compromise and its characteristics as described in Section 7.2.
3. Logging information produced by vulnerability patches (updated software that corrects or closes a vulnerability), if provided by the vendor and if turned on, can help identify a pattern in which an intruder exploits more than one vulnerability before gaining access. For example, a failed logged attempt to probe for an old vulnerability (produced by the vulnerability patch) could be followed by a successful probe for a new vulnerability that is not logged. The presence of the vulnerability patch logging information, along with other mechanisms such as integrity checking, could alert you to this type of intruder action.

6.5 Inspect Files and Directories for Unexpected Changes

The file systems in your network environment contain a variety of software and data files. Unexpected changes in directories and files, especially those to which access is normally restricted, may indicate an intrusion. Changes could include modifying, creating,

or deleting directories and files. What makes such changes unexpected may depend on who changed them and where, when, and how the changes were made.

Private data files and files containing mission-critical information are common targets of modification or corruption by intruders. Information about your organization that is accessible to the public or to subscribers via public networks and the Internet is also a common target. Numerous documented cases exist of prominent organizations that have had their web sites modified to include offensive content and other erroneous information.

Intruders often create, substitute, modify, and damage files on systems to which they have gained access, as described in Section 6.2 Introduction. Intruders may create new files on your systems. For example, they may install backdoor programs or tools used to gain privileged access on the system. Intruders may make use of the disk space on compromised systems to store their tools and other artifacts.

If you permit access to your systems and networks by third parties (vendors, contractors, suppliers, partners, customers, etc.), it is critical that you actively monitor their access to your systems and networks as well as any processing they do. This precaution helps ensure that all actions are authentic and authorized. Monitoring access includes examining all relevant directories and files.

6.5.1 Verify Integrity

Examine the directories and files on your system and prioritize how frequently you should check them. The more mission- or security-critical the file, the more frequently you should check it.

We recommend checking at least daily, perhaps at the start of the business day, to cover all processing done during the preceding 24 hours.

Compare the attributes and contents of files and directories to the authoritative reference (either complete copies or cryptographic checksums). Identify any files and directories whose contents or other attributes have changed, as described in Section 5.3.

Always access authoritative reference data directly from its secured, read-only media. Never transmit authoritative reference data over unsecured network connections unless you use mechanisms such as digital signatures and cryptographic checksums to verify data integrity.

6.5.2 Identify Unexpected Changes and Their Implications

Data from log files and other data collection mechanisms will help you to analyze changes to files and directories. These include the following (refer to Section 5.3, Table 5.2):

- Cryptographic checksums for all files and directories
- Lists of files, directories, attributes
- Accesses (open, create, modify, execute, delete), time, date
- Changes to sizes, contents, protections, types, locations
- Additions and deletions of files and directories
- Results of virus scanners

Also look for the following extraordinary occurrences:

- Unexpected file or directory access, creation, or deletion.
- Unexpected changes to file or directory protections or access control lists. Identifying these can aid, for example, in detecting the creation of files in user home directories that can be later used for backdoor access. Improperly set access control lists on system tools may indicate that an intruder has located and executed security tools that were installed by the authorized system administrator.
- Unexpected changes to file or directory sizes, contents, and other attributes. These may signify that a file or service has been replaced with the intruder's version, including the installation of a Trojan horse or backdoor. An intruder inadvertently enabling debugging can easily quadruple the size of a file.
- Unexpected changes to password files, such as unauthorized creation of new accounts and accounts with no passwords.
- Unexpected changes to system configuration files and other restricted and sensitive information, including firewall-filtering rules.
- Unusual or unexpected open files. These can reveal the presence of sniffer logs or programs.
- Violations of log file consistency (unexpected changes in file size, gaps in time between log records).
- The presence of viruses, backdoors, and Trojan horses detected by scanning tools, as described in Section 2.12.

Intruders can use compromised systems that support a promiscuous network interface to collect host and user authentication information that is visible on the network.

Sniffers are able to capture user keystrokes containing host, account, and password information. The presence of some sniffers can be detected by looking for Trojan horse programs, suspect processes, and unexpected modifications to files. See the discussion on network sniffers in Section 6.4.7.

6.5.3 Policy Considerations

Your organization's networked systems security policy should establish the following guidelines:

- Users should be notified that files and directories will be examined, and informed of the objective of such examinations.
- The responsibilities and authority of designated systems administrators and security personnel to examine files and directories on a regular basis for unexpected changes should be specified.
- Users should report any unexpected changes to their software and data files to system administrators or your organization's designated security point of contact.

6.5.4 Additional information

1. Some types of important files, such as log files and database tables, are expected to change frequently (perhaps several times per second). In general, the techniques described above will not be useful in distinguishing normal changes to these file types from those that might have been caused by intruders. Techniques based on transaction auditing are more useful in these cases.
2. As noted in Sections 6.3 and 6.4, whenever possible you should analyze and correlate data collected from multiple sources, as described in the other practices of this chapter. Refer to Section 7.2.

6.6 Investigate Unauthorized Hardware Attached to the Network

Unauthorized hardware may include computers connected to network segments or hubs and peripheral communication or input/output equipment such as modems, terminals, printers, and disk or tape drives.

Intruders actively attempt to circumvent network perimeter defenses. If they can gain physical access to your organization's internal network, they can install their own equipment and software. Alternatively, intruders may learn of insecure (unauthorized) equipment added by users that they can use to gain access to your organization's network. For example, users might install modems for the purpose of remote access to their office computers from home. Intruders often use automated tools to identify modems attached to public telephone lines. If the configuration of the dial-up access and the traffic through it is not secured, intruders may use such back doors to gain access to the internal network, bypassing preventive measures that may have been put in place to restrict external connections to your organization's network. They may then capture network traffic, infiltrate other systems, disrupt operations, and steal sensitive, private information.

Access to other peripheral equipment may also facilitate intrusions. Unsecured output and removable media devices, such as printers and disk drives, may give intruders the opportunity to generate copies of sensitive information that can be physically removed from your organization's premises.

In addition to periodically inspecting hardware as recommended below, you may need to conduct inspections in response to suspected intrusions. Watch for evidence of activities that indicate unusual access to your network, as described in Section 6.3.

6.6.1 Audit All Systems and Peripherals Attached to the Network Infrastructure

Periodic (for example, monthly) visits to physically examine equipment attached to the network should not be announced, so that unauthorized equipment cannot be hidden before the auditors arrive.

Using your documented hardware inventory, described in Section 5.3.12, identify any hardware that is missing, not in its designated location, unexpected, or extra.

6.6.2 Probe for Unauthorized Modems

Conduct a daily probe for unauthorized modems attached to your organization's telephone lines. You can do this using daemon dialer tools.[5] Because this process causes all dialed telephones to ring, we recommend that it be done outside normal working hours. However, even this approach will cause telephones that have been forwarded to ring.

5. Refer to the article "Sweeping Changes for Modem Security" (King 00) at *http://www.infosecuritymag.com/articles/june00/features1.shtml.*

6.6.3 Probe All Internal Network Segments to Identify Unauthorized Hardware

Examine daily (1) unauthorized devices attached to your network, (2) any new or unexpected IP or MAC addresses, and (3) any new or unexpected network ports on switches.

You can do this using public domain tools such as ARPWATCH[6] and a variety of commercial network management software packages.

Identify any hardware that is missing, not in its designated location, unexpected, or extra.

6.6.4 Look for Unexpected Routes Between the Organization's Network and External Networks

Daily, examine the network traffic logs for connections that originate outside your network and are destined for addresses outside your network. Traffic that moves in this way could indicate that an unauthorized computer is connecting to one of your hosts.

If possible, compare the network traffic logs from individual hosts/workstations with network traffic logs from the firewall host(s). Discrepancies or mismatches could indicate that traffic is being routed through unsecured connections or gateways directly to the individual host, bypassing your organization's firewalled Internet connection.

6.6.5 Policy Considerations

Your organization's networked systems security policy should do the following:

- Require the maintenance of documented hardware inventories
- Require the maintenance of a documented network topology
- Specify the authority and responsibility of designated security personnel to (1) perform physical audits of installed hardware and software and (2) establish network connections and routes
- Specify what kinds of hardware and software users are permitted to install on their workstations

---

6. Available at *ftp://ftp.ee.lbl.gov/*. ARPWATCH is only effective for hosts attached to your local area network, as external hosts are represented by your router/firewall.

6.7 Look for Signs of Unauthorized Access to Physical Resources

Although we tend to think of the information in networked computer systems as being in electronic form, we should remember that this information is held on physical media—CD-ROMs, tapes, disks, paper—that are subject to physical compromise by theft, destruction, corruption, or unauthorized duplication. To ensure the security of your network, you should also ensure the physical security of its components by periodically inspecting them for possible compromise.

In many organizations, designated personnel are responsible for the physical security of the premises. However, as a system or network administrator, you are often in a unique position to notice signs of physical access to system resources.

If a document or electronic storage medium is stolen, the confidentiality and availability of the information it contains is lost. Even if the item is recovered, you won't know the extent to which its contents have been copied and disseminated. Also, you won't know whether the information it contains has been corrupted or altered. Furthermore, if the compromised information is critical to security (e.g., user passwords, internal network addresses, or system configuration data), your entire network is potentially threatened by more damaging intrusions.

Therefore, it is just as important for you to keep track of physical resources and to promptly detect attempts at physical intrusion and access as it is for you to track and protect your electronic resources.

You may want to consider encrypting all backup and other selected electronic media in the event that your site, an offsite data storage site, or a disaster recovery site is physically compromised.

6.7.1 Check All Physical Means of Entrance or Exit

Perform this check daily, looking for signs of tampering, trespassing, or attempted trespassing. Keep in mind that intruders have many strategies for obtaining confidential or security-critical documents. For example, they may steal discarded copies of reports, console logs, system printouts, or other sensitive data. They search through trash containers or Dumpsters to find carelessly discarded physical copies. They may also attempt to steal backup or archive tapes, whose disappearance may not be noticed for some time.

6.7.2 Check Physical Resources for Signs of Tampering

Perform this check daily. For example, inspect locks or seals on hardware cabinets, review console logs, and monitor paper usage.

6.7.3 Perform a Physical Audit of All Movable Media

We recommend performing an audit weekly if possible. Ensure that write-disabled media continue to be so. Note that, as a complementary practice, you should also audit the contents of the media for electronic integrity.

6.7.4 Report All Signs of Unauthorized Physical Access

Report signs of unauthorized physical access to your organization's internal security point of contact. Such intrusion includes access to offsite data storage and disaster recovery sites.

6.7.5 Policy Considerations

Your organization's networked systems security policy should require the tagging and inventory of all physical computing resources as described in Section 5.3.12, and should specify how to respond when a physical intrusion has been detected

6.8 Review Reports of Suspicious System and Network Behavior and Events

In security-conscious organizations, users will report suspicious events and behaviors. As a system or network administrator, you should use those reports, along with information you gather, to help identify possible intrusions. When appropriate, you should also use external sources of information, such as reports from incident response teams, to help you decide whether or not you need to augment your monitoring and incident analysis efforts. Potential sources are listed in Chapter 1.

Recruiting users and external contacts to assist you in security monitoring greatly extends your ability to detect intrusions, potentially enabling you to detect intrusions of which you were previously unaware. Not only does this step increase the number of people alert to possible intrusions, but these individuals can often be more aware of the "normal" behavior of their personal computing environments than you are. Many intrusions are not discovered until someone with day-to-day experience using a particular system notices something unusual. Users are susceptible to intruder-initiated social engineering attempts (for example, to obtain passwords or to gain physical access) and need to understand how to identify and report these.

Intruders often compromise multiple systems when they attack a target site. At each compromised system, there may be telltale signs of intrusive activities that users of the system discover. Although a single user report may not be sufficient evidence of an intrusion, analysis of several reports may reveal a pattern of attack under way. By consolidating users' reports of suspicious system behaviors, you may also be able to determine the extent of the attacks against your networked systems.

Administrators from other organizations may contact you if they have reason to believe that an intrusion into their systems may involve or affect your organization. Always thoroughly investigate any reports you receive from incident response teams, such as the CERT/CC, to determine if an intrusion has in fact occurred at your site. If your network environment supports connections to external networks, it is possible that your systems may have been compromised and are serving as unwitting participants in a large-scale attack (such as a distributed DoS attack[7]) against several sites.

6.8.1 Perform "Triage" upon Receipt of a Report

Immediately gather as much information as necessary to make an initial assessment of whether there has been a probable intrusion and if so how severe it seems to be. You may need to make direct contact with the user to get a description of what was observed. Also acquire any records or data from logging, monitoring, or other data collection mechanisms that illustrate the problem. If the information clearly indicates an intrusion attempt, investigate it immediately.

7. Refer to CERT advisories on this subject at the CERT web site.

A report should include the following information:

- Contact information for the individuals discovering the problem and any responsible parties involved (such as the system administrator)
- Target systems and networks and all of their characteristics, such as operating system versions and IP addresses
- The purpose of the systems under attack, including the types of services and applications they provide, as well as an indication of the importance or criticality of the system
- Any evidence of intrusion, including methods of attacks used, vulnerability exploited, source IP address of attacker, and network contact information for this address
- A list of parties to notify, such as legal, other technical, management, and public relations

Refer also to the CERT tech tip *Incident Reporting Guidelines* at the CERT web site.

6.8.2 Evaluate, Correlate, and Prioritize Each Report

On a regular basis (daily, if possible), review all user and external reports. These include new reports, reports currently under investigation, and any reports that remain unresolved after investigation. Look for correlations or patterns among the reports. Prioritize and schedule investigations of all reports based on your assessment of their severity. If the suspicion proves unfounded, close the report and provide feedback to the user who reported the problem.

6.8.3 Investigate Each Report or Set of Related Reports

Based on the nature of the report, you may need to contact other users to document their observations. You may also need to verify the integrity of directories and files (as described in Section 6.5), examine your system and network logs (as described in

Sections 6.3 and 6.4), examine processes on affected systems (as described in Section 6.4), and install additional monitoring mechanisms to identify the cause of the anomalous behavior.

Document and report your findings. Regardless of the outcome of your investigation, record your findings and report them to the users who submitted the reports, the system and network administrators, the security personnel in your organization, and other appropriate individuals as specified in your organization's policies.

6.8.4 Policy Considerations

Your organization's networked systems security policy should establish the following guidelines:

- Users should immediately report any unexpected or suspicious system behavior to their designated security official and system administrator.
- Users should immediately report any physical intrusions to networked systems or offline data storage facilities to their designated security official and system administrator.
- System administrators should investigate each reported suspicious activity to determine whether it represents an intrusion.
- System administrators should notify users in advance of any changes that will be made to the systems they use, including software configurations, data storage and access, and revised procedures for using systems as a result of the changes.

6.9 Take Appropriate Actions

Upon discovering unauthorized, unexpected, or suspicious activity, you may need to (1) initiate your intrusion response procedures as described in Chapter 7 and (2) determine if the activity should be reflected in your characterization baseline, alerting, or other data collection mechanisms. Refer to Section 5.3 for information on developing a characterization baseline.

Identifying unauthorized or suspicious activities and then not taking appropriate follow-up actions will perpetuate any damage or other negative consequences. These consequences include possible loss of integrity, availability, or data confidentiality, as well as legal liability. In addition, these activities are likely to recur, placing your systems at considerable risk in the future.

6.9.1 Document Any Unusual Behavior or Activity That You Discover

Over time, you may see recurring kinds of unusual or suspicious activity. Maintaining records of these activities and noting your conclusion on their causes will help you and others to understand new occurrences more quickly and accurately.

For example, in *Network Intrusion Detection* Northcutt (99) writes:

> *To detect and classify a coordinated attack (one coming from or going to multiple locations), it helps to have a database of all traffic and techniques to complement your signatures (of known attacks). Without a database of traffic that covers a time window of at least a couple months, there is no way to determine whether this activity [that you are now investigating] has been going on and simply hasn't been detected, or whether it is a new pattern. (p. 171)*

Northcutt also recommends creating a directory to store data traces. The data traces can be examined when investigating an unknown attack pattern.

6.9.2 Investigate Each Documented Anomaly

Ask yourself the following questions:

- Is the apparent anomaly the result of a legitimate new or updated characteristic of your system? (e.g., the unexpected process is executing a recently added administrative tool)
- Can the anomaly be explained by the activities of an authorized user? (e.g., the user really was in Cairo last week and connected to the network; a legitimate user made a mistake)
- Can the anomaly be explained by known system activity? (e.g., there was a power outage that caused the system to reboot)
- Can the anomaly be explained by authorized changes to programs? (e.g., the mail log showed abnormal behavior because the system programmer made a mistake when the software was modified)
- Did someone attempt to break into your system and fail?
- Did someone break in successfully? Do you have the data that will tell you what he or she did?

6.9.3 Recognize the Iterative Nature of Analysis and Investigation

Often, you will observe an initial indication of suspicious behavior but will not have sufficient information to determine what occurred. In such cases you can take a number of steps:

- Look for past occurrences of similar behavior and study the results of that investigation.
- Formulate and ask different questions to better identify what data will best reveal what happened.
- Modify the configuration of selected data collection mechanisms to collect additional data or better filter and select from existing data (refer to Section 5.3 for further guidance).
- Add new data collection mechanisms.

6.9.4 Initiate Your Intrusion Response Procedures

If any activity or event cannot be attributed to authorized or explicable activity, initiate your intrusion response procedures immediately, as described in Chapter 7. Report such occurrences to your organization's designated security point of contact.

6.9.5 Update the Configuration of Alert Mechanisms

Updating the configuration of alert mechanisms is warranted if a previous event notification that occurred via logs, error reports, statistics reports, or another data collection mechanism is now of a sufficiently high priority.

The reverse is also true. An event that is reported as an alert all of the time may become less important and need to be changed to be captured as an error report.

6.9.6 Update All Characterization Information

Refer to Section 5.3 for a definition of typical characterization information. You need to reflect on what you learn from reviewing any unusual activity or event. This is important in four situations:

1. An unusual activity occurs frequently enough for you to consider it normal and expected, so that you should add it to an asset's characterization baseline.

2. A new activity has occurred and needs to be added to an asset's characterization baseline.
3. A previously normal or expected activity now needs to be considered suspicious or unexpected.
4. A previously normal or expected activity should be dropped from consideration for analysis altogether.

6.9.7 Update Logging and Data Collection Mechanism Configurations

Updating logging and data collection mechanism configurations is necessary to reflect information on new attack methods. Refer to Sections 5.3 (logging and data collection mechanisms) and Chapter 1 (information sources on new attack methods) for further guidance.

6.9.8 Dispose of Every Reported Event

You must somehow dispose of every reported event, either by resolution and closure, by deciding not to pursue it further unless it becomes more critical, or by taking no immediate action but preserving the event to see if it recurs or contributes to a pattern.

6.9.9 Policy Considerations

Your organization's networked systems security policy should do the following:

- Specify the actions to be taken following the discovery of unexpected, unusual, or suspicious activity
- Require the actions prescribed to be actually performed
- Specify the responsibilities and authority of designated systems administrators and security personnel to take the prescribed actions

Chapter 6 Checklist

Practice	Step Number	Step Description	Yes	Partial	No
P6.2: Ensure That the Software Used to Examine Systems Has Not Been Compromised	S6.2.1	Policy considerations			
P6.3: Monitor and Inspect Network Activities	S6.3.1	Notify users			
	S6.3.2	Review network alerts			
	S6.3.3	Review network error reports			
	S6.3.4	Review network performance			
	S6.3.5	Review network traffic			
	S6.3.6	Policy considerations			
P6.4: Monitor and Inspect System Activities	S6.4.1	Notify users			
	S6.4.2	Review system alerts			
	S6.4.3	Review system error reports			
	S6.4.4	Review system performance statistics			
	S6.4.5	Monitor process activity and behavior			
	S6.4.6	Monitor user behavior			

(*continued*)

Chapter 6 Checklist (*cont.*)

Practice	Step Number	Step Description	Yes	Partial	No
	S6.4.7	Monitor for the presence of network sniffers			
	S6.4.8	Run network mapping and scanning tools			
	S6.4.9	Run vulnerability scanning tools on all systems			
	S6.4.10	Policy considerations			
P6.5: Inspect Files and Directories for Unexpected Changes	S6.5.1	Verify integrity			
	S6.5.2	Identify unexpected changes and their implications			
	S6.5.3	Policy considerations			
P6.6: Investigate Unauthorized Hardware Attached to the Network	S6.6.1	Audit all systems and peripherals attached to the network infrastructure			
	S6.6.2	Probe for unauthorized modems			
	S6.6.3	Probe all internal network segments to identify unauthorized hardware			
	S6.6.4	Look for unexpected routes between the organization's network and external networks			
	S6.6.5	Policy considerations			

Practice	Step Number	Step Description	Yes	Partial	No
P6.7: Look for Signs of Unauthorized Access to Physical Resources	S6.7.1	Check all physical means of entrance or exit			
	S6.7.2	Check physical resources for signs of tampering			
	S6.7.3	Perform a physical audit of all movable media			
	S6.7.4	Report all signs of unauthorized physical access			
	S6.7.5	Policy considerations			
P6.8: Review Reports of Suspicious System and Network Behavior and Events	S6.8.1	Perform "triage" upon receipt of a report			
	S6.8.2	Evaluate, correlate, and prioritize each report			
	S6.8.3	Investigate each report or set of related reports			
	S6.8.4	Policy considerations			
P6.9: Take Appropriate Actions	S6.9.1	Document any unusual behavior or activity that you discover			
	S6.9.2	Investigate each documented anomaly			

(*continued*)

Chapter 6 Checklist (*cont.*)

Practice	Step Number	Step Description	Yes	Partial	No
	S6.9.3	Recognize the iterative nature of analysis and investigation			
	S6.9.4	Initiate your intrusion response procedures			
	S6.9.5	Update the configuration of alert mechanisms			
	S6.9.6	Update all characterization information			
	S6.9.7	Update logging and data collection mechanisms configurations			
	S6.9.8	Dispose of every reported event			
	S6.9.9	Policy considerations			