Appendix A. Critical Security Incident Indicators

The following tables, derived from National Institute of Standards and Technology (NIST) Special Publication 800-61: Computer Security Incident Handling Guide, list several common malicious actions that would be considered reportable Information Security Incidents and the possible indicators of such actions. Users, Service Desk, and Technical Support Teams need to be familiar with these indicators so they recognized the indicators of Security Instances and know when to report Security Incidents.

Table 1: Denial of Service Indicators

Malicious Action	Possible Indicators
Network-based DoS against a host	• Reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries
Network-based DoS against a network	• Reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system or application of a particular host	• Reports of system and application unavailability • Network and host intrusion detection alerts • Operating system or application log entries • Packets with unusual source addresses

Table 2: Malicious Code Indicators

Malicious Action	Possible Indicators
A virus that spreads through e-mail infects a host	• Antivirus software alerts of infected files • Sudden increase in the amount of e-mail being sent and received • Changes to templates for word processing documents, spreadsheets, etc.

	• Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes • If the virus achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
A worm that spreads through a vulnerable service infects a host	• Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes • If the worm achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
A Trojan horse is installed and running on a host	• Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes • If the Trojan horse achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
Malicious mobile code on a Web site is used to infect a host with a virus, worm, or Trojan horse	• Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerabilities on a host	• Unexpected dialog boxes, requesting permission to do something

	• Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the amount of e-mail being sent and received • Network connections between the host and unknown remote systems • If the mobile code achieves root-level access, see the indicators for "Root compromise of a host" listed below under Unauthorized Access Indicators
A user receives a virus hoax message	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others

Table 3: Unauthorized Access Indicators

Malicious Action	Possible Indicators
Root compromise of a host	• Existence of unauthorized security-related tools or exploits • Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems) • System configuration changes, including: o Process/service modifications or additions o Unexpected open ports o System status changes (restarts, shutdowns) o Changes to log and audit policies and data o Network interface card set to promiscuous mode (packet sniffing) o New administrative-level user account or group • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts)

Malicious Action	Possible Indicators
	• Significant changes in expected resource usage (e.g., CPU, network activity, full logs, or file systems) • User reports of system unavailability • Network and host intrusion detection alerts • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Highly unusual operating system and application log messages • Attacker contacts the organization to say that he or she has compromised a host
Unauthorized data modification (e.g., Web server defacement)	• Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification (e.g., defaced Web site) • Modifications to critical files (e.g., Web pages) • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems)
Unauthorized usage of standard user account	• Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools
Physical intruder	• User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host)
Unauthorized data access (e.g., database of customer information, password files)	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files

Table 4: Inappropriate Usage Indicators

Inappropriate Action	Possible Indicators
Unauthorized service usage	• Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host • New files or directories with unusual names • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, e-mail servers)
Access to inappropriate materials (e.g., downloading pornography, sending spam)	• Network intrusion detection alerts • User reports • Application log entries (e.g., Web proxies, FTP servers, e-mail servers) • Inappropriate files on workstations, servers, or removable
Attack against external party	• Network intrusion detection alerts • Outside party reports • Network, host, and application log entries

Appendix B: Handling a Breach of Protected Personal Identity Data

1. All suspected or confirmed breaches of protected personal information must be reported as security incidents to the service desk and classified as Critical Incidents.

2. The CISO must be assigned of all tickets that include suspected or confirmed breaches of protected personal information to determine the severity and what immediate actions are required such as who needs to be contacted to contain the incident and what evidence needs to be preserved.

3. The CISO (and External Privacy and Forensics Team if it is determined they are needed) must oversee additional forensics analysis to gather as much information as possible about what happened, being sure to properly protect evidence.

4. If after analysis the CISO has definitive evidence that the protected data was not breached, then no further special action is required and normal incident response procedures may continue. However, the security of this system and the need to store protected data on it should be carefully assessed.

5. If the analysis shows there is a possibility that protected data involving personal identity information was breached, the CIRT must do a closer review of the evidence and determine if a breach of protected personal identity data occurred or is "reasonably likely" to have occurred (wording of the state notification law).

6. If the CIRT determines that personal identities are not at risk, no further special action is required and normal incident management procedures may continue.

7. If the CIRT determines that personal identities are at risk, the primary CIRT and selected members of the secondary CIRT (e.g. The Attorney's Office, St Paul Police Department representative, Public Information Officer(s) etc.) oversees the response, addressing the following issues:

    - Determine if the affected individuals need to be notified and the appropriate method for notification
    - Determine who will draft and sign the notification (see Appendix C for sample notification letter)
    - Assign someone to collect victim mailing addresses and to distribute notifications
    - Determine the point of contact for inquiries from the victims, media, and other interested parties and the type of assistance to offer. In determining the type of assistance appropriate to the situation, consider assistance such as:
        - Providing personal assistance in getting free credit protection, if appropriate
        - Establishing a toll-free phone number for victims to call for assistance, and/or
        - Establishing an informational website.

- Determine the need for a news release and timing in relation to the communication with victims. The news release must be drafted by a representative from appropriate Public Information Officer(s) or designee and reviewed by the CIRT.
- Discuss how the incident could have been prevented and steps to take to prevent similar incidents in the future

8. If potential victims do need to be notified, the CIO or designee(s) should notify the following people as quickly as possible:
    - Mayor's Office
    - Attorney's Office
    - The Department Director of the Department responsible for the business data. (e.g. If the data was from the Police Records Management System – RMS then notification would include the Chief of Police.)

9. Deciding Whether to Notify Victims

    If protected data resides on a compromised computer, it is not always obvious whether the data were accessed and therefore whether potential victims need to be notified, especially in light of Minnesota law that requires notification if "misuse of the information has occurred or is reasonably likely to have occurred. The following questions should be considered when deciding whether protected data was breached:

    - Is the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information?
    - Is there evidence that information has been downloaded, copied, or otherwise accessed, for example: an ftp log that contains the name of a file containing notice triggering information?
    - Was a privileged (e.g. root or administrator) or non-privileged account, one with access to privileged information, compromised?
    - Was on system or multiple systems compromised?
    - Is the identity of the attacker known or unknown? If known was the attacker a disgruntled insider or an unaffiliated third party? Were multiple attackers involved?
    - Are there indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported?
    - Did the unauthorized person have access to the information for an extended period of time?
    - What was the time between compromise start and compromise discovery?
    - Did the compromise indicate a directed attack, such as a pattern showing the machine itself was targeted versus an automated attack?
    - Did the attack appear to seek and collect the information?

- Did the attack appear to include tampering with records (e.g., changing grades)?
- Did the attacker attempt to cover up their activity?
- Did the attacker release information about the nature or scope of the attack?
- Was the information encrypted and would the encryption method effectively prevent the information from being accessed.
- What is the potential damage to individuals if notification is not given?
- What is the potential damage to institutional credibility in the case of notification?
- What is the potential damage to institutional credibility in the case of failure to notify?

10. Incident Tracking and Reports

- The Scribe must take notes and record the incident as defined in the OTC Incident Management Process.
- The incident report for this type of incident is considered protected and should therefore be encrypted when stored or transmitted and disclosed only to authorized individuals. The protectivity of reports derived from the incident tracking data must be determined on a case-by-case basis by the CISO and/or the CIO.

Appendix C: Critical Security Incident Communication Guides

Audience	Communication Objectives
Employees	It is critical to ensure that employees are aware of the appropriate information to limit rumors. The communication should originate from a trusted and knowledgeable source with a description of important details and a clear indication of when recipients can expect follow-up communications. The source of the email will act as a single point of contact, which is enforced by "do not forward" instructions.
Customers	Explain the situation, the type of personal data that might have been exposed, the City's response to handling this incident and preventing future occurrences, and how the customer can contact the City for more information. CIRT, Communications and Legal teams should partner to create the customer notification letter in accordance with applicable laws and regulations.
Media	Since communication departments are usually responsible for handling interactions with the media, they must be part of the CIRT. A proactive statement should be preapproved to be released as soon as possible in situations where details of the incident cannot be immediately announced. **Checklist for Communicating with Media** • Always protect the City's integrity and reputation • Do not wait until the information is complete before sharing with the Communications team • Designate a point person from the Incident Response Team to work with the Communications team on crafting media announcements • Maintain a preapproved proactive statement –such as "We are aware of the developing situation and are currently gathering facts" –which can be shared immediately with media • Fully analyze the situation before releasing reports and understand what kind of information may be breached • Provide the media with comprehensive, accurate, and pertinent information • Perform an act of goodwill during or immediately after a crisis when appropriate and possible • Set up a communication mechanism that can be activated in almost any emergency situation • Communicate quickly and positively to focus attention on the most important aspects of the problem • Make amends to those affected by the incident and complete necessary actions to restore City reputation in the community • Consider any relevant legal, ethical, and organizational ramifications during press releases or other communications about the incident
Authorities	Certain circumstances require authorities and law enforcement to become notified of or involved in responding to an incident. The CIRT must know what those circumstances are and what information to provide.

- **Sample Press Release**

City officials announced that a security breach of the City's network resources has been detected. Immediate steps have been taken to stop the breach and an investigation is currently underway. As this is an ongoing investigation, limited information can be shared.

However, departments currently affected by the breach include _____. Those who are potentially affected have been (or are in the process of being) notified. More details will be released as the in-depth investigation continues.

The (database, server, workstation) contained some personal information of City e (employees, City citizens), although no (health care data, social security numbers) are known to have been compromised. City security personnel discovered that the attack occurred between (date/time) and (date/time).

City officials believe that this breach creates a (low, medium, high) risk to the City's (employees, constituents), but wanted to alert those who may potentially be affected. Security and network personnel have isolated the breach, and will continue to investigate this attack and work with law enforcement.

Affected individuals may call (1-800-XXX-XXX) for more information. In addition, the City will provide updates of the security breach and response at the www.xxx.xxx website

- **Sample City Personnel Security Alert**

A Severe Security Incident Has Occurred

To all personnel,

OTC identified a security breach/attack beginning on _____ (date) _____ and are currently responding to and investigating the breach. OTC has notified the appropriate departments and authorities and will notify media to help disseminate information when necessary.

Please be aware of the incident and stay alert for indications of the attack. We ask that you notify your management if you identify any suspicious activity.

To ensure that timely and accurate information is made available to the media and public, OTC management will coordinate the City response. Should you be notified by media, please inform your supervisor. Giving out unauthorized information could jeopardize work on fixing the breach as well as the ongoing investigation.

Please do NOT send any information about the breach electronically unless specifically asked to do so or unless secure communications are available.

For more information, please contact your management.

- **Resident Template for Social Security Number (SSN) Exposure**

  Date

  Dear:

  We are writing to you because of a recent computer security incident at the City of St Paul.

  [Describe what happened in general terms, what kind of PII was involved, and what you are doing in response.]

  To protect yourself from the possibility of identity theft, we recommend that you complete a Federal Trade Commission (FTC) ID Threat, located on their web site at http://www.consumer.ftc.gov/features/feature-0014-identity-theft. This will allow you to notify your creditors legally that your identity may have been compromised.

  You are encouraged to contact the St Paul City Attorney's Office, 15 Kellogg Blvd. West, 400 City Hall, Saint Paul, MN 55102. Their web site is located at www.stpaul.gov/departments/city-attorney, and their phone number is 651-266-8710

  We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts. You should receive letters from them, with instructions on how to get a free copy of your credit report.

  Equifax Experian TransUnion
  1-800-525-6285 1-888-397-3742 1-800-680-7289

  Please review your credit reports carefully when you receive them. Look for accounts you did not open, for inquiries from creditors that you did not initiate, and for personally identifiable information, such as home address or Social Security Number, that is not accurate.

  If there is anything you do not understand, call the credit-reporting department at the telephone number on your report. If you do find suspicious activity on your credit reports, you need to call your local police or sheriff's office to file a police report of identity theft. [Alternatively, if appropriate, give contact information for law enforcement department investigating the incident.] We suggest you get a copy of the police report, as it may be helpful in clearing up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you continue to check your credit report every three months for the next year. Call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you call FTC toll free at (877) 438-4338 and/or visit their Identity Theft Web Site at http://www.consumer.gov/idtheft/.

Should you have further questions or need additional information, please call us anytime at our toll-free number, _____.

Sincerely,

Appendix E: Identifying Anomalies within the Windows Environment[2]

This appendix is intended to provide some useful commands and areas to look for anomalous behavior within the Windows environment. To look for unusual processes and services use the following commands

a. taskmgr.exe – it displays running processes and services.

b. In command prompt use these three commands:

   i. tasklist – it displays a list of running services along with their corresponding PID (process ID), session name, session number, and memory usage. Getting a PID can be useful for using the taskkill command to end the questionable process.

   ii. wmic process list full – is a windows management interface control that will display all processes, along with detailed information such as their executable path and much more.

   iii. tasklist /svc – will display a list of all processes along with their corresponding PID, and services that are tied to them.

c. To look for unusual files and registry keys use the Windows search feature and look for files larger than 10MB, and use regedit to look for unusual entries in the following areas:

   HKLM\Software\Microsoft\Windows\CurrentVersion\Run

   HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce

   HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

   Generally, those three registry entries will contain startup configurations for specific programs, including malware.

d. To look for unusual network usage the following Windows commands in the command line interface (cmd) provides an excellent view of network activity on a system:

   i. net view \\127.0.0.1 (or localhost) – displays shared folders that are on the system. If there are shared folders that are not supposed to be there that can be a significant red flag.

   ii. inet session – displays open sessions with other systems on the network. This is useful for detecting communications with other systems on the network and determines whether the connections are legitimate. A good example: is an https connection to a rogue server on the internet and heavy bandwidth usage from the compromised computer in question with that rogue server.

   iii. inbstat –S will display NetBIOS activity over TCP/IP on the various network interfaces that a machine in question may have.

   iv. netstat and its various flags (e.g. netstat –na, netstat –nao, etc) provides a tremendous amount of information between listening and established TCP/IP

[2] http://sans.org/resources/winsacheatsheet.pdf

connections, along with their ports and whether the protocol used is TCP or UDP. This is useful for determining unusual traffic patterns on the computer in question.

e. To look for unusual start up (or scheduled) tasks, use the following commands:
    i. msconfig –displays all startup configurations from services to files in the startup folder, etc. This is also useful for disabling anything trying startup during Windows login or boot-up, and to troubleshoot problems that are caused by nefarious or poorly written programs.
    ii. schtasks – displays tasks schedule to run at specific times. This is useful for not only troubleshooting problems, but also looking for would be logic bombs.
    iii. wmic startup list full – displays all the services and programs that startup when Windows boots and/or upon Windows login.

f. To look for unusual accounts use the following three commands:
    i. lusrmgr.msc – this command is only useful for looking for local accounts on a machine. Two account types to specifically look for are Administrator accounts that are not supposed to be on the machine and active Guest accounts, as those can lead to serious security compromises.
    ii. net user (in command prompt) – displays all user accounts on a local machine.
    iii. net localgroup administrators – display all local administrator user accounts. This is useful for finding administrator accounts that do not belong on a particular machine.

g. The final and most crucial area to look for unusual behavior is within event viewer. It displays all the event log content that Windows actively records. The command for it to type in the run command box is eventvwr.msc.
    i. Look for warnings, errors, and other events (e.g. system reboots during usual times, etc.).
    ii. If the log files are missing, it is a reliable indicator that the machine has been or is compromised and the intruder is trying to hide his\her tracks.

Appendix F: Identifying Anomalies within the UNIX Environment[3]

This appendix is intended to provide some useful commands and areas to look for anomalous behavior within the UNIX environment

a. To look for unusual processes and services use the following commands:
    i. ps -aux – displays running processes along with their process-id (PID), associated user-ids (UID #), name, and other pertinent information. Pay particular attention to any process that is using the UID 0 user-id, because those processes are running with root permissions.
    ii. ps –ef – displays the full listing of all processes and can be useful for finding undesirable processes that are running.
    iii. lsof –p (PID) – displays a specific process in more detail, by displaying the files and ports associated with that process. This is appropriate for examining any Trojan, worms, and other network based malware on a UNIX system.
    iv. lsof +L1 – displays processes running from or accessing files that have been unlinked; basically, it will show one to figure out if the attacker is hiding data or running a backdoor.

b. To look for unusual files the "find" command along with its various flags allows one to search a UNIX system for malware. A few examples are listed below:
    i. find / -uid 0 -perm -4000 –print – searches for files that have root permissions.
    ii. find / -size +50000k –print – searches for files of a specified or greater size.
    iii. This is particularly useful for searching for files that may not belong on the
    iv. system, like movies, games, et al.

c. To look for unusual network usage coming from a system's network interface type in the following command: ip link | grep PROMISC – this command will display any network interfaces that are running in promiscuous mode, which can be a clear indication of an attacker running a packet sniffer.

d. Other useful commands to observe unusual network behavior are:
    i. netstat –nap – this displays listening ports and in turn can be useful for finding backdoors.
    ii. arp –a – displays all MAC to IP address mappings of the system and can be useful for finding addresses of systems that are not part of the network (e.g. a rouge wireless access point that allows one to gain access into the internal network from the outside).

e. To look for scheduled jobs (i.e. tasks) by root or any other user, type in the following command: contrab –u root –l – this is useful for detecting logic bombs, schedule connections to unknown hosts, and other potentially nefarious issues

[3] http://sans.org/resources/linsacheatsheet.pdf

i. Two additional commands to display system-wide cron jobs are:

   a. cat /etc/crontab – displays all jobs scheduled within the cron table.

   b. ls etc/cron.* - lists files within the cron subdirectories.

f. To look for unusual accounts use the following commands to check the following files:

   i. sort –nk3 –t: /etc/paswd | less – displays all accounts sorted by UID (e.g. UID0, etc), this is useful for finding accounts with root permissions or accounts that do not belong on the system.

   ii. egrep ':0:' /etc/passwd – displays only accounts with root permissions.

   iii. getent passwd | grep ':0:' – same as above, except for systems with multiple authentication mechanisms.

   iv. find / -nouser –print – searches the entire system for orphaned files that may have been deleted by an attacker's temporary account.

g. The best place to check for unusual system activity is the log files, especially in UNIX. Most log files are located in /var/log (or var/logs), or var/messages. A good command to use for viewing log files is: more –f /var/log/messages – this allows a page by page review of all logged events. Pay particular attention to user authentication logins and any unusual patterns such as missing entries and times that may indicate an intruder is trying to hide his/her tracks.

h. Other commands to check for possible clues are:

   i. uptime – displays how long a system has been up and running. If the system's uptime is shorter or longer than it should be, then it could be a clear indication that something has changed and therefore may need further review.

   ii. free – is useful for checking how much ram is used. This is useful for detecting processes that are using a lot of memory (e.g. an attacker searching or modifying a database, etc.).

   iii. idf – is useful for checking available disk space. This can provide a reliable indication as to whether an attacker is installing malware or removing files from a system.

Appendix G: Security Incident Cheat Sheet for Server Administrators[4]

Tips for examining a suspect system to decide whether to escalate for formal incident response.

Assessing the Suspicious Situation
To retain attacker's footprints, avoid taking actions that access many files or installing tools.
Look at system, security, and application logs for unusual events.
Look at network configuration details and connections; note anomalous settings, sessions or ports.
Look at the list of users for accounts that do not belong or should have been disabled.
Look at a listing of running processes or scheduled jobs for those that do not belong there.
Look for unusual programs configured to run automatically at system's start time.
Check ARP and DNS settings; look at contents of the hosts file for entries that do not belong there.
Look for unusual files and verify integrity of OS and application files.
Use a network sniffer, if present on the system or available externally, to observe for unusual activity.
A rootkit might conceal the compromise from tools; trust your instincts if the system just doesn't feel right.
Examine recently-reported problems, intrusion detection and related alerts for the system.

If You Believe a Compromise is Likely...
Involve an incident response specialist for next steps, and notify your manager.
Do not panic or let others rush you; concentrate to avoid making careless mistakes.
If stopping an on-going attack, unplug the system from the network; do not reboot or power down.
Take thorough notes to track what you observed, when, and under what circumstances.
Take thorough notes to track what you observed, when, and under what circumstances.

Windows Initial System Examination		Unix Initial System Examination	
Look at event logs	eventvwr	Look at event log files in directories (locations vary)	/var/log, /var/adm, /var/spool
Examine network configuration	arp –a, netstat –nr	List recent security events	wtmp, who, last, lastlog

[4] http://sans.org/score/checklists

List network connections and related details	netstat –nao, netstat –vb, net session, net use	Examine network configuration	arp –an, route print
List users and groups	lusrmgr, net users, net localgroup administrators, net group administrators	List network connections and related details	netstat –nap (Linux), netstat –na (Solaris), lsof –i
Look at scheduled jobs	schtasks	List users	more /etc/passwd
Look at auto-start programs	msconfig	Look at scheduled jobs	more /etc/crontab, ls /etc/cron.*, ls /var/at/jobs
List processes	taskmgr, wmic process list full	Check DNS settings and the hosts file	more /etc/resolv.conf, more /etc/hosts
List services	net start, tasklist /svc	Verify integrity of installed packages (affects lots of files!)	rpm -Va (Linux), pkgchk (Solaris)
		Look at auto-start services	chkconfig --list (Linux), ls /etc/rc*.d (Solaris), smf (Solaris 10+)
Check DNS settings and the hosts file	ipconfig /all, ipconfig /displaydns, more %SystemRoot%\System32\Drivers\etc\hosts	List processes	ps aux (Linux, BSD), ps -ef (Solaris), lsof +L1
Verify integrity of OS files (affects lots of files!)	sigverif	Find recently-modified files (affects lots of files!)	ls –lat /, find / -mtime -2d -ls
Research recently-modified files (affects lots of files!)	dir /a/o-d/p %SystemRoot%\System32	Verify integrity of installed packages (affects lots of files!)	rpm -Va (Linux), pkgchk (Solaris)
Avoid using Windows Explorer, as it modifies useful file system details; use command-line.		Look at auto-start services	

Incident Response Communications
Do not share incident details with people outside the team responding to the incident.
Avoid sending sensitive data over email or instant messenger without encryption.
If you suspect the network was compromised, communicate out-of-band, e.g. non-VoIP phones.

Key Incident Response Steps
Preparation: Gather and learn the necessary tools, become familiar with your environment.
Identification: Detect the incident, determine its scope, and involve the appropriate parties.
Containment: Contain the incident to minimize its effect on neighboring IT resources.
Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.
Recovery: Restore the system to normal operations, possibly via reinstall or backup.
Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.