SECURITY INCIDENT SURVEY CHEAT SHEET FOR SERVER ADMINISTRATORS

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.

Windows Initial System Examination

Look at event logs	`eventvwr`
Examine network configuration	`arp –a,` `netstat –nr`
List network connections and related details	`netstat –nao,` `netstat –vb,` `net session, net use`
List users and groups	`lusrmgr, net users,` `net localgroup administrators,` `net group administrators`
Look at scheduled jobs	`schtasks`
Look at auto-start programs	`msconfig`
List processes	`taskmgr,` `wmic process list full`
List services	`net start,` `tasklist /svc`
Check DNS settings and the hosts file	`ipconfig /all,` `ipconfig /displaydns,` `more %SystemRoot%\ ⏎` `System32\Drivers\etc\hosts`
Verify integrity of OS files (affects lots of files!)	`sigverif`
Research recently-modified files (affects lots of files!)	`dir /a/o-d/p ⏎` `%SystemRoot%\ ⏎` `System32`

Avoid using Windows Explorer, as it modifies useful file system details; use command-line.

Unix Initial System Examination

Look at event log files in directories (locations vary)	`/var/log,` `/var/adm,` `/var/spool`
List recent security events	`wtmp, who,` `last, lastlog`
Examine network configuration	`arp –an,` `route print`
List network connections and related details	`netstat –nap (Linux),` `netstat –na (Solaris),` `lsof -i`
List users	`more /etc/passwd`
Look at scheduled jobs	`more /etc/crontab,` `ls /etc/cron.*,` `ls /var/at/jobs`
Check DNS settings and the hosts file	`more /etc/resolv.conf,` `more /etc/hosts`
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+)`
List processes	`ps aux (Linux, BSD),` `ps -ef (Solaris),` `lsof +L1`
Find recently-modified files (affects lots of files!)	`ls –lat /,` `find / -mtime -2d -ls`

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

1. Preparation: Gather and learn the necessary tools, become familiar with your environment.

2. Identification: Detect the incident, determine its scope, and involve the appropriate parties.

3. Containment: Contain the incident to minimize its effect on neighboring IT resources.

4. Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.

5. Recovery: Restore the system to normal operations, possibly via reinstall or backup.

6. Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.

Other Incident Response Resources

Windows Intrusion Discovery Cheat Sheet
http://sans.org/resources/winsacheatsheet.pdf

Checking Windows for Signs of Compromise
http://www.ucl.ac.uk/cert/win_intrusion.pdf

Linux Intrusion Discovery Cheat Sheet
http://sans.org/resources/linsacheatsheet.pdf

Checking Unix/Linux for Signs of Compromise
http://www.ucl.ac.uk/cert/nix_intrusion.pdf