



How do you know if your system is being attacked?

Signs your enterprise computing system may have been compromised include:

Performance Symptoms

- Exceptionally slow network activity.
- Poor system performance - System appears to be slower than normal and less responsive than expected. (Note: Unexplained disk activity might be due to disk-related system maintenance such as disk file clean-up while the system is idle, this is completely normal).
- Unusual usage times (statistically, more security incidents occur during non-working hours than at any other time).
- System crashes.
- Abnormal disconnection from network service.
- Unusual network traffic.
- An indicated last time of usage of an account that does not correspond to the actual last time of usage for that account.
- High system activity when no users are logged on, especially during off-peak usage hours.

Access Symptoms.

- A system alarm(s) or similar indication(s) from your intrusion detection tool(s).
- Suspicious entries in system or network accounting (e.g., a UNIX user obtains privileged access without using authorized methods).

- Unsuccessful logon attempts.
- Unusually large number of logon attempts.
- Port scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts).
- Unusual log entries such as network connections to unfamiliar machines or services, login failures.
- Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console

Other Symptoms.

- New files of unknown origin and function.
- New software of unknown origin and function.
- Unexplained changes or attempts to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files.
- Unexplained addition, deletion, or modification of data.
- Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords.
- Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program).
- New user accounts of unknown origin.

Things NOT to Do

Things that you should not do if your system is being attacked:

If you think that your system has been compromised, there are a number of things that you should not do. These are:

- DO NOT disconnect the machine from the network. This will allow the Information Security Office to thoroughly investigate the attack as it occurs and collect real-time data to be used against the attacker.
- DO NOT turn the machine off or reboot unless instructed to do so by a team member. It is possible that the processes left by an attacker may not get restarted after rebooting, which may make it more difficult for a network security specialist to determine the root cause of the problem.

- DO NOT launch a return attack on a suspected source as most of the real attacks spoof their identity. Return attacks cause damage and inconvenience to innocent systems that share network or system resources with the system being attacked.
- DO NOT get into any exchange with the “suspected attacker”, as the actual identity is often purposefully obscured and spoofed, your response may abuse an innocent third party.

Things to Do

- DO report it to your Network Security Officer.
- Preserve and document the incident and all audit trails.
- Follow your incident response (IR) plan (Hopefully you had the forethought to establish an Incident Response plan).
- Check with internal security team to see if you are you required by law or mandate to report this breach of security.

COMMON Sense

- You need to have a "very formal" and “functional” set of policies and procedures and make those policies a part of every new employee's orientation.
- Proactively monitor and track all network activity via a series of detection and auditing packages.
- Carry out regularly scheduled network assessments and network audits.
- Maintain strict password controls.
- Establish a demilitarized zone for your World Wide Web servers to effectively isolate the corporate networks from the Internet.

"There is no such thing as being too alert - thoroughly test and assess your network at least once every 12 months".