Windows tools for investigating an attack

By Michael Cobb

- Run event viewer to look at logs:
  C:\> eventvwr.msc

- Look for suspicious events:
  “Event log service was stopped.”
  “Windows File Protection is not active on this system.”
  “The MS Telnet Service has started successfully.”

- Look for a large number of failed logon attempts or locked out accounts.

- Look at file shares, and make sure each has a defined business purpose:
  C:\> net view 127.0.0.1

- Look at who has an open session with the machine:
  C:\> net session

- Look at which sessions the machine has opened with other systems:
  C:\> net use

- Look at NetBIOS over TCP/IP activity:
  C:\> nbtstat –S

- Look for unusual listening TCP and UDP ports:
  C:\> netstat –na

- Look for unusual scheduled tasks on the local host, especially those that run as a user in the Administrators group, as SYSTEM, or with a blank user name by running:
  C:\> at

- Look for new, unexpected accounts in the Administrators group:
  C:\> lusrmgr.msc

- Look for unusual/unexpected processes:
  Run Task Manager

- Look for unusual network services:
  C:\> net start

- Check file space usage to look for sudden major decreases in free space:
  C:\> dir