

Proposed Pilot Questions to Answer

Version 0.81

Security related

1. What workstations that I don't manage use my DNS hosts as name servers?
2. Is someone mounting a man-in-the-middle attack on my mail services?
3. Is someone mounting an attack on my web services?
4. What networks are trying to gain access to my mail servers?
5. Who is probing my network for services that violate my security policy?
6. What users are accessing the fileserver X after working hours?
7. Who tried to su as root on all my web servers between the hours of 3 and 4 am?
8. Who had unsuccessful login attempts on the file servers on Friday the 23rd from hosts that are on the San Francisco network?
9. What hosts are violating my external firewall policy?
10. Snort is showing that a vulnerable Web page is being requested from a hacker outside my network. Did any Web server inside my network respond to that compromised page?

Configuration related

1. If I change the configuration to my router by adding an access filter to restrict the ccBay application to subnet 10.1.2.0/255.255.255.0, what workstations will be affected?
2. Is the new configuration of the firewall actually working as expected?
3. I want to find out if anyone besides Joe and Linda have successfully logged into the host ns6 after it was reconfigured for tightened security.
4. What hosts can access the ns7 fileserver outside the San Francisco network?
5. Has anonymous ftp been removed from our UNIX hosts?
6. Has any "guest" user tried to login since they have been removed from all of the fileservers?
7. Was TCP wrappers configured correctly so that telnet is restricted only between hosts on our entire network?
8. Are the workstations in the Boston office using printers other than on host cmu4?
9. Has the switch been configured so that the VLAN's are isolating packets correctly?
10. Have the browsers that were just installed on all the corporate workstations in Boston been configured correctly to use the new proxy server?
11. Is the new VPN software on all the remote office's workstations using the new firewall?

Network related

1. What workstations are using the secondary router when they shouldn't be?
2. What routers are running RIP on my network?
3. Who is running a web server on network 10.2.3.0?
4. What time did the SYN attack happen?
5. Is my NETBIOS traffic contained on my internal networks?

6. Who is ARPing the most on the Boston subnet?
7. What is the average Kbytes/sec flow of the San Francisco border router between midnight and 6 am?
8. Which external networks have accessed my mail servers?

Host related

1. Who logged into host cmu3 on Wednesday?
2. Has the mouse plugged into workstation cmu2?
3. What system errors occurred on the Windows file servers yesterday between 13:00 and 14:00?
4. Are the mail servers getting any errors?
5. What host is trying to do zone transfers to our primary DNS servers from our internal networks?
6. What web access violations have occurred on the WIN2K web servers?
7. The "named" process on host ns6 is running as what user?

Application related

1. Who sent mail to the ibm.com domain on the 26th of December??
2. Am I getting any HTTP errors on the web servers after the new code was released?
3. Who is accessing the MSSQL db between 2:00 and 4:00 today?
4. Who is using AOL AIM on my internal networks?
5. Is bind having any errors on ns6?
6. Who has accessed the www.weatherunderground.com web site on the Boston subnet?
7. How long did the backup run between hosts cmu4 and cmu7?
8. What subnets are accessing the ccBay application on subnets other than the San Francisco offices?
9. What workstations are using NAPSTER on my networks and what bandwidth are they using between normal working hours?
10. A student just called from home, saying she got "permission denied" on the web site for the distance class she's in. What's wrong?