**OS Hardening (Red hat / CentOS)**

|  |  |
| --- | --- |
| Hardening Step | Check |
| Step 1：Disable root SSH login。 sudo vi /etc/ssh/sshd\_config … | □ |
| Step 2：Remove unnecessary services。 yum remove postfix  … | □ |
| Step 3：Disable default users。 userdel postfix  userdel games  userdel ftp  … | □ |
| Step 4：Password complexity Setting  At least 7 characters and contain both numeric and alphabetic characters.  Change passwords at least once every 90 days  New password that is the NOT the same as any of the last four passwords has used.  … vim /etc/pam.d/system-auth  password requisite pam\_cracklib.so retry=6 minlen=7 ucredit=-1 lcredit=-1 dcredit=-1  password sufficient pam\_unix.so sha512 shadow nullok try\_first\_pass use\_authtok remember=4  … | □ |
| Step 5：Account lock setting  1． Accounts be locked out after not more than six invalid logon attempts. Remains locked for a minimum of 30 minutes  vim /etc/pam.d/sshd  ……  auth requiredpam\_tally2.so deny=6 unlock\_time=1800 | □ |
| Step 6：SSH Idel time (900 sec)。  vi /etc/ssh/sshd\_config  ………  #ClientAliveInterval 0  ClientAliveCountMax 900  #ShowPatchLevel no  UseDNS no | □ |
| Step 7：Symantec SEP (自動更新病毒碼、定期掃描)。  ./sav liveupdate –v (自動更新病毒碼)  ./sav scheduledscan –l (定期掃描) | □ |
| Step 8：NTP settng … vi /etc/ntp.conf  # Use public servers from the pool.ntp.org project.  # Please consider joining the pool ……..  restrict (IP)  server (IP) | □ |
| Step 9：執行centos-cis-benchmark script   1. gitclone   <https://github.com/massyn/centos-cis-benchmark>   1. cd centos-cis-benchmark 2. sudo bash run-cis-benchmark.sh | □ |