

File integrity monitor scheduling based on file security level classification

ABSTRACT

Integrity of operating system components must be carefully handled in order to optimize the system security. Attackers always attempt to alter or modify these related components to achieve their goals. System files are common targets by the attackers. File integrity monitoring tools are widely used to detect any malicious modification to these critical files. Two methods, off-line and on-line file integrity monitoring have their own disadvantages. This paper proposes an enhancement to the scheduling algorithm of the current file integrity monitoring approach by combining the off-line and on-line monitoring approach with dynamic inspection scheduling by performing file classification technique. Files are divided based on their security level group and integrity monitoring schedule is defined based on related groups. The initial testing result shows that our system is effective in on-line detection of file modification.

Keyword: Operating system security; Files integrity; Monitoring schedule; File security classification; Malicious modification; HIDS