TEST RESULTS FOR THE METHOD OF INFORMATION SECURITY EVENT MANAGEMENT IN LINUX-KERNEL-BASED OPERATING SYSTEMS

Nguyen H.H., student of group 567311

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Boiprav O.V. – PhD in Technical Sciences, Associate Professor, Head of the Information Security Department

Annotation. This paper presents the experimental results of an implemented method designed to manage information security events on Linux-kernel-based operating systems. These information security events encompass user logins and logouts, account management, access control management, and security management. These constitute critical security events, and their effective logging has demonstrated the feasibility of the proposed method.

Keywords. Information security, event rules, auditd tool.

To facilitate the logging of information regarding information security events within a Linux-kernel-based operating system, the Auditd tool [1] will be installed.

Auditd tool is a system event logging tool built into most Linux distributions. It allows you to configure event logging rules and save logged events to log files.

During the configuration process, the following steps were taken.

1 Performing the command sudo apt-get install auditd (Figure 1).

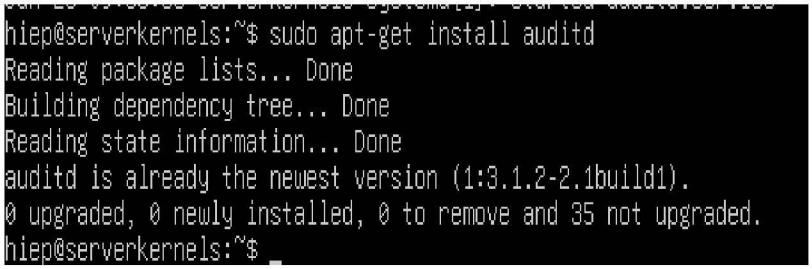

Figure 1 – Install auditd on the operating system

2 Configure Auditd by using the following command to access the configuration file: sudo nano /etc/audit/auditd.conf.

3 Creating Event Rules [2].

3.1 Login event rules: recording information about users logging into the system, including login name, IP address, login time, and login type. This constitutes a critical event for detecting intruders and preventing unauthorized access.

To configure login event rules on a Linux system, the rsyslog configuration file (/etc/rsyslog.conf) was used: sudo nano /etc/rsyslog.conf.

The following two rules were added (the two rules added to the /etc/rsyslog.conf file serve to record all logs related to authentication and security on the Linux system into two separate files): authpriv.* /var/log/auth.log, authpriv.* /var/log/secure.

3.2 Logout event rules: logging information about users logging out of the system, including the username, IP address, and logout time. The following rule was added: auth.* /var/log/auth.log.

3.3 Password change event rule: logging information indicating that a user is changing their password, including the login name, IP address, and time of the change. The following rule was added: password.* /var/log/auth.log.

Restart the rsyslog service to activate the added services using the following command: sudo systemctl restart rsyslog.

3.4 Access modification event rule [3]: logging information regarding how users change access permissions for system resources, including the username, IP address, time of modification, and access type.

To configure access modification event rules on a Linux system, the auditd configuration file (/etc/audit/rules.d/audit.rules) was used: sudo nano /etc/audit/rules.d/audit.rules.

The following rule was added: -w /etc/passwd/ -p wa -k passwd_changes, where -w /etc/sysconfig/ – is the path to the directory you wish to monitor; -p wa – specifies the type of event you wish to monitor. *w* represents a write event, and *a* represents an access modification event; -k sysconfig_changes – is a tag used to label these events.

3.5 System configuration change event rules: recording information about the user modifying the system configuration including their login name, IP address, time of modification, and the type of configuration changed. The following rule was added: -w /etc/sysconfig/ -p wa -k sysconfig_changes.

3.6 Attack event rules: recording information regarding attacks on the system including the attacker's IP address, the time of the attack, and the type of attack. The following rules were added: -a always,exit -F arch=b64 -S execve -k detect_attack; -a always,exit -F arch=b32 -S execve -k detect_attack, where -a always,exit – specifies the rule types; -F arch=b64 and -F arch=b32 – are conditions limiting the rule to 64-bit and 32-bit architectures, respectively; -S execve – is the specific event you wish to monitor.

3.7 Security event rules: recording information regarding security operations performed on the system including the username, IP address, time of execution, and the type of security operation performed. The following rules were added: -w /etc/passwd -p wa -k password_file; -w /etc/shadow -p wa -k password_file; -w /etc/sudoers -p wa -k sudoers_file.

Restart the auditd service to activate the added services using the following command: sudo systemctl restart auditd.

Records of information security activities: including logins, logouts, data security operations, password changes, and system configurations, are meticulously documented in log files configured with the assistance of auditd (Figures 2, 3, 4, 5). This demonstrates the effectiveness of the auditd tool in enabling users and administrators to maintain robust control over their devices in the face of security events, thereby facilitating the implementation of measures to prevent and mitigate potential threats arising from such incidents.

```
2026-03-19T03:00:46.273658+03:00 nguyen sudo:   nguyen : TTY=tty1 ; PWD=/home/nguyen
2026-03-19T03:00:46.276449+03:00 nguyen sudo: pam_unix(sudo:session): session opened
2026-03-19T03:00:46.292696+03:00 nguyen su[976]: (to root) root on pts/0
2026-03-19T03:00:46.293938+03:00 nguyen su[976]: pam_unix(su:session): session opene
```

Figure 2 – Log login activity to the file /var/log/auth.log.

```
root@nguyen:~# tail -5 /var/log/secure
2026-03-19T03:11:07.176288+03:00 nguyen sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin
2026-03-19T03:11:07.209467+03:00 nguyen sudo: pam_unix(sudo:session): session opened for user root(uid=0) by
2026-03-19T03:11:07.358519+03:00 nguyen sudo: pam_unix(sudo:session): session closed for user root
2026-03-19T03:11:42.673892+03:00 nguyen sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bas
2026-03-19T03:11:42.678068+03:00 nguyen sudo: pam_unix(sudo-i:session): session opened for user root(uid=0) b
root@nguyen:~#
```

Figure 3 – Log security activity to the /var/log/secure file.

```
root@nguyen:~# ausearch -k pawwsd_changes
<no matches>
root@nguyen:~# ausearch -k pawwsd_changes -i
<no matches>
root@nguyen:~# ausearch -k sysconfig_changes
<no matches>
```

Figure 4 – Record password change activity

```
nguyen@nguyen:~$ sudo ausearch -k passwd_changes -i
[sudo] password for nguyen:
----
type=PROCTITLE msg=audit(03/19/2026 03:31:06.792:450) : proctitle=/sbin/auditctl -R /etc/audit/audit.rules
type=PATH msg=audit(03/19/2026 03:31:06.792:450) : item=0 name=/etc/ inode=393217 dev=fc:00 mode=dir,755 ouid=root ogid=root rdev=00:0
one cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(03/19/2026 03:31:06.792:450) : cwd=/
type=SOCKADDR msg=audit(03/19/2026 03:31:06.792:450) : saddr={ saddr_fam=netlink nlnk-fam=16 nlnk-pid=0 }
type=SYSCALL msg=audit(03/19/2026 03:31:06.792:450) : arch=x86_64 syscall=sendto success=yes exit=1084 a0=0x3 a1=0x7ffef2fdc760 a2=0x4
1 pid=1124 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=auditc
subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(03/19/2026 03:31:06.792:450) : auid=unset ses=unset subj=unconfined op=add_rule key=passwd_changes list=e
----
type=PROCTITLE msg=audit(03/19/2026 04:08:01.355:48) : proctitle=/sbin/auditctl -R /etc/audit/audit.rules
type=PATH msg=audit(03/19/2026 04:08:01.355:48) : item=0 name=/etc/ inode=393217 dev=fc:00 mode=dir,755 ouid=root ogid=root rdev=00:00
ne cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(03/19/2026 04:08:01.355:48) : cwd=/
type=SOCKADDR msg=audit(03/19/2026 04:08:01.355:48) : saddr={ saddr_fam=netlink nlnk-fam=16 nlnk-pid=0 }
type=SYSCALL msg=audit(03/19/2026 04:08:01.355:48) : arch=x86_64 syscall=sendto success=yes exit=1004 a0=0x3 a1=0x7fff372930c0 a2=0x4
pid=590 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=auditctl
J=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(03/19/2026 04:08:01.355:48) : auid=unset ses=unset subj=unconfined op=add_rule key=passwd_changes list=ex
```

Figure 5 – The password change operation has been recorded.

List of Sources:

1. Configuring the Auditd Tool [Electronic Resource]. – Access Mode:https://habr.com/ru/articles/553036/.
2. Creating Event Rules [Electronic Resource]. – Access Mode: https://habr.com/ru/articles/553036/.
3. Creating Event Rules [Electronic Resource]. – Access Mode:https://www.redhat.com/en/blog/configure-linux-auditing-auditd.