Week 5: Advanced Security and Monitoring Infrastructure

Overview

In Week 5, I implemented advanced security controls and monitoring on my Linux server. The main tasks included enforcing access control with AppArmor, enabling automatic security updates, configuring fail2ban, and creating scripts for security baseline verification and remote monitoring.

1. Access Control: AppArmor

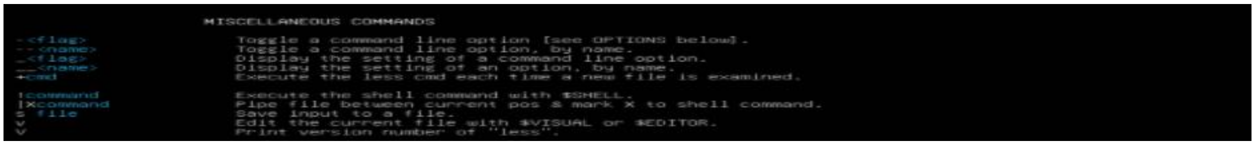
I enabled AppArmor to enforce mandatory access control on applications.

Commands:

```
sudo aa-status
sudo systemctl enable apparmor
sudo systemctl start apparmor
sudo apparmor_status
```

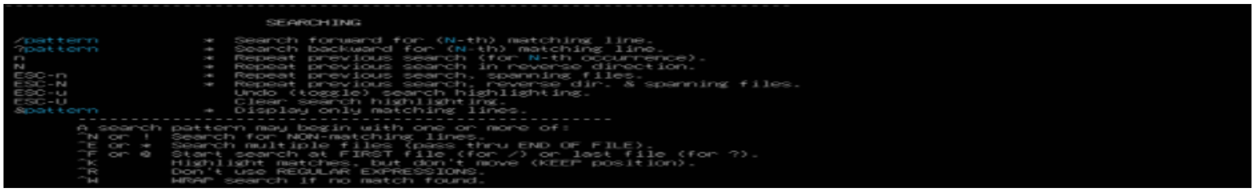
Explanation:

AppArmor restricts the actions of applications to reduce the risk of exploitation from compromised pro



```
                      MISCELLANEOUS COMMANDS

  -<flag>              Toggle a command line option [see OPTIONS below].
  --<name>             Toggle a command line option, by name.
  _<flag>              Display the setting of a command line option.
  __<name>             Display the setting of an option, by name.
  +cmd                 Execute the less cmd each time a new file is examined.

  !command             Execute the shell command with $SHELL.
  |Xcommand            Pipe file between current pos & mark X to shell command.
  s file               Save input to a file.
  v                    Edit the current file with $VISUAL or $EDITOR.
  V                    Print version number of "less".
```

```
                      LINE EDITING

        These keys can be used to edit text being entered
        on the "command line" at the bottom of the screen.

 RightArrow ..................... ESC-l ... Move cursor right one character.
 LeftArrow ...................... ESC-h ... Move cursor left one character.
 ctrl-RightArrow  ESC-RightArrow  ESC-w ... Move cursor right one word.
 ctrl-LeftArrow   ESC-LeftArrow   ESC-b ... Move cursor left one word.
 HOME ........................... ESC-0 ... Move cursor to start of line.
 END ............................ ESC-$ ... Move cursor to end of line.
 BACKSPACE ................................ Delete char to left of cursor.
 DELETE ......................... ESC-x ... Delete char under cursor.
 ctrl-BACKSPACE   ESC-BACKSPACE ........... Delete word to left of cursor.
 ctrl-DELETE .... ESC-DELETE .... ESC-X ... Delete word under cursor.
 ctrl-U ......... ESC (MS-DOS only) ....... Delete entire line.
 UpArrow ........................ ESC-k ... Retrieve previous command line.
 DownArrow ...................... ESC-j ... Retrieve next command line.
 TAB ...................................... Complete filename & cycle.
 SHIFT-TAB ...................... ESC-TAB   Complete filename & reverse cycle.
 ctrl-L ................................... Complete filename, list all.
HELP -- END -- Press g to see it again, or q when done
```



```
------------------------------------------------------------------------------

                            SEARCHING

/pattern            *  Search forward for (N-th) matching line.
?pattern            *  Search backward for (N-th) matching line.
n                   *  Repeat previous search (for N-th occurrence).
N                   *  Repeat previous search in reverse direction.
ESC-n               *  Repeat previous search, spanning files.
ESC-N               *  Repeat previous search, reverse dir. & spanning files.
ESC-u                  Undo (toggle) search highlighting.
ESC-U                  Clear search highlighting.
&pattern            *  Display only matching lines.
        ---------------------------------------------------
        A search pattern may begin with one or more of:
        ^N or !  Search for NON-matching lines.
        ^E or *  Search multiple files (pass thru END OF FILE).
        ^F or @  Start search at FIRST file (for /) or last file (for ?).
        ^K       Highlight matches, but don't move (KEEP position).
        ^R       Don't use REGULAR EXPRESSIONS.
        ^W       WRAP search if no match found.
```