SPIOT 2

Aim:

Exploring commands and tools in Attify OS.

Objective:

This practical aims to enhance understanding of Attify OS capabilities for effective security analysis.

Commands:

1. **sudo su**
   Switches to the root user, granting superuser privileges for executing administrative commands.
2. **passwd**
   Changes the password for the current user or another specified user (requires root privileges).
3. **sudo apt-get update**
   Updates the package lists for repositories, ensuring the system is aware of the latest available package versions.
4. **sudo apt-get upgrade**
   Installs the latest versions of all currently installed packages.
5. **ls**
   Lists the contents of the current directory, including files and subdirectories.
6. **mkdir**
   Creates a new directory.
7. **rmdir**
   Removes an existing directory.
8. **cd**
   Changes the working directory.
9. **cd ./desktop**
   Changes the current directory to the "desktop" directory within the current directory.
10. **cp**
    Copies a file to another folder or directory.
11. **touch**
    Creates or modifies the timestamps of a file.

12. **printf**
    Outputs formatted text, especially useful for variables or numbers.
13. **echo**
    Prints simple text to the terminal.
14. **sudo adduser username**
    Creates a new user account with administrative privileges.
15. **sudo su username**
    Switches to the specified user's account with root privileges.
16. **uname -a**
    Displays detailed system information (kernel version, architecture, etc.).
17. **df -h**
    Shows disk space usage of all mounted file systems in a human-readable format.
18. **pwd**
    Prints the full path of the current directory.
19. **ps**
    Displays a snapshot of currently running processes.
20. **cal**
    Displays a calendar for the current or specified month/year (e.g., `cal 12 2024`).
21. **ifconfig**
    Displays or configures network interfaces (IP address, subnet mask, etc.).

> *Note: `ifconfig` is deprecated in favor of `ip a`.*

Nmap in Attify OS

nmap is a powerful open-source tool used for:

- **Network Discovery:**
  `nmap 192.168.1.0/24` — scans all devices in the subnet.
- **Port Scanning:**
  `nmap -p 80,443 192.168.1.1` — scans ports 80 and 443.
- **Service Version Detection:**
  `nmap -sV 192.168.1.1` — detects versions of services on open ports.
- **OS Detection:**
  `nmap -O 192.168.1.1` — detects the operating system of the host.
- **Aggressive Scan:**
  `nmap -A 192.168.1.1` — performs an in-depth scan with multiple techniques.
- **Stealth Scanning:**
  `nmap -sS 192.168.1.1` — performs a SYN scan to avoid detection.

Additional Examples:

22. **nmap 31.13.79.254**
    Scans the target IP for open ports and services.
23. **nmap 192.168.1.1-4**
    Scans IPs from `192.168.1.1` to `192.168.1.4`.
24. **nmap 192.168.0.1 192.168.0.107 192.168.1.1 192.168.1.2**
    Scans multiple specified IP addresses for open ports and services.

Conclusion:

From this experiment, we learned about various commands and tools used in Attify OS for system management, networking, and security auditing.