System Information

Overview

Using the Linux terminal effectively is crucial for administration, auditing, and security testing. Understanding commands related to system information, users, network, and hardware helps in both routine operations and vulnerability assessments.

Logging In via SSH

SSH (Secure Shell) is a secure protocol for remotely accessing systems.

Command to connect:

```
ssh htb-student@[IP address]
```

System Information & User Enumeration

Command	Description
`whoami`	Prints current logged-in username. Useful for checking current access.
`id`	Displays UID, GID, and group memberships. Great for privilege auditing.
`hostname`	Shows the system hostname.
`uname`	Displays OS and hardware details.
`uname -a`	Shows all available system information.
`uname -r`	Prints the kernel release — helpful for searching exploits.
`pwd`	Displays current working directory.

Network & Interface Information

Command	Description
`ifconfig`	Views or configures network interfaces (deprecated, but still used).
`ip`	Manipulates routes, devices, tunnels, and more (modern replacement).
`netstat`	Shows network connections and status (deprecated in favor of `ss`).
`ss`	Modern socket investigation tool — faster and more detailed than `netstat`.

Processes & User Sessions

Command	Description
`ps`	Shows current running processes.
`who`	Lists users currently logged in.
`env`	Prints environment variables or runs a command in a modified environment.

Hardware & Devices

Command	Description
`lsblk`	Lists block devices (useful for mounted drives and partitions).
`lsusb`	Displays USB devices connected to the system.
`lsof`	Lists open files — handy for tracking file usage or troubleshooting.
`lspci`	Lists all PCI devices (e.g., graphics, network cards).

Practical Usage Examples

```
# Print hostname
hostname

# Check current user
whoami

# Show user ID and group memberships
id

# Kernel & system info
uname -a
uname -r   # Get kernel version only

# Current working directory
pwd

# View network configuration
ifconfig
ip a

# Check open ports and connections
netstat -tuln
ss -tuln

# List running processes
ps aux

# Show currently logged-in users
who
```

```
# Print all environment variables
env
```

Tips for Learning

- Use `man [command]` or `[command] --help` to understand more options.
- Experiment in a safe, virtual environment like Hack The Box labs.
- Focus on commands related to **users, kernel, processes,** and **network** — these are key areas in security assessments and privilege escalation.

Suggested Practice

1. Connect to a machine via SSH.
2. Try each command and note the output.
3. Use `uname -r` and search for related exploits online.
4. Explore man pages to uncover command options you didn't know existed.