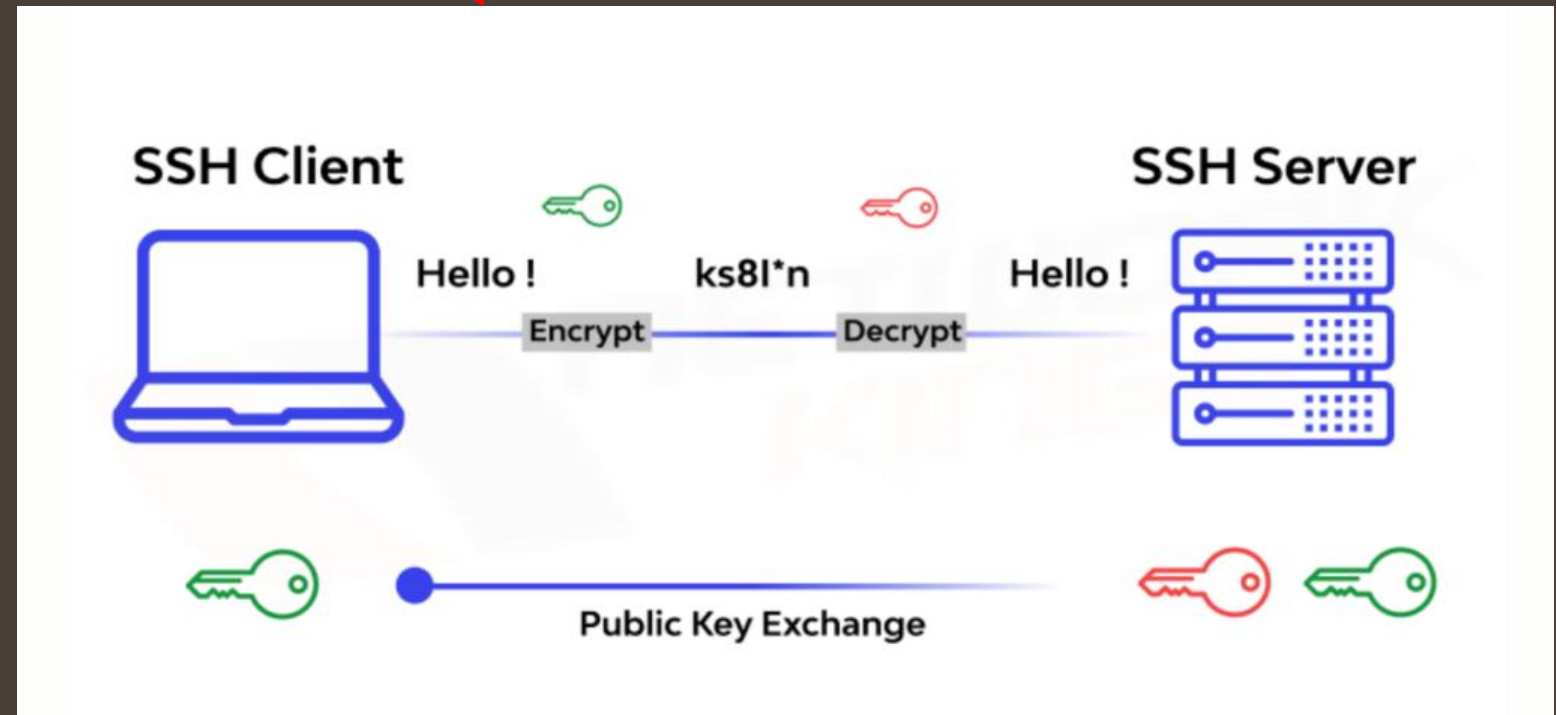


# Brute Force attack & its Prevention



# What is Brute Force attack?

- A trial-and-error method used by attackers to guess login credentials.
- Common on SSH servers exposed to the internet.



Source: [Medium](#)



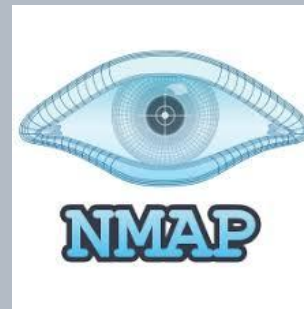
# How it Works?

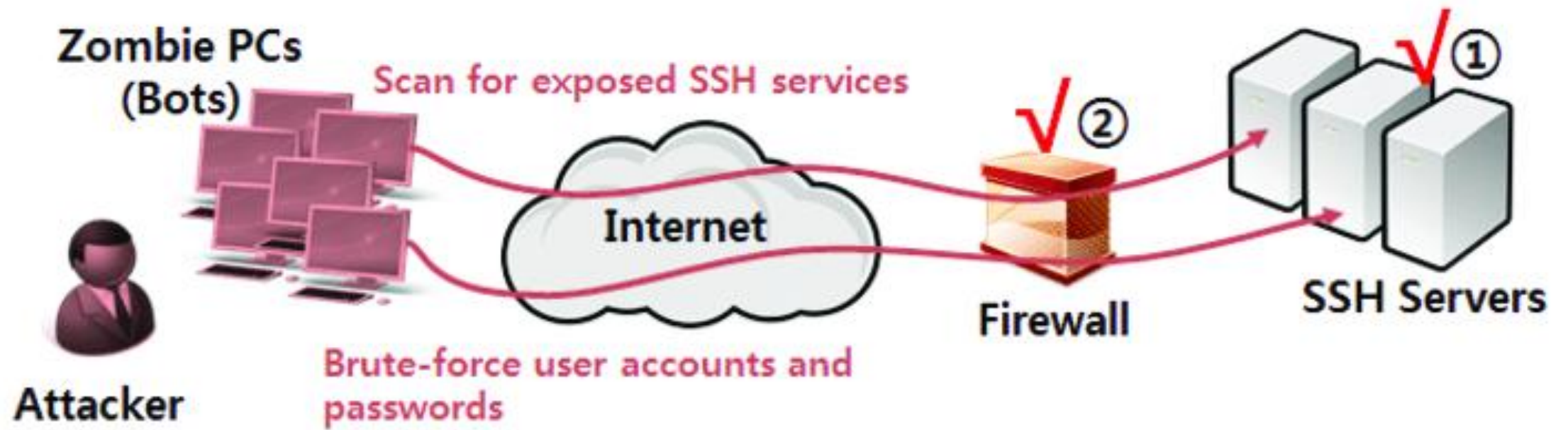
**Step 1:** Attacker scans for open SSH ports  
(`nmap -p 22 target-ip`).

**Step 2:** Uses automated tools (Hydra, Medusa) to try thousands of passwords.

**Step 3:** If successful, attacker gains full control of the system.

Tools used:





# Detecting Brute Force Attempts

As we have done demonstration of brute force attack, we can detect attempts made to login ssh server through log files in a system/server.

1)navigate to **/var/logs**

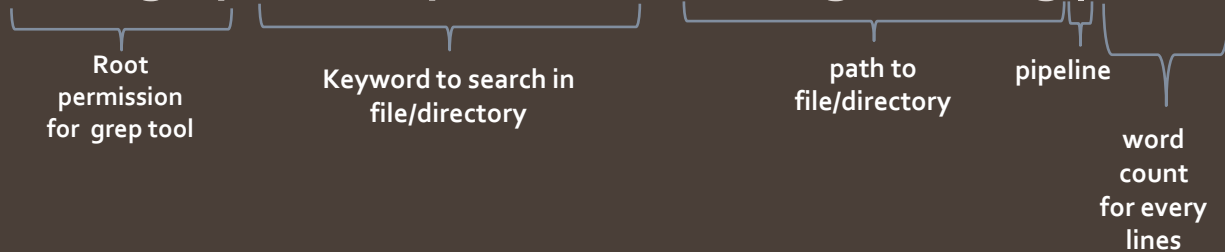
2)open with root permissions "**auth.log**" file

3) can search for keyword like "**Failed password**"

OR:

Using **grep command** for filter-n-display log file data in terminal.

**CMD: Sudo grep "Failed password" /var/log/auth.log | wc -l**



## Securing SSH

- **Disable root login** (`PermitRootLogin no`).
- **Use SSH keys instead of passwords** (`PasswordAuthentication no`).
- **Change the default SSH port**  
(Eg: Port 22 to 2222).
- **Limit login attempts with "Fail2Ban".**

# What is Fail2Ban?

- Fail2Ban is a **security tool** that **monitors logs** and **blocks IPs** after too many failed login attempts.
- Automatically updates firewall rules to **ban attackers**.

## Tools Used:

### For working with fail2ban

- Fail2ban
- SSH (Secure shell)
- Nmap (network mapper)

### For android and linux integration:

- Mobile SSH
- Vysor (android app for screen mirroring)

## Conclusion & Key Takeaways

- Brute force attacks are **common** but **preventable**.
- Always use **SSH keys** and **disable root login**.
- **Fail2Ban** helps **block attackers automatically**.



Questions?

THANK YOU...!



Source: [Heimdal](#)