Linux Security Hardening Playbooks Explained

HARDENING 1: SSH Security & File Permissions

What it does:

SSH Security Configuration:

- **MaxAuthTries 3**: Limits login attempts to 3 before blocking the connection (prevents brute force attacks)
- **ClientAliveInterval 300**: Sends keepalive messages every 5 minutes to detect dead connections
- **ClientAliveCountMax 2**: Disconnects after 2 failed keepalive responses (10 minutes total)
- **Protocol 2**: Forces SSH version 2 (version 1 has security vulnerabilities)
- **LoginGraceTime 60**: User has only 60 seconds to complete login (prevents connection hogging)
- **X11Forwarding no**: Disables GUI forwarding (reduces attack surface)
- **UseDNS no**: Disables DNS lookups for connecting IPs (faster connections, less logging)
- **Banner**: Shows warning message before login

File Permissions Hardening:

- **/etc/passwd (644)**: World-readable user account info (normal)
- **/etc/shadow (640)**: Password hashes readable only by root and shadow group (secure)
- **/etc/group (644)**: Group information world-readable (normal)
- **/etc/ssh/sshd_config (600)**: SSH config readable only by root (prevents tampering)

Test Command Breakdown:

```bash
grep -E "^(MaxAuthTries|...)" /etc/ssh/sshd_config
```

- **Purpose**: Checks if SSH security settings are configured
- **Output**: Shows active SSH configuration lines (not commented out with #)

```bash
ls -l /etc/passwd /etc/shadow /etc/group /etc/ssh/sshd_config
```

- **Purpose**: Shows file permissions and ownership

- **What to look for**:
  - First column shows permissions (rwx format)
  - 644 = rw-r--r-- (owner read/write, others read-only)
  - 640 = rw-r----- (owner read/write, group read, others no access)
  - 600 = rw------- (owner read/write only)

HARDENING 2: Network Security & Service Management

What it does:

Network Security (sysctl settings):

- **net.ipv4.ip_forward = 0**: Disables packet forwarding (prevents router functionality)
- **net.ipv4.tcp_syncookies = 1**: Enables SYN flood protection
- **net.ipv4.conf.all.accept_redirects = 0**: Ignores ICMP redirect messages (prevents routing attacks)
- **net.ipv4.conf.all.send_redirects = 0**: Doesn't send ICMP redirects
- **net.ipv4.conf.all.accept_source_route = 0**: Ignores source-routed packets (prevents spoofing)
- **net.ipv4.icmp_echo_ignore_broadcasts = 1**: Ignores ping broadcasts (prevents DDoS amplification)
- **net.ipv4.icmp_ignore_bogus_error_responses = 1**: Ignores malformed ICMP responses

Service Management:

- Checks for and disables risky services (telnet, rsh, rlogin, tftp, finger, talk)
- These services are unencrypted and vulnerable

Password Policy:

- **PASS_MIN_DAYS 1**: Must wait 1 day between password changes
- **PASS_MAX_DAYS 90**: Must change password every 90 days
- **PASS_MIN_LEN 8**: Minimum 8 characters
- **PASS_WARN_AGE 7**: Warning 7 days before expiration

Firewall (UFW):

- Sets default deny incoming, allow outgoing
- Allows SSH access only
- Enables firewall

Logging:

- Ensures rsyslog is running for system logging
- Configures log rotation to prevent disk space issues

Test Command Breakdown:

```bash
sysctl net.ipv4.ip_forward net.ipv4.tcp_syncookies...
```

- **Purpose**: Shows current kernel network security settings
- **Output**: Current values (0 = disabled, 1 = enabled)

```bash
grep -E "^(PASS_MIN_DAYS|...)" /etc/login.defs
```

- **Purpose**: Shows password policy settings
- **Output**: Active password rules

```bash
ufw status
```

- **Purpose**: Shows firewall status and rules
- **Output**:
  - "Status: active" = firewall running
  - Rules list shows what traffic is allowed/blocked

HARDENING 3: fail2ban Installation

What it does:

Intrusion Prevention:

- **fail2ban**: Monitors log files for suspicious activity
- **SSH Jail**: Specifically watches SSH login attempts
- **maxretry = 3**: Bans IP after 3 failed login attempts
- **bantime = 3600**: Bans IP for 1 hour (3600 seconds)
- **findtime = 600**: Counts failures within 10 minutes
- **logpath = /var/log/auth.log**: Monitors SSH authentication log

Test Command Breakdown:

```bash
systemctl is-active fail2ban; systemctl is-enabled fail2ban
```

- **Purpose**: Checks if fail2ban service is running and will start at boot
- **Output**: "active" and "enabled" = working properly

```bash
cat /etc/fail2ban/jail.d/ssh.conf
```

- **Purpose**: Shows SSH protection configuration
- **Output**: Settings for SSH attack detection and banning

```bash
fail2ban-client status ssh
```

- **Purpose**: Shows real-time SSH jail statistics
- **Output**:
  - Currently failed: Current bad login attempts being tracked
  - Currently banned: IPs currently blocked
  - Total banned: Historical count of blocked IPs

Security Impact Summary:

HARDENING 1: Secures SSH access and critical system files **HARDENING 2**: Hardens network stack, enforces password policies, enables firewall **HARDENING 3**: Adds automated intrusion detection and response

Together they create: A multi-layered defense system protecting against common attack vectors like brute force attacks, network exploits, and unauthorized access attempts.

Why These Matter:

1. **SSH Hardening**: SSH is often the main entry point for attackers
2. **Network Hardening**: Prevents network-based attacks and reconnaissance
3. **File Permissions**: Prevents privilege escalation and system tampering

4. **fail2ban**: Provides real-time response to attack attempts
5. **Firewall**: Creates a network barrier allowing only necessary traffic
6. **Logging**: Enables detection and forensics of security incidents