- ★ OS security checklist
- ★ OS: Window , kali Linux [VM]

1/16/2026

OS Security

Windows Security Checklist:

1. **Secure Boot:**

Verify Secure Boot is enabled in UEFI/BIOS settings and

confirm via msinfo32.

2. **BitLocker:**

Ensure BitLocker drive encryption is active with

recovery keys backed up securely.

3. **Antivirus:**

Confirm Microsoft Defender Antivirus is enabled with

real-time protection, cloud-delivered protection at high level, and regular scans scheduled.

4. **ASR :**

Check that Attack Surface Reduction (ASR) rules are

enforced, blocking Office macros, executable content from email, and credential theft from LSASS.

5. **UAC:**

Validate User Account Control (UAC) prompts for credentials on secure desktop for admins and standard users.

6. **Review local administrator accounts:**

Disable built-in admin, implement LAPS for unique passwords.

7. **Updates:**

Confirm OS patches are applied promptly; use WSUS

or Intune for management.

8. **Credential Guard:**

Enable Credential Guard and exploit protection mitigations like CFG, ASLR, and DEP.

9. **Port Protection:**

Audit firewall rules and endpoint device control to block untrusted USBs.

10. **Logs Check:**

Check logs in Event Viewer for anomalies and enable centralized auditing.

Kali Linux Security Checklist:

11. **Updates:**

sudo apt update && sudo apt upgrade -y.

12. **Firewall:**

sudo ufw enable then sudo ufw allow ssh (only if needed).

13. **SSH Secure:**

Edit /etc/ssh/sshd_config : set Password Authentication no, then sudo systemctl restart ssh.

14. **Fail2ban:**

sudo apt install fail2ban -y.

15. **Remove Junk:**

sudo systemctl disable apache2 nginx (if not used).

16. **Strong Root:**

sudo passwd root > set long password.

17. **Auto Updates:**

sudo apt install unattended-upgrades -y.

18. **Logs Check:**

sudo tail -f /var/log/auth.log for bad logins.