

VPS Vulnerability Checklist

A VPS vulnerability checklist is a list of items that should be regularly checked and addressed to ensure the security of a Virtual Private Server (VPS). Here's a general VPS vulnerability checklist:

1. Keep the VPS and all software up-to-date: Regularly update the VPS operating system and all installed software to address known vulnerabilities.
2. Use a strong and unique root password: Use a long, complex, and unique password for the VPS root user.
3. Limit access to the VPS: Only allow necessary users to access the VPS and use strong authentication methods such as SSH key pairs.
4. Use a firewall: Use a firewall to limit incoming and outgoing traffic to the VPS.
5. Monitor system logs: Regularly check the VPS system logs for unusual activity.
6. Use an intrusion detection system (IDS) or an intrusion prevention system (IPS): Use an IDS or IPS to detect and prevent malicious activity on the VPS.
7. Disable unnecessary services and ports: Disable any unnecessary services and ports on the VPS to reduce attack surface.
8. Use a VPN or other secure method to access the VPS remotely: Use a VPN or other secure method to access the VPS remotely to protect against eavesdropping and man-in-the-middle attacks.
9. Use strong file permissions: Use strong file permissions to protect sensitive files and directories on the VPS.
10. Regularly back up important data: Regularly back up important data to protect against data loss or corruption.

Revision #1

Created 25 January 2023 15:03:41 by Daniel Azimi

Updated 3 June 2023 06:28:08 by Daniel Azimi