Taming the Wild West: Finding Security in Linux_

SANS

SUMMARY

Linux Security Self-Assessment_

Security professionals around the globe are beginning to realize that the “single-track defense” method of protecting their environments is beginning to be much too simple to protect complex enterprise environments with global and multi-platform networks. In response to this, organizations are starting to implement Linux-based platforms to their networks due to their ease of use on-premises and in the cloud.

Follow the checklist below to discover how to protect your Linux environment against attackers.

How Do You Stack Up?

The most secure Linux environments out there follow these guidelines, as outlined by SANS. How does your environment compare?

- **Do you run as root?**
  Running as root is a common accident that hackers love to take advantage of. ☐
- **Do you have visbility into your systems?**
  This allows you to gain an understanding of how those systems contribute to business operations. ☐
- **Can you monitor users in real time?**
  This type of command execution in Linux systems can help the security team gain real insight into what users are up to. ☐
- **Do you have suspicious users in your system?**
  Any user attempting to run certain commands or binaries should cause suspicion, especially if repeated activity is detected. ☐

Read the full SANS report “Taming the Wild West: Finding Security in Linux” here:

https://info.cmd.com/taming-the-wild-west-finding-security-in-linux-sans-whitepaper

Now that you’ve completed the checklist, see how Cmd can improve your Linux environment:

TRY IT HERE: https://cmd.com/free-trial