



Among The Reindeer Answer-Key

1. (2) ElfShelf account **removed!**
2. (5) Everyone's Trusted Computing Base right has been **revoked!**
3. (2) Task 1: SMB **configured!**
4. (5) Sticky keys backdoor has been **removed!**
5. (3) Notepad fork bomb **removed!**
6. (2) SMB server wide encryption is **enabled!**
7. (2) Event logs service **running!**
8. (2) Windows defender Real Time Protection **enabled!**
9. (2) Windows Defender Heuristics **enabled!**
10. (3) Let Everyone permissions apply to anonymous **disabled!**
11. (2) Remote Desktop has been **disabled!**
12. (8) Hidden user **removed!**
13. (2) Recycle bins **cleared!**
14. (3) Everyone's right to assign primary tokens has been **revoked!**
15. (2) Super Elf Bowling has been **removed!**
16. (2) Task 2: Firefox has been **installed!**
17. (3) Keylogger **removed!**
18. (4) Malicious Group Policy Mechanism **subverted!**
19. (6) Meme stream malware **removed!**
20. (12) Imposters correctly identified and **ejected!**
21. (5) Forensics Question 1 **correct!**
22. (6) Forensics Question 2 **correct!**
23. (8) Forensics Question 3 **correct!**
24. (4) Forensics Question 4 **correct!**
25. (4) Forensics Question 5 **correct!**



Among The Reindeer Forensics Answers

Forensics Question 1 Answer:
`seTcbPrivilege` and `seAssignPrimaryTokenPrivilege`

Forensics Question 2 Answer:
`Shiegra123!`

Forensics Question 3 Answer:
`C:\ProgramData\Microsoft\Crypto\SystemKeys\keys`

Forensics Question 4 Answer:
`Lyman Baum`

Forensics Question 5 Answer:
`4d38f2eca3b2e729c9247e815f478021`



Among The Reindeer

Shoutout and Credits

Shoutout to [Eth007](#) & [Astro](#) to being the first two to complete this image!

Credits

shiversoftdev - Engine Lead, Design, Deployment

KaliPatriot - Software, Theme, Design, Deployment

RainbowDynamix - Design, Theme, Deployment

Matthew - Design, Theme

TheiMacNoob - Minor Theme