UNITED STATES SPACE FORCE

MMXIX

DEPARTMENT OF THE AIR FORCE

Space Force Practice Image Answer Key

Note: A full guide and video walkthrough are in the works. This is simply an answer key. Not all vulnerabilities give specific information on how to solve the check, but instead give you specific information on what is being scored. This is meant to give everyone a chance at learning from the image, even with the answer key. The full guide/walkthrough will have exact methods on how to solve the checks.

Huge shoutout to noahc3 for his engine ‘crack’. Attacks like this allow us to develop the engine further against attacks and ensure the integrity of our images. More information on the attack will be discussed in the full guide.

Nobody achieved a perfect score of 101 before the answer key was released. Shoutouts will be given to the first ace for all of our future images.

1. ProFTPd is running (FTP check)
2. Apache web server was purged, including website. (Web server check)
3. Quarantined /etc/dtsnd.mp3, /etc/dtimg.jpg (Quarantined media check)
4. Quarantined /home/contractors/.ssh/id_rsa, removed original key. (SSH check)
5. Records must match those found in the readme. (DNS Records Updated)
6. All files from web server private folder must be moved into the requested directory in the readme. (Private files have been migrated)
7. All files from web server public folder must be moved into the requested directory in the readme. (Public files have been migrated)
8. Group ‘topsecret’ must only contain the members specified in the readme. (Top Secret configured correctly)
9. /etc/znetdog.sh must be quarantined. (Access Terminal quarantined)
10. bind9 must be configured to hide its version number. (bind9 check)
11. bind9 must be configured to not allow zone transfers. (bind9 zone check)
12. dtrump must have his FTP access restored. (User check passed)
13. ProFTPd must have the anonymous access setup correctly, based on what is requested in the readme. (Anonymous access correct)
14. ProFTPd must have the correct login setup for the topsecret group. They must have access to the correct files and their home directory must be setup correctly. Refer to the readme for more information. (Private access correct)
15. Root account must not be allowed to login to the FTP server. (Login check)
16. The FTP user must not have a root UID. (Access check passed)
17. Apt sources.list must no longer contain tor sources. (Update check passed)
18. /usr/share/ hidden directory must be deleted. (Messaging channel destroyed)
19. /etc/init.d/ts.sh must be quarantined. (Timescript quarantined)
20. /usr/share/rus/пароли.текст must be quarantined. (Database quarantined)

Forensics

Question 1:

ANSWER: /etc/
ANSWER: /usr/share/
ANSWER: /home/

Question 2:

ANSWER: 2019-12-20 16:48:31

Question 3:

ANSWER: toor

Question 4:

ANSWER: h4il_St4l1n

Question 5:

ANSWER: /usr/bin/sudo
ANSWER: /bin/bash

Thank you to all those who attempted to complete the image before the key was released. We hope we taught you something new about debian or the critical services involved with this image.

Space Force Server Developers

shiversoftdev#7639

rainbowdynamix#5809

matthew#2334