Vulnhub: Avengers Arsenal Challenge

Uploaded by hackingarticles.in

This Capture the Flag (CTF) can be done anywhere since it is a downloadable image. We are using one of the many prebuilt vulnerable systems located on VulnHub.com.

The Challenge… Using whatever tool of your choice. Capture all the flags you can, identify and exploit as many vulnerabilities as you can, write a report, and write a walk through on how you found each item within. The findings and final report will then be graded, with the best combo being the winner. Make sure that the report and the walkthrough are two separate documents.

Winner will have their report and walkthrough showcased in a future issue of the Cyber Intelligence Report (CIR) and win a commemorative Bitcoin challenge coin (Not a real Bitcoin). Submit report and walkthrough to CTF@informationwarfarecenter.com.

Deadline: September 15th, 2020!

To compete, you must sign up here:
comms.informationwarfarecenter.com/?p=subscribe&id=3

Vulnhub Download

(vulnhub.com/entry/ha-avengers-arsenal,369)

This is a capture the flag. Once you download and install the virtual image, you can use any tool to get the flags. Write your own content and do not plagiarize from other work. That is the only real rule.

Scenario

Avengers are meant to be Earth's Mightiest Heroes, but some heroes just aren't mighty enough without their trusty weapon in hand.

The Goal is to gather all the 5 mightiest weapons:

- VIBRANIUM SHIELD
- MJØLNIR
- SCEPTRE
- STORMBREAKER
- YAKA ARROW
- ENUMERATION IS THE KEY!!!!!

For hints, you can visit:
hackingarticles.in/ha-avengers-arsenal-vulnhub-walkthrough

Remember: Score is based off the quality of the report and walkthrough.

CTF TARGET DETAILS

- Filename: HA-Avengers-Arsenal.ova
- File size: 4.9 GB
- MD5: 512DCEB15F9F185D6A5C77F79E89EFBE
- SHA1: FB06EEBA7E75558220FDD1DF3127A003D5779C0E
- Format: Virtual Machine (Virtualbox - OVA)
- Operating System: Linux
- DHCP service: Enabled
- IP address: Automatically assign

VirtualBox:

- www.virtualbox.org

Additional Resources:

- PTES Framework
- PTES Technical Guidelines
- OSSTMM
- OWASP Testing Guide

Sample Report Links:

- Offensive Security
- TBGSecurity
- github.com/juliocesarfort