2020 Hivestorm Image Hints

Note: This is not a complete answer key for each image. This is a sampling of the challenges contained on each image from the 2020 Hivestorm competition and the percentage of teams that gained points for that challenge.

Windows 10 – highest score achieved was 83 points

- Firewall protection has been enabled – 89%. All you would need to do in this case is turn on the Windows firewall.
- Removed Home Web Server – 65%. On this image there was a “Home Web Server” software package running. As this was not an authorized/approved software package you would need to remove it from the VM.
- Thunderbird has been updated – 41%. The README had this section in it “According to company policy, all Windows desktops (workstations) must also have the latest stable versions of…” and in that list was Thunderbird. You would need to update Thunderbird to make sure it complied with company policy.
- Removed prohibited mp3 files – 20%. The README told you non-work related media files were prohibited. You would need to search the image for media files and remove them.
- Simple TCP/IP Services have been stopped – 9%. The simple TCP/IP services on Windows consist of network services like quote of the day, echo, character generator, and daytime. In accordance with best practices, they’re usually disabled. On this image they’d been turned on and you would need to have stopped the services and disabled it to prevent it from starting again after a reboot.

Debian 9 – highest score achieved was 67 points

- Removed hidden user serrinwright – 63%. This was an unauthorized user account that you would remove from the system to gain points.
- SSH root login has been disabled – 40%. Allowing root to directly SSH into the system is considered by many to be a “high risk” setting and most security best practices recommend disabling direct root SSH logins.
- Root password is no longer blank – 32%. The root account on this VM did not have a password set on it.
- NFS has been stopped or disabled – 9%. NFS was not one of the critical services this system was supporting. Best practices recommend disabling any services (especially network services) that aren’t needed. The more you can reduce the attack surface of a network-connected system the easier it is to secure.

Ubuntu 16 – highest score achieved was 71 points

- Removed unauthorized user mkoh – 64%. The README contained the list of authorized users. You would need to audit the system and remove any user accounts that weren't listed in the README as authorized users.
- LibreOffice has been updated – 43%. The README indicated that Linux systems should be running the latest stable version of LibreOffice. You would need to update LibreOffice to get points.
- Prohibited software ophcrack removed – 34%. Ophcrack is a Windows password cracker based on rainbow tables. As it falls in the "prohibited software" and "hacking" tools category in the README, you would need to find and remove this software package.
- An account lockout policy is configured – 8%. An account lockout policy helps protect your system from brute force password guessing attacks. You would need to enable account lockouts and configure the attempts/timeout values to gain points.

Windows 2016 – highest score achieved was 80 points

- Removed Driver Booster – 79%. This software clearly didn't belong on the system and you would need to remove it to gain points.
- Audit Special Login (Success) – 38%. Event ID 4672 lets you know when accounts with administrative or administrator equivalent privileges have logged onto the system. It's generally a good idea to know when someone (or something) logs into your system with administrative level privileges. You would need to enable auditing for login success events to get points.
- Removed Beware IRC Server – 35%. This IRC server was not an authorized service or software package for this system. You would need to remove it.
- Deny access to this computer from the network includes Guest – 7%. In general, you don't want guest accounts accessing any resources across the network and whenever you can restrict Guest or Anonymous access to a service or system you should. This is a Local Security Policy setting under the User Rights Assignment category.

Windows 2019 – highest score achieved was 84 points

- Removed Plex Media Server – 70%. The Plex Media Server software package should not have been running on this system. You would need to remove it to gain points.
- A secure minimum password age exists – 46%. Best practices recommend setting a minimum password age to help prevent users from changing their password and then immediately changing it back to a password they've used before.
- Restrict CD-ROM access to locally logged on users only (enabled) – 14%. While this setting is a bit more obscure, it's generally a good idea to limit access to things like the CD-ROM drive to users logged into the console of the system. You can find this setting under Local Security Policy in the Security Options category.
- IIS default web site directory browsing disabled – 3%. Directory browsing allows web site visitors to view any files in the visible web directories and best practices recommend disabling

or turning off directory browsing whenever possible. You can turn off directory browsing in IIS in the IIS Manager, finding the default site, and clicking on “Directory Browsing” in the Features View.