# 2021 Hivestorm Image Hints

Thank you for playing in the 2021 Hivestorm event! To assist you and your team in preparations for future events, here are hints to some of the challenges contained on the 2021 images.

Note: This is not a complete answer key for each image. This is a sampling of the challenges contained on each image from the 2021 Hivestorm competition and the percentage of teams that gained points for that challenge. A full answer key is not released as we reuse some of the challenges in other events.

## Windows 10 – Highest score achieved was 72 points

- Firewall protection has been enabled – 87%. All you would need to do in this case is turn on the Windows firewall.
- Removed Ethereum crypto miner Geth – 63%. This was a crypto miner software that is not approved or authorized to be installed on this computer, therefore it needs to be removed.
- A secure maximum password age exists – 57%. This can be done under the Local Security Policy settings (\Account Policies\Password Policy). Change the security setting for the maximum password age.
- Firefox has been updated – 50%. The README mentions that the default web browser for all users on this computer should be the latest stable version of Firefox. You would need to update Firefox to comply with company policy.
- Audit System Integrity [Failure] – 24%. This policy setting allows you to audit events that violate the integrity of the security subsystem. You can enable this in the Local Security Policy under Advanced Audit Policy Configuration\System Audit Polices – Local Group Policy Object\System\Audit System Integrity.
- Xbox Live Game Save service has been stopped and disabled – 6%. This service syncs save data for Xbox Live save enabled games. This service is usually set to manual or disabled. However, this service is running and enabled when you power of the VM. To score this check, you would have to stop and disable this service to prevent it from starting after a reboot.

## Windows Server 2019 – Highest score achieved was 78 points

- Removed unauthorized user tolfdir – 75%. This was an unauthorized user account. Remove it from the system to gain points.
- Removed Teamspeak – 65%. Teamspeak is another program that isn’t allowed to be installed on this machine. Uninstall this to gain points.
- User wulfgar is not an Enterprise Admin – 36%. Although wulfgar is an authorized user, they are not allowed to have admin rights. In Active Directory, you can look in the properties of each user and click on the “Member Of” tab. Enterprise Admins was added to this user’s profile. Remove it and you’ll be awarded points.
- Removed prohibited music files – 14%. The README mentions that non-work-related media files are prohibited. This includes music files. Music media files can be mp3, m4p, wav, mid, etc.

- SMB 1.0 removed or disabled – 12%. This machine’s primary function is to run Active Directory and Domain Name Service. Still, removing SMBv1 is a good security practice.
- Windows Defender is running – 4%. To get points for this, check to see if the Windows Defender service is enabled and running.

**Debian 9 – highest score achieved was 100 points**

- Forensic Question 4 – 84%. This question asked for the UUID of the partition containing the root filesystem. There are several ways you could have found this information including using the “lbkid” or “lsblk” command or something like “ls -l /dev/disk/by-uuid”
- Removed user bahamut – 82%. This was an unauthorized user account that you would remove from the system to gain points. They weren’t listed as a valid user in the readme file so you’d want to remove them from the system.
- Samba service has been disabled or removed – 38%. Samba 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.
- A minimum password length is required – 37%. On this system, PAM was not setup to require secure passwords. If your team had set a minimum password length in the PAM configuration you would have gained points.
- Removed netcat backdoor – 25%. This system was compromised with a netcat based backdoor. You could have found the backdoor running as a service called nyan.service (/etc/systemd/system/nyan.service) – also as an executable /bin/nc/.
- Corrected insecure permissions on PostgreSQL configuration files – 2%. The configuration files for PostgreSQL on this system were viewable/editable by anyone on the system. Your team would need to address that insecurity to gain points.

**Ubuntu 18 – highest score achieved was 100 points**

- Removed unauthorized user alduin – 83%. 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.
- Firefox has been updated – 44%. The README indicated that Linux systems should be running the latest stable version of Firefox. You would need to update Firefox to get points.
- APT has been updated – 37%. Always a good idea to run “apt update” and “apt upgrade” to make sure your packages are up to date. If you updated your VM you would get points for this check.
- Prohibited MP3 files removed – 14%. The README stated that the “presence of any non-work related media files” was “strictly prohibited”. If you did a system wide search for “.mp3” files would have found some obviously not work-related media files that you needed to remove.
- An account lockout policy is configured – 11%. 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.

- Disabled password login for user bin – 3%.  The “bin” account is not a typical user account and there’s not really a good reason for anyone to be able to login to the bin account with a password like you would a regular user account.  You needed to fix this vulnerability to get points.