HIVESTORM

Thank you for playing in the 2023 Hivestorm competition! In order to assist you and your team in preparation in future events, here are some hints to some of the challenges contained on the 2023 images. Always remember to check the readme files for each image as they often contain hints for easy points like helping you identify which users to remove or what software packages to update.

Please note, this is **NOT** a complete answer key for each image. This is a sampling of the challenges from each image with the percentage of teams that gained points for completing these challenges. A full answer key will not be released as we reuse some of the challenges in other events. However, teams are welcome to create and share writeups of how they faced these challenges.

Windows Server 2019_1 – Highest score achieved was 81 points

- Removed StickyKeys backdoor – 20%. If stickykeys is activated on while on the logon screen (by pressing shift 5 times), an command prompt with administrative privileges is opened. This must be removed by deleting the “Debugger” key at the registry location "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe"
- IIS application pool does not run as LocalSystem identity – 4%. The ApplicationPoolIdentity determines what user account is used to run the worker processes. To find this setting, navigate to inetmgr.msc (IIS Management Console). Under Application Pools, you can select the application pool and view Advanced Settings. Under Process Model, you can change the Identity option. Using LocalSystem will give anyone who manages to exploit the web server System permissions. ApplicationPoolIdentity is the default and much more secure to use than LocalSystem.
- Removed GooseDesktop persistence malware – 3%. Quackers! This service was responsible for extracting and restarting the GooseDesktop software that was helping you out! In order to find this service, you can use ProcExp from Sysinternals to determine what is launching GooseDesktop, which points you to the binary at C:\Windows\System32\hyperv-start.exe. This service was launched on startup, and was hidden using specific SDDL permissions. Once you regain access to the binary with windows permissions, you can run strings from sysinternals on the binary, to locate the “killswitch” file at C:\Window\Temp\goosekill.txt. Create a file at that location, then reboot. Delete the original hyperv-start binary.
- Removed phpinfo file – 2%. Enumerating the authorized IIS web server located at C:\inetpub\wwwroot results in discovery of a file called info.php. This file executes the phpinfo()

function which displays debugging information about the webserver and php-cgi. This data could result in the server being exploited, so this file should be removed.
- Removed PHP backdoor – 1%. Further enumeration of the webserver reveals a php web shell located at /c99.php and /old/c99.php. Both of these files should be removed to gain points.

Windows Server 2019_2 – Highest score achieved was 78 points

- User Tashina is not an Enterprise Admin – 27%. The user Tashina is not listed in the README as an authorized administrator, so the user account should be removed from all Administrative groups, including Enterprise Admin. Given that this server is a domain controller, you cannot do user management through control panel or the local users and groups snap-in. You should use Active Directory Users and Computers (dsa.msc) program to manage these users within the domain.
- MNS: Digitally sign communications (always) – 12%. This setting requires packet signing on the SMB Server. This minimizes risk of session eavesdropping attacks between the server and SMB/CIF clients.
- Authenticated Users may not log on locally – 7%. As mentioned in the README, this machine is located in a server room and only authorized administrators should have physical access. So, authenticated users should not have interactive (local) log on abilities.
- Removed PowerShell-V2 – 1%. The Windows PowerShell 2.0 feature is deprecated and should be disabled. It lacks several security features in Windows PowerShell 5.x and can be used to evade PowerShell script block logging features.

Ubuntu 22_1 – Highest score achieved was 84 points

- Uncomplicated Firewall (UFW) protection has been enabled – 65%. If ufw hasn't been installed, a privileged user can open a terminal and type, apt-get install ufw. Then to enable it, type ufw enable.
- Prohibited software uno-java removed – 24%. Games are prohibited by company policy. Uno-java was installed using snap and can be removed using the command snap remove uno-java
- Forensics Question 2 correct – 8%. This question asks for the password needed to access a ruby backdoor. This backdoor hides itself from process monitoring and was listed under the name "[scci-loop]". The quickest and easiest way to find the backdoor was to search the files in /usr/bin and /usr/sbin for the string "ruby" as this will catch the shebang used in the script. Searching for this string will show the result of /usr/bin/jnf. You can read this script to find the password of knock-knock.
- Nginx server tokens disabled – 5%. This setting can be enabled by uncommenting "server_tokens off;" in /etc/nginx/nginx.conf. This security setting is intended to prevent information leakage from the server by hiding the server version number in the response header.
- Removed timed socat backdoor – 2%. There is a socat backdoor being ran every five minutes to attempt a reverse shell connection. This backdoor is started using the /etc/cron.d/ directory. You should remove either the binary located at /usr/bin/sqldb or the cron file named sqldb in the specified directory.

Ubuntu 22_2 – Highest score achieved was 64 points

- Forensics Question 1 correct – 46%. This question asked for two files with the same sha256 checksum within the /usr directory. You can use the find command with the execute option and piping it into a grep command to find both of these files. A working command is below:

```
find /usr/ -type f -exec sha256sum {} \; | grep deb1353bea87a41c4d5c012e898cc8b0e4af0f55e8dd4eaffe94ba66e9e34247
```

- Unauthorized repository removed from package sources – 14%. Kali Linux repositories are used by apt and are configured in /etc/apt/sources.list.d/sources.list. The Kali Linux repositories are unnecessary and contain extra hacking tools which would violate company policies, so this repository should be removed.
- Dovecot service file is no longer world writable – 6%. The dovecot systemd service file is world writable and was used to execute another backdoor. This file should have its permissions restored using the command chmod 644 /lib/systemd/system/dovecot.service
- Removed setuid bash backdoor – 1%. There is a copy of bash located at /usr/sbin/chsh that has suid bit enabled and can be used to get a root shell by running chsh -p. This file should be removed or the suid bit disabled.
- GDM X Server does not allow TCP connections – >1%. In the GDM configuration, located at /etc/gdm3/custom.conf, you should remove or enable the DisallowTCP setting. You should disable this as we do not require remote connections to the display manager at this time.

Fedora 36 – Highest score achieved was 46 points

- **NOT SCORED:** Fedora terminal is fixed. When gnome-terminal is opened by viktor, there is a preference configured to run a custom application instead of zsh. This program is a fake shell that is configured to ignore commands and “crash” after the third command. To remove this, you can open the gnome terminal and navigate to “Edit->Preferences->Command” and deselect “Run a custom command instead of my shell”.
- Removed Firefox addon Flash Player 2021 – 10%. Navigate in Firefox to the hamburger menu, Settings, and then “Extensions and Themes”. Click the three dots and select remove to delete the extension.
- RDP service has been disabled or removed – 7%. Use the command dnf remove xrdp to remove the RDP service. You can also disable and stop the service with systemctl.
- Removed credentials from webpage comment – 2%. The main index.html page contains a comment with the password for the root account on the SQL database. You should remove this comment while keeping the rest of the file intact.
- Prestashop install folder has been removed – 0%. The Prestashop install folder should be removed as it can be used to reinstall and corrupt the Prestashop website. You should delete the directory “/var/www/prestashop/install/”.