



HacknPentest

Linux Privilege Escalation

Linux Privilege Escalation via writeable /etc/passwd file

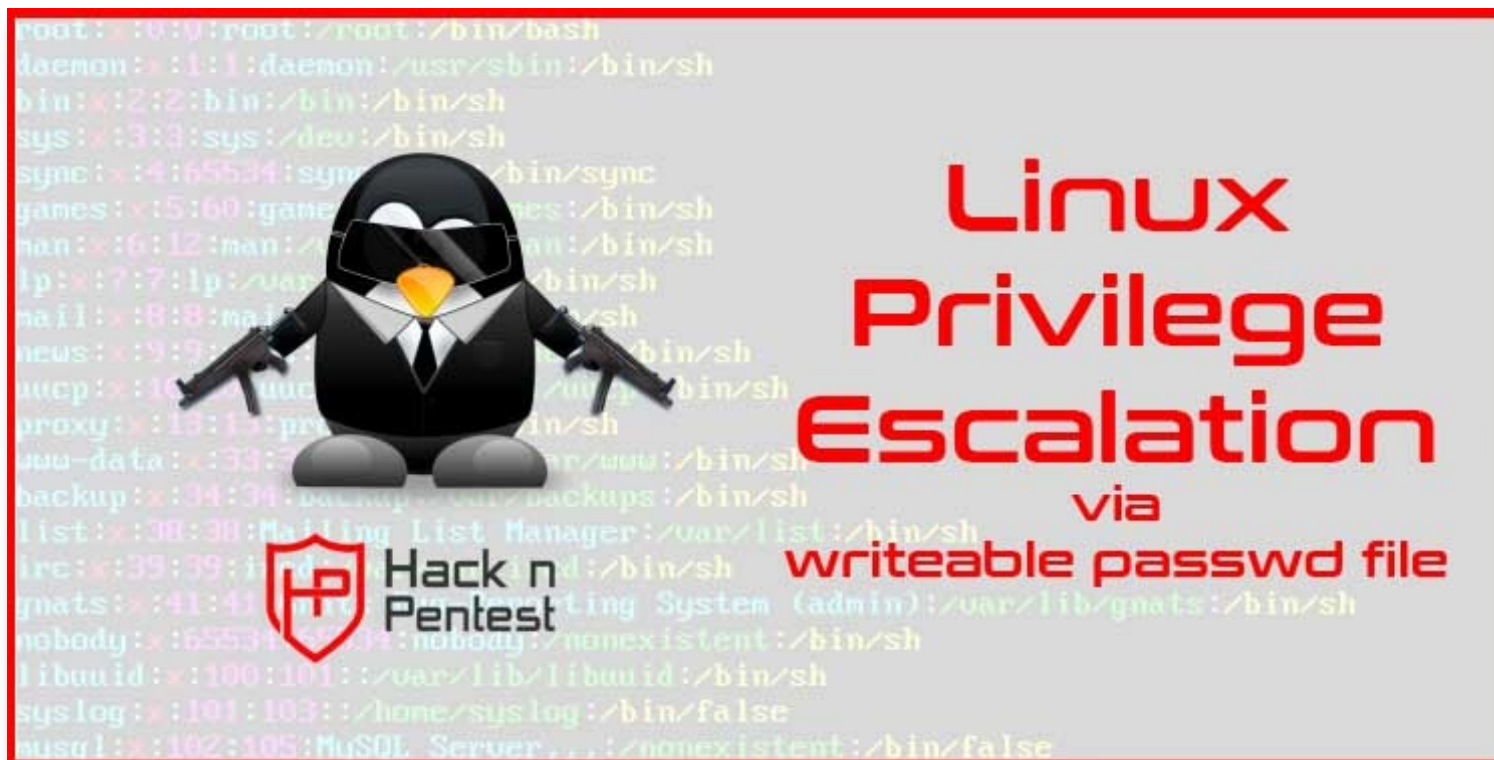
🕒 27th April 2019

Sharing is caring!

 Share

 LinkedIn

 Tweet



During the Red Team assessment, a Red Teamer faces many scenarios and one of the scenarios is a normal level shell or a low privilege shell. In the Windows environment, the Administrator or a member of Administrator has the high privileges and mostly the target is a high-end user. Similarly, In Linux environment root user or the user with sudo privileges are the most targeted one.

In this blog, we will be discussing about file misconfiguration which then leads to privilege escalation. Generally, during solving CTF, we always look at the passwd file to have an idea of the users available on the system.

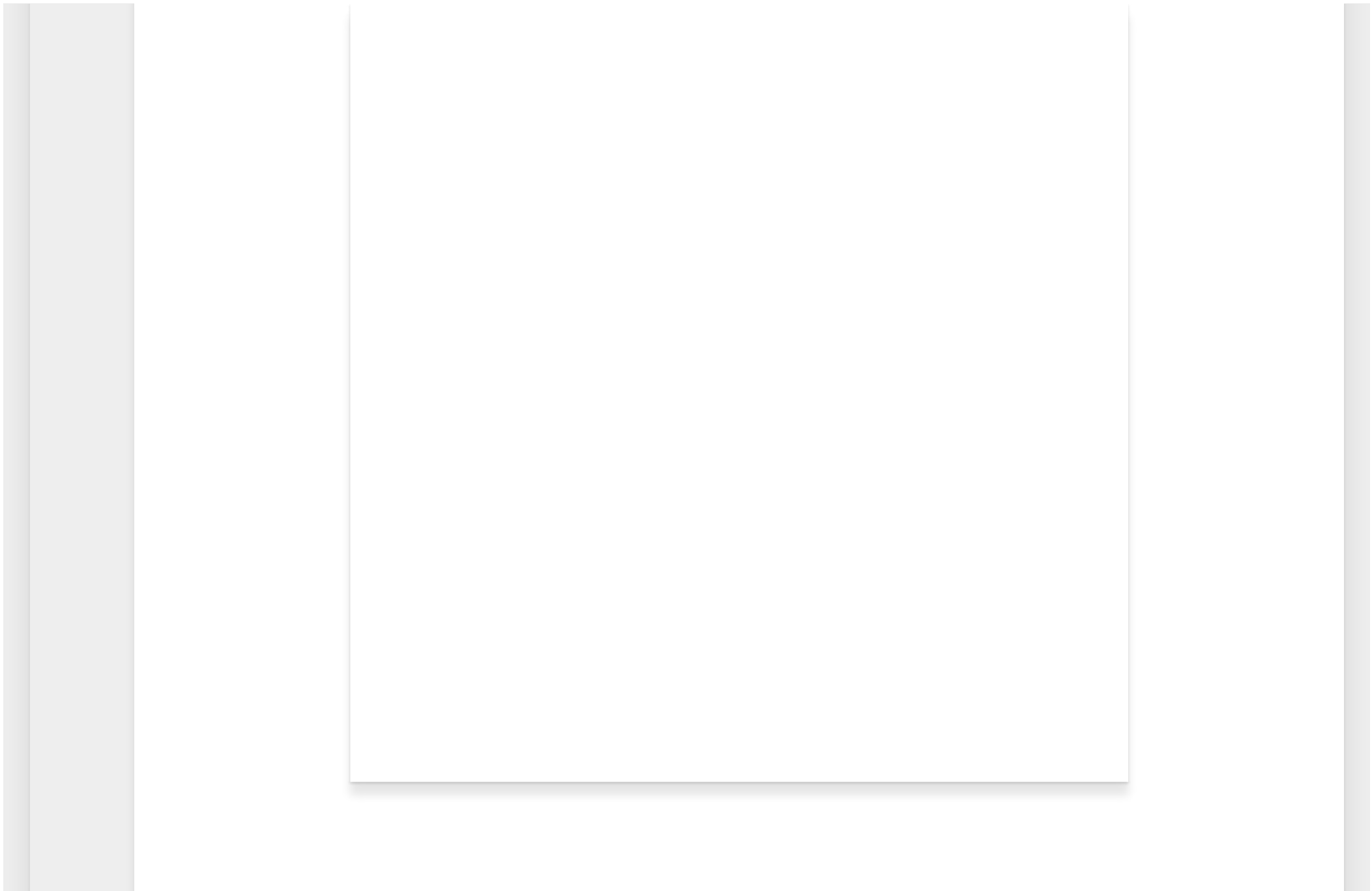
The passwd file is present at the **/etc** directory of the Linux root. The most important thing to note is that this file can be accessed by an unprivileged user.

/etc/passwd

/etc/passwd file is used to keep track of every registered user that has access to a system. It is a colon-separated file that contains the following information in sequence:-

- User Name
- Encrypted Password
- User ID (or UID)
- Group ID (or GUID)
- Full Name of the User
- User Home Directory
- Login Shell

Now, we will look at the /etc/passwd file: –



Let's have a detailed look at the `/etc/passwd` file, taking the root user as an example: –

- **root:** Username
- **x:** Placed for the User Password. The password is directly obtained from `/etc/shadow` file.
- **0:** UID of the root user.
- **0:** GID of the root user.
- **root:** Placeholder for user description.
- **/root:** Home Directory for the user. The user will be presented with this directory in a terminal session.
- **/bin/bash:** User's shell. Depending upon the user purpose, this shell would be spawned when the user logs on.

Environment Setup: –

Two Linux boxes with the following OS configurations set-up in VM with NAT Network mode (used to share host's IP Address).

OS Name	Role	OS Version	Machine IP	Kernel Version
Kali Linux (x64 bit)	Attacker Machine	Kali	192.168.245.134	4.12.0-kali2-686
Ubuntu (x64 bit)	Vulnerable Machine	Ubuntu 14.04.6 LTS	192.168.245.146	4.4.0-142-generic

Figure: OS Configuration

We are assuming that we have an initial foothold with hacknpentest user of the target system on our attacker machine (kali box). Now, we will upload `linuxprivchecker.py` python script to have a look at the misconfigurations at the target system.

We are using the wget (or web get) utility to download a file to the target server.



Figure: **Downloading enumeration script to the target server.**

By default, Python is installed on all linux machine. We will use the following command to run the enumeration script.

python linuxprivchecker.py





Figure: **Running the script**

Carefully looking at the script output, we found out that **passwd** file is world writeable that is have read, write and modify permissions to a normal user.





Figure: **Misconfigured Permissions on Passwd file**

Permission misconfigurations could be abused in a way that it leads to the escalation of current user privileges to root user. We will now try to write into the passwd file to make our way to root.

We will add a user to the passwd file explicitly giving the encrypted password in the respected fields. One can use perl language to generate an encrypted password with salt as follows:

```
$perl -le 'print crypt("THIS_IS_Original_PASSWORD","SALT")'
```

The following command will add a user with the encrypted password and UID, GID set to root [0] to the passwd file.

```
echo "Tom:Encrypted_Password:0:0:User_like_root:/root:/bin/bash" >> /etc/passwd
```

Let's discuss about the fields we are going to add to the passwd file.

Tom: Name of the User.

ad7t5ulalqMws: Encrypted User Password.

0: UserID of root.

0: GroupID of root.

User_like_root: User Description

/root: Home Directory for the User.

/bin/bash: User's Shell

'>>' sign redirects output to a file appending the redirected output at the end (here /etc/passwd file).

Now, let's make our way to root!

```
perl -le 'print crypt("Password@973","addedsalt")'
```




Figure: **Generating encrypted password**

The above command will generate a hash with the following password and salt:-

Original Password: Password@973

Salt: addedsalt

Encrypted Password: ad7t5ulalqMws

With the above encrypted password, let's now append the following to **/etc/passwd** file.

```
echo "Tom:ad7t5uIalqMws:0:0:User_like_root:/root:/bin/bash" &gt;&gt; /etc/passwd
```




Figure: **Appending to passwd file**

The Tom user is successfully appended to /etc/passwd file.

cat /etc/passwd

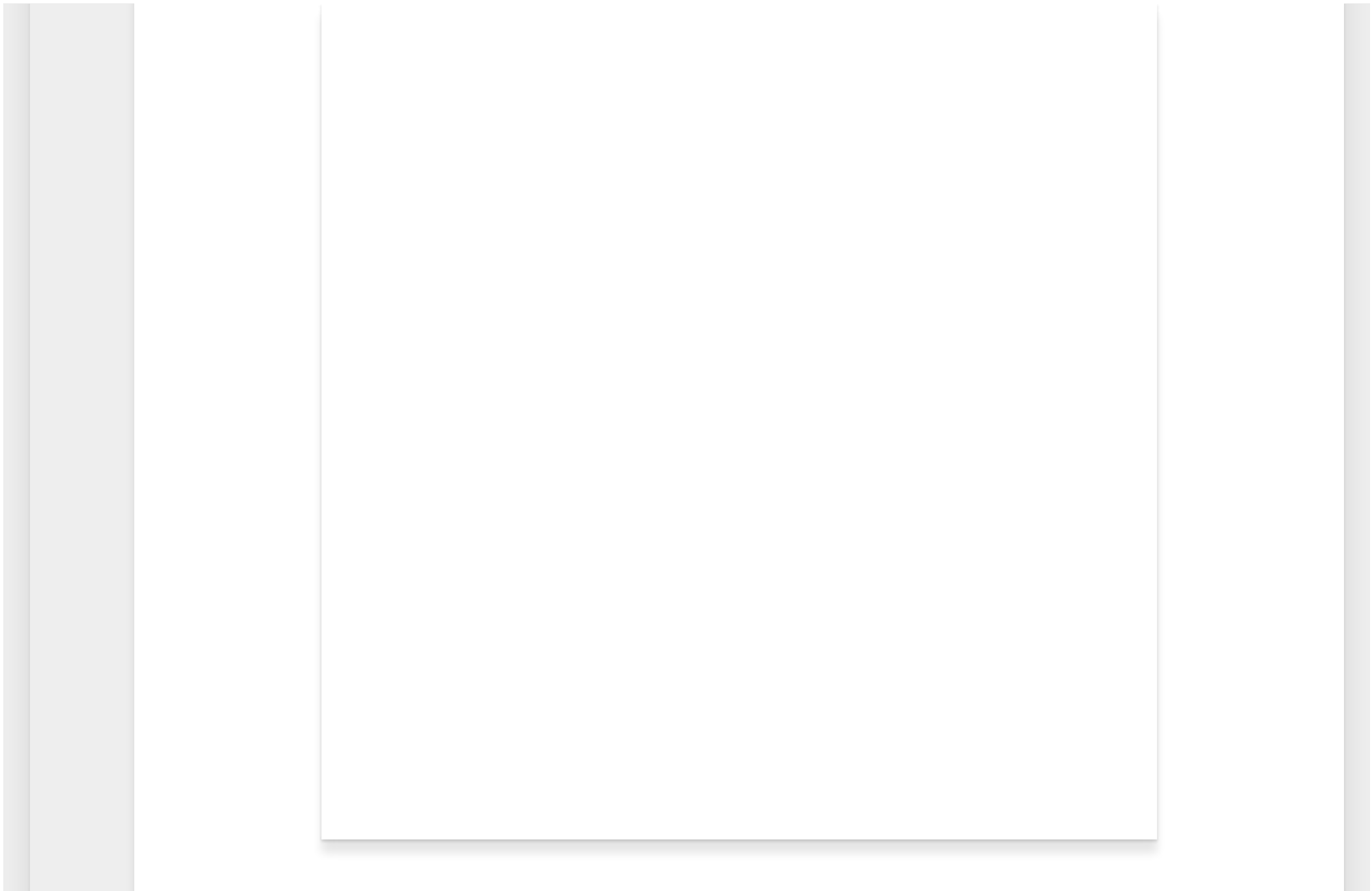
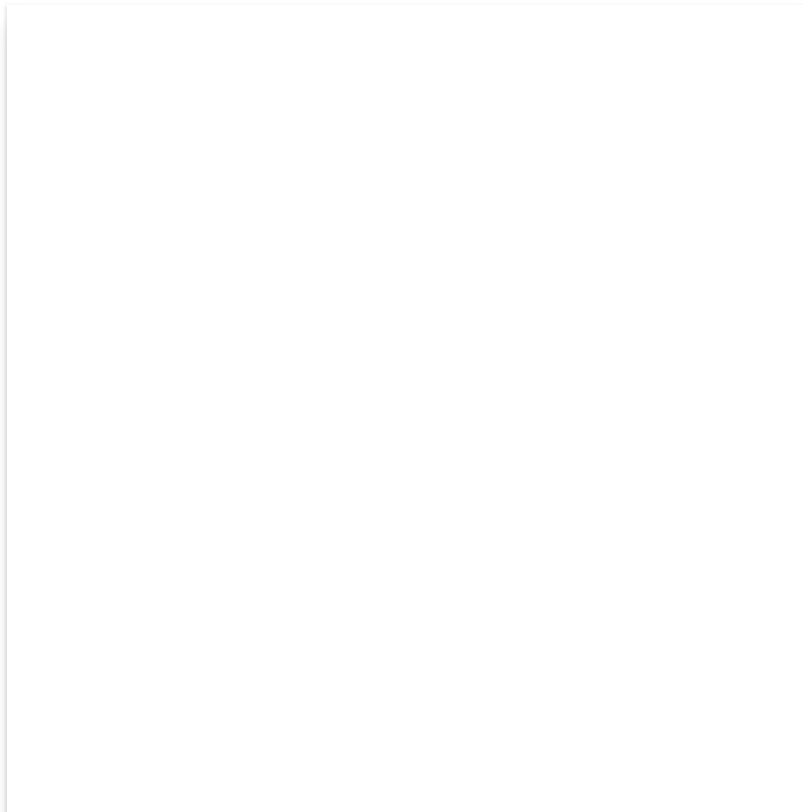


Figure: **User Added to passwd file**

Now using **su** command we will try to login with Tom user.



Oops!! We don't have a proper terminal, we will migrate to bash shell using the following python one liner (python is installed on the target server): –

```
python -c 'import pty; pty.spawn("/bin/bash")'
```




Figure: **Migrating to stable shell**

Now, we try to login with Tom user using the following command: –

```
su - Tom
```

And **BOOM!!** we are able to login with root privileges ????.

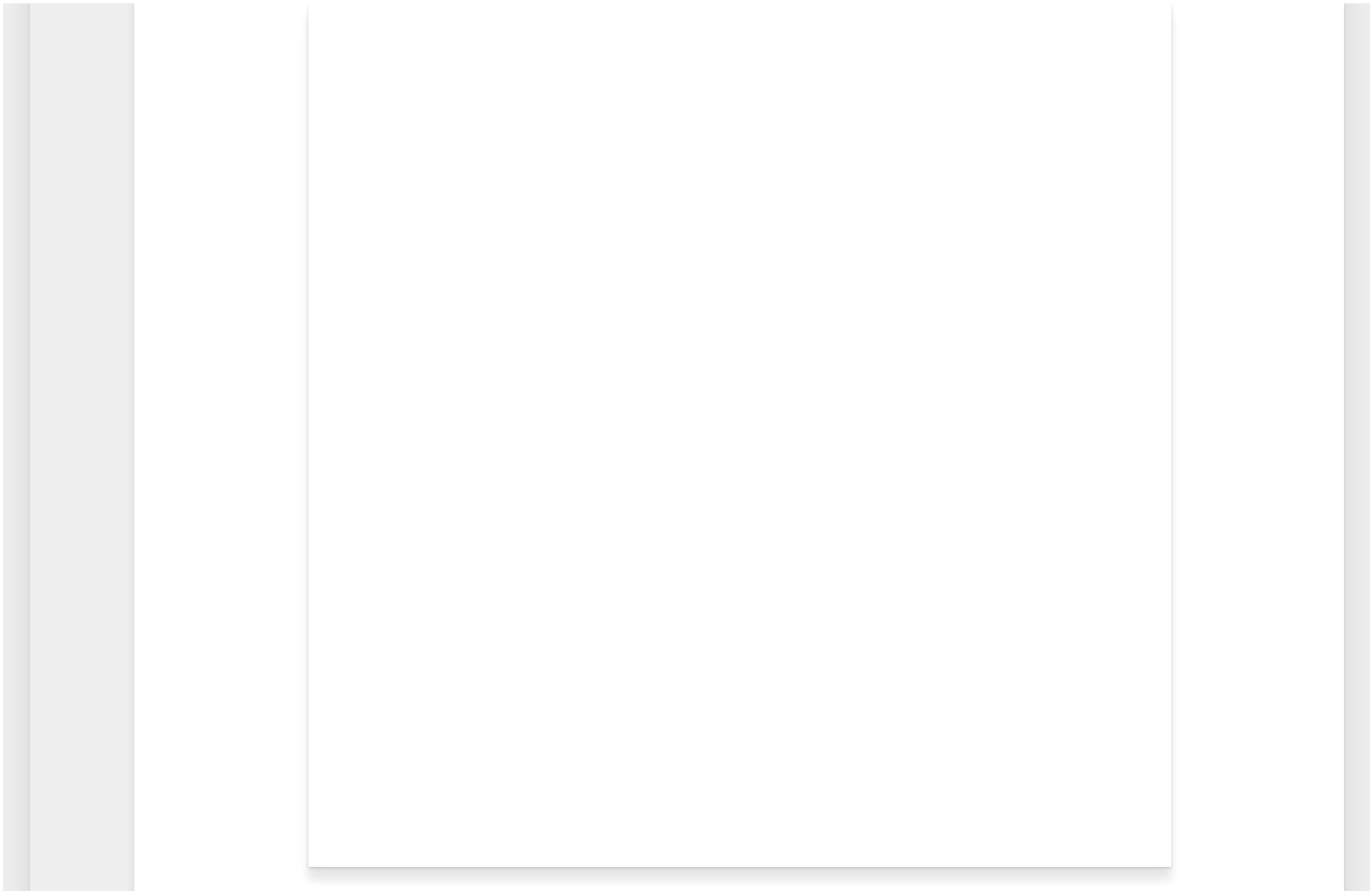


Figure: Escalated our privileges to root!

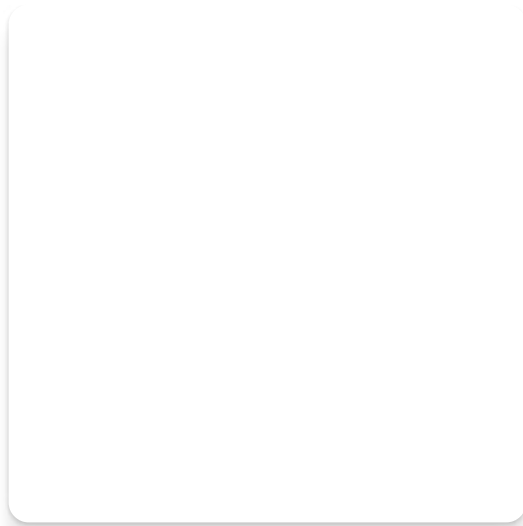
We had found permission misconfiguration on the passwd file, leveraging this we have made our way to login as root user. In the next blog post, we will be discussing about various other methods for Linux privilege escalation.

Till then hacknpentest!!!

Tags: [Linux](#) [Post Exploitation](#) [Ubuntu](#)

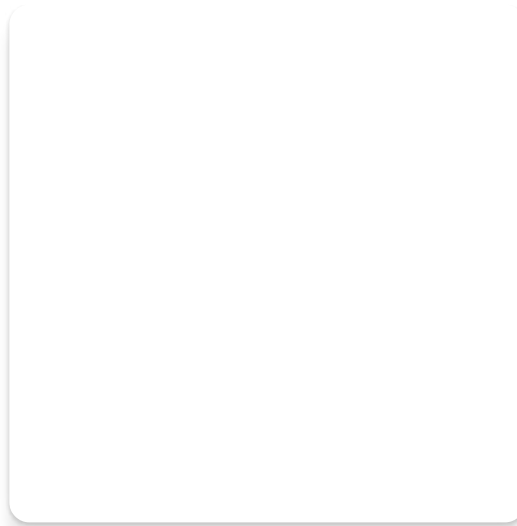


 You may also like...



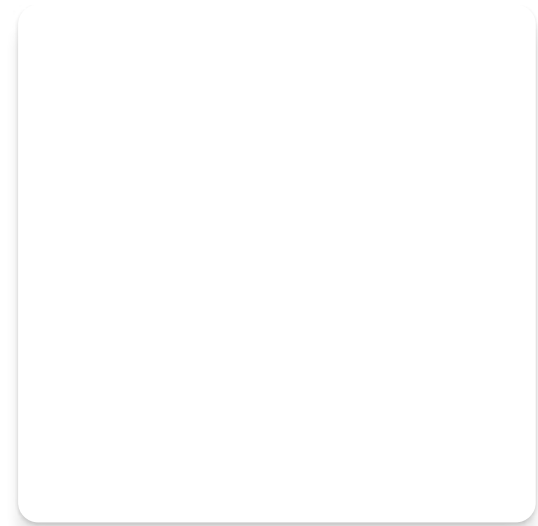
Windows Privilege Escalation Via AlwaysInstallElevated Technique

29th June 2019



Privilege escalation through Token Manipulation



8th July 2019



Privilege Escalation Using PowerShell

10th April 2019

2 Responses

 **Comments** **2**  **Pingbacks** **0**



Team Security  28th April 2019 at 9:21 pm

very nice tutorial

Reply



Yash Bharadwaj  28th April 2019 at 10:01 pm

Thanks!

Stay tuned for more 😊

Reply

Leave a Reply

Comment

Name *

Email *

Website

☐

Save my name, email, and website in this browser for the next time I comment.

Post Comment

NEXT STORY

Windows Privilege Escalation Via AlwaysInstallElevated Technique










Mimikatz – Windows Tutorial for Beginner (Part-1)

 To search type and hit enter





Recent Posts



-  Privilege escalation through Token Manipulation
-  Windows Privilege Escalation Via AlwaysInstallElevated Technique
-  Linux Privilege Escalation via writeable /etc/passwd file
-  Mimikatz – Windows Tutorial for Beginner (Part-1)
-  Exploit Active Directory Using PowerShell Remoting (PART-1)

Recent Comments



-  Yash Bharadwaj on Mimikatz – Windows Tutorial for Beginner (Part-1)
-  Louise on Mimikatz – Windows Tutorial for Beginner (Part-1)
-  Satyam Dubey on Windows Privilege Escalation Via AlwaysInstallElevated Technique
-  Aviral on Windows Privilege Escalation Via AlwaysInstallElevated Technique

