Testing Local System Security
-hackerXcreed-

ls /etc | grep version

The Distro Version Files

uname -a

- Checking Kernel Version

INFO: You should check the Current Version os Distro agains exploitdb,security focus,vuldb etc.

uptime

- Checking The Uptime of the system

cat /etc/timezone

- Check Time zone used

dpkg -l

- list the number of packages on the system

NOTE:The Number of Packages on the System should be limit and useless packages should be removed

ps -edf | grep log

- Check Which logging mechanism is used in the system

NOTE:The Can be Used To Guess the desired struture and location of log file in the system.

ifconfig -a

- Checking The network interfaces Present

NOTE: You can Check How can a attacker approach this target. From Where He can Approach Target.

route -n

- Checking The Current routes.

cat /etc/nsswitch.conf

- Checking The Full Picture Of How Dns,Users are configured

iptables -L -v

- Checking The Firewall Rules for Ipv4

NOTE: We can Check Whether the Firewall rules are installed or not if yes There You can Check Which Service is allowed to access to access from outer side from the internet and etc.

ip6tables -L -v

Checking The Firewall Rules for ipv6

*NOTE:*If There is no rules for The Ipv6 The rules should be set and if its not necessory it should be disabled.

cat /etc/fstab

Checking The Disks partition

*NOTE:*the Files Disks should have "noatime" "noexec" "nosuid" tags so that on intrusion no user binary files will not be executed on the system from the user accounts.

cat /etc/*sensitive_files

Checking Permission of Sensitive files Files lIke /etc/passwd and /etc/shadow

/etc/shadow.backup /etc/mysql/my.cnf

Their Permissions should be set in such a way that They Should be accessed By The users of the system.

find / -perm -4000 -ls

Checking Suid Files in the system

This command check the files set with suid which runs on the owner permission rather than the current user permission.

find / -type f -perm -006 2>/dev/null

listing the files that can be Readed from user accounts

find / -type f -perm -002 2>/dev/null

listing the files that can be Writed from user accounts

ls /var/www/

- Listing files in www folder

NOTE: Theese Files can be accessed by anyone in the system.

ls -n /etc/passwd

- Checking The UID's in The Password file

NOTE: On opening The File If The check out all the accounts if the any user have UID set to 0 he is working as root.

cat /etc/shadow

- Checking The Password Encryption Strenght

NOTE:By checking The files check The password encryption using hash-identifier

/etc/pam.d/common-password

Checking The default algorith to Encrypt the passwords.

$ cat /etc/pam.d/common-password

- Checking The Current Password Rules
- For The Default setting The password strenght is set to low

$ libpam-cracklib

- To Enhance the security you can install libpam-cracklin
- *$ apt-get install libpam-cracklib*
- *gedit /etc/pam.d/common-password*
- *set pam_cracklib.so retry=3 minlen=8 difok=4*
  - Whihc tells minimus length of Your password should be 8 and old password shold not be equal to new password.
- *pam_cracklib.so retry=3 minlen=8 difok=4 ocredit=-2 dcredit=-1*
  - *Tells Users to Add special characters in your password*

$ egrep -v '^#|^$' /etc/sudoers

- Checking User Restrictions

NOTE: This cammand Will list all The files in the User and all the privaliges a user can change to with or without Password.

$ ps -edf

- Checking The Current all running processes.

NOTE: The Tester Can Check the all the processes on the running on the system and can analyse the milicious and vulnerable processes.

$ lsof

- to get the list of network connection and especially services listening on the network.

NOTE: Using This Command The Tester Can grab a list of all services communicating with the network and tester can perform the vulnrability analysis on the basis of these tests.

$ lsof -i udp

- to get the list of network UDP connection and especially services listening on the network.

$ cat /etc/ssh/ssh_config

- This Command will Give us Information related to ssh service and config.

NOTE: So using this cammand you can check the ssh connection setting if you are using ssh service on your system. The most important the "PermitRootLogin" options which allows to connect as root in the system its value should be set to "NO"

$ mysql -u root

- Checking if I can get root access to mysql.

$ cat /etc/apache2/apache2.conf

- Review Apache Config file.
- $ leafpad /etc/apache2/apache2.conf
- $ leadpad /etc/apache2/envvars
- search for user and group
- and check if their permission is set to www-data or root
- keeping it with as root is highly unsecure as if the hacker was able to exploit the webapp her can compromise the whole security.

$ ls -lR /var/www/website/

- This Command is gonna show the permission of the Hosting on webserver.

NOTE: If any of the file are with root permission it may give attacker access to whole file system.

$ gedit /etc/apache2/conf.d/security

- and Tester can Manipulate some of the setting of the file and can protect webserver agains information leakage attacks.
- $ gedit /etc/apache2/conf.d/security
- $ search TRACE and Desable it
- set ServerTokens = Prod;
- set ServerSignature = Off;

$ cat cat /etc/apache2/mods-enabled/php.x.x.x.load

- cat /etc/apache2/mods-enabled/
- you will get an binary file from this copy the address
- string /usr/lib/apache2/modules/libphp5.so | grep apache
- it will help you to get some extra information about the configration of apache server.
- display_errors should be turned Off in production;
- error_reporting should be set to E_ALL ;
- log_errors should be turned On ;
- safe_mode can be bypassed but it will definitely slow down an attacker; it should be turned On ;
- disable_functions can be used to block access to sensitive functions like: eval , exec , passthru , shell_exec , system , proc_open ,popen …
- allow_url_include should be turned Off .

$ crontab

- Crontab is used on Linux/UNIX to run tasks at a given time.
- So if any crontab is running one the system anf if any user have access to edit that he can get run his desired scripts into the system
- $ cat /var/spool/cron/crontabs ----- Get the list of crontabs
- after executring this command you will get a list of scripts for automatic executrion you can go to their location
- and ls -lR to check the files permission.