All Offsec Pg Easy Machine's Notes

BBSCute Offsec Pg

User

1. CuteNews 2.1.2 - Remote Code Execution

Root

1. hping3 suid binary

CyberSploit Offsec Pg

User

1. Web source & Robots

Root

1. kernel exploit *3.13.0-32-generic* 'overlayfs' Local Privilege Escalation

Dawn Offsec Pg

User

1. Dirsearch check logs
2. SMB writeable permission

Root

1. sudo as Root

DC-1 PG offsec

User

1. Drupalgeddon2 Exploit

Root

1. find suid

Deception Offsec Pg

User

1. Web source
2. ssh

Root

1. python2.7 suid binary

FunBoxEasyEnum Offsec Pg

User

1. Mini shell
2. www-data to user passwd reuse (phpmyadmin)

Root

1. sudo su

Funboxeasy Offsec Pg

User

1. Dirsearch
2. Bookstore add book shell upload.

Root

1. Many binaries has sudo no passwd perm
2. sudo /usr/bin/time /bin/sh

FunBoxRookie Offsec Pg

User

1. FTP
2. Zip crack
3. ssh

Root

1. Privesc sudo su.

Gaara Offsec Pg

User

1. ssh
2. hydra password cracking

Root

1. gdb suid

Geisha Offsec Pg

User

1. Nmap port 7125
2. Dirsearch
3. hydra password cracking

Root

1. base32 suid

Ha-natraj Offsec Pg

User

1. LFI
2. Ssh log poisoning
3. apache2.conf writeable

Root

1. sudo nmap

Inclusiveness Offsec Pg

Initial foothold

1. Robots
2. User agent restriction bypass

User

1. LFI to RCE
2. File upload in ftp access over lfi

Root

1. Export Path Variable

InfosecPrep Offsec pg

User

1. robots.txt
2. private key

Root

1. suid binary
2. lot of another ways

Katana Offsec Pg

User

1. Nmap Port 8088
2. Dirsearch
3. Upload reverse shell

Root

1. python2.7 capabilities

Lampiao Offsec Pg

User

1. drupal 7 vuln to RCE

Root

1. Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)

Monitoring Offsec Pg

Root

1. nagioxi 5.6.0 vlun to rce and to root!

OnSystemShelldredd Offsec Pg

User

1. Ftp id_rsa

Root

1. mawk suid binary

Photographer Offsec PG

User

1. smb
2. koken 0.22.24 exploit

Root

1. php7.2 suid binary (./php7.2 -r "pcntl_exec('/bin/sh', ['-p']);")

Potato Offsec Pg

User

1. Ftp hints
2. PHPMagicTricks-TypeJuggling on password field 3.
lfi

Root

1. sudo su
2. path abuse

Sar Offsec Pg

User

1. sar2htm RCE

Root

1. Crontab runs a file that has writeable perm by user.

Seppuku Offsec Pg

User

1. Port 7601
2. Dirsearch
3. Bruteforce ssh

Horizontal privesc

seppuku to samurai

1. Check home directory files

samurai to tanto

1. Private key got from web

Root

1. sudo -l
2. Create malicious binary

Shakabrah Offsec Pg

User

1. RCE on host param

Root

1. vim.basic SUID Binary

Solstice Offsec Pg

User

1. Enumerate ports
2. Apache log poisoning

Root

1. check ps running
2. overwrite php file which root runs.

Sumo Offsec Pg

User

1. Apache cgi-bin exploit

Root

1. 3.2.0-23-generic vuln to dirtycow.

SunsetDecoy Offsec Pg

User

1. Zip Crack
2. Hash crack
3. ssh
4. Restricted Shell rbash

Root

1. pspy
2. honeypot.decoy

SunsetNoontide Offsec Pg

User

1. UnrealIRCd RCE

Root

1. su passwd is root that shows on linpeas.

Vegeta Offsec Pg

User

1. Dirsearch
2. wav file decrypt

Root

1. Writeable /etc/passwd and it .bash_history shows cmds.

Wpwn Offsec Pg

User

1. wordpress plugin social-warfare vlun to RCE!
2. wp-config passwd reuse to user.

Root

1. sudo no passwd for all sudo su.