**Hackthebox Lame**

I ran my nmap 10.10.10.3

nmap -T4 -p- -A 10.10.10.3

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-14 13:09 EST

Nmap scan report for 10.10.10.3

Host is up (0.10s latency).

Not shown: 65530 filtered ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 10.10.14.20

| 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

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

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

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Arris TG862G/CT cable modem (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.4.27 (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%), Linux 2.6.22 (92%), Linux 2.6.8 - 2.6.30 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 5h03m06s, deviation: 0s, median: 5h03m06s

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| NetBIOS computer name:

| Workgroup: WORKGROUP\x00

|\_ System time: 2020-11-14T13:14:41-05:00

|\_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 22/tcp)

HOP RTT ADDRESS

1 102.86 ms 10.10.14.1

2 102.92 ms 10.10.10.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

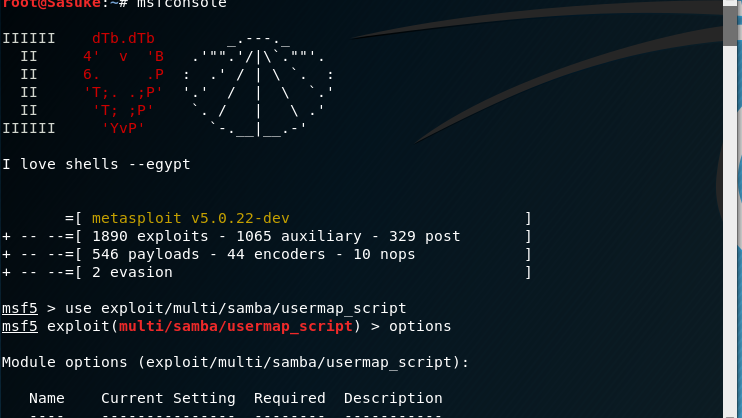
Nmap done: 1 IP address (1 host up) scanned in 154.13 seconds

I found smb version 3.0.20 exploit

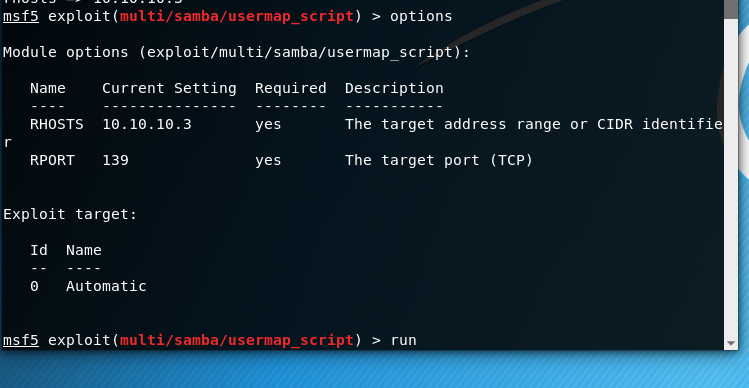
I googled that exploit above:

<https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script>

I opened msfconsole

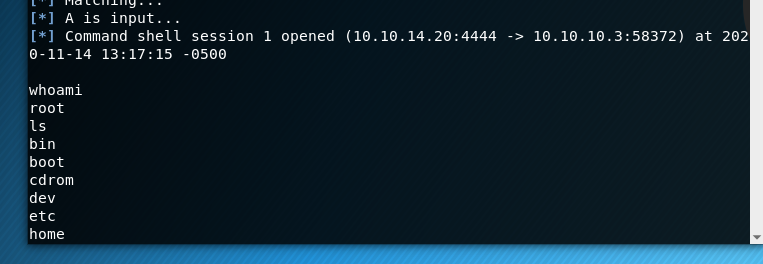


Set the rhost for the domain



Ran the exploit

Ran whoami



Located root flag! Success

