**HackTheBox Legacy**

**Legacy 10.10.10.4 -Windows machine**

Enumeration:

Opened terminal

Run my nmap command



After the scan is finished, I look at the results below:

Nmap scan report for 10.10.10.4

Host is up (0.10s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows XP microsoft-ds

3389/tcp closed ms-wbt-server

Device type: general purpose|specialized

Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (88%)

OS CPE: cpe:/o:microsoft:windows\_xp::sp3 cpe:/o:microsoft:windows\_server\_2003::sp1 cpe:/o:microsoft:windows\_server\_2003::sp2 cpe:/o:microsoft:windows\_2000::sp4 cpe:/o:microsoft:windows\_server\_2008::sp2

Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows XP (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows XP SP2 or Windows Server 2003 (91%), Microsoft Windows 2003 SP2 (90%), Microsoft Windows Server 2003 (90%), Microsoft Windows 2000 SP4 (90%), Microsoft Windows XP Professional SP3 (90%), Microsoft Windows XP SP2 (90%)

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

Network Distance: 2 hops

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

Host script results:

|\_clock-skew: mean: 5d01h00m23s, deviation: 1h24m50s, median: 5d00h00m23s

|\_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:f5:1a (VMware)

| smb-os-discovery:

| OS: Windows XP (Windows 2000 LAN Manager)

| OS CPE: cpe:/o:microsoft:windows\_xp::-

| Computer name: legacy

| NetBIOS computer name: LEGACY\x00

| Workgroup: HTB\x00

|\_ System time: 2020-11-11T07:48:29+02:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

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

TRACEROUTE (using port 3389/tcp)

HOP RTT ADDRESS

1 99.85 ms 10.10.14.1

2 99.90 ms 10.10.10.4

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

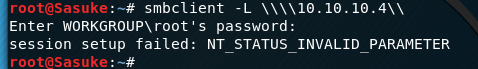
Nmap done: 1 IP address (1 host up) scanned in 387.34 seconds

I check and see smb ports are open so I go straight to the command:

Smbclient -L 10.10.10.4

I get the root password prompt and nothing

I then try this as well:



No success

Going back to: 445/tcp open microsoft-ds Windows XP microsoft-ds

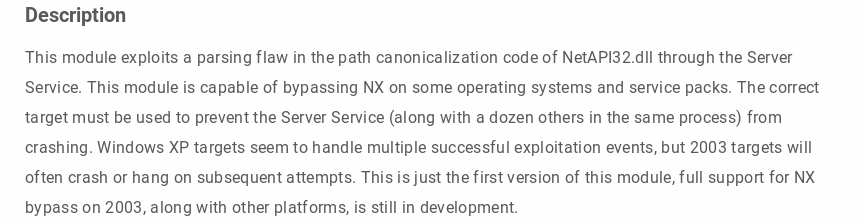
Windows XP shows but not the version

With that,

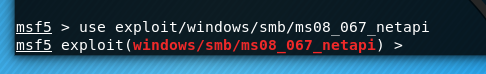
I use enumeration again and google: SMB Windows XP exploit

I then find a URL (Rapid7 – known for metasploit)

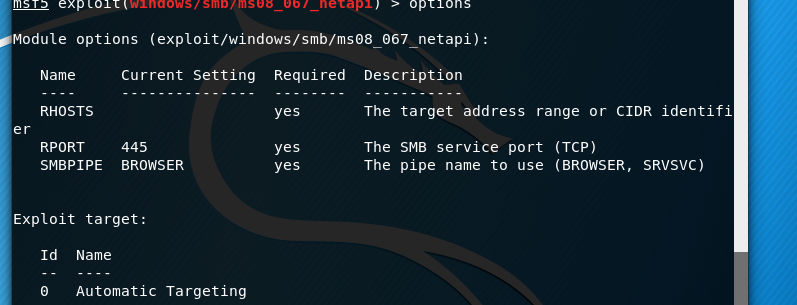
The description of the URL shows exactly what I am looking for:



I then copy there msf code and open Metasploit



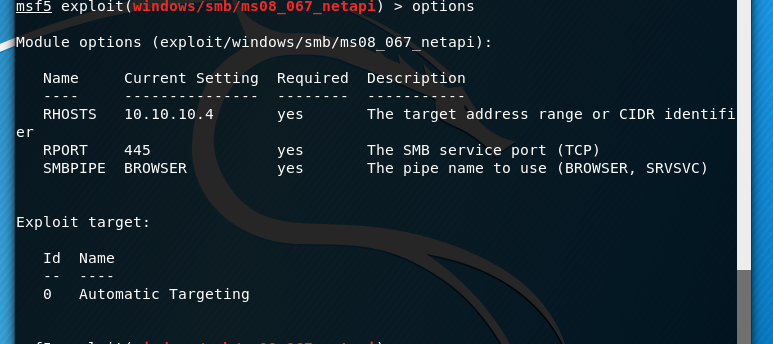
I enter the command Options to see all module options:



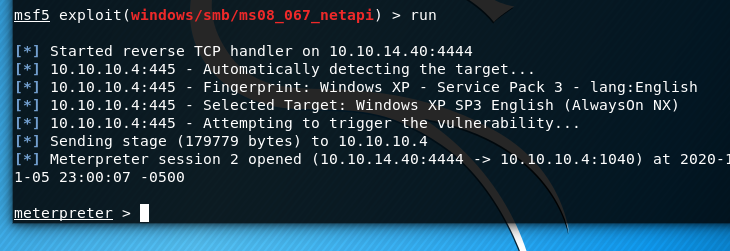
I need to set rhosts as the 10.10.10.4



To prove it worked:



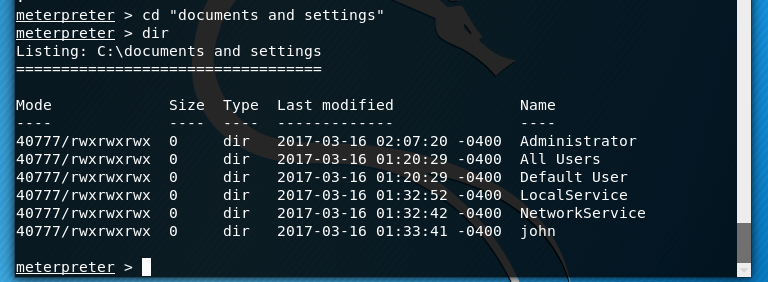
After that I exploit it:



Success! A reverse shell was complete

Now I can enter commands in this windows terminal

After that I look at the c: drive and find a documents and settings directory



I then cd to John and find a user.txt in his desktop and pull that and the user flag shows there

Same as root: from Administrator\Desktop\root.txt



Success both flags submitted

Below shows both user and root flags successful:

