SMB

Now, we are going to focus on SBM over port 139.

SMB is a file share system/application. Co-workers can share file on the same directory. SMB is usually internal.

Also, if we have scan folders. ie: if we can scan documents in the printer, and those documents "magically" appear in the "scan folders folder in our computer. These usually are SMB services.

The nmap scan already retrieve some information regarding SMB.

It returned the NetBIOS name: KIOPTRIX

and a potential version for the service : SMB2 ? maybe

The first tool we are going to be using here is Metasploit.

Metasploit SBM enumeration:

Msfconsole auxiliary mode helps us with scanning and enumeration. There are many modules to use, and help us gather more info on our target service's. Here, we will use the "smb_version" auxiliary scanner module to gather more information on the version of the service.

The auxiliary modulo has many "types". There are scanners, fuzzers, server, adminn, DOS, spoof, among others. Make sure to understand which type is each, and leverage them the best way possible within the rules of engagement, and the scope of the assessment.

What are we looking for here?

Any additional information from this service. The version, if its well configured (ie: does it allow anonymous login, what is the password policy, is the password policy strong enough, does the service allows us to fingerprint usernames, what are the shares in the system, can we access them, can we leverage info found in the shares, are there any known exploits available for the particular version, etc.)

By running the "smb_version" auxiliary module, we can find an specific version for the service:

```
[*] 192.168.163.131:139   - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.163.131:139   -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.163.131:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Then, we can use the #smbclient commands to gather more info.

#smbclient is going to attempt to connect to the Samba share that is out there

#smbclient -L \\\\IP_ADDRESS\\ to show all shares in the address

Then, we can use the same command to connect to the shares listed in the previous command output using

#smbclient \\\\IP_ADDRESS\\SHARE_NAME$ will attempt to connect to the specified share.

For this machine, we will only enumerate SMB until here.

Do not forget about

-#enum4linux command used to enumerate smb, and the additional auxiliary modules in Metasploit.

Question: My enum4linux and/or smbclient are not working. I am receiving "Protocol negotiation failed: NT_STATUS_IO_TIMEOUT". How do I resolve?

Resolution:

On Kali, edit /etc/samba/smb.conf

Add the following under global:

client min protocol = CORE

client max protocol = SMB3