

Username: Palm Beach State College IP Holder **Book:** Kali Linux – Assuring Security by Penetration Testing. No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

SMB enumeration

If you are testing a Windows environment, the easiest way to collect information about that environment is by using the **Server Message Block (SMB)** enumeration tool such as `nbtscan`.

The `nbtscan` tool can be used to scan the IP addresses for the NetBIOS name information. It will produce a report that contains the IP address, NetBIOS computer name, services available, logged in username, and MAC addresses of the corresponding machines.

This information will be useful in the penetration testing steps. The difference between `nbtstat` and `nbtscan` of Windows is that `nbtscan` can operate on a range of IP addresses. You should be aware that using this tool will generate a lot of traffic, and it may be logged by the target machines.

Note

To find the meaning of each service in the NetBIOS report, you may want to consult Microsoft Knowledge Based on *NetBIOS Suffixes (16th Character of the NetBIOS Name)* located at <http://support.microsoft.com/kb/163409>.

To access `nbtscan`, go to the console and type `nbtscan`.

If you are connected to a `192.168.56.0` network and want to find the Windows hosts available in the network, you can use the following command:

```
nbtscan 192.168.56.1-254
```

The following is the result of this command:

```
Doing NBT name scan for addresses from 192.168.56.1-254
```

IP address address	NetBIOS Name	Server	User	MAC

192.168.56.103	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00

From the preceding result, we are able to find out one NetBIOS name, `METASPLOITABLE`.

Now let's find the service provided by that machine by giving the following command:

```
nbtscan -hv 192.168.56.103
```

The following is the result of this command:

```
Doing NBT name scan for addresses from 192.168.56.103
```

```
NetBIOS Name Table for Host 192.168.56.103:
```

```
Incomplete packet, 281 bytes long.
```

Name	Service	Type

METASPLOITABLE	Workstation Service	
METASPLOITABLE	Messenger Service	
METASPLOITABLE	File Server Service	
METASPLOITABLE	Workstation Service	

METASPLOITABLE	Messenger Service
METASPLOITABLE	File Server Service
WORKGROUP	Domain Name
WORKGROUP	Browser Service Elections
WORKGROUP	Domain Name
WORKGROUP	Browser Service Elections

Adapter address: 00:00:00:00:00:00

From the preceding result, we can see that there are various services available on METASPLOITABLE such as File Server Service and Messenger Service .