NetBIOS Enumeration Wtih nmap & nbstat

NetBIOS Enumeration

With NetBIOS Enumeration we can scan a local area network or a specific target on the intranet and extract NetBIOS information from it like.

- Devices that belong to a domain
- Storage shares on the network
- Domain policies and passwords
- Printers on the network
- Group information and users

NetBIOS

Stands for Network Basic Input Output System and allows communication between different applications running on different systems within a LAN.

The service uses a 16 ASCII character string to identify a device on a local network.

The first 15th characters are for identifying devices, the last 16th character is to identify services.

Services and ports.

- UDP/137 Name service
- UDP/138 Datagram service
- TCP/139 Session service

In this quick guide i am using nmap, nbtstat on Windows, and NBTScan on Kali Linux. NBTSan can be run on Windows to if you what to try it there.

You can find several tools on all platforms that you can use for NetBIOS Enumeration, if you wish to test some other tools.

DISCLAIMER: This software/tutorial is for educational purposes only. Please don't use it for illegal activity. The author is not responsible for the use of the application or the users action.

Common NetBIOS Name Table (NBT) names

NetBIOS Code	Type	Information
<00>	UNIQUE	Hostname
<00>	GROUP	Domain name
<host name><03>	UNIQUE	Messenger service
<use rname><03>	UNIQUE	Logged-in user
<20>	UNIQUE	File Server Service

NetBIOS Code	Type	Information
<21>	UNIQUE	RAS Client Service
<22>	UNIQUE	Microsoft Exchange
<1B>	UNIQUE	Domain Master Browser
<1C>	GROUP	Domain Controllers
<1D>	GROUP	Master Browser
<INet~Services>	GROUP	IIS

Requirements

- Kali Linux
- NBTScan
- Nmap
- Windows AD
- Windows client on the same LAN as the Windows AD

Step 1: NetBIOS Enumeration With nbtstat in Windows

Open a CMD in windows and type in the fallowing syntax.

```
nbtstat -A 192.168.100.11
```

```
Ethernet0:
Node IpAddress: [192.168.100.12] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ONLINE-IT      <00>  GROUP       Registered
    SRV1           <00>  UNIQUE      Registered
    ONLINE-IT      <1C>  GROUP       Registered
    SRV1           <20>  UNIQUE      Registered
    ONLINE-IT      <1B>  UNIQUE      Registered

    MAC Address = 01:0c:29:3c:83:4e


Npcap Loopback Adapter:
Node IpAddress: [169.254.33.233] Scope Id: []

    Host not found.

C:\>
```

Step 2: NetBIOS Enumeration With NBTScan

NBTScan is by default installed on Kali Linux, but there is a Windows version as well.

NOTE: You need to open the tool in CMD for it to work in Windows.

We can use the tool to scan a whole network or just one target.

```
C:\NBTScan>nbtscan.exe  192.168.100.11-254
```

```
Doing NBT name scan for addresses from 192.168.100.11-254

IP address       NetBIOS Name     Server    User            MAC address
------------------------------------------------------------------------------
192.168.100.11   SRV1             <server>  <unknown>       01:0c:29:3c:83:4e
192.168.100.12   SRV2             <server>  <unknown>       01-0a-49-67-b8-01

C:\NBTScan>
```

Adding more arguments to the syntax to extract more information.

```
C:\NBTScan>nbtscan.exe -v 192.168.100.11
```

```
Doing NBT name scan for addresses from 192.168.100.11


NetBIOS Name Table for Host 192.168.100.11:

Incomplete packet, 191 bytes long.
Name             Service          Type
----------------------------------------
ONLINE-IT        <00>              GROUP
SRV1             <00>             UNIQUE
ONLINE-IT        <1c>              GROUP
SRV1             <20>             UNIQUE
ONLINE-IT        <1b>             UNIQUE

Adapter address: 01:0c:29:3c:83:4e
----------------------------------------

C:\NBTScan>
```

You can find more arguments in NBTScan:s official documentation.

Step 3: NetBIOS Enumeration With Nmap Scripting Engine

To run the nbstat.nse script, open Nmap and run the following syntax.

```
nmap -sV 192.168.100.11 --script nbstat.nse -v
```

```
Host script results:
```

```
| nbstat: NetBIOS name: SRV1, NetBIOS user: <unknown>, NetBIOS MAC:
01:0c:29:3c:83:4e (VMware)

| Names:

|   ONLINE-IT<00>        Flags: <group><active>

|   SRV1<00>             Flags: <unique><active>

|   ONLINE-IT<1c>        Flags: <group><active>

|   SRV1<20>             Flags: <unique><active>

|_  ONLINE-IT<1b>        Flags: <unique><active>



NSE: Script Post-scanning.

Initiating NSE at 17:50

Completed NSE at 17:50, 0.00s elapsed

Initiating NSE at 17:50

Completed NSE at 17:50, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

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

Nmap done: 1 IP address (1 host up) scanned in 141.97 seconds

           Raw packets sent: 1033 (45.436KB) | Rcvd: 1011 (41.756KB)
```

Conclusion

As we can see it easy to extract information with NetBIOS Enumeration techniques and tools.

We have used tools on both Windows and Linux and scanned an AD server on the domain.

To countermeasure NetBIOS enumeration you need to disable the service, however some old applications still relays on NetBIOS communication.

Check out the Ethical Hacking notes for more Kali Linux quick guides.

WordPress Enumeration with WPScan

WPScan is a vulnerability scanner that comes preinstalled with Kali Linux, but can be installed on most Linux distros.

The tool can be used to scan WordPress installations for vulnerability and security issues.

You can download the Turnkey image from here.

In this tutorial i am using WPScan to enumerate a WordPress website that is running on a Linux lab server, i am using Turnkey Linux with a WordPress preinstalled images for a server, the server is running on VMware Workstation.

DISCLAIMER: This software/tutorial is for educational purposes only. Please don’t use it for illegal activity. The author is not responsible for the use of the application or the users action.

Requirements

- Kali Linux
- WordPress Website

Step 1: WPScan Syntax

1.1 Update WPScan vulnerabilities database.

```
wpscan --update
```

1.2 Scan a website for vulnerabilities, you can either use a host name or a IP address.

```
wpscan --url 172.168.200.140
```

```
wpscan --url www.wordpress.local
```

NOTE: If you run WPScan on a website that is not running WordPress you will be notified in the output that the remote site is up, but not running WordPress.

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.6.0
           Sponsored by Sucuri - https://sucuri.net
       @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________


Scan Aborted: The remote website is up, but does not seem to be running WordPress.
root@iPhone:~#
```

1.3 Enumerate plugins

```
wpscan --url www.wordpress.local --enumerate p
```

1.4 Scan custom directory

```
wpscan --url www.wordpress.local --wp-content-dir custom-content
```

1.5 Enumerate themes

```
wpscan --url www.wordpress.local --enumerate t
```

1.6 Stealth Scan

```
wpscan --url www.wordpress.local --stealthy
```

1.7 Enumerate users, scan the target site for WordPress authors and usernames.

```
wpscan --url www.wordpress.local --enumerate u
```

```
[i] User(s) Identified:

[+] admin
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] testuser
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)


[+] Finished: Thu Jul 18 15:09:44 2019
[+] Requests Done: 16
[+] Cached Requests: 42
[+] Data Sent: 3.339 KB
[+] Data Received: 26.85 KB
[+] Memory used: 102.207 MB
[+] Elapsed time: 00:00:01
root@iPhone:~#
```

NOTE: limit how many usernames WPScan will enumerate

Step 2: Brute Force WordPress Account Password

2.1 We can use WPScan to brute force a WordPress account.

To run the attack we need a password wordlist, there is one called “rockyou.txt” in Kali Linux.

You can find it in “/usr/share/wordlists/ “

Type the command into terminal to brute force the password for a user

```
wpscan –url [wordpress url] –wordlist [path to wordlist] –username [username]
–threads [number of threads]
```

```
wpscan --url www.wordpress.local –wordlist /usr/share/wordlists/rockyou.txt
–username testuser –threads 2
```

NOTE: Eventually, you should see the password listed in the terminal next to the login ID of the user.

Step 3: Optional

3.1 Use WPScan with Tor and proxychains, for more information on how to setup Tor and proxychains please check out our notes.

NOTE: You need to start the Tor service before running the command.

```
proxychains wpscan --url www.wordpress.local
```

Conclusion

As we can see it is very easy for a attacker to scan a WordPress site and brute force a account.

To avoid WordPress enumeration and brute force attacks use WordPress plugins that limits the number of login attempts for a specific username and IP address.

Furthermore administrators should avoid using usernames as nicknames and display names, display names ares shown in WordPress and easy to scan.

WPScan scans the URL’s for usernames, if the administrator username is not used for publishing, then the account wont be scanned by WPScan”

DISCLAIMER: This software/tutorial is for educational purposes only. Please don’t use it for illegal activity. The author is not responsible for the use of the application or the users action.