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.

How To Uncover Hidden SSID With Kali Linux

In this quick lab we will go trough how to Uncover hidden SSID with Kali Linux and a wireless card that can be set to monitor mode.

SSID is short for service set identifier (SSID), SSID is the sequence of characters that uniquely identify a wireless local area network, the name can be up to 32 alphanumeric character and is case sensitive .

By default the configuration mode for a access point is to broadcast the SSID in a beacon frame, this allows clients to discover them easily.

Some network administrators disables the broadcasting of SSID in the configuration file, this tells the access point to not broadcast the SSID in the beacon frame, it is done in believe that it will add one more security layer to the network, the effect of not sending out the SSID is that only devices that knows the name of the SSID can connect to

the network.

Unfortunately hiding the SSID will not add any extra security layer to the WLAN, there are lots of different method to uncover a hidden SSID, you can use windows and android tools to automatically discover SSIDs, hiding the SSID should not be considered as a extra security layer.

Requirements

- Kali Linux
- Wireless card capable of monitor mode and packet injection, like the ALFA AWUS1900
- Your wireless card name

I am using a old D-link router with disabled SSID, for wireless card i am using is my 8 year old AWUS036H-

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

Step 1: Set Wireless card in monitor mode

1.1 Display wireless card name

```
sudo iwconfig
```

```
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
```

```
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Here we can see that my wireless card name is called wlan0.

1.2 Kill interfering processes

```
sudo airmon-ng check kill
```

1.3 Put the interface into monitor mode, this can be archived in different ways, i am using airmon-ng to start the card in monitor mode.

```
sudo airmon-ng start wlan0
```

NOTE: The command will create a new virtual interface with the same name as your old interface plus the word mon.

1.4 Display wireless card to confirm the new interface

```
sudo iwconfig
```

```
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
eth0      no wireless extensions.
```

```
lo        no wireless extensions.

root@iPhone:~#
```

Step 2: Scan for available networks

2.1 Use airodump-ng to scan for nearby networks and look for your router. i know that my BSSID is 84:C9:B2:6A:9E:90 and i am using channel 6.

```
sudo airodump-ng wlan0mon
```

```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -29      144       11    0   6  130  WPA2 CCMP   PSK  <length:
0>
 F0:9F:C2:AA:6C:B9  -47       45        0    0   1  195  WPA2 CCMP   PSK  Perham
 32:CD:A7:15:AD:49  -49       29        0    0   6  54e  WPA2 CCMP   PSK  DIRECT-
SoM2020 Series
 BC:EE:7B:7E:18:90  -49      124       12    0   9  195  WPA2 CCMP   PSK  nocco1
 80:2A:A8:44:C5:B1  -51       76        3    0   1  195  WPA2 CCMP   PSK  PontuS
 82:2A:A8:44:C5:B1  -51       63        0    0   1  195  WPA2 CCMP   PSK  <length:
0>
 F2:9F:C2:AA:6C:B9  -47       51        0    0   1  195  WPA2 CCMP   PSK  <length:
0>
 08:86:3B:DD:2C:95  -54       20        4    0   1  130  WPA2 CCMP   PSK
belkin.24d
```

I can see that the first SSID network have no SSID “<length: 0>” and it matches my BSSID and channel.

Now type down the BSSID and the channel of your access point and cancel the current command and rerun it specifying the BSSID and channel of the hidden SSID.

```
sudo airodump-ng -c 6 --bssid 84:C9:B2:6A:9E:90 wlan0mon
```

```
CH  6 ][ Elapsed: 18 s ][ 2019-07-15 20:21 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -25  87      185       35    0   6  130  WPA2 CCMP   PSK
<length:  0>
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0       21
```

We have two options while scanning the network, we can either wait for a new device to connect. The new device will send out a beacon frame, airodump-ng will immediately populate the SSID in the terminal output.

I will now connect a device to the network to demonstrate how it will show up in the output.

```
CH  6 ][ Elapsed: 6 mins ][ 2019-07-15 20:27 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -24 100     3247      416    0   6  130  WPA2 CCMP   PSK
HoneyP01
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0      262
 84:C9:B2:6A:9E:90  00:C0:CA:95:EA:8B   -7    0 - 1      2        6
```

Observer that the ESSID is now showing the name HoneyP01

Second options is to force disconnect one or all of devices that are associated with the AP. We can use aireplay-ng to disconnect devices by flooding them with de-authentication packets.

2.2 Open a new terminal and send de authentication packets to all connected devices on

the router. The command will send out 5 de-authentication packets to the access point.

```
sudo aireplay-ng -0 5 -a 84:C9:B2:6A:9E:90 --ignore-negative wlan0mon
```

```
20:38:49  Waiting for beacon frame (BSSID: 84:C9:B2:6A:9E:90) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:38:49  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:50  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:50  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:51  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:51  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
root@iPhone:~#
```

2.3 Go back to terminal one, now you should see the ESSID of the hidden WLAN.

```
CH  6 ][ Elapsed: 7 mins ][ 2019-07-15 20:39 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -16  96     4204      608    0   6  130  WPA2 CCMP   PSK
HoneyP01
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0      322
 84:C9:B2:6A:9E:90  00:C0:CA:95:EA:8B   -7    0 - 1e     0       37
```

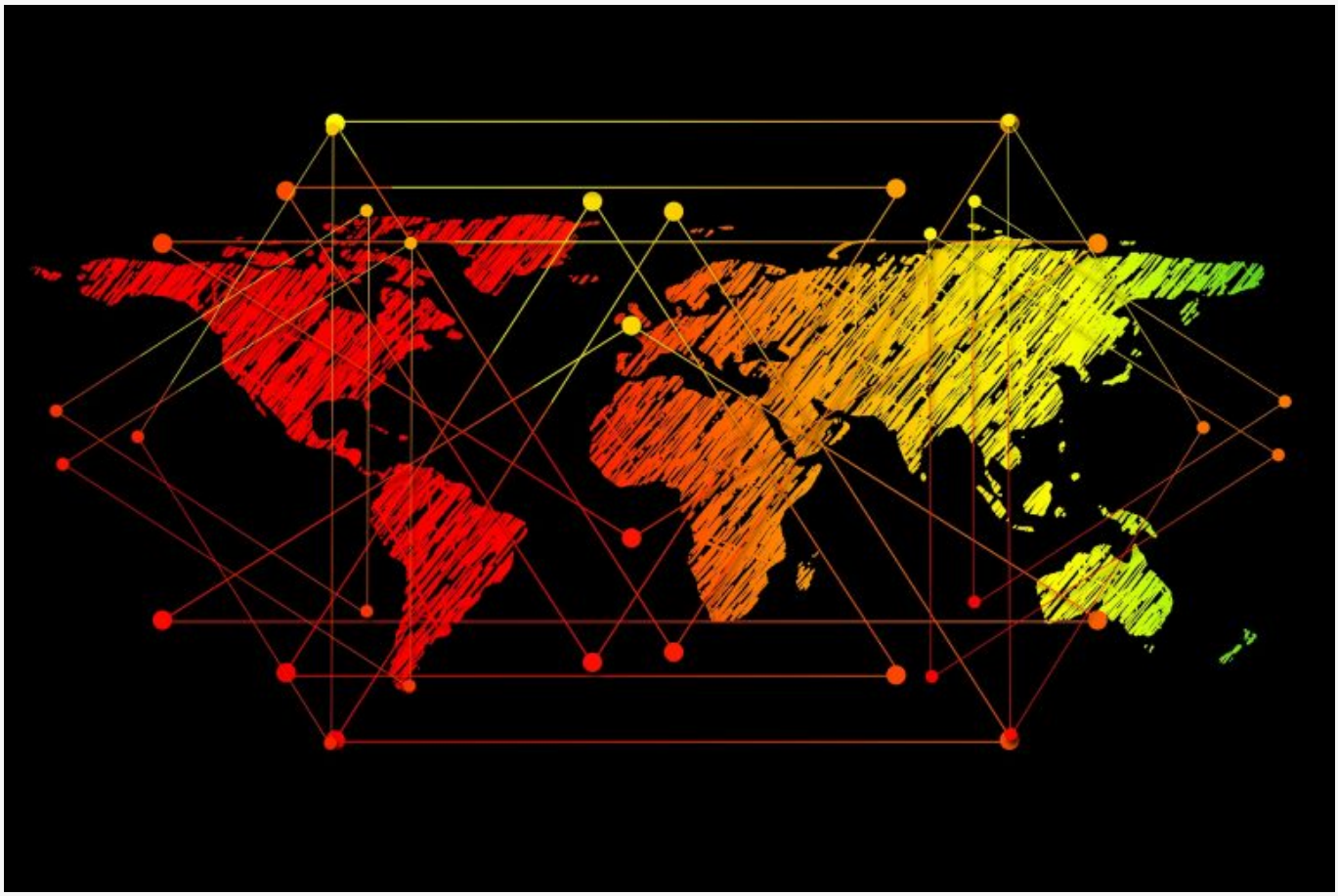
We can refine our scan and just target one associated device, modify the command by adding a target station.

```
sudo aireplay-ng -0 5 -a 84:C9:B2:6A:9E:90 -c 00:C0:CA:95:EA:8B --ignore-negative
wlan0mon
```

Conclusion

Uncovering a hidden SSID is easy, due to when a device connects to an access point. The device and the access point exchanges probe requests and response packets.

We have covered some basic terminal commands to uncover a hidden SSID. All equipment used on the lab is mine. Please don’t preform the commands on unauthorized networks.



How To Use Proxychains Kali Linux

Proxychains

Proxychains is open source software for Linux systems and comes pre installed with Kali Linux, the tool redirect TCP connections through proxies like TOR, SOCKS and HTTP (S)

and it allows us to chain proxy servers.

With proxychains we can hide the IP address of the source traffic and evade IDS and firewalls. We can use use proxychains in alto of situations, like when we want to avoid giving up our IP address or when scanning a target or visiting a website.

Furthermore chaining multiple proxies makes it difficult to track down the source IP address of the TCP connection, the application gives us a way to hide ourselves and stay anonymous. However proxy servers are likely to log your traffic and have to obey local law and jurisdiction.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step:1 Upgrade/Update & Install Tor

1.1 Upgrade and update the OS.

```
sudo apt-get update
sudo apt-get upgrade
```

1.2 Install the tor service.

```
sudo apt-get install tor
```

1.3 Start Tor service.

```
sudo service tor start
```

1.4 Display Tor service status.

```
sudo service tor status
```

NOTE: Tor service needs to run for proxychains to work.

Step2: Configure Proxychains

2.1 The proxychains configuration file is located in the “/etc/” directory edit the configuration file.

```
sudo nano /etc/proxychains.conf
```

There is three methods we can run proxychains.

1. strict_chain
2. dynamic_chain
3. random_chain

strict_chain: is the default option in proxychains, every connection goes through the proxies in order that is listed in the configuration file. Strict chaining is best used when you want the source traffic appear from a particular locations.

dynamic_chain: works like the strict chain but it does not require all the proxies in the configuration file to work. If a proxy is down then the connection will jump to the next proxy server in the list.

random_chain: randomnesses proxy connections from the list on the configuration file, the chain of proxy will look different to the target.

Uncomment out the “dynamic_chains” line, it will enable dynamic chaining.

```
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
```

NOTE: Uncomment “*chain_len*” if you are using random_chain , the parameter establishes the number of IP addresses in the chain which are utilized in generating your randomized chain of proxies.

2.2 By default proxychains sends traffic through the host at 127.0.0.1 on port 9050. This is the default Tor configuration, *if you are planing to use Tor leave the “defaults set to “tor” as it is. If you are not using Tor, you will need to comment out this line.*

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

2.3 Add proxy servers to the proxychains configuration file, there are free proxy servers on the Internet, i am using free proxy in this lab, you can find them here, another good site with free proxies is spys.one.

Before adding custom proxies add Tor socks5 support, and “socks5 127.0.0.1 9050”

```
# meanwile
# defaults set to "tor"
socks4         127.0.0.1 9050

SOCKS5          103.21.161.105 6667
HTTPS           156.202.174.101 8080
HTTPS           183.76.154.184 8080
HTTP            142.93.130.169 8118
SOCKS5          178.62.59.71 23187
SOCKS5          50.63.26.13 43001
```

2.4 Prevent DNS leaks, uncomment “Proxy DNS requests — no leak for DNS data”.

```
# Quiet mode (no output from library)
#quiet_mode

 Proxy DNS requests - no leak for DNS data
proxy_dns
```

Exit & Save

Step 3: Proxychains Syntax

3.1 Verify that the proxychains is working.

```
proxychains firefox www.whatsmyip.org
```

3.2 Use Proxychains with nmap.

```
proxychains nmap 1.1.1.1
```

```
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-14 22:00 CEST
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 57.22 seconds
root@iPhone:~#
```

Summit

We have covered how to run proxychains and hide the identity of our source traffic and stay anonymous without being detected.

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

DISCLAIMER: This software/tutorial is for educational purposes only.

The tutorial should not be used for illegal activity and the author is not responsible for its use or the users action.

How To Install GestióIP (IPAM) Ubuntu 18.04.02

In the guide i will Install GestióIP, “GestióIP is an automated web based IPv4/IPv6 address management (IPAM) software”.

GestioIP IPAM – IP Address Management

IP address management (IPAM) tools help us plan, deploy, mange and monitor IP addresses on our infrastructure.

We can automatically discovers IP addresses of servers and other devices that are connect to the network or have a domain name entire on the local DNS servers.

You can even send SNMP requests to gateways and get response back on connect devices.

I am running Ubuntu 18.04.2 as operating system, but you can install the application on all major Linux distributions.

Prerequisite

- Ubuntu Server 18.04
- User with sudo privileges.
- Static IP address
- Host name

For more information on how to create a sudo user and configure a static IP please see the quick guides Create Sudo User , Set Static IP address and Configure Host-Name. Check out the Linux guides for more quick guides on basic Linux configuration.

Step 1: System Preparation

1.1 Lets start by updating the repository's and software packages.

```
sudo apt update -y
sudo apt upgrade -y
```

1.2 GestióIP requires an Apache Web Server and MySQL/MariaDB database, as well as some SNMP MIBs.

```
sudo apt-get install make mysql-server mysql-client apache2 apache2-utils
libapache2-mod-perl2 snmp snmp-mibs-downloader wget
```

1.3 Download required MIBs

```
sudo download-mibs
```

1.4 Enable SNMP descovery, comment out the line “mibs :” in /etc/snmp/snmp.conf

```
sudo nano /etc/snmp/snmp.conf
```

```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
##mibs :
```

Exit & Save

Step 2: Configure MySQL

2.1 Start MySQL

```
sudo systemctl start mysql
```

2.2 Set a MySQL root password

```
sudo mysql_secure_installation
```

Set a root password and answer all following questions with “Y”

2.3 Change authentication plugin to “mysql_native_password”. Open the MySQL console.

```
sudo mysql
```

2.4 Switch to mysql databse

```
use mysql;
```

2.5 Display current authentication plugin method for the root user

```
select Host, User, plugin from user where user="root";
```

```
mysql> select Host, User, plugin from user where user="root";
+-----------+------+-------------+
| Host      | User | plugin      |
+-----------+------+-------------+
| localhost | root | auth_socket |
+-----------+------+-------------+
1 row in set (0.00 sec)
```

2.6 Change authentication plugin to “mysql_native_password”

```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';
```

Enter your password in ‘password’:

2.7 Display current authentication plugin method again

```
select Host, User, plugin from user where user="root";
```

```
mysql> select Host, User, plugin from user where user="root";
+-----------+------+-----------------------+
| Host      | User | plugin                |
+-----------+------+-----------------------+
| localhost | root | mysql_native_password |
+-----------+------+-----------------------+
1 row in set (0.00 sec)
```

2.8 Flush privileges and exit

```
FLUSH PRIVILEGES;
```

```
Exit
```

Step 3: Installation

3.1 Download the installation packet from www.gestioip.net and upload it to the server.

3.2 Unpack the gestioip_3.4.tar.gz file

```
sudo tar vzxf gestioip_3.4.tar.gz
```

3.3 Change to the gestioip_3.4 directory

```
cd gestioip_3.4
```

3.4 Runt the installation script

```
sudo ./setup_gestioip.sh
```

“Setup will propose a couple of parameters e.g. (“Where is Apache daemon binary?”). If you do not have special requirements you can confirm all default parameters by typing ENTER.”

Enter Y to everything the script wants to install.

NOTE: The setup will ask for the user which should be created for the HTTP Standard Authentication.

The script does not create the user automatically. You need to open a second shell and create the user for HTTP Standard Authentication manually by executing the command “htpasswd”

Open a new terminal and enter

```
sudo /usr/bin/htpasswd -c /etc/apache2/users-gestioip gipadmin
```

Create the new password

3.5 Go back to terminal one and press enter and continue with the installation

```
+-----------------------------------------------------+
|                                                     |
|    Installation of GestioIP successfully finished!  |
|                                                     |
|   Please, review /etc/apache2/sites-enabled/gestioip.conf
|            to ensure all is good and                |
|                                                     |
|              RESTART Apache daemon!                 |
|                                                     |
|            Then, point your browser to              |
|                                                     |
|           http://server/gestioip/install
|                                                     |
|          to configure the database server.          |
|         Access with user "gipadmin" and the
|        the password which you created before        |
|                                                     |
+-----------------------------------------------------+

origin@ipam:~/gestioip_3.4
```

3.6 Restart apache service

```
sudo systemctl restart apache2
```

3.7 Open the web based database configuration to complete the installation.
http://ip-address/gestioip/install

“Access with the rwuser and the password which you created during the setup with the command “htpasswd” (default rwuser: gipadmin):”

Step 4: Complete the installation

4.1 After entering credentials click “next” on the GestióIP’s installation “Welcome” site.

4.2 Enter the database configuration parameters and click “send”.

4.3 The fallowing page will show if the database parameters was successfully created.

Click “next page” to proceed with the configuration.

4.4 On Configure Sites and Categories enter your site name and network category.

You can change all this values later via the web GUI.

Click “next” to proceed.

4.5 If the configuration was successfully created

Click “next page” to proceed.

4.6 The last page shows if the installation has completed successfully.

If the installation was successful you will be asked to finish the installation by executing a command in the terminal window.

Copy the command and run it in the terminal on the server to delete the installation directory “/var/www/html/gestioip/install/”.

```
sudo rm -r /var/www/html/gestioip/install
```

The installation is now complete and you can open the web GUI by opening http://Your-Server-IP-Address/gestioip/

For mor information on how to configure GestioIP i recommend the official documentation which you can find here.

Conclusion

In this quick guide we have Install GestióIPan open source IPAM server on Ubuntu 18.04.02 and done some basic configuration to get the server up and running.