PRACTICAL ASSESSMENT SHEET

Experiment number: - 10

Title of experiment: - Study of Security Tool - NETSTUMBLER

Name of Student: - Niraj Nitin Surve

Roll number: - 68

Date of performance: -

Date of submission: -

Attendance 03 marks	Submission 03 marks	Performance 03 marks	Oral 03 marks	Result 03 marks	Total 15 marks

Faculty Signature with date

Practical No. 10

TITLE: STUDY OF SECURITY TOOL - NETSTUMBLER

AIM: TO STUDY SECURITY TOOL - NETSTUMBLER

THEORY:

What is NETSTUMBLER?

- NetStumbler (also known as Network Stumbler) was a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards.
- It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.
- A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system.
- Netstumbler has become one of the most popular programs for wardriving and wireless reconnaissance, although it has a disadvantage. It can be detected easily by most intrusion detection system, because it actively probes a network to collect information. Netstumbler has integrated support for a GPS unit.
- With this support, Netstumbler displays GPS coordinate information next to the information about each discovered network, which can be useful for finding specific networks again after having sorted out collected data.

Use of NETSTUMBLER -

- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detecting causes of wireless interference
- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links

The Right Hardware for the Job –

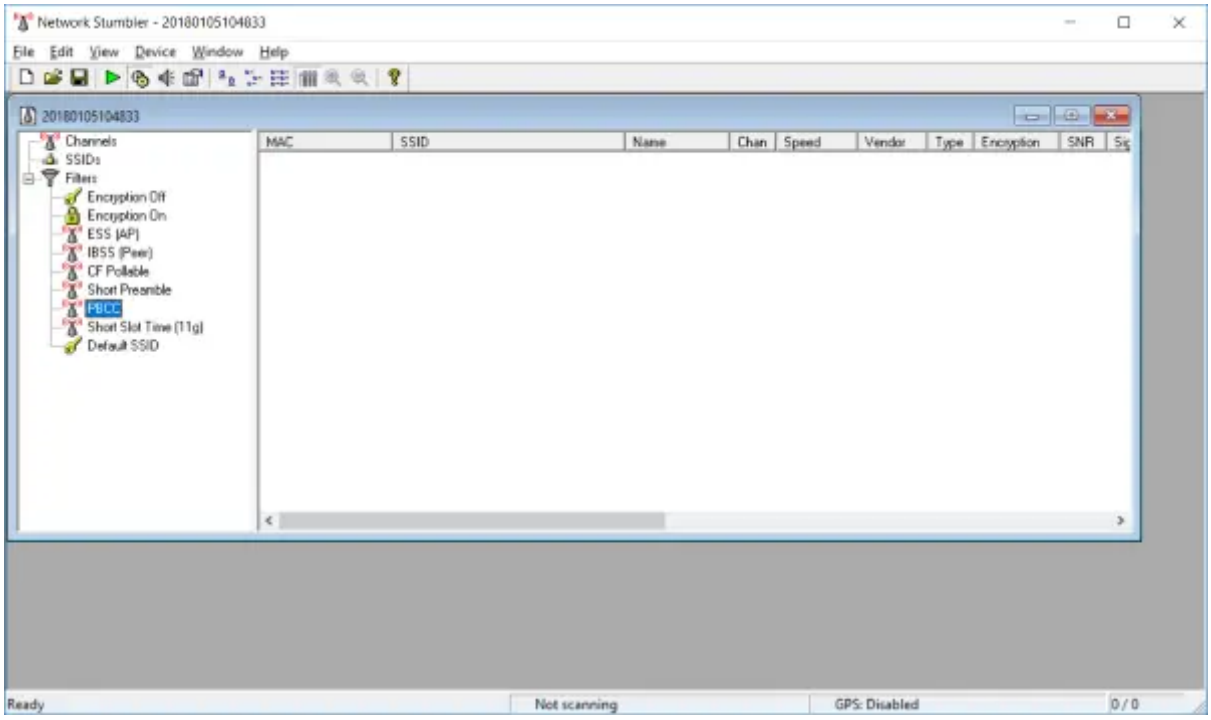
Requiring Windows 2000, XP or newer, NetStumbler functions best with a supported wireless card. Determining precisely which cards are fully supported can take some sleuthing.

NetStumbler fully supports cards based on the Proxim 8410-WD and 8420-WD, which have most commonly been sold under the names Orinoco Classic Gold and Orinoco Gold. Other cards based around this chipset include the Dell TrueMobile 1150, Compaq WL110, and Avaya Wireless 802.11b PC Card. Also supported are cards based on the Intersil (now owned by

Conexant) Prism and Prism2 wireless chipsets, such as the popular D-Link DWL-650. Unfortunately, there is no single comprehensive source of information on wireless card chipsets and retail models. Seattle Wireless maintains a wiki, and NetStumbler hosts user-submitted compatibility reports, although they do not indicate which chipset a card uses.

Wireless cards which are fully supported in NetStumbler are able to report accurate noise and signal strength levels. The latest 0.4 version of NetStumbler partially supports most wireless cards, but those without full support will not be reliable for noise and strength readings, and may cause instability in NetStumbler itself.

How to use NetStumbler for Scanning Wireless Networks?



1. Download the NetStumbler and Install it.

2. Run the NetStumbler. Then it will automatically starts scanning the wireless Networks around you.

3. Once its completed, you will see the complete list of wireless networks around you as shown in thesnapshot below:
   hacking wifi, hacking wireless,hacking wireless modem

List of Wireless Networks Scanned by NetStumbler

There you will see different columns such as MAC, SSID, SPEED, VENDOR, TYPE and much more...

4. Now select anyone of the MAC address that you wish to hack and want to explore more about that. If you click on the MAC address of one of the discovered wireless networks under channels, you will see a graph that shows the wireless network's signal strength. The more green and the less spaces are there, it indicates better is signal strength.
5. As you can see NetStumbler provides a lot more than just the name (SSID) of the wireless network. It provides the MAC address, Channel number, encryption type, and a bunch more. All of these come in use when we decide that we want to get in the secured network by cracking the encryption.

   There are two most common types of Encryption Methods used by Wireless Networks:

   a. WEP (Wired Equivalent Privacy) – WEP isn't considered safe anymore. Many flaws have been discovered that allow hackers to crack a WEP key easily.
   b. WAP (Wireless Application Protocol) – WAP is the currently the most secure and best option to secure your wireless network. It's not as easily cracked as WEP because the only way to retrieve a WAP key is to use a brute-force or dictionary attack. If your key is secure enough, a dictionary attack won't work and it could take decades to crack it if you brute-force it. This is why most hackers don't even bother.

Finding Access Points

While running NetStumbler, the right-hand pane shows APs currently detected and available under the current view filter. By default, you have no view filter set, so all detected APs are displayed.

Each AP listing is marked with a colored dot indicating the signal strength to that access point, alongside its MAC address, the unique identifier assigned to each network device. The colors range from red (signal too low) to yellow (marginal) to green (good). A grey dot marks an AP which had been detected but is now gone. A lock appears on the dot icon when the AP is operating with encryption enabled.

For many NetStumbler users, detecting available APs is the software's primary feature. Typically, the software is run on a mobile computer, which you either carry to some location or drive around with in the car, scanning the air for detected access points. The practice of hunting for access points has come to be known as "war-driving," another unfortunate term, since detecting APs alone is not itself an aggressive or malicious act.

To clear the record, NetStumbler does not connect you to available access points. While NetStumbler can detect them, you still need to rely on either Windows or your wireless card's management software to join a wireless network. Since your connection software also displays available networks, you may wonder, why bother with NetStumbler?

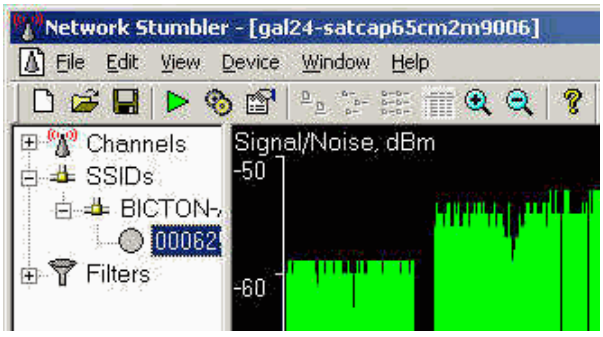
NetStumbler may better disambiguate access points which share an SSID, for one example. But more often, NetStumbler can continuously scan for access points as you roam about an area, presenting a convenient log of its activity, including audio notification. This functionality is typically not available from Windows' or vendor-provided wireless client software.

Exploring Access Points

The left pane of NetStumbler is an Explorer-like interface for navigating available wireless access points. Under the "Channels" heading, you will find all detected access points listed under their channel frequencies. Under "SSIDs," you will find all detected access points sorted by their network name. You may find two or more APs listed under the same SSID. This could indicate two separate wireless networks overlapping in range, which could cause problems for clients. Alternatively, it may indicate one wireless network with multiple APs available from your current location.

In cases where you find multiple APs sharing the same SSID, look at the "Subnet" field in the right pane. Here you will see which IP network the APs are operating on.

Signal-to-Noise Graphs



Clicking on an AP's MAC address in the left pane will replace the right pane with a live signal-to-noise graph. Note that this graph is accurate only if your network card is fully supported by NetStumbler. Signal-to-noise readings can be a powerful tool for troubleshooting your network and optimizing AP or antenna placement.

The graph overlays two sets of values – signal strength (green) and noise (red), measured in dBm. The "taller" your green plot, the stronger your signal; likewise, the taller your red plot, the more noise is present. For the best wireless performance, you want to maximize your signal and minimize your noise. Typical sources of noise in the Wi-Fi 2.4GHz range include microwave ovens, cordless phones, wireless video transmitters, and perhaps neighbouring wireless networks. You can also observe the consistency of your graph to determine the presence of sources of intermittent interference.

Partially supported network cards will produce signal strength (green) plots which may or may not be accurate, along with no noise (red) plots.

Access Point Filters

The "Filters" item in the left pane expands to a list of criteria for filtering the right pane list of available access points. If you click the "Encryption Off" filter, only open APs will be listed on the right. Some of the filters are quite technical, and are only useful in specialized situations. One thing to keep in mind – if you're not seeing an AP on the right that you know is available, check that you have not selected a filter which may exclude it from appearing.

Mobile Tracking with GPS

If your NetStumbling PC sports an attached GPS receiver, you can enable GPS support in NetStumbler to track the location of detected APs. Use the View, Options, GPS menu to configure your receiver. NetStumbler will fill in the latitude and longitude fields in the right pane, and will record GPS data in logs that you can output through the File, Export menu.

Extending NetStumbler

NetStumbler exposes a small library of functions which can be accessed through active scripting languages under Windows, including VBScript, JScript, and ActiveState's PerlScript and Python. You can connect NetStumbler to external scripts through the View, Options, Scripting menu.

One popular approach to scripting connects NetStumbler events to text-to-speech output, particularly valuable for so-called “war-driving.”

Conclusion- Thus we studied the security tool NETSTUMBLER.