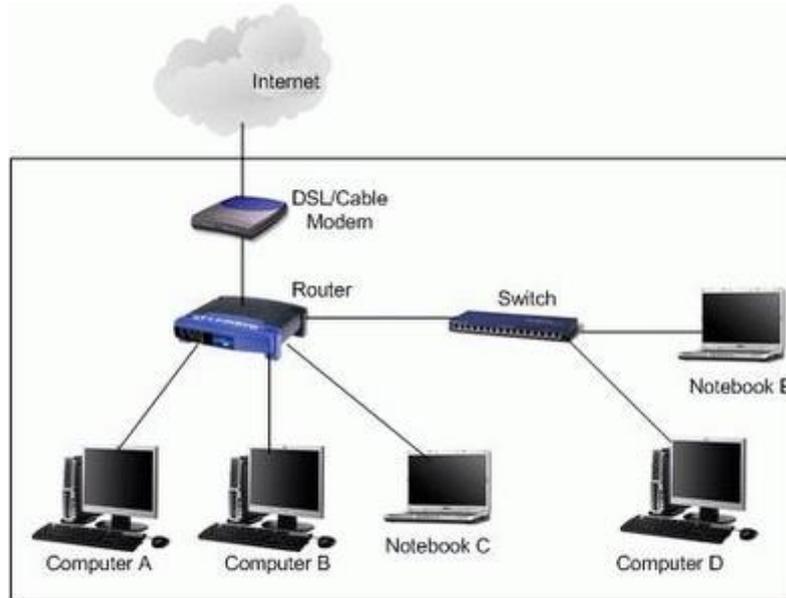


Wi-Hawk

I. Vulnerabilities and types of attacks in Wireless networks:

The elements that play major role in today's network architecture are router, gateway, switch, hub, access points etc. A typical network architecture looks like following:



In a typical network, wireless or wired router is the key element responsible for connecting the Local Area Network (LAN) to the internet. A router can be connected to two or more data lines from different network which play the important role of forwarding data packets within computer networks. Home/Small office routers are the most familiar type of routers that simply pass data between home computers and Internet. One such example is the DSL/Cable modem, which through ISP connects the LAN to Internet. As these networks are used to access internet, sensitive data that needs to be confidential and private is being transmitted in these networks. Ineffective or weak security in networks can lead to major security breaches and attackers can gain access to this sensitive data.

Security measures at each and every component in network are imperative and there has been significant development in last decade to make networks even more secure. While powerful security rules have been implied at different components of network, router has been one such sensitive and essential element in network which is still poorly configured by companies. They can be compromised by attackers to gain unauthorized access to the private network and can lead to malicious activities like following:

1. An attacker could configure the router to use a malicious DNS (Domain Name System) server, which would allow the attacker to redirect users to malicious websites.
2. An attacker can set up port forwarding rules to expose internal network services to the Internet.

Vulnerabilities in the management interfaces of wireless routers, vulnerabilities in protocols, inconsistencies in router software and weak authentication can expose the device to remote attacks and thus can be compromised by attackers. These issues had been raised by researchers in late 2013.

Even if companies provide patches to upgrade management interface and inconsistencies in router software, these vulnerabilities are unlikely to go away soon because many users never update their routers and other embedded systems. That's because they don't know how or because they're not aware of the risks. Also a lack of clear communication about security issues from many vendors adds up to this problem.

Due to above said vulnerabilities there are different types of attacks possible on routers which have been identified.

1. Distributed Denial of Service Attack

As the name suggests, a distributed denial of service attack can use hundreds and potentially thousands of computers to send packets to routers at the same time. The attacker uses software scripts on each computer's hard drive to launch the attack. Once attack is successful ability to target routers and overpower their resources is achieved.

2. Syn Flood

The TCP protocol uses synchronization referred to as TCP/SYN packets for a connection request between computers and servers. When a SYN flood attack occurs, the source computer sends a large number of TCP/SYN packets using a forged address. The destination server on the network is unable to successfully establish a connection to the source due to the address being unreachable. If there are lots of such open connection made then it can lead to consumption of resources at server leading to a form of denial of service.

3. Brute Force

Routers can experience a brute force attack when a hacker is attempting to guess the password and gain access. This type of attack is not limited to a business router; it can also occur whenever a hacker is in range of a home wireless router.

4. Disgruntled Employee

A disgruntled employee with knowledge of the network topology, router login and password information can access routers without authorization and compromise the network.

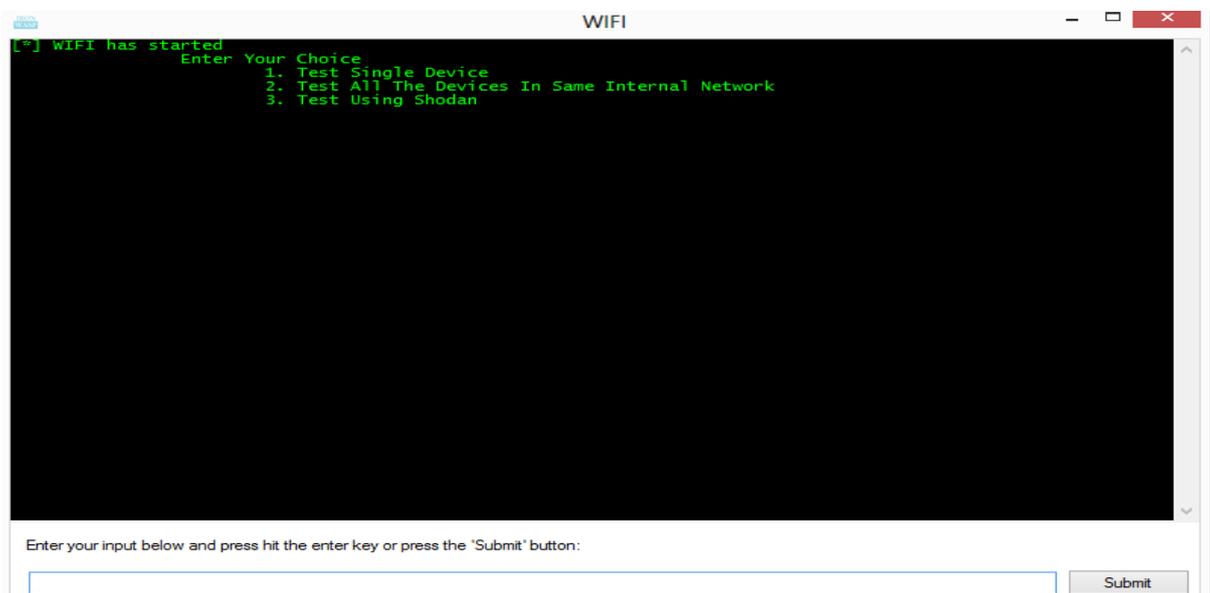
When we talk about providing security at routers, ideally things that come into our mind are Antivirus & firewall. But leaving your wireless router at its default configuration creates a loophole in your network which can lead to unauthorized access to your network. If you keep your wireless router at the defaults, then hackers can control your firewalls, what ports are forwarded, and more.

In a wireless network there are thousands of Wi-Fi routers which are configured with default user name and passwords, which make them vulnerable to security breaches. A wireless router when newly installed has a default configuration including its user name and password depending on its manufacturer and model. If these default configurations are not changed or software of the router is not updated, the router can be compromised by an adversary to hack into the wireless network. A list of default username and passwords which is used for router's configuration can be obtained readily from internet which then can be used by adversaries to identify whether the router is using their default password or not. If you are not updating your router's software it makes your router vulnerable too.

II. Wi-Hawk:

Wi-Hawk is an open source tool for auditing a range of IP addresses to sniff out Wi-Fi routers which are configured with default admin passwords and find out the routers which are vulnerable to bypass Authentication. The tool provides capability to scan network for such default configured routers by taking input in one of the following format:

1. Single IP
2. Range of IP
3. SHODAN^[1]
 - SHODAN is a search engine which returns a customized list of IPs/servers. The search criteria can be based on any of the following inputs :
Country, City, Port, Host name, Geo Location, Server, OS, Date range, SSL Filters.



The tool can be used to identify following two types of security vulnerabilities in routers/IPs provided in any of the above way:

1. Authentication Bypass
2. Routers configured with default username/passwords

Authentication Bypass:

Authentication plays a critical role in the security of web applications. When a user provides his login name and password to authenticate and prove his identity, the application assigns the user specific privileges to the system, based on the identity established by the supplied credentials.

While most applications require authentication for gaining access to private information or to execute tasks, not every authentication method is able to provide adequate security. Negligence, ignorance, or simple understatement of security threats often result in authentication schemes that can be bypassed

by simply skipping the login page and directly calling an internal page that is supposed to be accessed only after authentication has been performed. In addition to this, it is often possible to bypass authentication measures by tampering with requests and tricking the application into thinking that the user is already authenticated. This can be accomplished either by modifying the given URL parameter or by manipulating the form or by counterfeiting sessions.

Authentication bypass vulnerabilities, like buffer overflows, are generally caused by programmers when they assume that users will behave in a certain way, failing to foresee the consequences of users doing the unexpected. Penetration testing framework like Metasploit^[2] includes a number of authentication bypass modules which use techniques such as exploiting buffer overflows in the authentication mechanism, but there are simpler methods that hackers can use as well.

Wi-Hawk has been successfully able to identify routers for which authentication can be bypassed just by editing the http request URL to the IP. Wi-Hawk maintains such a list of URL which when appended to the http request can bypass authentication of the router.

Identifying routers with default Username/Password

The tool uses a database which contains a list of possible router's default username/passwords. Based on type of input given it scans a single IP, or a range of IPs, or uses SHODAN search engine to scan the IPs returned by the search.

III. Demo:

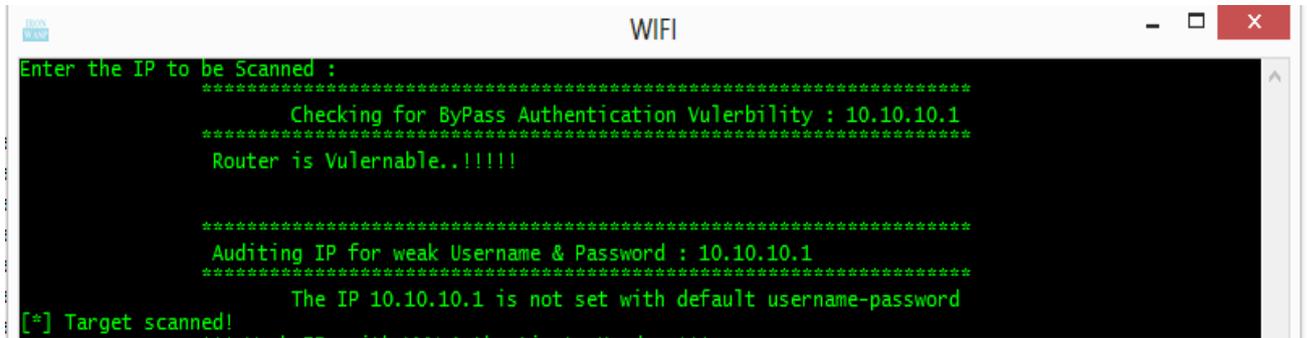
Single IP:

When user provides IP in xxx.xxx.x.x format, Wi-Hawk first checks whether router is vulnerable to bypass authentication or not, then it goes for auditing the password for the given IP.

1. Provided IP of router is Vulnerable but not configured with Default Username & password.



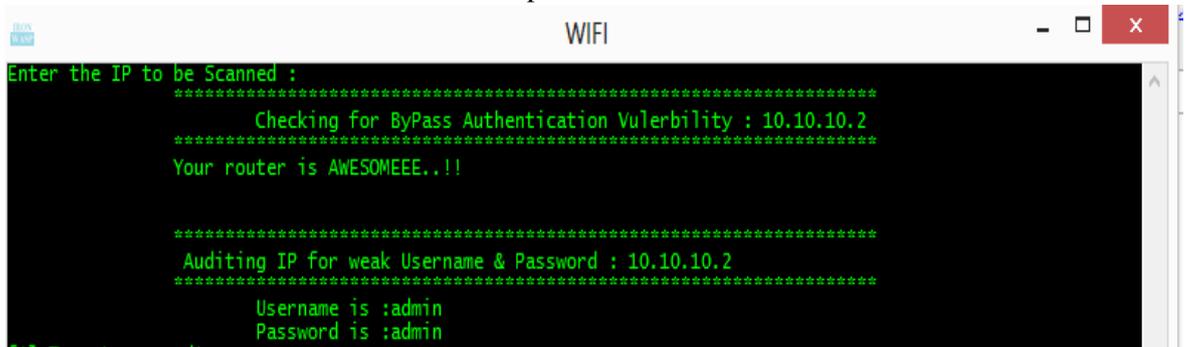
Results:



```
WIFI
Enter the IP to be Scanned :
*****
Checking for ByPass Authentication Vulnerability : 10.10.10.1
*****
Router is Vulernable..!!!!

*****
Auditing IP for weak Username & Password : 10.10.10.1
*****
The IP 10.10.10.1 is not set with default username-password
[*] Target scanned!
```

- 2. Provided IP of Router is not Vulnerable to Bypass Authentication but uses Default Username and password.



```
WIFI
Enter the IP to be Scanned :
*****
Checking for ByPass Authentication Vulnerability : 10.10.10.2
*****
Your router is AWESOMEEE..!!

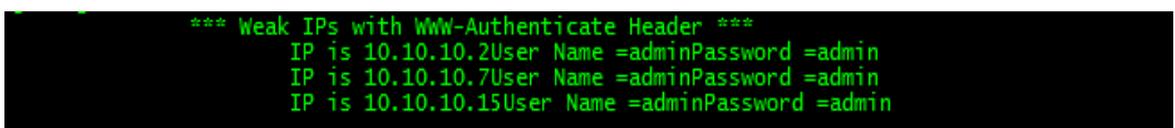
*****
Auditing IP for weak Username & Password : 10.10.10.2
*****
Username is :admin
Password is :admin
```

Range of IP:

Wi-HAWK supports different format for range of IPs, User can provide IPs in XXX.XX.X.X-X or XXX.XX.X.X/X format.

When provided a range of IP in above format, Wi-Hawk performs the same action as it does in scan for Single IP. For each IP in the given range, Wi-Hawk will first check if router is vulnerable to bypass authentication followed by auditing of each IP for default Username and Password.

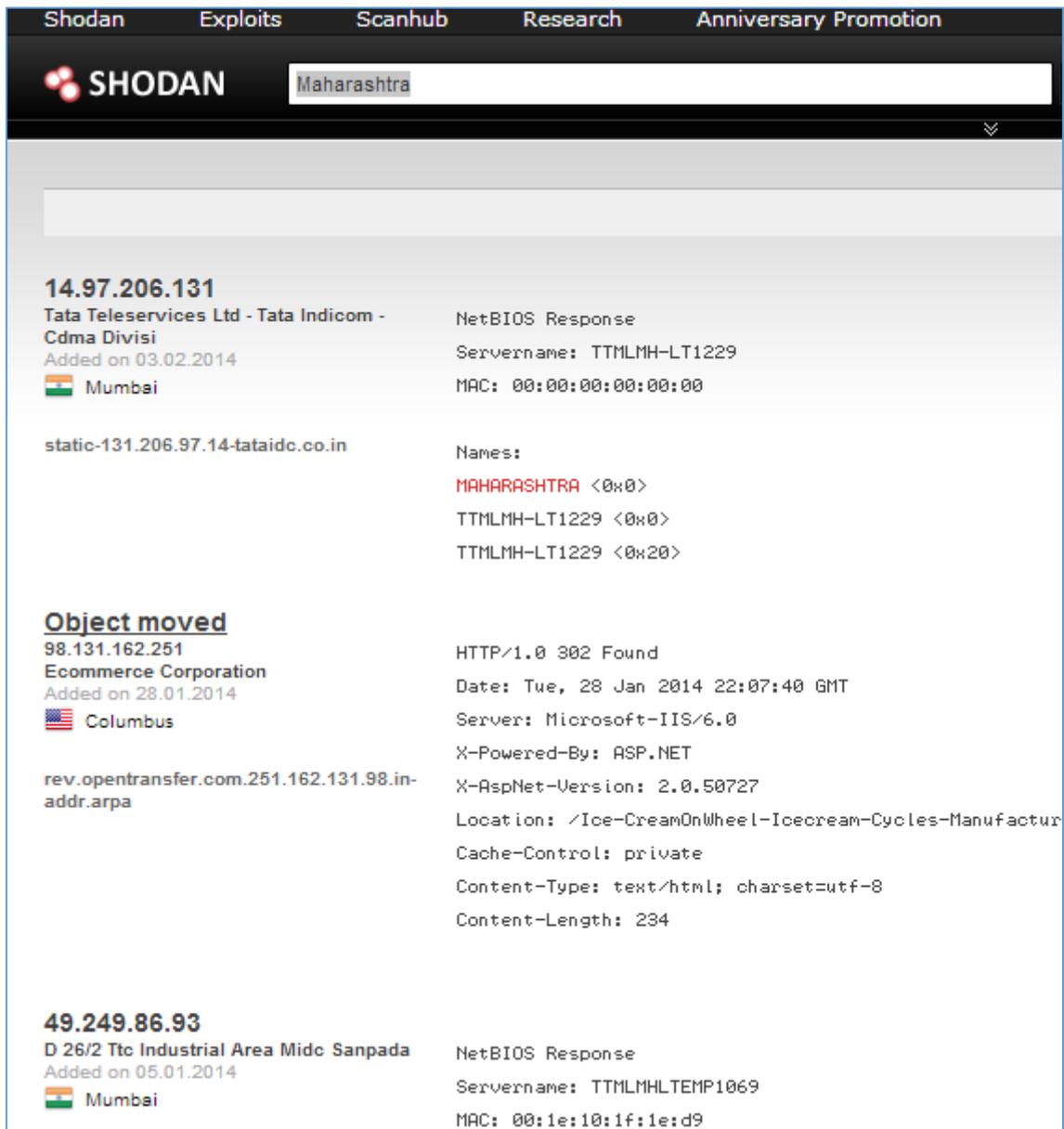
In results it will print all the IPs of the routers which are vulnerable to bypass authentication or are configured with default Username & password.



```
*** Weak IPs with WWW-Authenticate Header ***
IP is 10.10.10.2User Name =adminPassword =admin
IP is 10.10.10.7User Name =adminPassword =admin
IP is 10.10.10.15User Name =adminPassword =admin
```

SHODAN:

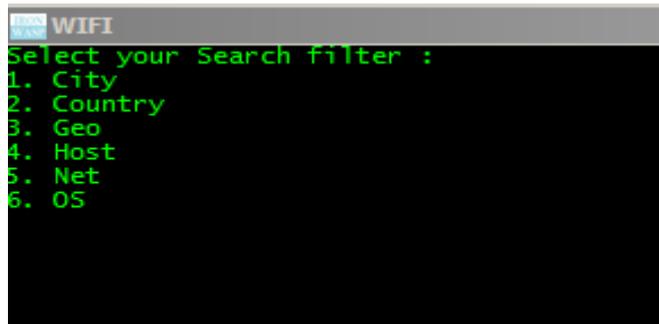
Shodan is a search engine that lets you find out specific types of computers (routers, servers, etc.) in the internet using a variety of filters. If you try to find out all the routers/servers which are there in Maharashtra, you will get a list of IPs something like below:



The screenshot shows the Shodan search engine interface. At the top, there are navigation links: Shodan, Exploits, Scanhub, Research, and Anniversary Promotion. The Shodan logo is on the left, and a search bar on the right contains the text 'Maharashtra'. Below the search bar, there are three search results. Each result displays an IP address, a description, a location, and a date added. The first result is for IP 14.97.206.131, identified as 'Tata Teleservices Ltd - Tata Indicom - Cdma Divisi' in Mumbai, with a NetBIOS response showing 'Servername: TTMLMH-LT1229' and 'MAC: 00:00:00:00:00:00'. The second result is for IP 98.131.162.251, identified as 'Ecommerce Corporation' in Columbus, with an HTTP 302 Found response showing 'Date: Tue, 28 Jan 2014 22:07:40 GMT', 'Server: Microsoft-IIS/6.0', and 'X-AspNet-Version: 2.0.50727'. The third result is for IP 49.249.86.93, identified as 'D 26/2 Ttc Industrial Area Midc Sanpada' in Mumbai, with a NetBIOS response showing 'Servername: TTMLMHLTEMP1069' and 'MAC: 00:1e:10:1f:1e:d9'.

| IP Address | Description | Location | Date Added | Response Type | Response Details |
|--|--|----------|------------|--------------------|---|
| 14.97.206.131 | Tata Teleservices Ltd - Tata Indicom - Cdma Divisi | Mumbai | 03.02.2014 | NetBIOS Response | Servername: TTMLMH-LT1229 MAC: 00:00:00:00:00:00 |
| static-131.206.97.14-tataidc.co.in | | | | Names: | MAHARASHTRA <0x0> TTMLMH-LT1229 <0x0> TTMLMH-LT1229 <0x20> |
| 98.131.162.251 | Ecommerce Corporation | Columbus | 28.01.2014 | HTTP/1.0 302 Found | Date: Tue, 28 Jan 2014 22:07:40 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 2.0.50727 |
| rev.opentransfer.com.251.162.131.98.in-addr.arpa | | | | Location: | /Ice-CreamOnWheel-Icecream-Cycles-Manufactur Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Length: 234 |
| 49.249.86.93 | D 26/2 Ttc Industrial Area Midc Sanpada | Mumbai | 05.01.2014 | NetBIOS Response | Servername: TTMLMHLTEMP1069 MAC: 00:1e:10:1f:1e:d9 |

Wi-Hawk has been integrated to use SHODAN and its customized search engine to find out vulnerable IPs worldwide. The search filter which has been integrated to Wi-Hawk using Shodan looks like following:



```
WIFI
Select your Search filter :
1. City
2. Country
3. Geo
4. Host
5. Net
6. OS
```

If we select the search filter 'CITY', and enter the city name as Mumbai it will return all the IPs which are vulnerable to bypass authentication or are configured with default username/passwords.

IV. References:

1. <http://www.shodanhq.com/>
2. <http://www.rapid7.com/products/metasploit/>