International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9	**VOL**	01
Website	www.iciems.in	**eMail**	iciems@asdf.res.in
Received	10 - July -2015	**Accepted**	31- July- 2015
Article ID	ICIEMS045	**eAID**	ICIEMS.2015.045

ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE

MuthuPavithran. S[1], Pavithran. S[2],
[1,2] Department of computer science and engineering
Velammal Engineering College, Chennai, India

ABSTRACT: *In the emerging world of electronics the wireless devices are used by millions of people in their day to day life. Every person is constantly in contact with the cyberspace. Thus, ensuring the proper encryption facility is a major undertaking to offer dependable communication. The aim of this paper is to transmit a wireless penetration test and compares the encrypted key of a wireless network with a file that contains the captured packets as alphanumeric letters with the help of Kali Linux. This paper shows penetration tests in WEP and WPA/WPA2 protocols, and also the methods to develop these protocols using various attacks and to supply tools that separate the vulnerable access point protocol for the web administrators to protect their networks.*

I. INTRODUCTION

As the technologies and, along with it, the threats facing the wireless communications have risen in numbers with the rapidly increasing number of deployments, there is a need for protection. Nonetheless, the risk if often surpassed by the benefits and convenience of wireless technologies, which have been a big component in the scatter of these devices within homes, agencies and enterprises spanning the world. The popularity of wireless technologies has created an acute involvement in other popular wireless protocols such as Wi-Fi interest. Wi-Fi has been manifesting itself to attack, research and vulnerabilities within the protocols and the execution of those protocols in devices. With this growth in wireless technologies, these nets have become increasingly attractive to Hackers who will seek for data to steal or compromise functionality. While the traditional security measures are less efficient the wireless attack surface presents a singular and difficult challenge. Most of the wireless nets are much unprotected so it is vulnerable to assault. When we consider Wi-Fi most of the people have consciousness about two major encryption techniques (WEP) Wired Equivalency Protocol and (WPA) Wi-Fi Protected Access which were frequently employed. WPA is modern and securing when compared to WEP.

LITERATURE SURVEY

[1].Test and confirm the plausibility of WEP attack in a university wireless LAN ,also suggests some mitigation techniques.[2].Analyzes wireless protocol enhancements to existing handshake mechanism in WPA by using Eliptic Curve Cryptography.[3]. Analyzes functional intrusion detection system that combines them in order to offer resilient detection of the most common attacks in 802.11

Cite this article as: MuthuPavithran S, Pavithran S. "ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE." *International Conference on Information Engineering, Management and Security (2015)*: 266-271. Print.

networks.[4].Explains WEP and RC4 used in WEP.FMS attacks and PTW attacks are described.[5].How to secure our wireless world and gives steps to take care by the user for not affected by the attacker.[6].Describes 2 attacks on IEEE 802.11 WEP,WPA.Deals with TKIP to encrypt traffic. How to deal with ARP request and response and to send with custom network.[7].Effective security protocols right from evolution to existing scenario and discusses various pros and cond of security protocols in WLAN with respect to its countermeasure techniques on various attacks.[8].Challenges and solutions for emergent security technologies ,WIFI.[9].Solution for WPA2 shortcomings and thus provide protection to wireless networks from several attacks.[10].Suggetions on wifi protected access2(WPA2)protocol vulnarabilities might be mitigated and addressed through the enhancement new protocols.

II. BASIC ENCRYPTION

A. Enable WEP encryption settings

Wired Equivalent Privacy (WEP) is an IEEE 802.11 wireless protocol, which provides the security algorithm for the data during the wireless transmission. WEP uses a 24 bit initialization vector (IV) to form the stream chipper and the CRC -32 checksum for integrity of the wireless transmission. 64 bit WEP uses a 40 bit key, 128 bit WEP uses the 104 bit key, 256 bit WEP uses 232 bit key size.

B. WPA/WPA2 Encryption

WiFi Protected Access (WPA) is a data encoding method for WLAN based on the 802.11 standard. WPA was developed after WEP to provide a stronger encryption by configuring two different ways –pre-shared key mode and enterprise mode. The TKIP (Temporal Key Integrity Protocol) is applied to migrate vulnerability by increasing the size of the IV and by using the mixed use. In WPA and WPA2 encryption keys (TK) are derived during the four way handshake. It serves to go through the sequence counter for security against the reply attack. Temporal Keys are changed for every 10,000 packets and this makes TKIP protected network more resistant to cryptanalytic attacks involving the key reuse.

C. WPA/WPA2 Enterprise

Whenever a user connects it dynamically creates the PMK every time in the WPA based network enterprise mode. The PMK is generated by the authentication server and then transmitted down to the client. The AP and the server address over a protocol called RADIUS. The determination to admit or reject the user can be served by the host. Since the AP acts as a relay to forward the packets from clients that are for authentication purposes.

III. SCANNING

As we categorize the tools into passive and active tools.

A. Active scanning

Probe request packets are periodically sent by the tools that carry out the active scanning. These packages are used by the clients whenever they are awaiting for a network. I.e. The client may post the broadcast probe requests. Beacon packets are charged by the Access Points every tenth of a second. Beacon packets are sometimes accessed by active scanners.

B. Passive scans

Passive scanning is too known as Monitor Mode. They listen to all bundles on a gifted channel and then study them.

IV. SNIFFING AND CRACKING TOOL

Aircrack-ng is developed by Christophe Devine, which causes a packet sniffer, packet injector, WEP and WPA/WPA2-PSK cracker and analyzer for 802.11 wirelesses LAN and it will go with whatever wireless network interface controller which supports raw monitoring and sniff 802.11a, 802.11b, 802.11g.

Aircrack-ng

It uses WEP and WPA/WPA2-PSK cracking tools.

Aireplay-ng

It is employed for traffic generation, fake authentication, packet replay, and ARP request injection.

Airodump-ng

It is applied to capture packet of a raw 802.11 builds.

V. ATTACKING WEP-PROTECTED 802.11 NETWORK

Before we attack, we demand to recognize the Mac filtering most of AP`s allow you to set up list of trusted MAC addresses. Any packets transmitted from other IPs will get cut. MAC addresses are very static things, fired into the chip and are immutable. We can simply steal Mac from a person who is already on the web. To answer this we need to hunt down a passive scanner on the network it will that will give the list of addresses whose are connected to that network (CLIENT). We need to wait for the user to disconnect from the net because we can tie to that network with his destination. There is some other direction to make this it's called "DOSING". E.g.: ifconfig wlan0 HW ether 00:11:22:33:44:55.

A. Dictionary attack against WEP

A dictionary attack on wep involves feeding a cracking utility a dictionary and pcap file. The instrument serves to check words in dictionary with words in the backup file, it won't come out until it's found or words are blended.It's a stranded way to translate a password into WEP keys. We need to be given at least three different algorithms (NEESUS, DATACOM, MD5, APPLE).

B. Cryptographic attack against WEP

This attempt is present even if the WEP key completely random. Rc4 is the stream cipher used in WEP and then it makes it used in the WEP it make a perfect prey for this vulnerability the main trouble is how WEP uses the initiation vectors (IV) in each WEP packet. When the WEP encrypt the packet, it prepends the IV to secret key before feeding the key into rc4 this shows that the first three bytes is carrying the secret key used in the every packet.

Cite this article as: MuthuPavithran S, Pavithran S. "ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE." *International Conference on Information Engineering, Management and Security (2015)*: 266-271. Print.

C. Break WEP when the client is bound

Put our card into monitor mode

#airmon-ng start wlan1

Then we need to start the airodump on the specific channel and in specific BSSID to capture the packets and stored in a file.

#airodump-ng –channel –bssid –write filename wlan1

In our target access point there is a client is attached we need to use its MAC address to inject the ARP packet to generate more traffic and besides we can get more packet to crack and besides in a faster manner.

#aireplay-ng –arpreplay –h –client address –b –access point address wlan1

Move to the airodump window we can realize that the information package will get increased like a skyrocket. We need more than 40,000 packets we can begin cracking the key of 104 bit WEP key. The 40,000 packet have the 50% of chance to breach the key the more packets it will increase the probability of finding the key. Then fire the aircrack-ng to crack.

#aircrack-ng. /captured file.cap -0

D. Break WEP without client attached

.First step: we need to capture the entire packet from the access point so we are using the airodump-ng tool helps to capture packet by selecting particular Mac address and its channel and with the network interface and it`s saved in the file called the pcap file.

#airodump-ng –channel –bssid –write file wlan1

Second step: now we are starting to do fake authentication attack which leaves us to associate to its target access point and utilize either two types of authentication open and shared key which will help to produce a fake an authentication to the AP for in order to communicate with the AP

#aireplay-ng –fakeauth 0 –o 1 –e ESSID –a –accesspoint –h –attackerid wlan1

It's gone bad due to Mac is filtering use Mac spoofing method

Third step: Now we are proceeding to perform the fragmentation attack which is the most advanced cracking method. It is employed for the retrieval of key stream from the data packet. It can turn the few bytes of key stream into more or equal 1500bytes of key stream in a few moments. It helps in attack by multiplying an attacker's key stream by the factor up to 16 on each round. The common initial key stream sources are SNAP header. The first three bytes of a SNAP header are 0xAA, 0xAA; 0x03.It is used to make the three bytes of key stream which is enough to take up the fragmentation attack. Then XOR the first three bytes of a SNAP header with first three bytes of captured packet, it will result in three bytes of key stream, then craft an ARP broadcast packet break this packet into 12 three-byte fragments then encrypt and the beam. Each fragment can reuse the same three bytes of key stream. After transmitting then look for the 36 Byte packet that is sent by an AP. This is the ARP packets relayed from the AP. When you have crafted the package in the first place you know the 36-bytes of spare text. Then XOR the encrypted packet with the plaintext, now you recovered the 36 bytes of key stream, then try to craft long ARP packet you can also padded NULLs while crafting. Until you get to full bytes of key stream

Aireplay-ng –fragment –b –access point –h –attacker wlan1.

Fourth step: now we are proceeding to do the chop chop attack, it's a modifying an encrypted packet one byte at a time and played back to an AP. If it has a modified packet chop chop can slowly decrypt the packet, it is protected by WEP regardless of key size as said before, even an AP will generate some packets when no node is attached then remove the final act from what we captured from AP. Then adjust the checksum by assuming the byte is 1. Retransmit it towards a multicast address. If the AP relay the packet then we assumed checksum was correct, then you guessed plain text value was correct now we have recovered the one byte of plain text and key stream. If the AP dose not relay the packet, then our hypothesis was incorrect, so try to keep on guessing for 256 attacks. At the conclusion of the attack, we have the patent text and key stream.

Aireplay-ng –chopchop –b access point –h attacker wlan1

Fifth step: we are going to craft the ARP packet we need for the output of the any one of the attack chop chop or fragmentation. By injecting particular, ARP packet that will cause the AP to generate more traffic at present we are starting to get the ARP packet.

#packet forge-ng –arp –a access point –h attacker –k 255.255.255.255.255 –l 255.255.255.255 –y fileof.xor –w file

Most of the network will accept the ARP packet crafting. If it is fails check the output of the chop chop attack of the plain text and tailor value to the Subnet then The resultant will be encrypted using the key stream and IV in the.Cursor file

Sixth step: now we are starting to inject the crafted ARP packet that is replaying the encrypted ARP packet what we are set up with the assistance of the aireplay-ng after injecting we can view the information packet is increasing in the airodump-ng

Aireplay-ng –interactive –f –r./forged_arp wlan1

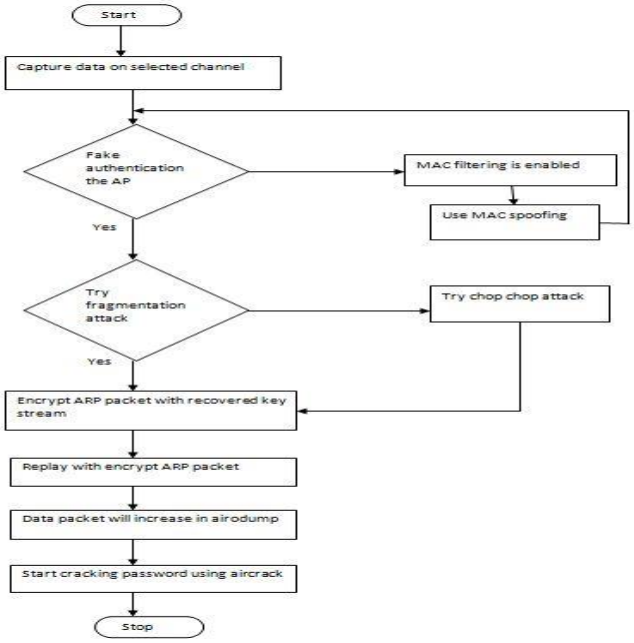
Seventh step: Now we are going to crack the key from the pcap file by passing the argument to the aircrack-ng

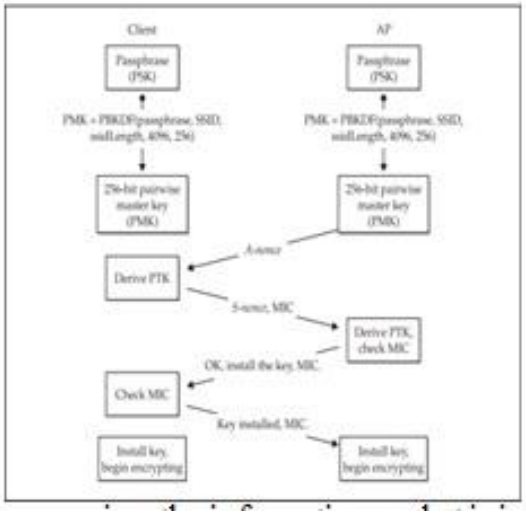
Aircrack-ng./File. cap -0

A. How to defend WEP attack

The best room to defend from this attack you needs to switch to WPA2 with CCMP.

Cite this article as: MuthuPavithran S, Pavithran S. "ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE." *International Conference on Information Engineering, Management and Security (2015)*: 266-271. Print.





VI. ATTACKING WPA-PROTEDTED 802.11 NETWORKS

As we seen before WPA/WPA2 improve our wireless network protection, notwithstanding the extra protection also comes with a cost. Even though WPA was developed with high complexity, it holds its own flaws that are starting to take advantage, attacking the authentication that gives direct access to the wireless web. When attacking WPA-PSK authentication, the attacker can also hold the power to decrypt traffic since the PMK is recovered. Encryption attacks are just emerging against WPA networks. These approaches provide the power to decrypt traffic but do not permit the attacker to fully join the mesh as a lawful user.

A. Breaking authentication WPA-PSK (pre-shared key)

WPA-pre-shared key is also called as WPA- personal. This method is a shared secret among all devices on the network for authentication. The four way handshake that allows the client and the access point to negotiate the key used to encrypt the traffic sent over the wireless. We are starting to crack the key, and this handshake will be executed while a client getting try to connect to the any specific access level. From the diagram, we see that the access level (AP) first sends the A-nonce and, the S-nonce sent by the customer.And so the client MAC address and the AP`s MAC address are mailed, and MIC to verify with the exclusion of the SSID.These values can start in the four way handshake. Can see through wireshark. Sometime they are replicated across the chassis.

B. Passive sniffing

Equally we have already witnessed in the scanning we can seize the four way hands shake in the passive sniffing (scanning). This four way handshake will occur if we are in the right groove and at the proper time. Equally we have already known about the airodump-ng

Cite this article as: MuthuPavithran S, Pavithran S. "ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE." *International Conference on Information Engineering, Management and Security (2015)*: 266-271. Print.

of the aircrack - ng suite, it is the lightweight sniffer. Before that we must match our card is in monitor mode & locked onto a particular channel, and we are saving sniffer data into a file, we`ll stay board by just targeting a single groove.

#airmong-ng start wlan0

#airodump-ng –channel –write –bssid wlan0

These commands will put our card into monitor mode that will lock our card onto the channel. The AP is transmitted, and the transmitted data will lock into the file, remember that.

C. Active sniffing

We have more serious things to do than wait around for new user to join. Alternatively we can sound off the user off and then follow him to reconnect. To kick off the user we use the de-authentication attack for that we need aireplay-ng. We catch the four way handshake.

D. Cracking pre shared key

#aircrack-ng –w wordlist.txt –some.cap

Cracking WPA-PSK can be done by offline brute-force attack. It is challenging the character position for the pre-shared key and can be between 8 and 63 printable ASCII characters and the chosen passphrase is hashed 4096 times before using it within the PMK.

Even though aircrack-ng was a powerful it causes its own limitations, so to improvise the methods we use capacity that needs the limited number of frames than aircrack-ng to crack the key in offline. The great problem because WPA-PSK the PMK of this is not just hashed of the pre shared key, but also the SSID. This implies that even the different network can receive the same pre shared key, but the PMK will differ. Thither is a way to create they our own hash table, by using the genpmk

#genpmk –f wordlist –d wordlist.genpmk –s <BSSID>

Now we are going to increase the speed of the cracking the password. By utilizing the customized field-programmable gate array, it's applied to perform the simple logical operation at incredible velocity. More incredible speed was achieved by using the improvised graphical process units (GPUS) it is merely called as video card which handles the graphic version. Only the help of NVDIAs CUDA (computed unified device architecture) and the c developer can offload the tasks to the video card to leverage its GPU for password checking.

E. Decrypting WPA-PSK captures

After we crack the key, we can able to read other users packets. But there is problem that every user has a unique pair wise transient key (ptk) that was generated when they associated with the network. Even though we have the PMK, we can decode the packets sent and receive from the user by using the wire shark tool have built in methods to decrypt the packets we need that not only the PMK and SSID of the target user. Because of the most of the encryption is mixed up with the SSID.

F. How to Defend WPA/WPA2 personal attack

Most of the home based Wi-Fi networks attacks are increased because the users are using their mobile numbers, birthdates or some favorite names and soon which can be easily guessed by the hackers. Thus, we necessitate to use maximum number of alpha-numeric-special character and we demand to switch it every week. The word should not connect to your personal. Everyone must bear their own updated firewall.

VII. BREAKING AUTHENTICATION: WPA ENTERPRISE

This case of authentication will be practiced in most of the establishments. Because it offers better security and also economical. WPA enterprise supports a kind of authentication schemes with the usage of EAP (extensible authentication protocol). Some of the authentication schemes are considered more safe.

A. **LEAP (Lightweight Extensive Authentication Protocol):**

It is one of the Cisco`s proprietary. The EAP types are established on the MS-CHAPv2 it's a challenge-response protocol. The customer gets connected to the network, sending its username and the authentication server return the 8-byte challenge. The client works out the NT hash of the password and uses them as seed material to encrypt the challenges using DES. When the server delivers the same computation and verifies the solution. LEAP is seemed to be a decent protocol. Its major downfall is the challenge and responses are communicated in the open. If we can sniff a user authenticating, we can set up an offline approach to obtain the user`s password.

A. **PEAP and EAP-TTLS:**

Protected EAP and EAP-TTLS tunneled transport layer security. They provide the best authentication by establishing a TLS tunnel between client and the authentication server, then passing their information within the tunnels using less secure inner authentication protocol. This case of authentication protocol worked in the networks so sniffing on this mesh is less viable. They are protected from the eavesdropping attack. This tunnel additionally provides the customer to secure the authentication server identity by TLS certificate via trusted certificate authority.

B. Attacking PEAP and EAP-TTLS

If we start attacking against the tunnel we won't win because the tunnel is extremely dependable, but if we found vulnerability in that tunnel we can proceed some sort of attack, but mostly we can't able to get results if we discover the vulnerability in the implementation or misconfiguration in the certificate validation on the customer side by skipping the validation. Most of the admin will not notice this shape and then now its vulnerability to access point impersonation attacks and human being in the middle attack.

Cite this article as: MuthuPavithran S, Pavithran S. "ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE." *International Conference on Information Engineering, Management and Security (2015)*: 266-271. Print.

To launch, we need an access point with the same SSID of the target network with better signal we ensure that the net must be same as the objective web.It must attract the guest to connect this network before that we need the radius server to reply to the customer request.There is an open source server free RADIUS that will have any inner authentication protocol sent by a client and respond to it. To start RADIUS we use #radiusd. At once the server has started it works in the background when the client connects inner authentication protocol, which will save every request and responds, even the username and password in the log files. If the client used some other authentication like MSCHAP we need to use sleep to crack it and we can plug in to their net.

C. EAP-TLS

This method was very safe, because it uses client and host credentials to authenticate the user along the web. Thither is a large problem with the managing the certificates for all other users in the system because of computer storage management. Most of the company doesn't suffer the level of PKI required. The working of EAP-TLS uses the server that sends the client certificate which is verified and the public key is applied to encrypt the further message. At once the customer transmits the authentication server certificate, which is verified by the host. After the verification the client and server will generate the random key. This is utilized to initialize the symmetric cipher to encrypt the data from the TLS session. On the EAP success message the PMK is transmitted from the RADIUS server to the AP.

D. Attacking EAP-TLS

It is pretty much impossible to attack this EAP-TLS protocol; we can't say that EAP-TLS have flaws. Till today at that place is no weakness are found because this protocol is very robust as we require to defeat in a practical way by stealing the private Key. Most of the pin or key stored in the smart cards or it uses the RSA secure ID token. The largest trouble is if you gained the access to the network you can't decrypt anyone else`s traffic because it use the unique PMK.

E. How to defend WPA/WPA2 enterprise attack

Every day new vulnerability has been establish in every technology because it was contrived by humankind. And at that place is the way to protect them from those injuries. And then every system should update their technology day to day by their administrator. It is possible only if the administrator updates his knowledge every day. The most significant thing is during the design and conformation of the organization's networks some admin misses some configuration that makes the major fault in their net. The users of the network also receive knowledge of security they should not miss use it.

VIII. CONCLUSION

In this paper, we proposed several advanced attacks against wireless network These varieties of approaches will pass off in most of the wireless nets that will have many losses like money, important data or whole network may be compromised.Then we must aware of these approaches with the supporter of network administrator of every system. In future these kind of wireless attacks plays a major function in top cyber complains in nation because every day wireless technology is emerging tremendously. Therefore each and every individual must aware of these varieties of attacks to have a secured wireless communication.

IX. ACKNOWLEDGMENT

For the help and encouragement, we would wish to thank many of our college professors especially Dr. A. Balaji Ganesh, professor, department of electrical and electronics at Velammal engineering college, Dr. V. Vijaya Chamundeeswari, head of the computer science at Velammal college of engineering, Mr. R. Prakash, research associate department of electronics instrumentation at Velammal engineering college, Mr. Siva V Girish, research associate department of electronics instrumentation at Velammal engineering college, Mrs.R. Ramyadevi, assistant professor, department of computer science at velammal engineering college and Mrs. S Deepa. Class adviser and assistant professor, department of computer science at velammal engineering college.

X. REFERENCE

1. WarrenHarrop, GrenvilleArmitage, Transparent IP Layer Interception on Enterprise 802.11 b/g networks.
2. Kshitiz Saxena, The Analyses of Wireless Encryption to handshake mechanism in WPA-NITTTR, 2010.
3. Guzman Santaf'e-An anomaly based Intrusion detection system for IEEE 802.11 networks, S2ISec information security labs, 2006.
4. LIU Yong-lie, JIN Zhigang, Research on attack to WEP Protocol, Nov-2010.
5.Popuri Manoj Kumar,Attacks and Mitigations over wireless network networks-Insecure Wireless world,The International Journal of Engineering & Sciences.-2013.
6.Martin Beck,Practical attacks against WEP & WPA ,Erik Tews TU-Darmstadt-Nov,2008.
7.Latha.P.H,Vasantha.R-Review of existing security protocols techniques and their performance analysis in WAN-IJETCAS-2014.
8.Paul S.Henry and Hui Luo,AT&T Labs-Research wifi:what is next? December 2002.
9.R.N.Rajotiya,PridhiArora,-Enhancing security of wifi network,The International Journal of Computer Application,June 2012.
10.Paul Arna,Benefits and vulnarabilities of wifi protocol access2 (WPA2)-INFS612-Fall,2006.

Cite this article as: MuthuPavithran S, Pavithran S. "ADVANCED ATTACK AGAINST WIRELESS NETWORKS WEP, WPA/WPA2-PERSONAL AND WPA/WPA2-ENTERPRISE." *International Conference on Information Engineering, Management and Security (2015)*: 266-271. Print.