DATA BREACHING IN CLOUD COMPUTING CAUSED BY MAN-IN-THE-MIDDLE (MITM) ATTACK.

Siti Naquiah Binti Ahmad Tarmizi Lim
Faculty of Electrical Engineering, UITM Shah Alam, Malaysia.
siti_naqquiah@yahoo.com

***Abstract*— Data breach is one of the biggest issue faced by organization whether in public or private sector. The main objective of this research is to simulate Man-in-the-middle (MITM) attack in cloud computing environment using Graphical Network Simulator (GNS3) and Virtual Box. Using this set-up, attacker machine launch MITM attacks such as DNS Spoofing, session hijacking, SSL hijacking and remote hijacking against victim machines. The main motivation of this project is to gain unauthorized access and causing data breach. This project also indicate to prove that https is not really secure.**

***Index Terms*—Data breach, Man-in-the-middle, DNS spoofing, session hijacking, SSL hijacking and remote hijacking.**

I. INTRODUCTION

Nowadays, data breach has become one of the biggest issue faced by organizations. It is occurred when unauthorized user copied, transmitted, viewed, stolen or used sensitive, protected and confidential data [1]. According to the Verizon Data Breach Reports [2], last year, 2014 or known as data breach year, 1540 breach happen that is 46% increasing compare to the 2013, causing one billion data loss compare to 575 million in 2013. Home Depot is the highest with 109,000,000 records, Korean Credit Bureau with 104,000,000 records follow by JP Morgan Chase with 83,000,000 records follow by AliExpress with 300,000,000 records and Sony Pictures Entertainment with 47,000 records.

Man in the Middle attack is one technique data breaching. This happened when an attacker intercept and modify communications by placing himself between the two users that is known as eavesdropping. The entire conversation is controlled by the attacker that has ability to modify the content of messages sent between users.

This research focus on analyzing the occurrence of data breach in cloud environment using MITM techniques that are ARP Resolution Protocol (ARP) cache poisoning, (Domain Name System) DNS spoofing, session hijacking, Secure Socket Layer (SSL) hijacking and Remote hijacking using Graphical Network Simulator 3 (GNS3) for cloud topology, virtual box (Kali Linux) for launching MITM attack, virtual box (Window) as victim and the traffic is measure using Wireshark.

Problem: Data breach has becoming one of the main security problems in organization whether public or private sector. Attackers use many kinds of attack in order to gain unauthorized access to the company confidential data that can cause data breach as the attackers may edit, delete or publish the data online. One of it is by using Man-In-The-Middle Attack.

The goal of this study is to demonstrate MITM attack in cloud computing environment to gain unauthorized access and causing data breach as well as proving that https is not really secure. The scope of this project is done in private network that connects to the real network using cloud. This study is important for analyzing variety of vulnerabilities attack that caused data breaching in cloud computing environment. The outcome will benefits security experts in designing new ways of protecting cloud services and environment.

II. Related Works

S. Gangan [3] review Man-In-The-Middle-Attack using techniques such as ARP Resolution Protocol (ARP) cache poisoning, (Domain Name System) DNS spoofing, session hijacking, and Secure Socket Layer (SSL) hijacking [4].

ARP cache poisoning happen when attacker spoofed the MAC address by using forged ARP request and reply to change the ARP cache causes network traffic redirection to the attacker [3]. H. A. Mangut [5] examined on ARP Cache Poisoning Mitigation and Forensics Investigation. Attackers launch ARP Cache poisoning using virtual machine to the DHCP server. The result gained based on Wireshark and TCP Dump shows that when victim request MAC address from DHCP server, the ARP reply claiming to have originated from the second target that is victim with IP address 192.168.50.7 but with MAC address of 00 : 0C : 29 : 00 : 4f : 2d which was the MAC address of the attacker machine.

DNS spoofing is MITM technique that give false DNS information to hosts so they are directed to the fake website instead the real one that causing data breaches when hosts start communicating with the malicious website. R. Zhang [6] launch Man-In-The-Middle Attacks using DNS spoofing

on VoIP from Remote Attackers. Result gain show that attacker managed to gain victim credential as the attacker directed the victim to the fake website. As victim enter their credential, the attacker capture the credential and gain unauthorized access to the real website. This show that, VoIP can be used to launch DNS spoofing although DNS is non-VoIP specific protocol.

Session hijacking happen when attacker obtain certain parts of the session establishment such as by capturing cookies that were used for the session establishment before. R. LaBarge [7] conduct CLOUD PENETRATION TESTING using OpenStack Essex Cloud Management Software. During the test, HTTP session has been hijack using stolen session cookies. Ferret program capture the session cookie and stores it in a text file, along with URL data of the web pages that user visit during the session when the OpenStack user use Horizon Dashboard to connect to the OpenStack server. Stolen session cookie and URL information from the text file that has been created by Ferret will be retrieved using Hamster program, and allows an unauthorized user gain access to restricted Horizon Dashboard web pages by hijacking the OpenStack user's HTTP session.

Previous research by B.Sumitra [8] on A Survey of Cloud Authentication Attacks and Solution Approaches, Secure Socket Layer (SSL) is important as it encrypts the information transmitted between client and server by providing authenticated service running on cloud environment. Research then tested as attacker hijacking communication between web server and the victim. Result showed that attacker unable to gain the victim credential as SSL encrypted the communication.

R. K. Yadav [9] conduct research on MAN IN MIDDLE ATTACK using SSL AND HTTPS. In this paper, attack focus more on HTTPS that is attacking SSL over HTTP as it is the most common use of SSL. Email and online banking services running applications using HTTPS to ensure that communications between web browser and their servers in in encrypted form. Three protocol SSL, HTTP and hybridization of SSL and HTTP (HTTPS) has been tested and result shows that connection speed of HTTPS slower compare to the other two and will causing users not an aware of this attacks.

L. Xu [10] conduct research on Secure Web Referral Services for Mobile Cloud Computing using MITM attack. SSLStrip (MITM attack) has been used for breached the web site especially banking website to gain personal private information such as login credential. Attacker (impersonate as user) sends HTTP request by ARP spoofing and DNS poisoning to find any vulnerabilities present in the website. When request is received, secure web server sends HTTP 302 message to initiate SSL session and intercepts by attacker to initiate an SSL session to the web server without forwarding the redirect message to the user. Attacker then sends unencrypted web page to the user When user enter username and password using mobile devices, the credential will be transmitted unencrypted to the attacker.

F. Holik [11] done research on Effective penetration testing with Metasploit framework and methodologies in Kali Linux by using MS08-067_netapi vulnerabilities. Result shows that, the metasploit was successful and gained unauthorized access to the remote server. H. Gupta [13] conduct research on Protection against penetration attacks using Metasploit, using network monitoring tools to monitor attack. Same with A. Donevski [12] that conduct research on Nessus or Metasploit: Security Assessment of OpenStack Cloud. Both are using metasploit to launch attack and monitored by network monitoring tools. Result gaining shows that, the network monitoring tools successfully prevent the attack by blocking the suspicious connection between attacker and the victim. Everytime the window upgrate, it is being patched. Window XP is well known for MS08-067_netapi vulnerabilities that can cause remote hijacking.

M. Pangaria [14] conduct research on compromising windows 8 with metasploit's exploit. Windows 8 is more secure than previous versions as it's built in Anti-malware protection system so no need to worry if an Antivirus is not installed. Result gained shows that this attack bypass the proctection by using metasploit exploit/multi/handler and meterpreter payload windows/meterpreter/reverse_tcp. This conclude that, the latest version is not always secure.

E. G. Singh [15] do a research on Armitage: A Penetration testing tool to evaluate Destructive Vulnerabilities in cloud environment. Result gain shows that Armitage not only can do remote hijacking, but also can extract email address using auxiliary module called search_email_sollector to gather the information of email addresses.

III. METHODOLOGY: ATTACK STIMULATION IN GNS3

In this research, test has been done in Graphical Network Simulator 3 (GNS3) by using virtual box that has been configured with window XP (victim) and Kali Linux (attacker).This network topology has been designed in cloud and been connected to the real network. Attacker launched MITM attack such as DNS spoofing, Session hijacking, SSL hijacking and Remote hijacking.

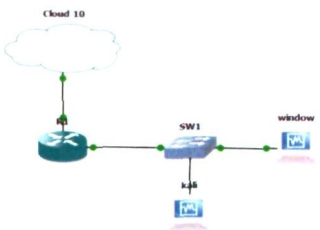

Figure 1: network topology

Equipment	IP Address	Subnet Mask	Default Gateway
Window 7 (real netwok)	192.168.137.2	255.255.255.0	192.168.137.1
Router Fa0/0 (DHCP)	192.168.137.56	255.255.255.0	N/A
Fa1/0	172.17.0.1	255.255.255.0	N/A
DNS server	192.168.137.2	N/A	N/A
Attacker (DHCP)	172.17.0.3	255.255.255.0	172.17.0.1
Window (DHCP)	172.17.0.2	255.255.255.0	172.17.0.1

Table 1: IP address configuration

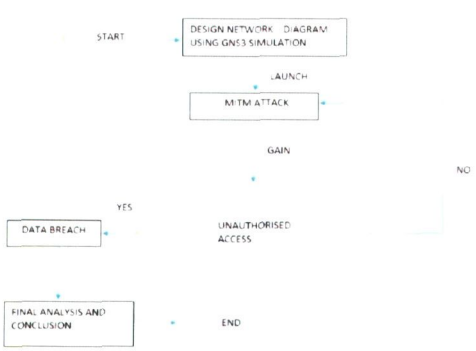

Figure 2: Flow-chart

A. *DNS Spoofing*

This technique create fake website and directed victim into it instead of the real one to gain credential for unauthorized access. DNS (Domain Name System) is important to resolve web address into the IP address. As example, when user enter www.google.com in browser, DNS request has been send to DNS server asking what is the IP address that the name resolve to. This is because Internet does not understand google.com, they only understand address 8.8.8.8. In this test, Social Engineering toolkit has been used to create fake website using same domain name. As example, the IP address of www.gmail.com is 74.125.79.83. Fake website that has been created by social engineering toolkit use same domain that is www.gmail.com but with different IP address that is 172.17.0.3 (attacker IP address). Ettercap is used for spoofing the domain name system (DNS) that is by redirect victim to the fake website instead of the real one.

B. *Session Hijacking*

Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by surreptitiously obtaining the session ID (stored within a cookie) and masquerading as the authorized user. In this test, Ettercap, hamster and ferret have been used to steal cookies when victim establish the connection with the server. When victim insert username and password as authentication to establish connection with the web server, cookies is sent to the browser at the start of the session. Ferret is a tool that used to grab session cookies that pass the network using port 80 while Hamster works as proxy server to manipulate all cookies that has been grabbed by Ferret. Ettercap is used to sniff in the network.

C. *SSL Hijacking*

SSLstrip has been used to perform SSL hijacking. SSL (Secure Socket Layer) is an encryption technique designed to provide security for network communication. HTTPS that is SSL over HTTP has been uses mostly by email services and internet banking to ensure the communication between users and servers is encrypted. In this test, SSLstrip transparently hijacks HTTP traffic on a network, watch for HTTPS links and redirects, and then map those links into look-alike HTTP links or homograph-similar HTTPS links.

D. *Remote Hijacking*

In this test, Armitage and Subterfuge has been used to gain control of the remote PC that is in the same network. This tool is completed build with NMAP for scanning hosts and find victim vulnerabilities. For this test, victim is vulnerable to the ms08-067_netapi. Using this vulnerability, attacker gain access to the victim PC and start browsing files, upload files, key logger, take screenshot and shutdown the PC.

IV. RESULT AND ANALYSIS

This section present the data gain from the attack launch.

A. DNS SPOOFING

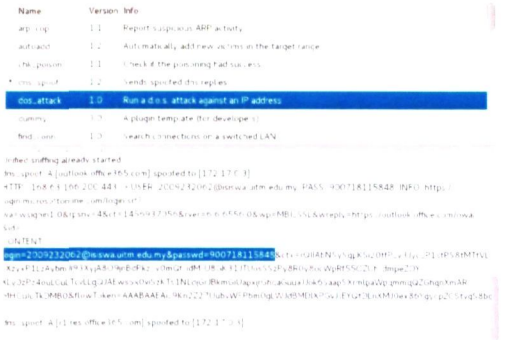

Figure 3: Ettercap

This test has been repeated using different website.

Browser	Successful
www.gmail.com	x
www.outlook.office365.com	/
www.maybank2u.com	x
www.facebook.com	x
www.yahoo.com	x

Table 2: DNS Spoofing

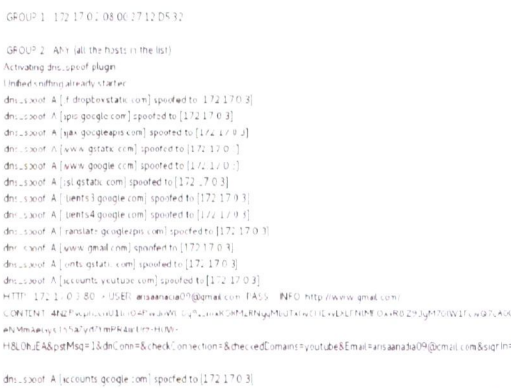

Figure 4: Ettercap unable to capture credential on 2 page login

Result for this test above indicate that this type of attack managed to capture credential but only works for the websites that are using first page login. If the websites are using two page login, Ettercap only managed to capture what on the first page.

B. SESSION HIJACKING

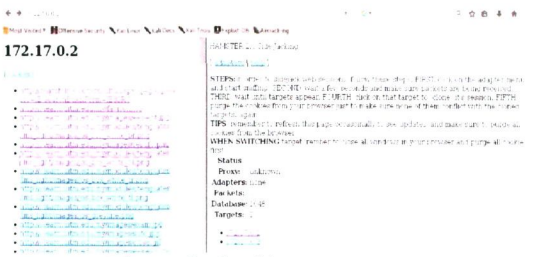

Figure 5: Cookies capture

Website	Successful
UITM student portal	X
Facebook	/
Maybank2u	X
Gmail	/
yahoo	/

Table 3: Session hijacking

Result from this test indicate that without using username and password, attacker can still gain unauthorized access to the website using stolen cookies.

B. SSL HIJACKING

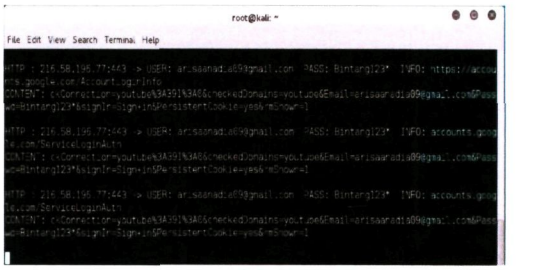

Figure 6: SSLSTRIP

This test has been repeated using different website.

Website	Successful
UPM student portal	/
www.cimbclick.com	x
www.maybank2u.com	x
www.dropbox.com	x
www.facebook.com	/
www.outlook.com	/
www.yahoo.com	/

Table 4: SSL Hijacking

Results from this type of attacks indicate that HTTPS is not really secure. Ettercap unable to capture both username and password when the website use two page login but when using SSLSTRIP, Ettercap manage to capture both username and password.

C. REMOTE HIJACKING

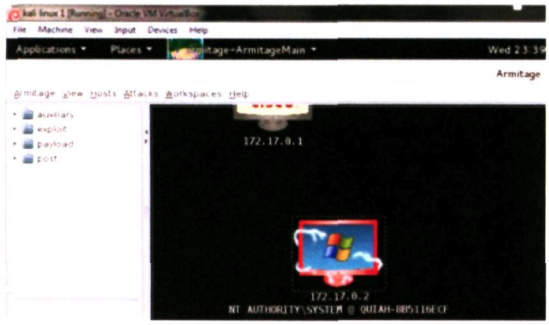

Figure 9: Remote hijacking (Armitage)

1. Create directory in victim PC

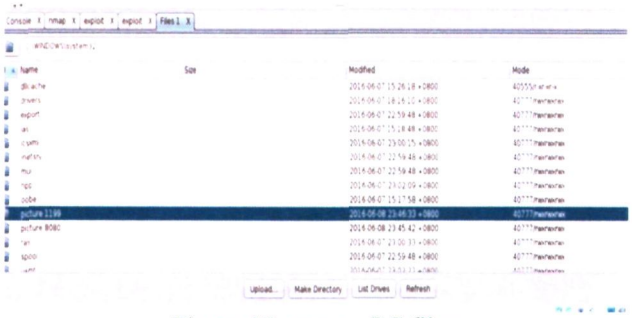

Figure 10: remote PC files

2. Insert picture in directory that is created in victim PC remotely

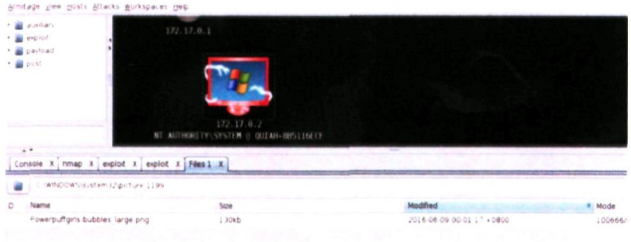

Figure 11: directort that created by attacker

3. Keylogging victim typing

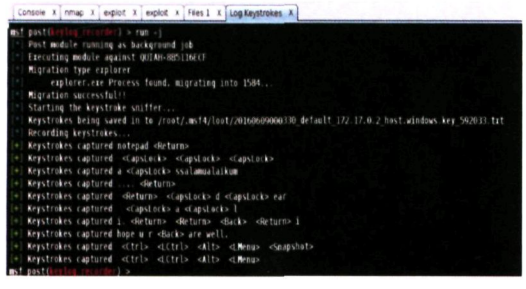

Figure 12: keylogger

4. Take screenshot of what victim done

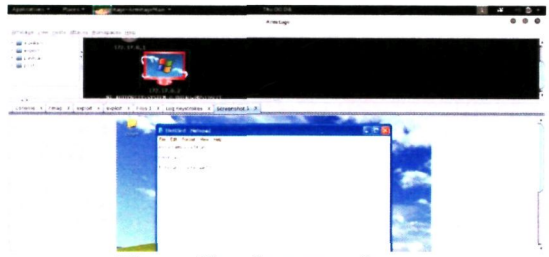

Figure 13: take screenshot

5. Attacker shutdown victim PC

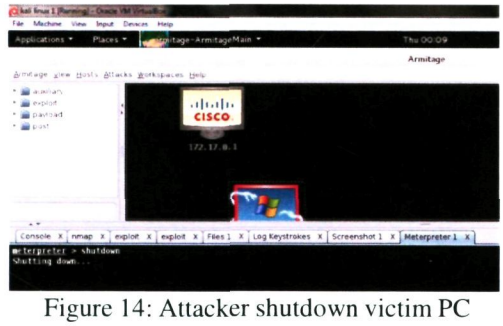

Figure 14: Attacker shutdown victim PC

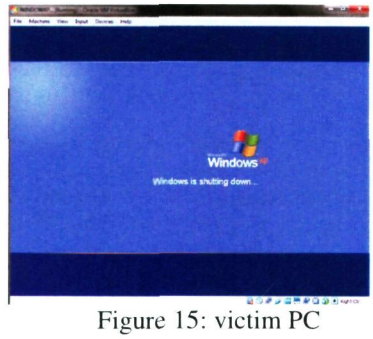

Figure 15: victim PC

Result from this test shows that remote hijacking is very dangerous as attacker managed to gain access to the remote PC, not only causing data breach but can cause loss of the PC. Vulnerabilities ms08-067_netapi for this test show attacker gaining unauthorized access to the victim PC and causing breach by make new directory, upload files in it, key logger victim typing, take screenshot what victim done and shutdown victim PC.

V. CONCLUSION AND RECOMMENDATION

This research demonstrates data breach using different network attack scenario. The main objective is to prove that Man-In-The-Middle attack can cause data breach in cloud computing environment by gaining unauthorized access. On the other hand, the research also aiming to prove that https is not really secure. Based on the result gained, prevention must be taken in order to prevent this incident from happen.

For DNS spoofing and SSL hijacking, it is recommended for user to use passcode, secure words or picture for identification instead of using only password and username. This is more secure as sniffing tools such as Ettercap cannot capture passcode, picture and secure words. For session hijacking, user should disable cookies or delete it after using the website. Website admin also should disable session after a certain time period when not receiving response from user. For remote hijacking, user should keep all software updated with the latest security patches, use strong passwords on all system and close unused network ports to avoid exploitation.

REFERENCE

[1] T.-S. Chow, "SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES," International Journal of Computer Science & Information Technology (IJCSIT), vol. Vol 5, no. No 3, June 2013

[2] Verizon, "2014 Data Breach Investigations Reports," 2014. [Online]. Available: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf. [Accessed 15 October 2015].

[3] S. Gangan, "A Review of Man-in-the-Middle Attacks," [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf. [Accessed 22 October 2015].

[4] H. Shah, Shrikanth and S. S. Anandane, "Security Issues on Cloud Computing," [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1308/1308.5996.pdf. [Accessed 22 October 2015].

[5] H. A. Mangut, A. Al-Nemrat, C. Benzaid and A.-R. Tawil, "ARP Cache Poisoning Mitigation and Forensics Investigation," in The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, Jul 11, 2015

[6] R. Zhang, X. Wang, R. Farley and X. Y. a. X. Jiang, "On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers," [Online]. Available: http://www.csc.ncsu.edu/faculty/jiang/pubs/ASIACCS09.pdf. [Accessed 22 October 2015].

[7] R. LaBarge and T. McGuire, "CLOUD PENETRATION TESTING," in International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2012.

[8] B.Sumitra, C. Pethuru and M.Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 10, October 2014.

[9] R. K. Yadav, "MAN IN MIDDLE ATTACK IN SSL AND HTTPS," International Journal of Computer Science and Mobile Computing, vol. 4, no. 5, pp. 566-573, May 2015.

[10] L. Xu, L. Li, V. Nagarajan and D. H. a. W.-T. Tsai, "Secure Web Referral Services for Mobile Cloud Computing," in Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium, Redwood City, 25-28 March. 2013.

[11] F. Holik, J. Horalek, O. Marik, S. Neradova and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," in *Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on*, 19-21 Nov. 2014.

[12] A. Donevski, S. Ristov and M. Gusev, "Nessus or Metasploit: Security Assessment of OpenStack Cloud," in The 10th Conference for Informatics and Information Technology (CIIT 2013).

[13] H. Gupta and R. Kumar, "Protection against penetration attacks using Metasploit Reliability," in Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2-4 Sept. 2015.

[14] M. Pangaria, V. Shrivastava and P. Soni, "Compromising windows 8 with metasploit's exploit," IOSR Journal of Computer Engineering (IOSRJCE), vol. 5, no. 6, pp. 01-04, Sep-Oct. 2012.

[15] E. G. Singh and M. Kaur, "Armitage: A Penetration testing tool to evaluate Destructive Vulnerabilities," International Journal of Modern Computer Science and Applications (IJMCSA), May, 2016.