Technical report investigation topic: **Hacking into the Cloud Systems**
Contents

1- Abstract ........................................................................................................................... 3
2- Introduction ....................................................................................................................... 3
3- Overview of cloud systems ............................................................................................... 3
   3-1 Characteristics of cloud system .................................................................................... 4
   3-2 Cloud system deployment models ............................................................................... 4
   3-3 Cloud system service models ..................................................................................... 4
   3-4 Cloud system’s security concerns .............................................................................. 5
4- Practical work of hacking into the cloud systems .............................................................. 5
5- Cloud system’s security issues ........................................................................................ 15
   5-1 Network threat issues: ............................................................................................... 15
   5-2 Security threat issues: .................................................................................................. 16
6- Cloud system’s security threat countermeasures ............................................................... 17
   6-1 General security threat countermeasures .................................................................... 17
   6-2 Typical security and network threat countermeasures .............................................. 18
      6-2-1 Security threat countermeasures ......................................................................... 18
      6-2-2 Network threat countermeasures ........................................................................ 19
7- Conclusion ....................................................................................................................... 20
8- References ......................................................................................................................... 20
1- Abstract

Cloud computing system is one of the Information Technology (IT) activities, as predicted by International Data Corporation (IDC), which will allow at least 80% of the industry growth by the end of the decade (Ref 4). This market prediction aspect show how important is the cloud computing systems emerging industry. Therefore the implementation of a secure environment of this industry should be the key element to help prevent hackers from getting access to private data mostly used in that IT environment. In this technical report we will expose on the cloud computing systems security threats, implement a penetration testing and elaborate over security countermeasures to help secure the cloud systems against hackers.

2- Introduction

“Cloud computing system consists of hardware and software resource made available on the internet as managed 3rd party services” (Ref 2). In other terms cloud computing is the process of remotely storing and accessing computer hard drive resources (data, programmes or applications), mostly from a dedicated server, over the internet rather than using your physical computer hard drive for the same resources. Cloud computing therefore relies on virtual sharing computing resources instead of having it on local personal devices to be handled. “The concept of cloud computing dates back to 1950’s when computer mainframe becomes available in corporations through Client/Terminal computers with no internal processing capacities” (Ref 3). Then with today “smart” technology environment, and the highly increasing demand of data storage, cloud computing system provides user with entire set of IT services including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These IT services aim are cost effective, time saving and less dependence of the user over hardware and software technical issues, improving business growth at all levels. But security in the cloud computing systems has became a real concern with permanent security threats from hacker who tend to abuse or take advantage of cloud computing system technology vulnerability. It is therefore recommended to implement a robust security countermeasure that can help provide a secure environment to the increasing cloud computing system market for business continuity. In our technical report investigation over hacking in the cloud systems, we will give an overview of the cloud systems, demonstrate the vulnerability of the cloud systems through a practical penetration testing of a Storage Area Network (SAN), using Internet Small Computer System Interface (iSCSI) as data transfer medium and the OpenFiler as software platform for disk and volume management of the SAN, built for the purpose. Then we will emphasize over the cloud system security issues and finally we will discuss on proposed security threat countermeasures to help secure cloud systems against hacker activities in general.

3- Overview of cloud systems

As defined previously in the introduction, cloud computing system services and utilities are delivered through network via internet for user to access remotely data and distributed computer infrastructure in the contrary of the local computing tied on onsite services. To
better understand the difference between cloud system and local computing, we will describe the characteristics, the deployment models, and the system models of cloud system (Ref 5).

3-1 Characteristics of cloud system

Cloud computing has five particularly characteristics

- On-demand self-service: Allowing user to access its needed computer capabilities from the source.
- Broad network access: Allowing user, on move or tied to one location, to access resources from anywhere via internet connection.
- Resource pooling: Allowing users to share the same overall set of resources from a provider according to their needs and they have no concern over the electricity power needed to run their services.
- Rapid elasticity: Allowing users to quickly increase or decrease their services on demand from provider for their immediate needs.
- Measured service: Allowing amount of usage of service provided to users being monitored by the provider and used for billing and other purposes.

To satisfy the above cloud systems characteristics, a deployment model is needed.

3-2 Cloud system deployment models

There are four deployment models of cloud systems satisfying all needs of users or providers.

- In public cloud: Also call external cloud, in which provider supplies one or more cloud computing services to large group of independent users. In that aspect security and other concerns could restrict user ability to fully use the services provided.
- The private cloud: Also call internal cloud, similar to public cloud but using private network in which the data transfer is controlled and use by single organisation with less security concern.
- The community cloud: In which group of organizations with similar requirement to share infrastructure, it is more customizable for users needs and can meet its specific security requirement more effectively.
- The hybrid cloud: It allows a combination of private or community and public cloud provider. Its flexibility is particularly attractive to many organizations but still with security concern.

But cloud system deployments can only be effective through cloud systems services models well structured.

3-3 Cloud system service models

Cloud system provides three basic service models.
- **Software as a Service (SaaS):** In this service, user is provided with applications made available remotely on demand by provider. SaaS include web-base services such as Google Maps, online-storage and others.

- **Platform as a Service (PaaS):** In this service, user creates applications on the provider’s infrastructure using programming language tools supply by provider. The customer controls the application created via the platform while the provider deal with the service maintenance.

- **Infrastructure as a Service (IaaS):** In this service, provider supplies fundamental computer resources used by customer as he wishes by installing operating system (OS) and applications. The provider only maintains the cloud infrastructure.

### 3- 4 Cloud system’s security concerns

As mentioned in the characteristics of cloud system through its different characteristics, security is a concern, because potential attacks (which could be service disruption or theft of sensitive data including espionage) of the cloud system infrastructure still a permanent threat from the hacker via the internet or from insiders. In that aspect, Public cloud deployment model appears to be more vulnerable to hacker attacks. But also privacy concern can be raised over public and hybrid cloud service and this is due to the effective direct control that private cloud gives to its users over hardware and software, providing them with more control over management privacy. In other words none of the cloud deployment model gives a clear guaranty of security over data transferred or privacy through the cloud system.

But what are the security issues of cloud systems?

To answer the above question we will first implement a practical test of hacking into the cloud system using a penetration testing of an iSCSI SAN online-storage web server built for the testing purpose then emphasize over security issues of cloud systems.

### 4- Practical work of hacking into the cloud systems

For our penetration testing, we will be using three devices as Personal Computer (PC) and three mains software described as follow:

- **Software:**
  
  - OpenFiler SAN (enabling iSCSI data transfer): Kernel version 2.6.30 (Linux)
  - BackTrack 5
  - MetaSploit 4.5.0

- **Devices:**
  
  - PC1 (Server - Victim), running OpenFiler SAN (enabling cloud system capability)
  - PC2 (Hacker), running BackTrack 5 and MetaSploit 4.5.0
  - PC3 (For Server web browser access), running OS Windows 7

After building our iSCSI SAN on PC1 (server), and using PC3 for Server OpenFiler web page access for administration purpose, we will be able to access any new drive or volume, created on PC1 from any device connected to internet, only if provided with appropriate authentication. Our iSCSI SAN will be a Cloud System with online-storage capability.
allowing access to three new Target drives or volumes with authentication access from Initiator screen, using iSCSI Initiator properties from control panel, as shown on (Fig A) and (Fig B).

Fig A- Authentication process of iSCSI SAN online-storage volume (iqn.2006-01.com.openfiler:tns.14d8985c1ad8) from initiator (10.62.0.11) via internet

Fig B- Evidence of access to authenticated iSCSI SAN cloud system volumes (F, H and I), on Target (PC1-server) from Initiator (10.62.0.11) screen via internet.
For the penetration testing of our cloud system implemented above, we will use two phases of approach to target the cloud system server PC1: The server discovery and the server exploitation

- PC2 running BackTrack 5 will be used to discover the server (PC1-victim) vulnerability.
(1) We log into BackTrack then open a terminal window and type the command “`ifconfig`” to disclose PC2 (Hacker) IP address (10.62.0.14) as shown in Fig 7.

![Fig 7- Hacker PC2 IP address 10.62.0.14 discovery using “ifconfig” command](image)

(2) We select a pool of IP address within PC2 network address from 10.62.0.0 to 10.62.0.30 and use “`nmap –sP 10.62.0.0-30`” command to perform a host sweep and check which PCs are up as shown in Fig 8.

![Fig 8- Hosts sweep using “nmap –sP 10.62.0.0-30” command](image)

(3) Then using the “`genlist –s 10.62.0.0-30`” command we will automate the use of Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP) packets to produce a list of existing live host as shown in Fig 9.
(4) After discovering live target host we will use “xprobe2 10.62.0.25” command to operate OS fingerprinting on each host from 10.62.0.1 to 10.62.0.25 and identify the host server, usually running Linux, as shown in Fig C and Fig D below.

Fig 9- List of automated host using “genlist –s 10.62.0.0-30” command

Fig C (1) HOST 10.62.0.1 OS information using “xprobe2 10.62.0.1” command
Fig C (2) - Host 10.62.0.1 OS information using “xprobe2 10.62.0.1” command

Fig D (1) - Host 10.62.0.25 OS information using “xprobe2 10.62.0.25” command
(5) From (Fig D) above, it shows clearly that host 10.62.0.25 will be our potential server victim, because running Linux as OS with 100% probability.

Now we will operate a **TCP port scanning** for a full connect scan to the victim (PC1) to complete the 3-way handshake scanning the victim for all ports defined in the nmap-services using \textit{“nmap –sT 10.62.0.25”} command, giving us the result below for port scanning in Fig 10. Simultaneously we will check applications and versions for network services running on open ports found using \textit{“nmap –sV 10.62.0.25”}, and execute scripts against PC1 for more useful information using \textit{“nmap –sC 10.62.0.25”} command shown on Fig 11.
Fig 11- TCP port scanning using “nmap –sV 10.62.0.25” command

- PC2 running MetaSploit 4.5.0 will be used to exploit server (PC1-victim) vulnerability over open ports with respective services, unreal Internet Relay Chat (IRC) daemon services discovered in Fig 10.

(1) From MetaSploit console interface, we will find an exploit to use against the open services: ssh, rpcbind, wbem-https and iscsi. To do so we will use “search unreal” command as shown in Fig 12.

Fig 12- List of exploits to use against open services on victim using “search unreal” command
(2) We then chose “unreal_ircd_3281_backdoor” as exploit and use commands: “use exploit/unix/irc/unreal_ircd_3281_backdoor” as most useful and “show options”, to display the exploit module options to be used as shown in Fig 13.

![Fig 13- Exploit option and its module using “show options” command](image1.png)

(3) We set host victim 10.62.0.25 as a Remote HOST (RHOST) and 446 as Remote PORT (RPORT), and “show options” command to display the new options setting to be used as shown below in Fig 14.

![Fig 14- Using appropriate RHOST and RPORT for exploit option modules](image2.png)
(4) From the compatible list payload names option as shown in Fig 14, we will set one module using “set payload cmd/unix/bind_perl” command then we adjust the show payload options with appropriate RHOST and Listen PORT (LPORT) settings of the victim as shown in Fig 15 and Fig 16 below.

![Fig 15: Payload option selection using “set payload cmd/unix/bind_perl” command](image)

(5) Finally we start exploiting (hacking) PC1-victim (iSCSI SAN server allowing online-storage for cloud system) from PC2-hacker using “exploit” command showing by the reverse shell been launched from 10.62.0.14:43983 to 10.62.0.25:446 as shown in Fig 17.

![Fig 16: Adjusted payload options with appropriate LHOST 446](image)
Fig 17- Hacking into iSCSI SAN cloud system server (PC1) allowing online-storage.

The penetration testing used above against the iSCSI SAN cloud system server (PC1) allowing online-storage has demonstrated how cloud system can be hack using BackTrack 5 and MetaSploit 4.5.0 simple tools and commands to breach implemented security and gain access to files or data stored via internet on server drives. This hacking tools used over our iSCSI SAN cloud system server vulnerability, will allow us to emphasize on the cloud system’s security issues in general.

5- Cloud system’s security issues

From our experience of hacking into the cloud system above and all researches involved, we discover that cloud systems are facing two types of exploitation threat from the hacker:

- Network threat issues
- Security threat issues

5-1 Network threat issues:

- Port scanning:
  Used in our practical hacking experience above, allows the hacker to use any port open vulnerability to exploit the cloud system. Referring to the above hacking method, only port 22, 111, 3260, and 5989 were still open during the port scanning process. That aspect allows us to exploit the system using BackTrack and MetaSploit tools.

- Denial of Service (DoS):
  Used by hacker to overflow network or web server with frequent request of services to damage the network.
- **Man in the middle attack:**
  This issue occurs when secure socket layer (SSL) is not properly configure and hacker can hack communication between two parties.
- **Network sniffing:**
  This type of issue allows hacker to intercept unencrypted data communication between two parties.
- **Cross site scripting (XSS):**
  In this issue, user enters the right URL of a website and hacker redirects him to its own website to obtain his (user) credential.
- **SQL injection attack:**
  This threat issue allows hacker to use special character like 1==1 in SQL scripting to return full table or the data (Ref 6).
- **Reused IP address:**
  It is a threat which can occur when an old IP address of a user who moved out from the network is attributed to a new user. In this aspect the new user and previous user data vulnerability becomes effective by other users as the address still exists in DNS cache.
- **Security concerns with the hypervisor:**
  This type of threat is due to the fact that cloud systems work mainly on virtualization therefore the hypervisor known as Virtual Machine Manager (VMM) which allows all OSs to run simultaneously on a single hardware platform can underperform and permit security breach.
- **Cookie poisoning:**
  This threat consists of changing or modifying the content of cookie to access applications or webpage. And because holding user credential, they contents can be use for security breach.

### 5-2 Security threat issues:

- **Browser security:**
  In this security issue, hacker sniffs user credential using sniffing packet from server web browser allowing SSL point-to-point communication once user log into server.
- **Cloud malware injection:**
  For this issue attacker attends to infect the cloud structure with virus using spiteful application, service or virtual machine uploaded on the cloud system structure. User gets affected when requesting for the spiteful application.
- **Flooding attacks:**
  This is an open attack from the hacker emitting several nonsense requests to a typical server service until he (hacker) gets to a very huge number of requests consuming considerable resource of the cloud system which become unable of dealing with normal requests from user. Then hacker attacks the cloud service.
- **Data protection:**
  Clause of data protection with cloud service provider can be the way of inside hacker to get access to user privacy. This is an important issue user should be key on prior any use of service to avoid inappropriate transformation of its data.
- **Multi-location of the private data:**
  This issue is effective when a third party device is use to store private data and where control over the cloud system is not completely guaranty by the provider.
- Multi-location of the service provider:
  Issue is due to the client been unable to know how the cloud provider performs his
  declare services to allow direct relationship with user for effective control over data
  privacy
- Data combination and commingling:
  This threat issue takes place when client private data is stored in a cloud provider
  shared drive increasing the risk of virus attack or transmitted from another client
  private data therefore exposing data to vulnerability.
- Restriction on techniques and logistics:
  This is a permanent threat issue which does not allow user to guaranty his preferred
  data location. In some cases cloud service provider like Amazon cannot guaranty the
  locations of data stored in data centres as it has many of them all over the world.

From the threat issues listed above, we can clearly state with no doubt that their aims are to
prevent the cloud availability which makes its services accessible at any time and at any
place, prevent its confidentiality and data integrity which can keep users’ data secret and with
no losses, prevent its user privacy which can insure protection over personal information,
prevent its identity and access management (IAM) enabling a robust combined identity
management architecture, prevent its control allowing the provider to regulate the use of the
entire system service, prevent its audit which can give an effective monitoring of what
happened in the system, prevent its compliance to help prepare the cloud service provider
(CSP) and the user to address critical requirement for improvement of the business, and
finally prevent its Security as a Cloud Service (SaaS) which can allow a proactive control
for information security and needs to effectively allow business growth and continuity within
the IT market (Ref 8).
But the aims of the hacker, which are threatening the cloud system’s security, can be robustly
tackle with well implemented security threat countermeasures.

6- Cloud system’s security threat countermeasures

To effectively tackle cloud systems security and network threats, we will exploit two aspects
of countermeasure:

- General security threat countermeasures
- Typical security and network threat countermeasures

6-1 General security threat countermeasures

These countermeasures will be used in the cloud system architecture security, its data
security, for its transparent cloud protection system (TCPS), its protection from attacks at
different levels, use for mirage image management system and finally use for client based
privacy manager (Ref 7).

- Countermeasures in cloud system architecture security:
  These countermeasures involve access management security, application program
  interface (API) security, network security and storage security assessment. These
components reside within the cloud architecture to enable strong security over the cloud system.

- Data security:
  It will involve the use of policies and assessment procedures allowing privacy enhancement and data in transit in the cloud. This procedure will be a large scale of system search and information exchange between internet and covert channel to control data transfer. This aspect will solve the data leakage problem within the cloud system.

- Protection from attacks at different levels:
  This countermeasure enables web service security using Extensible Makeup Language (XML), Simple Object Access Protocol (SOAP) messages and SSL. The method will consist of computing intensive workloads involving security attack, encryption algorithm and authentication.

- Transparent cloud protection system (TCPS):
  It is a protection system for clouds and monitors the integral cloud components. It allows host to monitor guest Virtual Machines (VM) and its infrastructure components.

- Mirage image management system:
  It is a countermeasure addressing issues related to secure management of VM images encapsulating applications of cloud system. It consists of four components which are Image Transformation, Access Control, by Running Filters, Image Maintenance and Provenance Tracking.

- Client based privacy management:
  It is a countermeasure helping reduce risk of data leakage and breach over data privacy within the cloud. It has as features, obfuscation allowing automatic data structure field obfuscation prior transfer, preference setting allowing user to set data preference security, data access allowing user to access his personal information in the cloud for accuracy, Feedback allowing user to receive periodic feedback over personal file management.

6-2 Typical security and network threat countermeasures

Emphasizing over these countermeasures, referring to the list of network and security threat issues, we will subdivide them in two groups:

- Security threat countermeasures
- Network threat countermeasures

6-2-1 Security threat countermeasures

- Browser security:
  To tackle this threat, cloud provider should use web service security (WS-security) concept on web browser to enable XML and SOAP continuous encryption which cannot be decrypted by man in the middle attack.

- Cloud malware injection:
  For this threat, authenticity check for received messages should be the key option. And to do so, original image file should be stored using hash function and verify it
with hash value of all upcoming service requests, forcing hacker to use legitimate hash value to enter the cloud system.

- Flooding attacks:
  This threat is similar to DoS attacks, therefore to tackle it, Intrusion Detection System (IDS) and firewall should be enabled on the cloud systems to filter malicious requests.

- Data protection:
  The countermeasure in this aspect of threat is left to the cloud user who must check the lawful handling of its personal data by the cloud provider.

- Multi-location of the private data:
  To tackle this threat, cloud user must guaranty it basic business continuity by choosing a cloud provider who does not hire third party device to store its client private business data.

- Multi-location of the service provider:
  To overcome this threat cloud provider should allow direct relationship with user for effective control over its data privacy.

- Data combination and commingling:
  To avoid this threat, cloud provider must guaranty virus-free and implement strong privilege policy over its shared devices, to tackle data manipulation through its cloud systems.

- Restriction on techniques and logistics:
  This is a permanent threat which can be tackled by user choosing cloud provider operating within the Small Medium Business (SMB) IT market that mostly has their data-centre located within a close area for a better data location control.

### 6-2-2 Network threat countermeasures

- Port scanning:
  To avoid this threat taking place, a strong firewall setting policy must be implemented to secure data from port attacks and close automatically unused cloud server ports.

- Denial of Service (DoS):
  This threat can be tackled by reducing the cloud user privileges connecting to the server avoiding repetitive request from same IP address. Also the use of IDS should be a primarily option.

- Man in the middle attack:
  In this case of threat, SSL must be well implemented and configured to avoid communication between two parties within the cloud been intercepted by the hacker. Other options to tackle this issue will be evaluating virtualization at the end-point, evaluating SaaS security and separating endpoint and server security process.

- Network sniffing:
  Strong data encryption methods should be used between parties of cloud user to tackle the network sniffing threat. And to detect sniffer on the cloud network, malicious sniffing detection platform (MSDP) based on address resolution protocol (ARP) and round trip time (RTT) can be used.

- Cross site scripting (XSS):
  In this threat issue, various techniques like active content filtering and content based data leakage prevention technology can be used to tackle XSS. Also powerful tool like blueprint based approach for less dependency over web browser to identify malicious content on cloud network can be used.

- SQL injection attack:
To tackle this type of threat, filtering technique like proxy based architecture towards SQL injection attack can be used.

- Security concerns with the hypervisor:
  This issue can be tackle using advanced cloud protections system to monitor guest VMs activities and inter-communication between cloud system various infrastructure components.
- Cookie poisoning:
  This threat can be tackle by performing regular cookies cleanup or operate encryption scheme over cookie data.

These security threat countermeasures listed above should be performed regularly over the cloud systems to guaranty a robust security.

7- Conclusion

Cloud computing systems allowing shared devices run on server infrastructure via internet facilitating user ability of running his daily activities efficiently at any time and from anywhere, has seen its business market growth rapidly increase giving the prediction from Gartner inc stating that “Cloud computing will become the bulk of the new IT spend by 2016” (Ref 9). This business market prediction, shows how attractive will be the cloud computing systems in the next decade. But beside this impressive cloud business prospect we have an impressive technical cloud security threat demonstrated through our practical work of hacking into the cloud showing the use BackTrack 5 and MetaSploit 4.5.0 to exploit open port scanned to enable hacking activity on the iSCSI SAN cloud system with online-storage capability. This practical cloud system penetration testing allowed us to enumerate some important cloud security and network threat issues. These threat issues are basically the aims of the hacker who tends to prevent the good functionality of the cloud systems in general. Therefore to robustly tackle these cloud systems security threats the above listed security threat countermeasures should be regularly performed to guaranty an effective growth of the emerging cloud systems IT market and more importantly for its business continuity. But can the implementation of an ideal cloud computing systems, free of security threats, be achieved with these growing sophisticated hacking techniques and “cloud computing is everywhere.” said (Ref 1)?

8- References

(Ref 2) http://compnetworking.about.com/od/internetaccessbestuses/f/cloud-computing.htm
(Ref 3) http://en.wikipedia.org/wiki/Cloud_computing
(Ref 4) http://www.cloudpro.co.uk/cloud-essentials/public-cloud/4593/cloud-based-services-set-double-digit-growth
(Ref 5) http://www.fas.org/sgp/crs/misc/R42887.pdf


(Ref 7) http://asecuritysite.com/pdfs/Lab10.pdf

(Ref 8) http://www.ijaiem.org/volume1Issue2/IJAITEM-2012-11-3-076.pdf

(Ref 9) http://www.gartner.com/newsroom/id/2613015


A. Liu, Y. Yuan, A Stavrou, “SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks”, SAC March 8-12, 2009