Cloud Computing
Security Breaches and Threats Analysis

Deba Prasead Mozumder[1], Md. Julkar Nayeen Mahi[2], Md Whaiduzzaman[3]

[123]Institute of Information Technology (IIT), Jahangirnagar University, Bangladesh

Abstract— Cloud solutions deliver a powerful computing platform which enables individuals and Cloud users to perform variety levels of responsibilities such as - use of online storage system, embracing of business applications, growth of customized computer software, and formation of a realistic network environment. In recent years, the number of people using cloud services has been intensely increased and plenty of data has been put away in cloud computing environments. In consequences, data breaches of cloud services are also increasing every year due to hackers, who are always trying to exploit the security vulnerabilities of the architecture of cloud. In this paperwork, we investigate and analyse real world cloud attacks to demonstrate the techniques that hackers used against cloud computing systems and prevention against such malicious activities.

Index Terms— Cloud security, Data breaches, Cloud service model security analysis, Cloud vulnerability assement.

————————————— ◆ —————————————

1 INTRODUCTION

CLOUD computing has been involved in everybody's life. It delivers applications and storage spaces as services over the Internet for little to no cost [1]. Most of us utilize cloud computing services on a daily basis for many purpose [2]. For example, we are using web-based email systems to exchange messages with each-others social networking sites (e.g. Facebook, LinkedIn and Twitter) to share information and stay in contact with friends, on-demand subscription services (e.g. Netflix and Vudu) to watch TV shows and movies; cloud storages (e.g. google drive, Dropbox, OneDrive etc.) to store music, videos, photos and documents online teamwork tools (e.g. Google docs) to work with people on the same document in real time. Cloud computing has also been involved in businesses, E-commerce, companies rent services from cloud computing service providers to reduce operational costs and develop money drift. Presently, google started professional business mail service (e.g. G-suite), storage, data loss prevention and many more for G-suite users[3].

Without any doubt it can be state that, the convenience and low cost of cloud computing services have changed our daily lives. For example, currently most of mobile phone company **attached** free cloud service for certain time. However, the security issues associated with cloud computing make us vulnerable to cybercrimes that happening every day. Hackers employ a variety of techniques to gain access to clouds without legal authorization or disrupt services on clouds in order to achieve specific objectives[4]. Hackers could trick a cloud into treating their illegal activity as a valid instance, therefore, gaining unauthorized access to the information stored in the cloud. Once the exact location of data is located, hackers steal private and sensitive information for criminal activities. According to Data-LossDB, the 2015 Data Breach Quick View report shows that 77.7% of reported incidents were the result of external agents or

activity outside the organization with hacking accounting for 64.6% of incidents and 58.7% of exposed records. Incidents involving U.S. entities accounted for 40.5% of the incidents reported and 64.7% of the records exposed. Epsilon and Stratford were two data breach victims. In the data leakage accident, Epsilon leaked millions of names and email addresses from the customer databases. Stratford's 75,000 credit card numbers and 860,000 user names and passwords were stolen. Hackers could also take advantage of the massive computing power of clouds to fire attacks to users who are in the same or different networks. For instance, hackers rented a server through Amazon's EC2 service and carried out an attack to Sony's PlayStation Network. Therefore, a good understanding of cloud security threats is necessary in order to provide more secure services to cloud users. Few of those techniques were showcase in my paperwork to describe how such attack are very simple to deploy against any systems through security backdoor [5].

Cloud computing involves delivering computing resources (e.g. servers, storages, and applications) as services to end users by cloud computing service providers. End users access on-demand cloud services through Web browsers. Cloud computing service providers offer specific cloud services and ensure the quality of the services. Basically, cloud computing includes three layers: the system layer, the platform layer, and the application layer [6].

The bottom layer is the system layer, which includes computational resources such as infrastructure of servers, network devices, memory, and storage. It is known as Infrastructure-as-a-service (IaaS). The computational resources are made available for users as on-demand services [7]. With the use of virtualization technology, IaaS provides virtual machines that allow clients to build complex network infrastructures. This approach not only reduces the cost in buying physical equipment for businesses, it
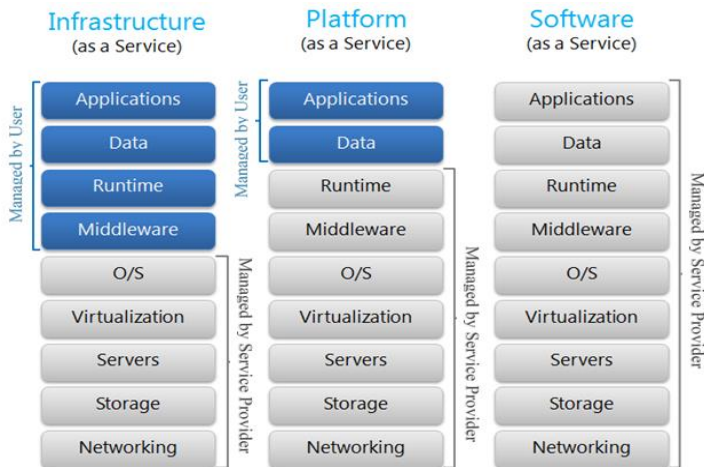
Figure (1): Cloud Service Model

also eases the load of network administration because IT professionals are not required to continuously monitor the health of physical networks. An example of a cloud computing service provider of IaaS are Oracle Cloud, MS Azure, Amazon EC2 and IBM- SmartCloud Enterprise, etc. It provides a virtual computing environment with Web service interfaces; by using the interfaces, users can deploy Linux, Solaris or Windows based virtual machines and run their own custom applications [3].

The middle layer is the platform layer and is known as Platform-as-a-Service (PaaS). It is designed to provide a development platform for users to design their specific applications. Services provided by this cloud model include tools and libraries for application development, allowing users to have control over the application deployment and configuration settings [8]. With PaaS, developers are not required to buy software development tools, therefore reducing the cost. Google Apps is an example of PaaS; it is a suite of Google tools that includes Gmail, Google Groups, Google Calendar, Google Docs, Google Talk, and Google Sites [9].Finally, the top layer is the application layer, also known as Software-as-a-Service (SaaS). This layer allows users to rent

Figure (2): Cost of a data breach for Human error, system glitch and malicious attack thru IBM 2016 data breaches report.

applications running on clouds instead of paying to purchase these applications. Because of its ability to reduce costs, SaaS is popular among companies that deploy their businesses. Groupon is an example that uses SaaS [10].

2.DATA BREACHES STUDY AND COST ANALYSIS

A breach is defined as an event in which an individual's name, medical record, a financial record or debit card is potentially put at risk—either in electronic or paper format. As per global data breach reports and our study, we have identified three main causes of a data breach:

- a malicious or criminal attack,
- System malfunction,
- Human error.

The costs of a data breach can vary according to the cause and the precautions in place at the time of the data breach.

Nowadays Data Breaches is become most intellectual thread to all over the world, somewhere data breaches are very sensitively attached to the world economy as well. WikiLeaks is one of the leading international non-profit organization that broadcasts secret evidence, news leaks, and categorized media from anonymous sources.

To explorer this area, IBM is proud to sponsor the eleventh annual Cost of a Data Breach Study, the industry's gold-standard benchmark research, independently conducted by Ponemon Institute which was published in the year 2016. [5] This year's study found the average consolidated total cost of a data breach is $4 million. The study also reports that the cost incurred for each lost or stolen record containing sensitive and confidential information increased from a consolidated average of $154 to $158. In addition to cost data, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent.

The research also involved the collection of detailed information about the financial consequences of a data breach. For purposes of this research, a data breach occurs when sensitive, protected or confidential data is lost or stolen and put at risk. Over a 10-month period, Ponemon Institute researchers interviewed IT, compliance and information security practitioners representing 383 organizations in 12 countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (a consolidation of organizations in the United Arab Emirates and Saudi Arabia), Canada and for the first time, South Africa.

As per our data mining we found that, big amount of data breaches is happening by malicious attack or activity. Therefore, almost twenty-five percent of data breaches linkup thru negligent employees or human intervention. System failure or process
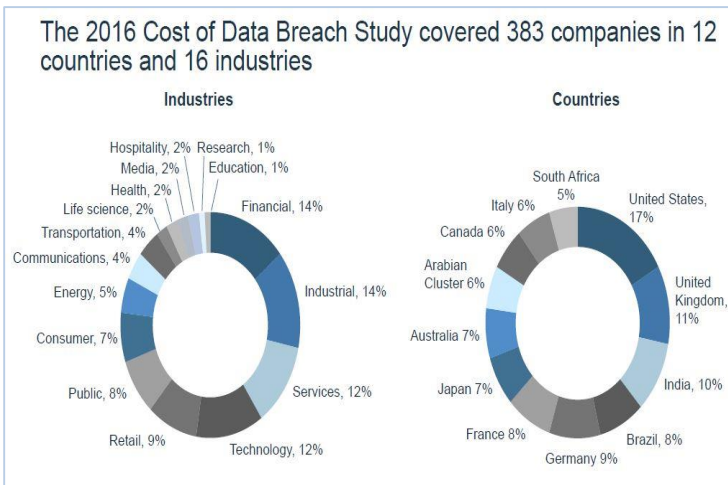
Figure (3): IBM initiated Data Breach Statistics of 2016

gap is playing the vital role which is twenty-seven percent of total amount of data breaches.

3. SECURITY ANALYSIS AND EXPLORATION ON CLOUD

Three cloud service models (SaaS, PaaS and IaaS) not only provide different types of services to end users but also disclose information security issues and risks of cloud computing systems. Few listed concern areas can illustrate the most fearing part of cloud services –

- Data confidentiality
- Web application security
- Virtualization vulnerability
- Data Availability
- Data security
- Network security
- Data locality
- Data integrity
- Data access
- Data Backup process
- Identity management
- sign-on process.

IaaS Security Fears: Primarily, the hackers might abuse the powerful computing capability provided by clouds by conducting illegal activities. IaaS is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. It maximizes extensibility for users to customize a convincing environment that includes virtual machines running with different operating systems. Hackers could rent the virtual machines, analyze their configurations, find their vulnerabilities, and attack other customers virtual machines within the same cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Since IaaS supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks (e.g. distributed denial of service (DDoS) attacks) that require a large number of attacking instances.

SaaS Security Fears: Subsequently, data loss is an important security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customer's data in the data centers. In PaaS cloud models, developers use data to test software integrity during the system development life cycle (SDLC). In IaaS cloud models, users create new drives on virtual machines and store data on those drives. However, data in all three cloud models can be accessed by unauthorized internal employees, as Well as external hackers. The internal employees are able to access data intentionally or accidently. The external hackers gain access to databases in cloud environments using a range of hacking techniques such as session hijacking and network channel snooping.

PaaS Security Fears: In PaaS, the provider mostly gives some control to the customers to develop their own applications. However, it's still remain security issue in between application or host and network security which is totally in scope of the service provider to assure about platform security standard of access control and management for distribution purpose or customer service. This scenario completely assures that; PaaS is more extended platform than SaaS whereas provider have to assurance about more ready facilities for customer. Therefore, there would be enterprise service bus level process metrics which is placed for assess application or program security along with sufficient security metrics related to coding quality checking, vulnerability scoring and patch security coverage. Application level and machine level service oriented architecture (SOA) application are being effectively scoring on cloud platform nowadays [11].

Consequently, traditional network attack strategies can be applied to harass three layers of cloud systems. For example, Web browser attacks are used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems. Malicious programs (e.g. virus and Trojan) can be uploaded to cloud systems and can cause damage. Malicious operations (e.g. metadata spoofing attacks) can be embedded in a normal command, passed to clouds, and executed as valid instances. In IaaS, the hypervisor (e.g. VMware, vSphere, Hyper-V and Xen) conducting administrative operations of virtual instances can be compromised by zero-day attack.

Concerning SaaS security any malicious users can target any vulnerable system to gain the access or control the data or systems as well. Underneath these items are perfect extent to process as same.

- Cross-site scripting[XSS]
- Access control weaknesses
- SQL injection flaws
- Cross-site request forgery[CSRF]
- Cookie manipulation
- Hidden Data field manipulation
- Insecure storage
- Insecure configuration.

It is compulsory to identify the possible cloud threats in order to implement better security mechanisms to protect cloud computing environments. In the following subsections, we explored security threats presented in clouds from three perspectives: abuse use of cloud computational resources, data breaches, and cloud security attacks. Recent real world cloud attacks were also included to demonstrate the techniques that hackers used in exploiting the vulnerabilities of cloud systems.

4. MISUSE AND DATA BREACHES

In the past, hackers used multiple computers or a botnet to produce a great amount of computing power in order to conduct cyber-attacks on computer systems. This process is complicated and can take months to complete. Nowadays, a powerful computing infrastructure, including both software and hardware components, could be easily created using a simple registration process in a cloud computing service provider. By taking advantage of the prevailing computing power of cloud networks, hackers can fire attacks in a very short time. For example, brute force attacks and DoS attacks can be launched by abusing the power of cloud computing.

4.1 Misuse of Cloud Computational Resources

A brute force attack is a technique used to break passwords. The success of this attack is greatly reliant on powerful computing capability because thousands of possible passwords are needed to be sent to a target user's account until it finds the correct one to access. Cloud computing system provides a perfect platform for hackers to launch this type of attack. Thomas Roth, a German researcher, demonstrated a brute force attack in the Black Hat Technical Security Conference. He managed to crack a WPA-PSK protected network by renting a server from Amazon's EC2. In approximately 20 minutes, Roth fired 400,000 passwords per second into the system and the cost of using EC2 service was only 28 cents per minute.

DoS attacks attempt to disrupt a host or network resource in order to make legitimate users unable to access the computer service. They come in a variety of forms and aim at a variety of services. Generally, they are categorized into three basic types: consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, and physical destruction or alteration of network components. Among them, flooding is the most common way in which hackers crumble the victim's system with the use of an overwhelming number of bogus requests; therefore, the services to legitimate users are blocked. When the flooding attack is applied to cloud services, two types of DoS could happen in cloud computing systems: direct DoS and indirect DoS. When a cloud server receives a large volume of flooded requests, it will provide more computational resources to cope with the malicious requests. Finally, the server exhausts its full capability and a direct DoS is occurred to all requests from legitimate users. Moreover, the flood attack could possibly cause indirect DoS to other servers in the same cloud when the servers share the workload of the victim server, which results a full lack of availability on all of the services.

Cloud computing services can be used to send a large amount of packets to concerns networks. For example, two security consultants, Bob and Alice, launched cloud-based DoS attacks to one of their clients in order to test its connectivity with the help of Amazon's EC2 cloud infrastructure. By spending only few dollars they rent virtual servers on EC2 and used a homemade "Thunder Clap" program to successfully flood their client's server and made the company unavailable on the Internet. According to his report, Bit-bucket, a Web-based hosting service company hosted by Amazon, was attacked by massive-scale DDoS attacks used by two flooding techniques: a flood of UDP packets and a flood of TCP SYN connection requests. The attacks caused the company to become unavailable and hence, many developers lost access to projects hosted on Bit-bucket.

4.2 Data Breaches

Security threats can occur from both outside of and within organizations. internal actors Were responsible for 43% of data loss, half of which was intentional, and half accidental. Intel also found that in 68% of data breach incidents, the data penetrated from the network was serious enough to require public disclosure or have a negative financial impact on the company. The same was true for 70% of incidents in smaller commercial organizations, and in 61% of breaches in enterprises.

4.2.1 Malicious Insider

The vulnerabilities of cloud computing to malicious insider are: unclear roles and responsibilities, poor enforcement of role definitions, need-to-know principle not applied, AAA vulnerabilities, system or OS vulnerabilities, inadequate physical security procedures, and impossibility of processing data in encrypted form, application vulnerabilities or poor patch management.

While moving data and applications to cloud computing environments can expand businesses, malicious sabotage of an organization's sensitive information resources could jeopardize the entire victim organization's operation. There are three types of cloud-related insider threats: the rogue administrator, insiders who exploit cloud vulnerabilities, and the insiders who use the cloud to conduct nefarious activity. Rogue administrator has privilege to steal unprotected files, brute-force attack over passwords, and download customer's data from the victim organization. Insiders who exploit cloud vulnerabilities try to gain unauthorized access to confidential data in an organization. They could make a fortune by selling the sensitive information, or use the information for their future businesses. Insiders who use the cloud to conduct nefarious activity carry out attacks against its own employer's IT infrastructure. Since the insiders are familiar with the IT operations of their own compa-

nies, in that view, attacks are generally difficult to be traced using forensic analysis.

4.2 .2 Online Cyber Theft

Cloud computing services provide users with powerful processing capability and massive amounts of storage space. With their inexpensive cost, companies could move their business into clouds so that they do not need to buy their own servers to store customer's information and handle traffic from customers and visitors. For example, Netflix leases computing space from Amazon Web Services (AWS) to provide subscription service for watching TV episodes and movies. Dropbox offers cloud storage service to customers for storing terabytes of data. Cloud-based services are now becoming a part of our daily lives. In the meantime, the sensitive data stored on clouds becomes an attractive target to online cyber theft. Online retailer Zappos (owned by cloud provider Amazon) was the victim of online cyber theft. Almost 24 million client accounts might have been compromised in the breach. The compromised information includes names, email addresses, billing and shipping addresses, phone numbers, the last four digits of credit card numbers, as Well as encrypted versions of account passwords.

Stealing data stored on clouds could be happening on social networking sites. Social networking sites, such as Twitter, MySpace, and Facebook, have attracted people who use them to interact with friends in their daily lives. USA Today found that 35 percent of adults Internet users have a profile on at least one social networking site. These networks provide a platform for users to share information with others, e.g. personal profile (sex, birthdate, email, telephone, and education) and digital media (music, photos and videos). However, that private data can possibly be hacked by online cyber thieves, if they find a way to access the clouds. For example, LinkedIn is world's largest professional networking Website that owns 175 million users and reported that their password database was compromised in a security breach for once. Approximately 6.5 million hashed passwords Were stolen and posted onto a Russian Web forum. More than 200,000 of these passwords have been cracked.

The online cyber thieves could use stolen passwords to access users accounts as Well as to launch malicious attacks to users. Dropbox has confirmed that its users suffered from a spam attack. Usernames and passwords stolen from other Websites Were used to sign in to Dropbox users accounts. Furthermore, a stolen password was used to access a Dropbox employee's account containing a project document with user email addresses. Then, the hacker sent spam emails about online casinos and gambling sites to other users.

Online cyber thieves could also take the advantage of the computing power offered by cloud computing service providers to launch attacks. As per wiki reference of Bangladesh Bank heist, In February 2016, instructions to steal US $951 million from Bangladesh Bank, the central bank of Bangladesh Were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered).

The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It was identified later that Dridex malware (Dridex also known as Bugat and Cridex is a form of malware that specializes in stealing bank credentials via a system that utilizes macros from Microsoft Word) was used for the attack [8]. Amazon's EC2 cloud service was used by hackers to compromise private information. By signing up Amazon's EC2 service with telephony information, hackers rented a virtual server and launched an attack to steal client's data from Sony's PlayStation Network. The hackers didn't break into the Amazon servers during the incident; however, the personal accounts of more than 100 million Sony PlayStation Network Subscribers were compromised.

4.2.3 Malware Injection Attack

Web-based applications provide dynamic Web pages for Internet users to access application servers via a Web browser. The applications can be as simple as an email system or as complicated as an online banking system. The attacks included cross site scripting, injection flaws, information leakage and improper error handling, broken authentication and session management, failure to restrict URL access, improper data validation, insecure communications, and malicious file execution.

Malware injection attack is one category of Web-based attacks, where hackers exploit vulnerabilities of a Web application and embed malicious codes into it that changes the course of its normal execution. Like Web-based applications, cloud systems are also vulnerable to malware injection attacks. Hackers craft a malicious application, program, and virtual machine and inject them into target cloud service models SaaS, PaaS and IaaS, respectively. Once the injection is completed, the malicious module is executed as one of the valid instances running in the cloud; then, the hacker can do whatever s/he desires such as eavesdropping, data manipulation, and data theft.

Among all of the malware injection attacks, SQL injection attack and cross-site scripting attack are the two most common forms. SQL injections target SQL servers that run vulnerable database applications. Hackers exploit the vulnerabilities of Web servers and inject a malicious code in order to bypass login and gain unauthorized access to backend databases. If successful, hackers can manipulate the contents of the databases, retrieve confidential data, remotely execute system commands, or even take control of the Web server for further criminal activities. Sony's PlayStation was a victim of an SQL injection attack. Sophos Lab's blog reported that an SQL injection attack has been successfully used to plant unauthorized code on the PlayStation games, "Sing Star Pop" and "God of War" .

There are plenty of open tools and techniques a Hacker can use during attack. Most of the cases, Hacker always perform as per situation demand. There is no such rule apart from powerful hacking tools or systems.

5. CUSTOM CLOUD SETUP AND SECURITY BREAKDOWN MEASUREMENT

To execute this project, we have used VMware Work-station 10 to facilitate cloud platform. Therefore, we used Debian 7/ Kali Linux 2016.2, CentOS 6.7 as guest and Windows 10 pro as Host. Also, Own Cloud 9 (freeware) has been install on CentOS as SaaS.

5.1 SaaS readiness

OwnCloud provides data access using Web interface. It also provides options to sync and share across devices—all under your control. Using OwnCloud We can easily implement restrictions on file (ACLs) per user. OwnCloud provides its desktop clients (Windows, MAC, Linux) as Well as mobile apps (Android and iPhone) to keep our data sync on your devices

5.2.1 Features of OwnCloud

- OwnCloud provides data accessibility through an-droid, iOS and desktop clients.

- OwnCloud provides data to store on external storage like Dropbox, S3, Google Docs etc.

- OwnCloud maintains files previous versions, so that We can recover from any accidental delete.

5.3 OwnCloud Installation

First We need to enable REMI & EPEL yum repositories in system.

```
rpm -Uvh http://rpms.famillecol-
let.com/enterprise/remi-release-6.rpm
```

Before installation, We first need to setup a running LAMP server.
Install Apache

```
# yum --enablerepo=remi,epel install
httpd
```

After successfully configuring lamp server on system, we have downloaded latest OwnCloud then create a mysql database and user account for configuring OwnCloud. Use following set of command to login to mysql server and create database and user.

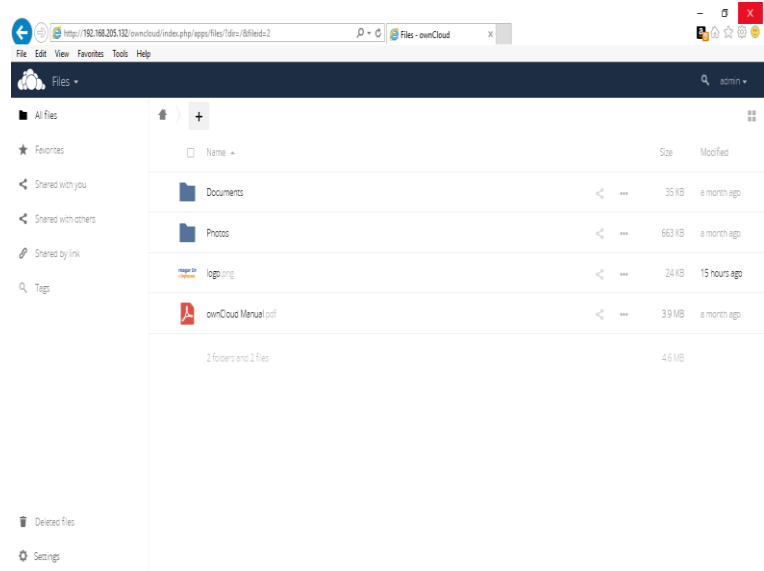Enter new admin credentials to create admin account and provide location of data folder

Figure (4): After Login Admin Panel/user panel.

OwnCloud Web access platform has been showcased conse-quently along with admin dashboard.
After login into OwnCloud, the Dashboard details has been showcase

6. METHODOLOGY OF VAPT

Such deep-drive methodology is considered about to find 'holes' in any IT infrastructure which can be exploit thrugh bad guys most intentionally to hampered business continuity or as intellectual threat.

6.1 Vulnerability Assessment and Penetration Testing

Retrieve Document of Organization.
- the Domain Name Service (DNS)
- the Internet registration database (RIPE)
- bulletin boards, forums and other social media
- the Web

Identify Front-end router
- active ports
- login ports for remote access
- SNMP (if active)
- finger (if active)
- supported routing protocols.

Examines Firewall
- identifying all active TCP ports
- identifying all active UDP ports
- establishing the security rule base
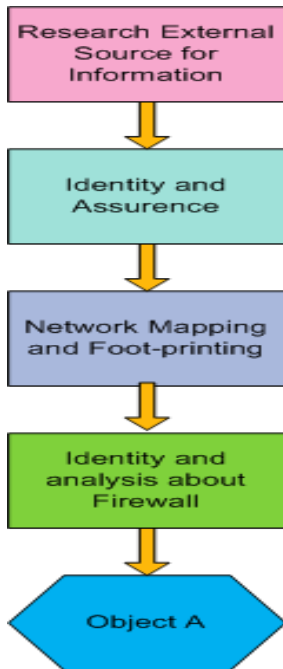- testing for known security flaws

Figure (5): Vulnerability Assessment and Penetration Testin workflow (i)

Identify and analyses accessible machines in front of and behind the firewall which can be identified as a host:

- have an active TCP session established
- have an active UDP port identified
- be tested for known security flaws

Identify and exploit series of vulnerable systems using public vulnerability information:

- configuration errors
- design errors

Develop scenarios and conduct a series of scenario analysis over the entire network to establish:

- what unauthorized traffic can be passed to the local area network (LAN)
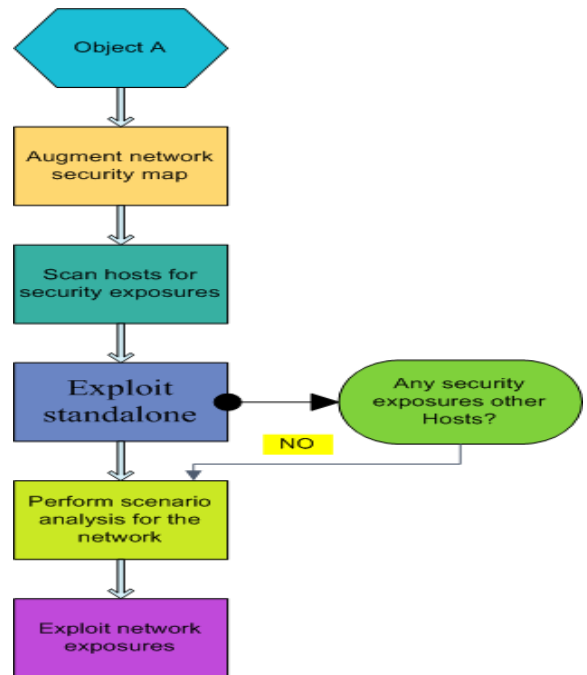- what security exposures can be exploited on the target systems

Figure (6): Vulnerability Assessment and Penetration Testin-workflow (ii).

7. PENETRATION TEST

Information gathering is very first step to get clear picture of target object, only after it is possible to commit successful action in terms of any security act. Security testing is a process to determine that an information system protects and maintains functionality as intended.

7.1. Nonintrusive Target Research

There are many more open source cyber intelligence tools to obtain targeted information.

nslookup: The nslookup tool is set up as a standard program for majority of the operating systems we come across. This is a method of querying DNS servers to determine information about a potential target. It is very simple to use and provides a great deal of information.
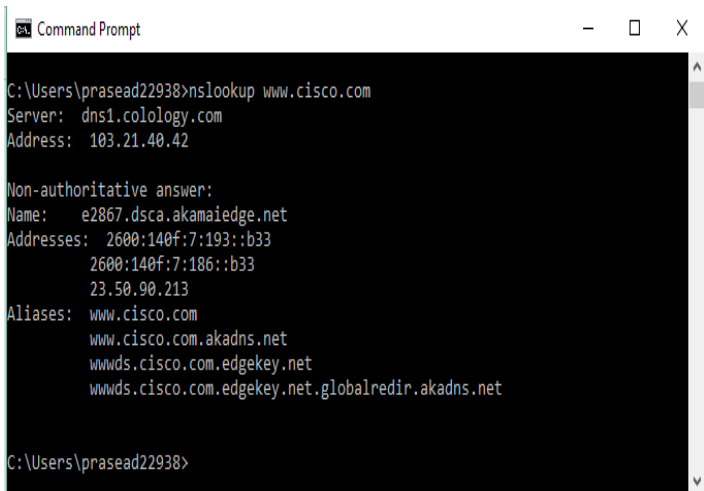
Figure (7): Using nslookup to get targeted information.

W3snoop: Snoop any website's traffic, estimated earnings, server ip and location, world-wide rankings, etc
Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path).
Here after, next consecutive tool set has been used to get deep level information of specified area.

Amap is the first next-generation scanning tool for pentesters. It attempts to identify applications even if they
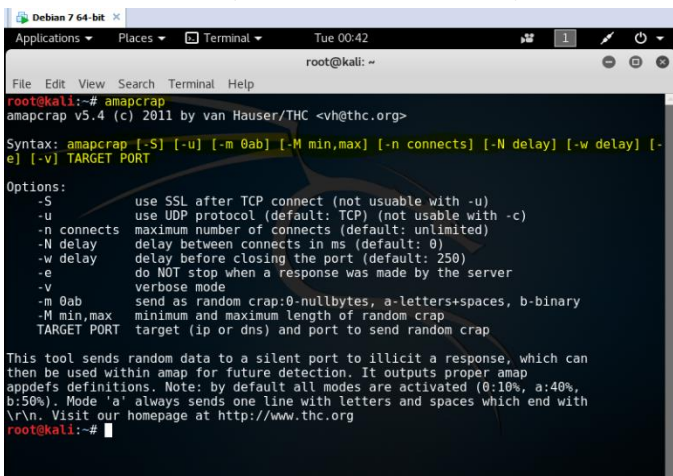

Figure (8): Resource scanning for Port and protocol

are running on a different port than normal. It's also identifies non-ASCII based applications. This is achieved by sending trigger packets, and looking up the responses in a list of response strings.
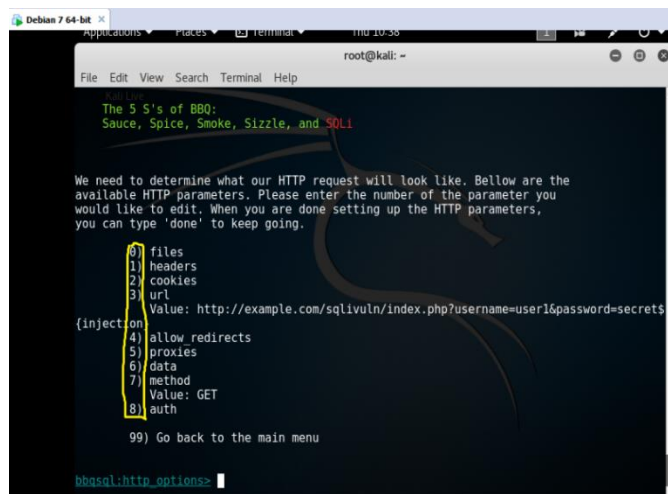
Aamap is Application MAPper which is one of the next-generation scanning tool for pentesters.

Figure (9): Resource vulnerability Analysis through SQL Injection(i)

Amapcrap - sends random data to a UDP, TCP or SSL port to illicit a response Scan port 80 on 162.214.30.199. Displaying the received banners (b), did not display closed ports (q), and used verbose output (v). As well as it is exposed requested specific port status for one of well-known site.

7.2 Vulnerability Analysis

Blind SQL injection can be a pain to exploit. When the available tools work they work well, but when they don't you have to write something custom. This is time-consuming and tedious. BBQSQL can help you address those issues.

BBQSQL is a blind SQL injection framework written in Python. It is extremely useful when attacking tricky SQL injection vulnerabilities. BBQSQL is also a semi-automatic tool, allowing quite a bit of customization for those hard to trigger SQL injection findings. The tool is built to be database agnostic and is extremely versatile. It also has an intuitive UI to make setting up attacks much easier. Python Gevent is also implemented, making BBQSQL extremely fast and Similar to other SQL injection tools which is provide certain request information.
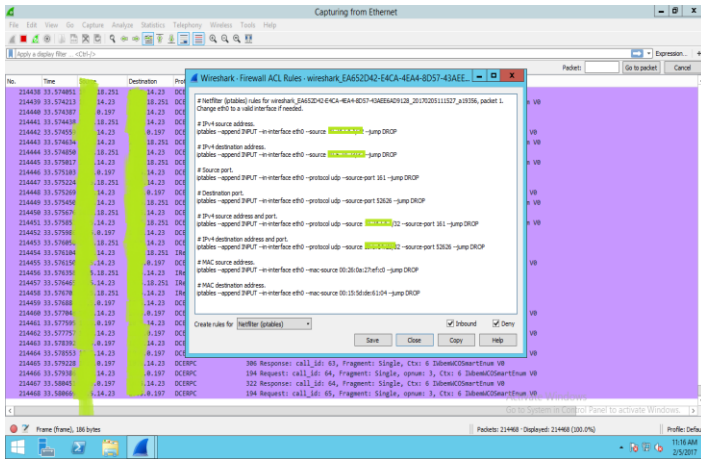
Figure (10): Network traffic analysis to comply firewall ACL rules (i)

Must provide the usual information:

- URL
- HTTP Method
- Headers
- Cookies
- Encoding methods
- Redirect behavior
- Files
- HTTP Auth
- Proxies

7.3 Basic SQL Injection

SQL Injection Case:

UNAME = "pwned' or '1'='1";
PASS = "pwned";
QUERY = "select * from users where pass=md5
(""+PASS+"') and uname='"+UNAME+"'";
QUERY evaluates to:
select * from users where pass=md5('pwned') and uname='pwned' or '1'='1'

The injection can go ANYWHERE:
- url => "http://google.com?vuln='${query}[1]"
- data => "user=foo&pass=${query}"
- cookies => {'PHPSES-
  SID':'123123','FOO':'BAR${query}'}

bbqsql doesn't understand data and doesn't care about Database. Execute as -
- Serialization format
- Processes and rules
- Encodings

There is several SQL Injection process are open for VAPT performance.

7.4 Traffic and Packet Analysis

Wireshark is the world's foremost and widely-used network protocol analyzer. It can see what's happening on network at a microscopic level.

The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
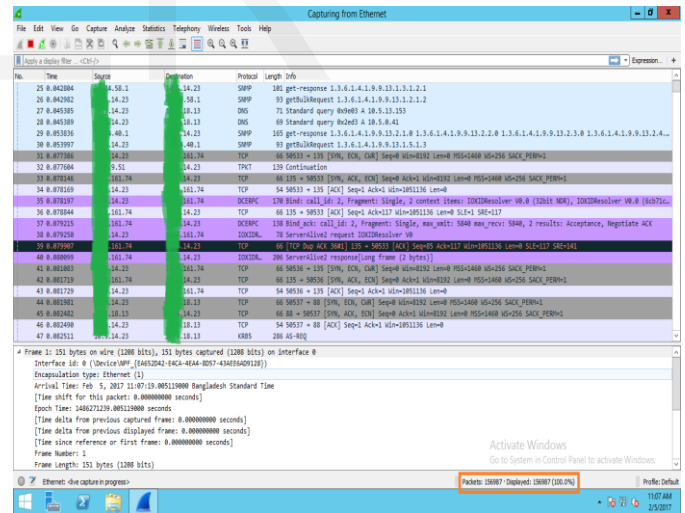- Colorize packet display based on filters.
- Create various statistics.

Figure (11): Network traffic analysis to comply firewall ACL rules (ii)
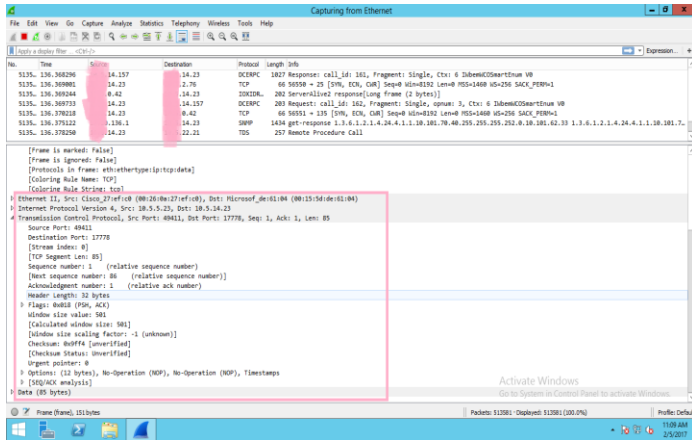
Figure (12): Network traffic analysis as Well as Deep packet inspection

8. RECONCILIATION

As per security standard and compliance of cloud, some listed security module can be imposed in order to develop security situation.

- Monitoring and Incident Response
- Compliance with Regulatory Standards
- Strong Access Control
- End-End Secure Architecture
- Data Security and Privacy Controls
- Data Encryption
- Data Control
- Auditable
- Trusted Cloud
- Governance

8.1 Countermeasures

A cloud computing infrastructure including a cloud service provider, which provides computing resources to cloud based end users who consuming those resources. In order to assure the best quality of service, the providers are responsible for ensuring the cloud environment is secure by sufficient security techniques. This can be done by defining stringent security policies for end-user's area and applying advanced security technologies in cloud architecture.

8.2 Security Policy Enhancement

With a valid credit card, anyone can register to utilize resources offered by cloud service providers. This causes hackers to take advantage of the dominant computing power of cloud to conduct malicious activities, such as spamming and attacking other computing systems. By mitigating such abuse behavior caused by Weak registration systems, credit card fraud monitoring and block of public black lists could be applied. Also, implementation of security policies can reduce the risk of abuse

use of cloud computational power. Well-established rules and regulations can help network administrators manage the clouds more effectively.

8.3 Specified Access Management

The end user's data stored in the cloud is sensitive and private; and access control mechanisms could be applied to ensure only authorized users can have access to their data. Not only do the physical computing systems (where data is stored) have to be continuously monitored, the traffic access to the data should be restricted by security techniques. Firewalls and intrusion detection systems are common tools that are used to restrict access from untrusted resources and to monitor malicious activities. In addition, authentication standards, Security Assertion Markup Language (SAML) and Access Control Markup Language (XACML), can be used to control access to cloud applications and data. SAML focuses on the means for transferring authentication and authorization decisions between cooperating entities, while XACML focuses on the mechanism for arriving at authorization decisions.

8.4 Data Protection

Data breaches mostly caused by insiders, it could be either accidental or intentional. Since it is mostly difficult to identify the insider's behavior, it is better to apply proper security tools to deal with insider threats. The tools include: data loss prevention systems, anomalous behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization technologies. These tools provide functions such as real-time detection on monitoring traffic, audit trails recording for future forensics, and trapping malicious activity into decoy documents.

9. CONCLUSION

In this paper, we experimentally showcased how to create cloud environments platform which is completed from publishing via global DNS service for users. Afterward, we attempted for information gathering about to find out less secure Web services and disclosed those specific connections which is responsible for data breaches. Furthermore, SQL injection has been described as part of pretesting and showcased about to detect network traffic packets along with Firewall ACL policy which confirmed and alerted if any anomaly packets has been passing or not. About to reconciliation of security few steps described along with seal door architecture of cloud. Mostly, key based accessed might be imposed or offered for such environments or services. Real time threat detection system could be applied or agent based services tracking also recommended during access from specific or random devices. We should follow access rule, daily check-maker and impose security for every single attributes placed in onsite datacenter, cloud and remote location along with arrangement of advanced Security applications and appliance which could reduce the risk level.

REFERENCES

1. Gani, A., et al., *A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing.* Journal of Network and Computer Applications, 2014. **43**: p. 84-102.

2. Ahmed, E., et al., *Network-centric performance analysis of runtime application migration in mobile cloud computing.* Simulation Modelling Practice and Theory, 2015. **50**: p. 42-56.

3. Shiraz, M., M. Whaiduzzaman, and A. Gani, *A study on anatomy of smartphone.* Computer Communication & Collaboration, 2013. **1**(1): p. 24-31.

4. Whaiduzzaman, M. and A. Gani. *Measuring security for cloud service provider: A Third Party approach*. in *Electrical Information and Communication Technology (EICT), 2013 International Conference on*. 2014. IEEE.

5. Whaiduzzaman, M., A. Gani, and A. Naveed, *An empirical analysis of finite resource impact on cloudlet performance in mobile cloud computing.* Kuala Lumpur, Malaysia: CEET-2014, 2014.

6. Nasir, M.K. and M. Whaiduzzaman, *Use of cell phone density for Intelligent Transportation System (ITS) in Bangladesh.* Jahangirnagar University Journal of Information Technology, 2012. **1**: p. 49-54.

7. Whaiduzzaman, M., A. Naveed, and A. Gani, *MobiCoRE: Mobile device based cloudlet resource enhancement for optimal task response.* IEEE Transactions on Services Computing, 2016.

8. Whaiduzzaman, M., A. Gani, and A. Naveed, *TOWARDS ENHANCING RESOURCE SCARCE CLOUDLET PERFORMANCE IN MOBILE CLOUD COMPUTING.* Computer Science & Information Technology: p. 1.

9. Whaiduzzaman, M., A. Gani, and A. Naveed. *PEFC: Performance enhancement framework for cloudlet in mobile cloud computing*. in *Robotics and Manufacturing Automation (ROMA), 2014 IEEE International Symposium on*. 2014. IEEE.

10. Qi, H., et al., *Sierpinski triangle based data center architecture in cloud computing.* The Journal of Supercomputing, 2014. **69**(2): p. 887-907.

11. Whaiduzzaman, M., et al., *A survey on vehicular cloud computing.* Journal of Network and Computer Applications, 2014. **40**: p. 325-344.