Module Objectives

Module Objectives

- Understanding Cloud Computing Concepts
- Understanding Cloud Computing Threats
- Understanding Cloud Computing Attacks
- Understanding Cloud Computing Security
- Cloud Computing Security Tools
- Overview of Cloud Penetration testing

Module Flow

1. Cloud Computing Concepts
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Introduction to Cloud Computing

- Cloud computing is an on-demand delivery of **IT capabilities** where IT infrastructure and applications are provided to **subscribers** as a metered service over a network

Characteristics of Cloud Computing

- On-demand self service
- Broad network access
- Distributed storage
- Resource pooling
- Rapid elasticity
- Measured service
- Automated management
- Virtualization technology

Types of Cloud Computing Services

SYS ADMINS

Infrastructure-as-a-Service (IaaS)

- Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API
- E.g., Amazon EC2, Go grid, Sungrid, Windows SkyDrive, Rackspace.com, etc.

DEVELOPERS

Platform-as-a-Service (PaaS)

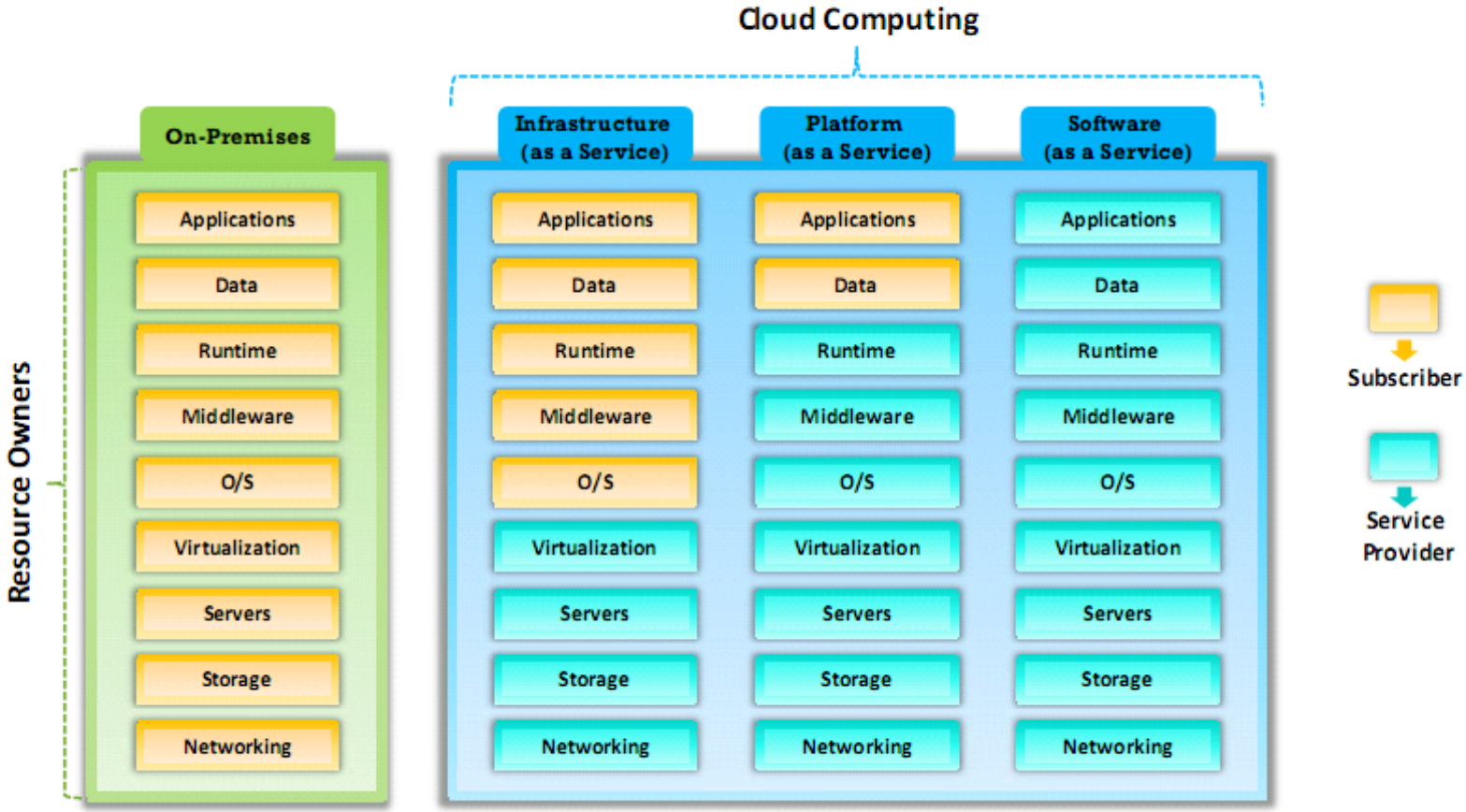
- Offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications
- E.g., Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.

END CUSTOMERS

Software-as-a-Service (SaaS)

- Offers software to subscribers on-demand over the Internet
- E.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, Freshbooks, basecamp, etc.

Separation of Responsibilities in Cloud



Cloud Deployment Models

Cloud deployment model selection is based on the **enterprise requirements**

Public Cloud

Services are rendered over a **network that is open for public use**

Private Cloud

Cloud infrastructure operated solely for a **single organization**

Community Cloud

Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)

Hybrid Cloud

Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models

NIST Cloud Deployment Reference Architecture

NIST cloud computing reference architecture defines five major factors:

Cloud Consumer

A person or organization that uses cloud computing services

Cloud Provider

A person or organization providing services to interested parties

Cloud Carrier

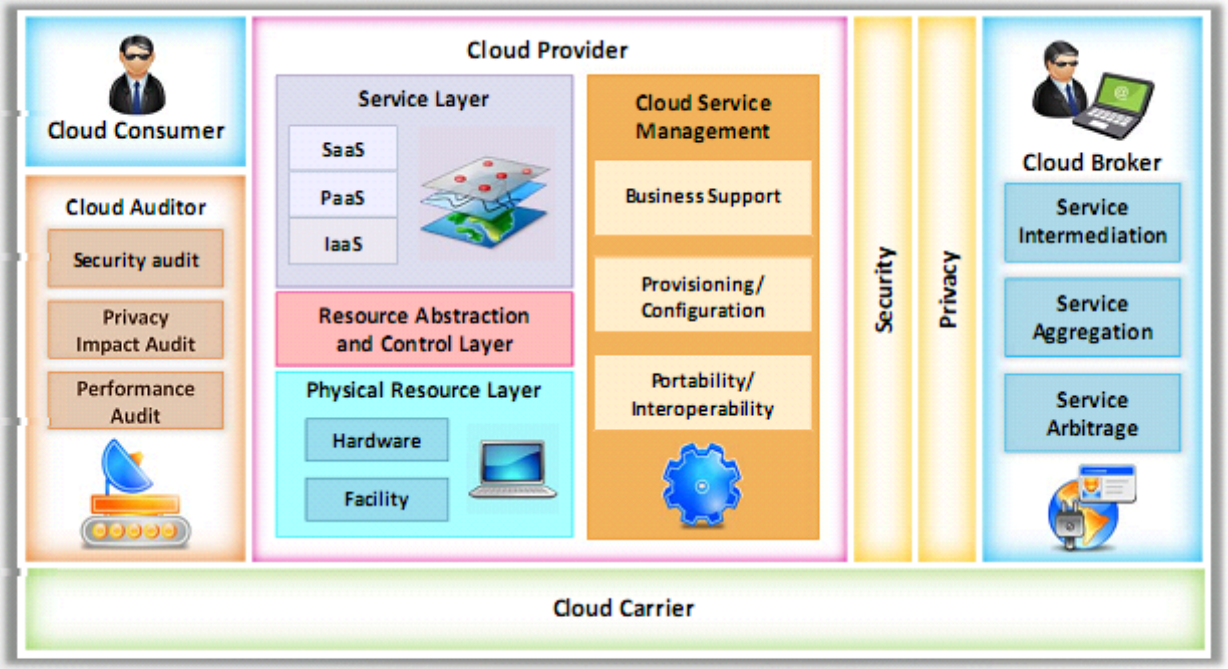
An intermediary for providing connectivity and transport services between cloud consumers and providers

Cloud Auditor

A party for making independent assessments of cloud service controls and taking an opinion thereon

Cloud Broker

An entity to manage cloud services in terms of use, performance, and delivery who also maintains relationship between cloud providers and consumers



Cloud Computing Benefits

Economic

- Business agility
- Less maintenance costs
- Acquire economies of scale
- Less capital expense
- Huge storage facilities for organizations
- Environmentally friendly
- Less total cost of ownership
- Less power consumption

Operational

- Flexibility and efficiency
- Resiliency and redundancy
- Scale as needed
- Less operational problems
- Deploy applications quickly
- Back up and disaster recovery
- Automatic updates

Staffing

- Streamline processes
- Well usage of resources
- Less personnel training
- Less IT Staff
- Multiple users utilize resources on cloud
- Evolution to new model of business
- Simultaneous sharing of resources

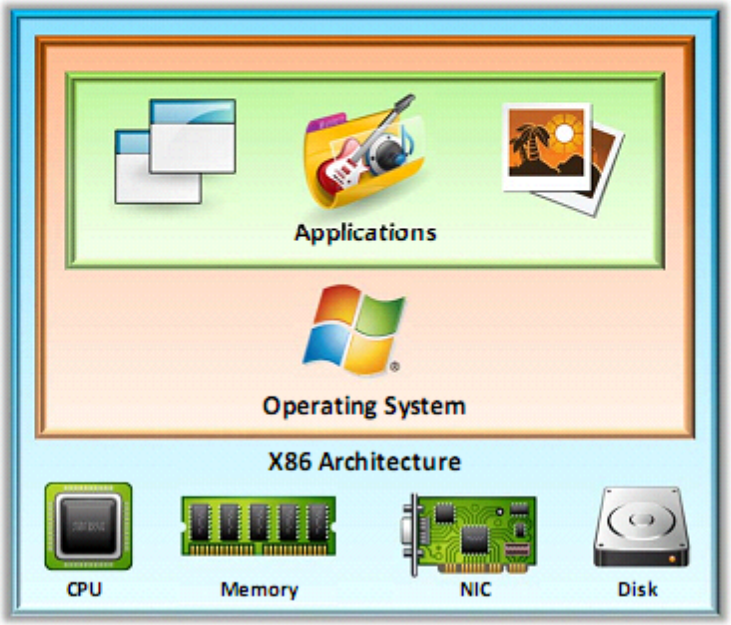
Security

- Less investment in security controls
- Efficient, effective, and swift response to security breaches
- Standardized, open interface to managed security services (MSS)
- Effective patch management and implementation of security updates
- Better disaster recovery preparedness
- Ability to dynamically scale defensive resources on demand
- Resource aggregation offers better manageability of security systems
- Rigorous internal audit and risk assessment procedures

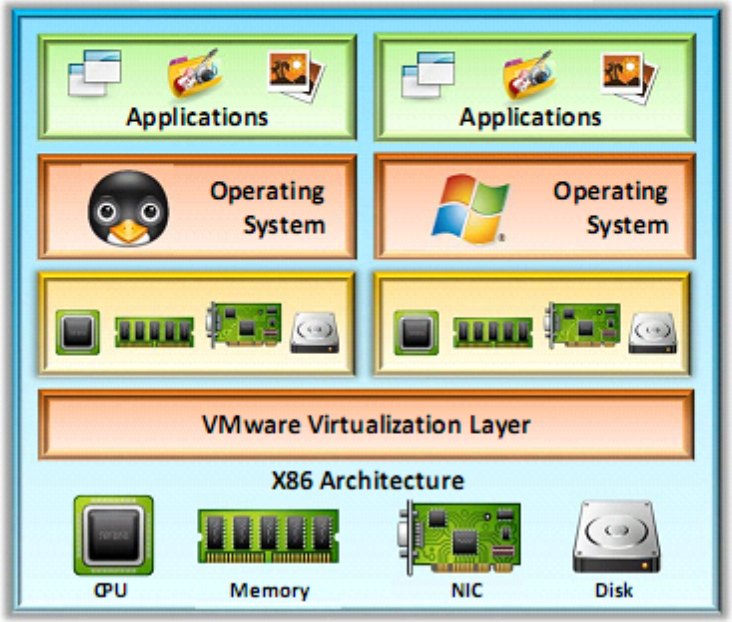
Understanding Virtualization

- Virtualization is the ability to **run multiple operating systems on a single physical system** and share the underlying resources such as a server, a storage device or a network

Physical Machine



Virtual Machine



Understanding Virtualization (Cont'd)

Characteristics of Virtualization

- Partitioning
- Isolation
- Encapsulation

Types of Virtualization

- Storage Virtualization
- Network Virtualization
- Server Virtualization

Benefits of Virtualization in Cloud

- Increases **business continuity**
- Reduces **setup cost**
- Improves the way organizations manage IT and **deliver services**
- Improves operational **efficiency**
- Reduces system administration work
- Facilitates **better backup** and **data protection**
- Increases service levels and enable **self-service provisioning**
- Helps administrators to ensure control and compliance

Module Flow

1. Cloud Computing Concepts
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Cloud Computing Threats

1. Data breach/loss
2. Abuse and Nefarious Use of Cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Unsynchronized system clocks
8. Inadequate infrastructure design and planning
9. Conflicts between client hardening procedures and cloud environment
10. Loss of operational and security logs
11. Malicious insiders
12. Illegal access to cloud systems
13. Loss of business reputation due to co-tenant activities
14. Privilege escalation
15. Natural disasters
16. Hardware failure
17. Supply chain failure
18. Modifying network traffic
19. Isolation failure
20. Cloud provider acquisition
21. Management interface compromise
22. Network management failure
23. Authentication attacks
24. VM-level attacks
25. Lock-in
26. Licensing risks
27. Loss of governance
28. Loss of encryption keys
29. Risks from changes of Jurisdiction
30. Undertaking malicious probes or scans
31. Theft of computer equipment
32. Cloud service termination or failure
33. Subpoena and e-discovery
34. Improper data handling and disposal
35. Loss or modification of backup data
36. Compliance risks
37. Economic Denial of Sustainability (EDOS)

Cloud Computing Threats

Data Breach/Loss

Data loss issues include:

- **Data is erased**, modified or decoupled (lost)
- **Encryption keys are lost**, misplaced or stolen
- **Illegal access to the data** in cloud due to Improper authentication, authorization, and access controls
- **Misuse of data** by CSP

Abuse and Nefarious Use of Cloud services

Attackers **create anonymous access to cloud services** and perpetrate various attacks such as:

- **Password** and **key** cracking
- Building rainbow tables
- **CAPTCHA**-solving farms
- Launching **dynamic attack points**
- Hosting **exploits** on cloud platforms
- Hosting **malicious data**
- **Botnet** command or control
- **DDoS**

Insecure Interfaces and APIs

Insecure interfaces and APIs related risks:

- Circumvents **user defined polices**
- Is not credential leak proof
- Breach in **logging and monitoring facilities**
- Unknown API dependencies
- Reusable **passwords/tokens**
- Insufficient input-data validation

Cloud Computing Threats (Cont'd)

Insufficient Due Diligence	Ignorance of CSP's cloud environment pose risks in **operational responsibilities** such as security, encryption, incident response, and more issues such as contractual issues, design and architectural issues, etc.
Shared Technology Issues	Most underlying components that make up the cloud infrastructure (ex: GPU, CPU caches, etc.) **does not offer strong isolation properties** in a multi-tenant environment which enables attackers to attack other machines if they can exploit vulnerabilities in one client's applications
Unknown Risk Profile	Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing, and logging, etc. as they are less involved with **hardware** and **software ownership** and maintenance in the cloud
Unsynchronized System Clocks	▪ Unsynchronized clocks can **affect the working of automated tasks** ▪ Network administrator would be unable to accurately analyze the log files for any malicious activity, if the time stamps are mismatched

Cloud Computing Threats (Cont'd)

Inadequate Infrastructure Design and Planning

- Shortage of computing resources and/or poor network design gives rise to unacceptable **network latency** or **inability to meet agreed service levels**

Conflicts between Client Hardening Procedures and Cloud Environment

- Certain client hardening procedures may conflict with a **cloud provider's environment**, making their implementation by the client impossible

Loss of Operational and Security Logs

- The loss of security logs poses **a risk for managing the implementation of the information security management program**
- Loss of security logs may occur in case of under-provisioning of storage

Malicious Insiders

- Disgruntled current or former employees, contractors, or other business partners who have authorized access to cloud resources can misuse their access to compromise the **information available in the cloud**

Cloud Computing Threats (Cont'd)

Illegal Access to the Cloud

Weak authentication and authorization controls could lead to illegal access thereby compromising confidential and critical data stored in the cloud

Loss of Business Reputation due to Co-tenant Activities

Resources are shared in the cloud, thus malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down organization's reputation

Privilege Escalation

A mistake in the access allocation system causes a customer, third party, or employee to get more access rights than needed

Natural Disasters

Based on geographic location and climate, data centers may be exposed to natural disasters such as floods, lightening, earthquakes, etc. that can affect the cloud services

Hardware Failure

Hardware failure such as switches, servers, etc. in data centers can make the doud data inaccessible

Cloud Computing Threats (Cont'd)

Supply Chain Failure

- Cloud providers outsource certain tasks to third parties. Thus the security of the **cloud is directly proportional to security of each link** and the extent of dependency on third parties
- A disruption in the chain may lead to **loss of data privacy** and **integrity**, **services unavailability**, **violation of SLA**, **economic** and **reputational losses** resulting in failure to meet customer demand, and cascading failure

Modifying Network Traffic

- In cloud, the network traffic may be modified due to flaws while provisioning or de-provisioning network, or **vulnerabilities in communication encryption**
- Modification of network traffic may cause **loss**, **alteration**, or **theft of confidential data** and communications

Isolation Failure

- Due to the **isolation failure**, attackers try to **control operations** of other cloud customers **to gain illegal access** to the data

Cloud Computing Threats (Cont'd)

Cloud Provider Acquisition

Acquisition of the cloud provider may **increase the probability of tactical shift** and may affect non-binding agreements at risk. This could make it difficult to cope up with the security requirements

Management Interface Compromise

Customer management interfaces of cloud provider are accessible via the Internet and facilitate **access to a large number of resources**. This enhances the risk, particularly when combined with **remote access** and **web browser vulnerabilities**

Network Management Failure

Poor network management leads to **network congestion**, **misconnection**, **misconfiguration**, lack of resource isolation, etc., which affects services and security

Authentication Attacks

Weak authentication mechanisms (weak passwords, re-use passwords, etc.) and inherent limitations of **one-factor authentication mechanisms** allows attacker to gain unauthorized access to cloud computing systems

Cloud Computing Threats (Cont'd)

VM-Level Attacks	Cloud extensively use **virtualization technology**. This threat arises due to the **existence of vulnerabilities in the hypervisors**
Lock-in	Inability of the client to **migrate from one cloud service provider to another** or in-house systems due to the lack of tools, procedures or standards data formats for data, application, and service portability
Licensing Risks	The organization may **incur huge licensing fee** if the software deployed in the cloud is charged on a per instance basis
Loss of Governance	In using cloud infrastructures, **customer gives up control to the cloud service provider** regarding issues that may affect security
Loss of Encryption Keys	The loss of encryption keys required for **secure communication** or systems access provide a potential attacker with the possibility to get **unauthorized assets**

Cloud Computing Threats (Cont'd)

Risks from Changes of Jurisdiction	Change in jurisdiction of the data leads to the risk, the **data** or **information system is blocked** or **impounded** by a government or other organization
Undertaking Malicious Probes or Scans	Malicious probes or scanning allows an attacker to collect **sensitive information** that may lead to **loss of confidentiality**, **integrity**, and **availability of services and data**
Theft of Computer Equipment	Theft of equipment may occur due to **poor controls on physical parameters** such as **smart card access at the entry** etc. which may lead to loss of physical equipment and sensitive data
Cloud Service Termination or Failure	Termination of cloud service due to non-profitability or disputes might lead to **data loss** unless end-users are **legally protected**
Subpoena and E-Discovery	Customer data and services are subpoenaed or subjected to a cease and **desist request from authorities or third parties**

Cloud Computing Threats (Cont'd)

Improper Data Handling and Disposal	01	It is difficult to ascertain data handling and disposal procedures followed by CSPs due to **limited access to cloud infrastructure**
Loss/ Modification of Backup Data	02	Attackers might exploit vulnerabilities such as **SQL injection**, insecure user behavior like **storing passwords**, **reusing passwords** etc. to gain illegal access to the data backups in the cloud
Compliance Risks	03	Organizations that seek to obtain compliance to standards and laws may be put at risk if the CSP **cannot provide evidence of their own compliance** with the necessary requirements, outsource cloud management to third parties and/or **does not permit audit** by the client
Economic Denial of Sustainability (EDOS)	04	If an attacker engages the cloud with a malicious service or executes malicious code that **consumes a lot of computational power and storage from the cloud server**, then the legitimate account holder is charged for this kind of computation until the primary cause of CPU usage is detected

Module Flow

Cloud Computing Attacks

1. Service Hijacking using Social Engineering Attacks
2. Service Hijacking using Network Sniffing
3. Session Hijacking using XSS Attack and Session Riding
4. Domain Name System (DNS) Attacks
5. Side Channel Attacks or Cross-guest VM Breaches
6. SQL Injection Attacks
7. Cryptanalysis Attacks
8. Wrapping Attack
9. DoS and DDoS Attacks
10. Man-in-the-Cloud Attack

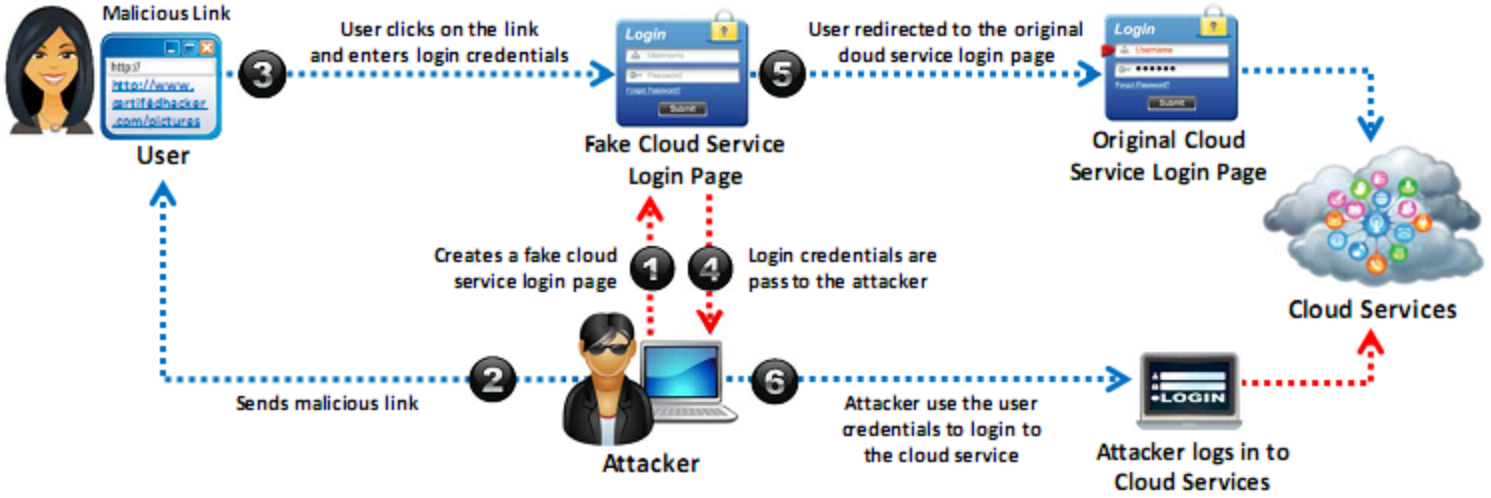
Service Hijacking using Social Engineering Attacks

1. Social engineering is a non-technical **intrusion that relies heavily on human interaction** and often involves tricking other people to break normal security procedures

2. Attacker might target the cloud service provider to **reset the password** or **IT staff accessing the cloud services to reveal passwords**

3. Other ways to obtain passwords include: **password guessing**, using **keylogging malware**, implementing **password cracking techniques**, sending **phishing mails**, etc.

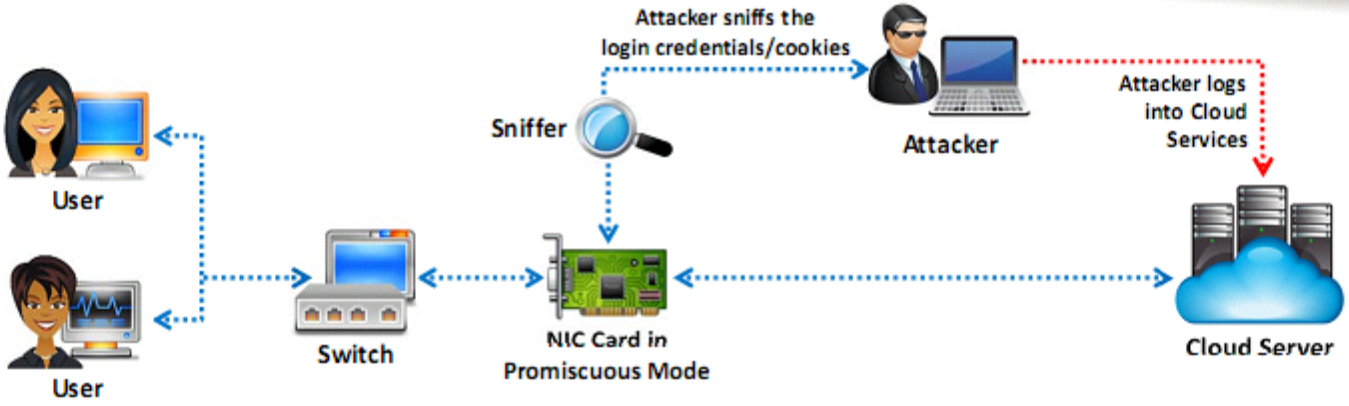
4. Social engineering attack results in **exposing customer data**, credit card data, **personal information**, **business plans**, staff data, identity theft, etc.



Service Hijacking using Network Sniffing

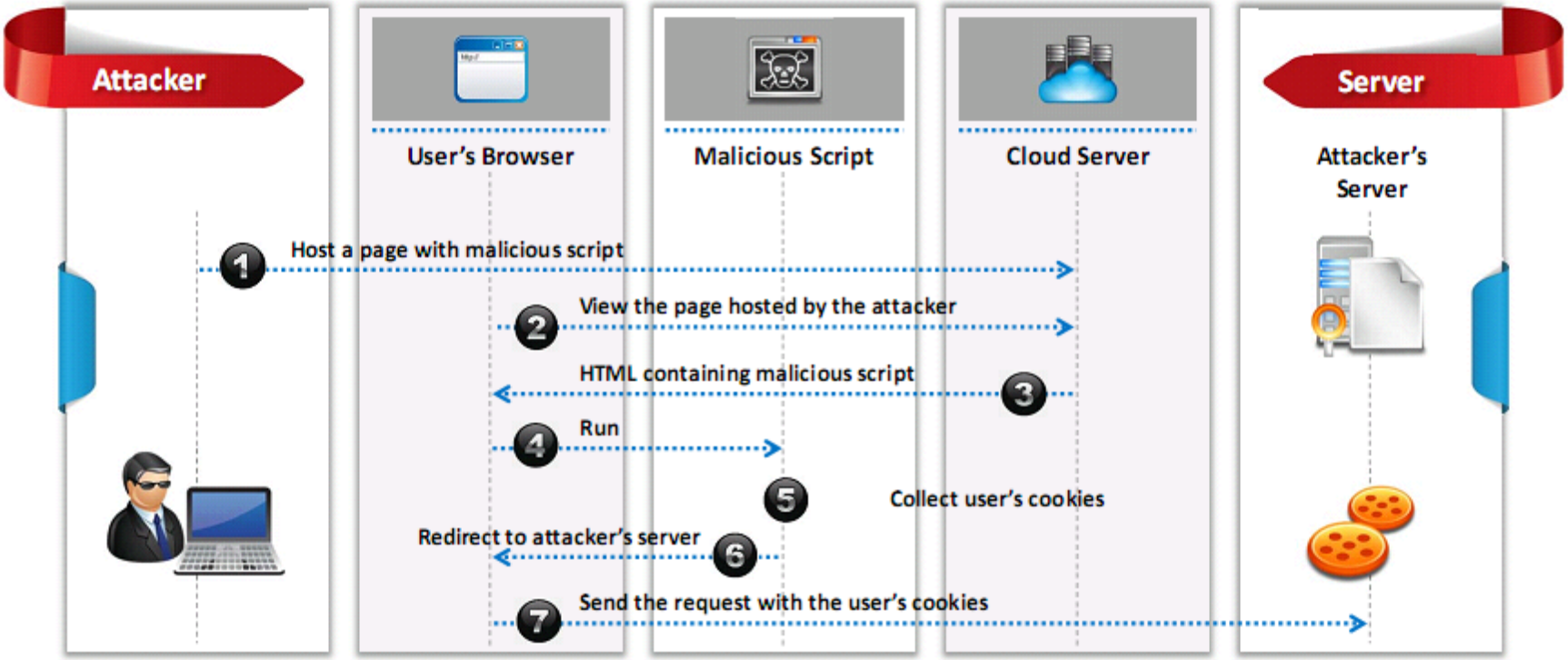
Network sniffing involves **interception and monitoring of network traffic** which is being sent between the two cloud nodes

Attacker uses packet sniffers to capture sensitive data such as **passwords**, **session cookies**, and other web service related security configuration such as the **UDDI** (Universal Description Discovery and Integrity), **SOAP** (Simple Object Access Protocol) and **WSDL** (Web Service Description Language) files



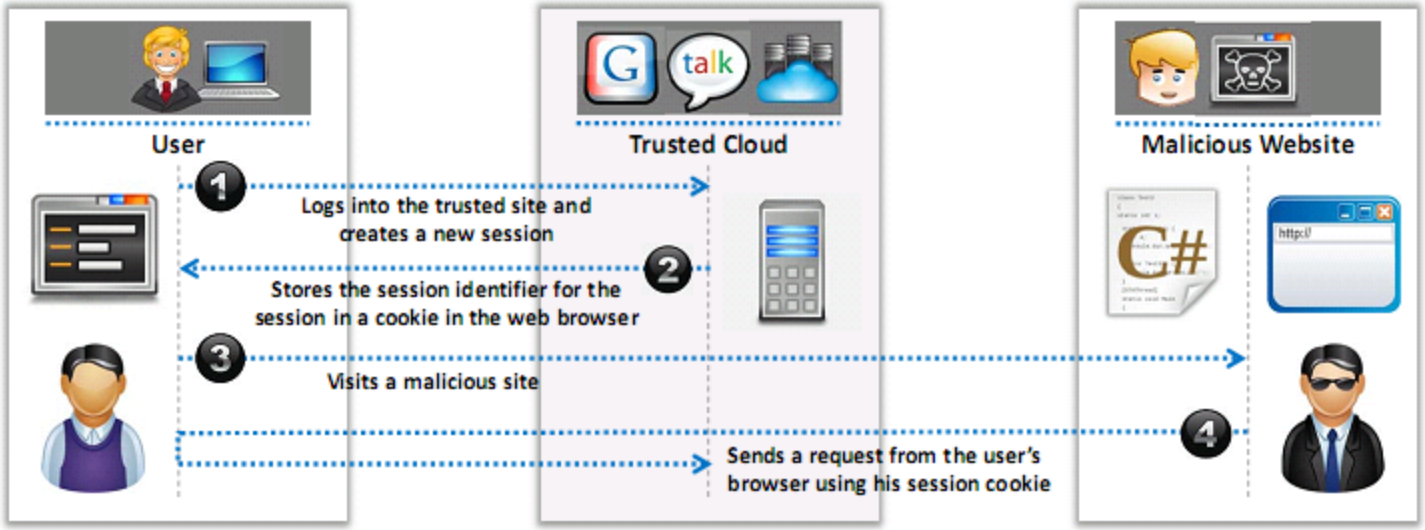
Session Hijacking using XSS Attack

- Attacker implements Cross-Site Scripting (XSS) to **steal cookies that are used to authenticate users**, this involves injecting a malicious code into the website that is subsequently executed by the browser



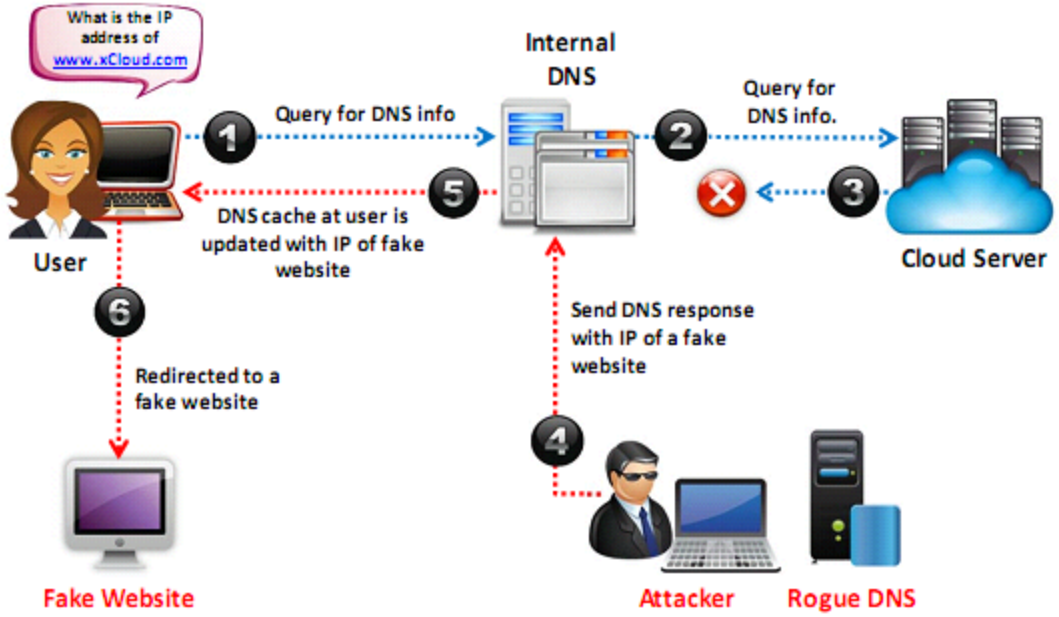
Session Hijacking using Session Riding

- Attacker exploits website by implementing **cross-site request forgery** to transmit unauthorized commands
- In session riding, attacker rides an active computer session by **sending an email** or **tricking the user to visit a malicious webpage** while they are logged into the targeted site
- When the **user clicks the malicious link**, the website executes the request as the user is already authenticated
- **Commands used include**: Modify or delete user data, execute online transactions, reset passwords, etc.



Domain Name System (DNS) Attacks

- Attacker performs DNS attacks to obtain **authentication credentials** from internet users



Types of DNS Attacks

DNS Poisoning

Involves **diverting users to a spoofed website** by poisoning the DNS server or the DNS cache on the user's system

Cybersquatting

Involves conducting **phishing scams by registering a domain name** that is similar to a cloud service provider

Domain Hijacking

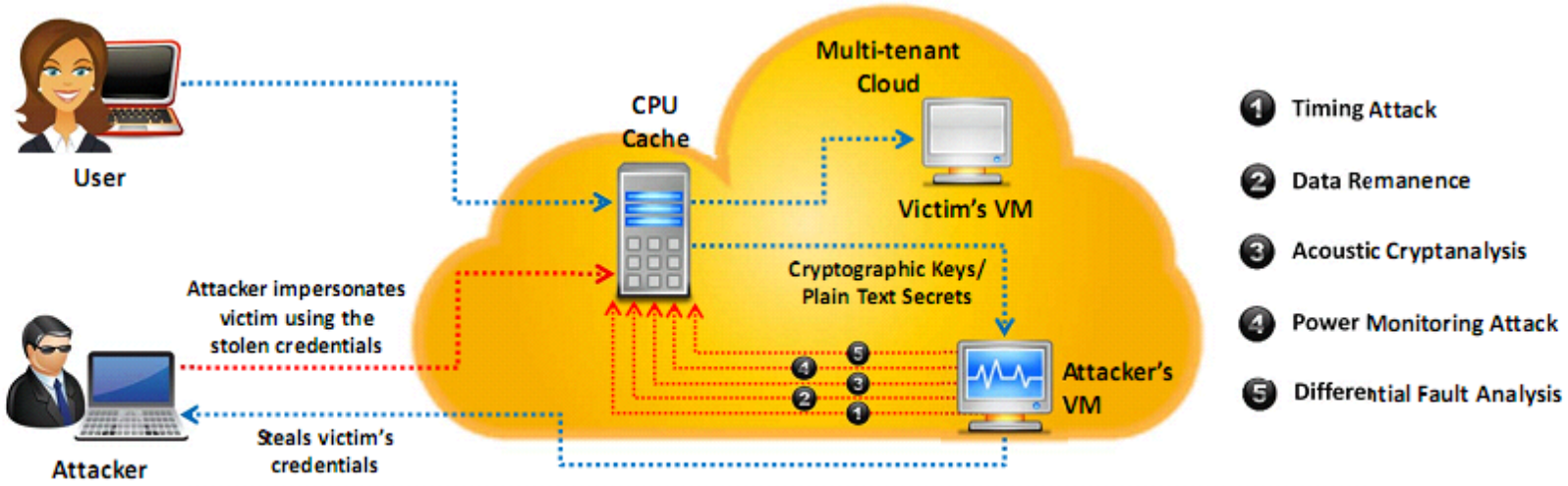
Involves **stealing** a cloud service provider's domain name

Domain Snipping

Involves **registering** an elapsed domain name

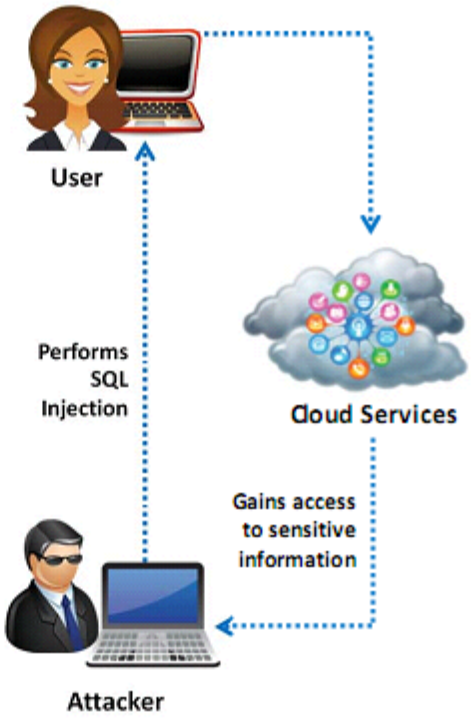
Side Channel Attacks or Cross-guest VM Breaches

- Attacker compromises the cloud by placing a **malicious virtual machine** near to a target cloud server and then launch side channel attack
- In side channel attack, attacker **runs a virtual machine on the same physical host of the victim's virtual machine** and takes advantage of shared physical resources (processor cache) to **steal data** (cryptographic key) from the victim
- Side-channel attacks can be implemented by any **co-resident user** and are mainly due to the vulnerabilities in shared technology resources



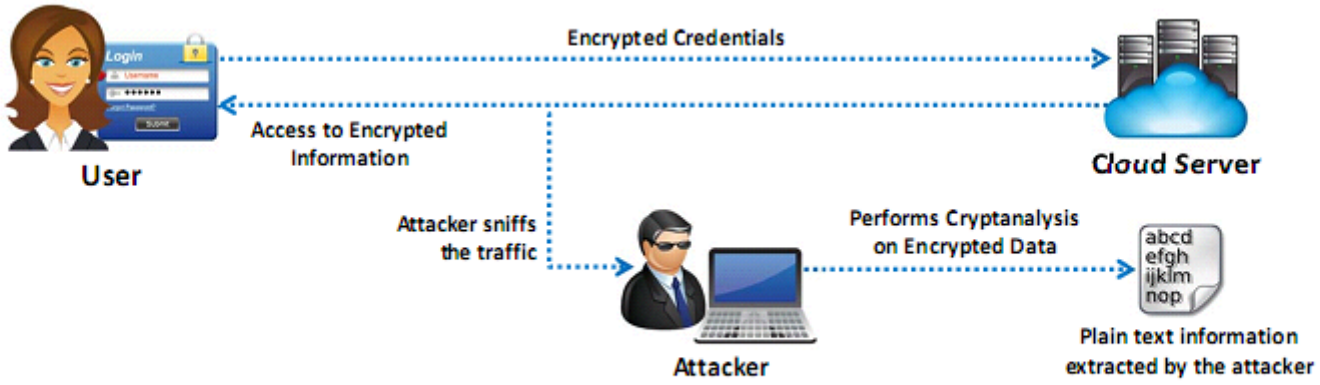
SQL Injection Attacks

- Attackers target SQL servers running **vulnerable database applications**
- It occurs when application uses input to **construct dynamic SQL statements**
- In this attack, attackers **insert a malicious code** (generated using special characters) into a **standard SQL code** to gain unauthorized access to a database
- Further attackers can **manipulate the database contents**, **retrieve sensitive data**, remotely execute system commands, or even **take control of the web server** for further criminal activities



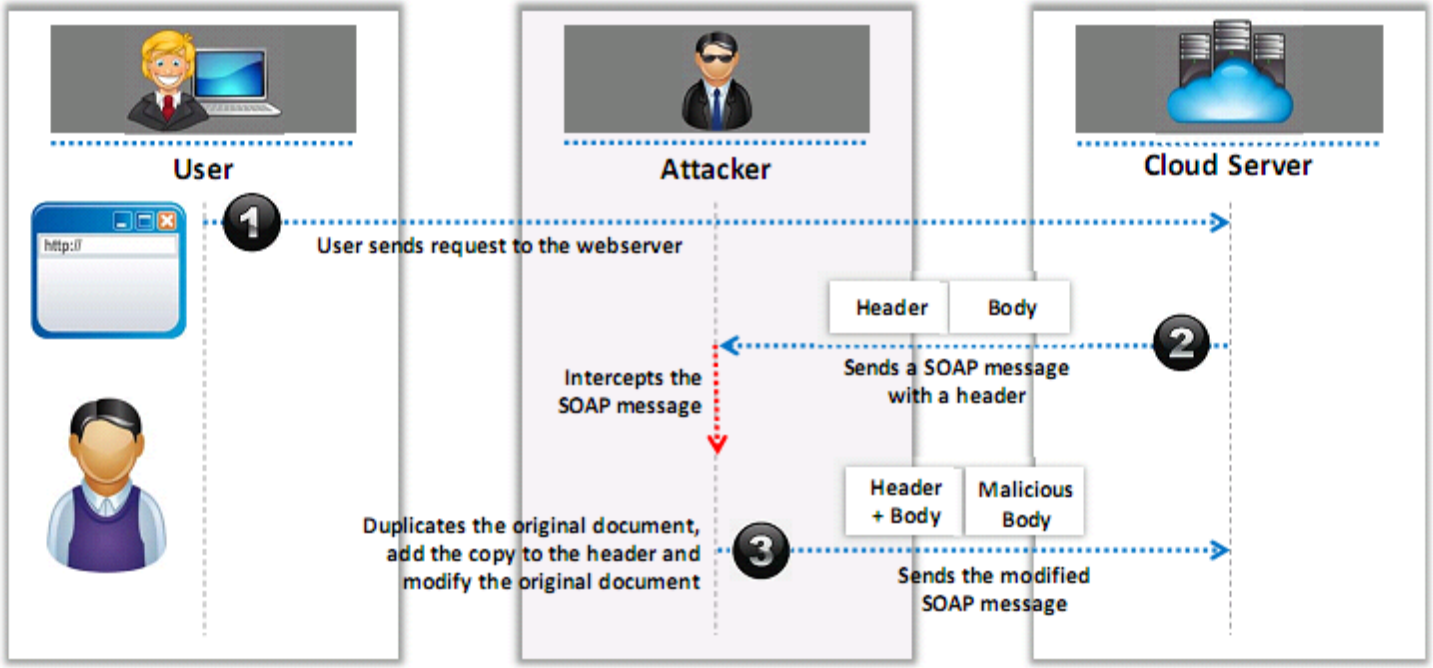
Cryptanalysis Attacks

- **Insecure** or **obsolete encryption** makes cloud services susceptible to cryptanalysis
- Data present in the cloud may be encrypted to prevent it from being read if accessed by malicious users. However **critical flaws in cryptographic algorithm** implementations (e.g.: weak random number generation) might turn strong encryption to weak or broken, also there exists novel methods to break the cryptography
- Partial information can also be obtained from encrypted data by monitoring **clients' query access patterns** and **analyzing accessed positions**



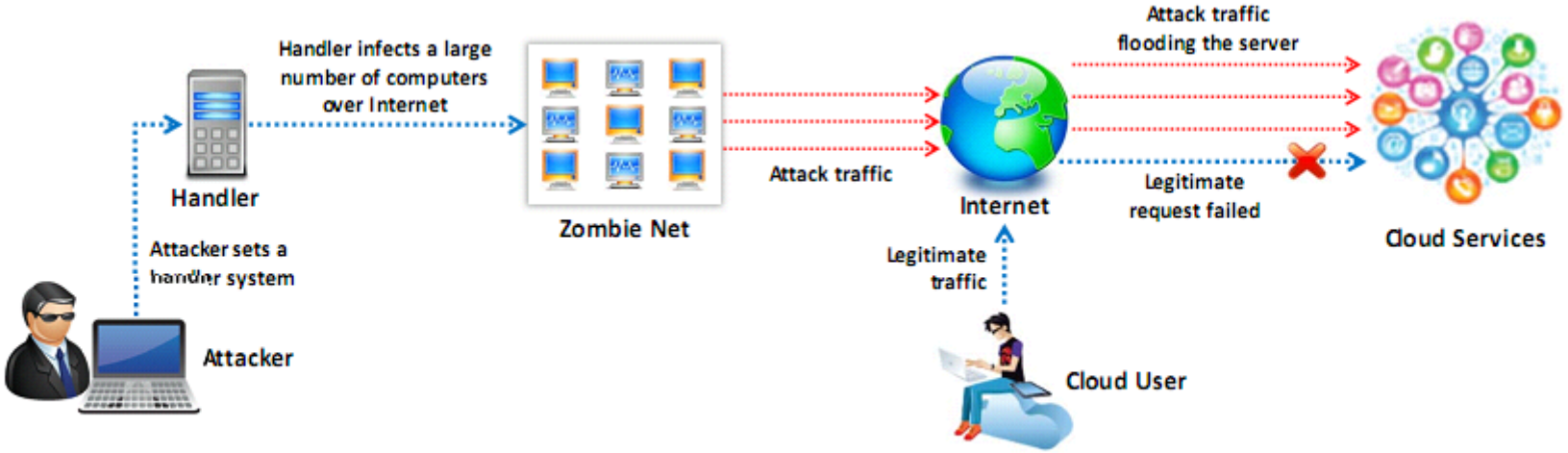
Wrapping Attack

- Wrapping attack is performed during the **translation of SOAP message** in the TLS layer where attackers duplicate the body of the message and send it to the server as a legitimate user



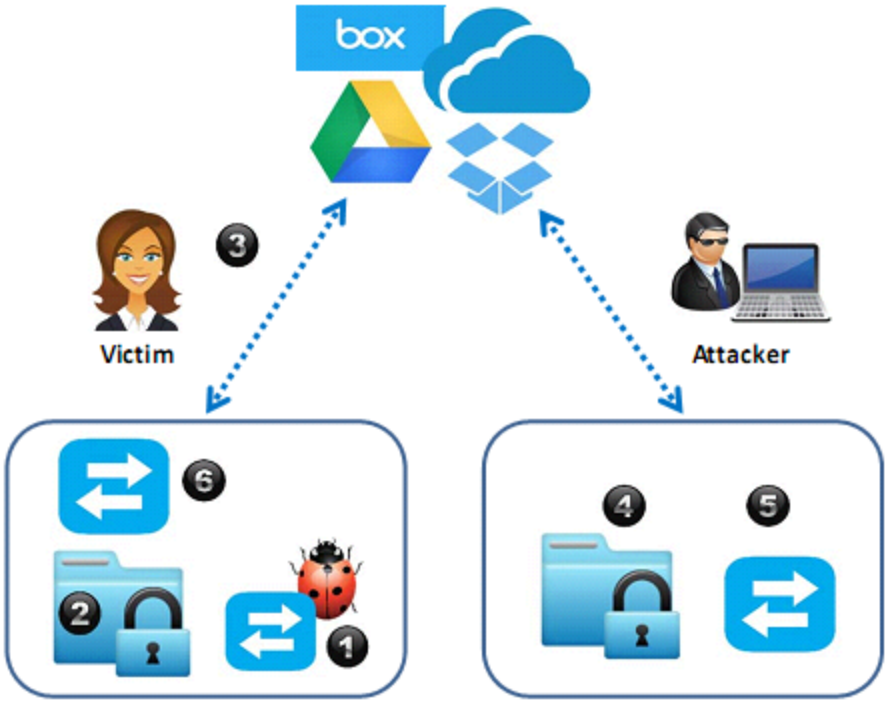
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

- Performing DoS attack on cloud service providers may **leave tenants without access** to their accounts
- DoS can be performed by:
  - **Flooding the server** with multiple requests to consume all the system resources available
  - **Passing malicious input** to the server that crashes an application process
  - **Entering wrong passwords** continuously so that user account is locked
- If a DoS attack is performed by using a **botnet** (a network of compromised machines) then it is referred to as DDoS attack

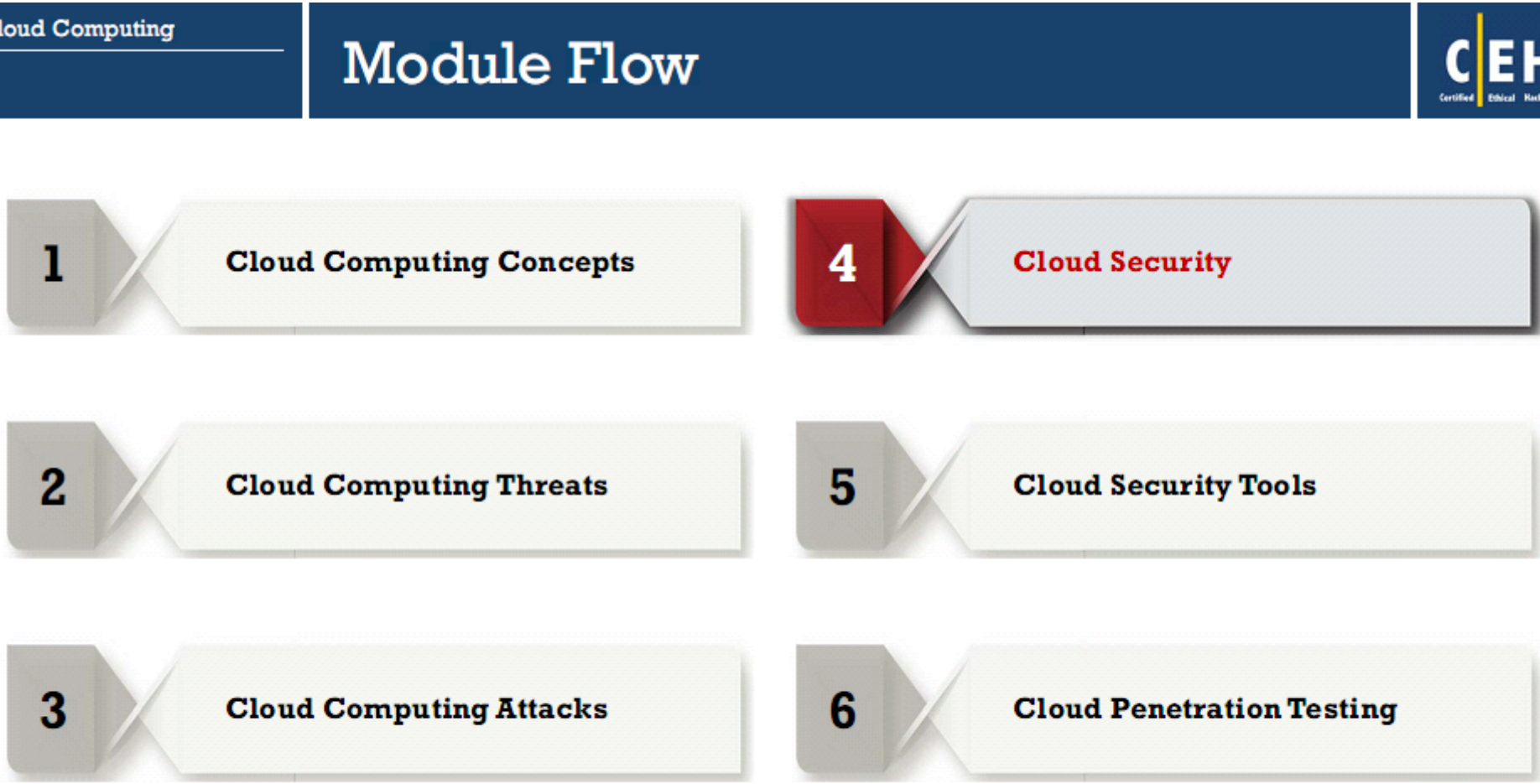


Man-in-the-Cloud Attack

- Man-in-the-Cloud (MITC) attacks are an advanced version of Man-in-the-middle (MITM) attacks
- In the MITM attacks, an **attacker uses an exploit** that intercepts and manipulates the communication between two parties while the MITC attacks are carried out by **abusing cloud file synchronization services** such as Google Drive or Drop Box for **Data compromise, command and control (C&C), data exfiltration**, and **remote access**
- The attacker tricks the victim to **install a malicious code** which plants attacker's **synchronization token** on the victim's drive
- Then, the attacker steals the victim's synchronization token and uses the stolen token to **gain access** of victim's files
- Later, attacker **restores the malicious token** with the original synchronized token of the victim, returning the drive application to its **original state** and stays undetected



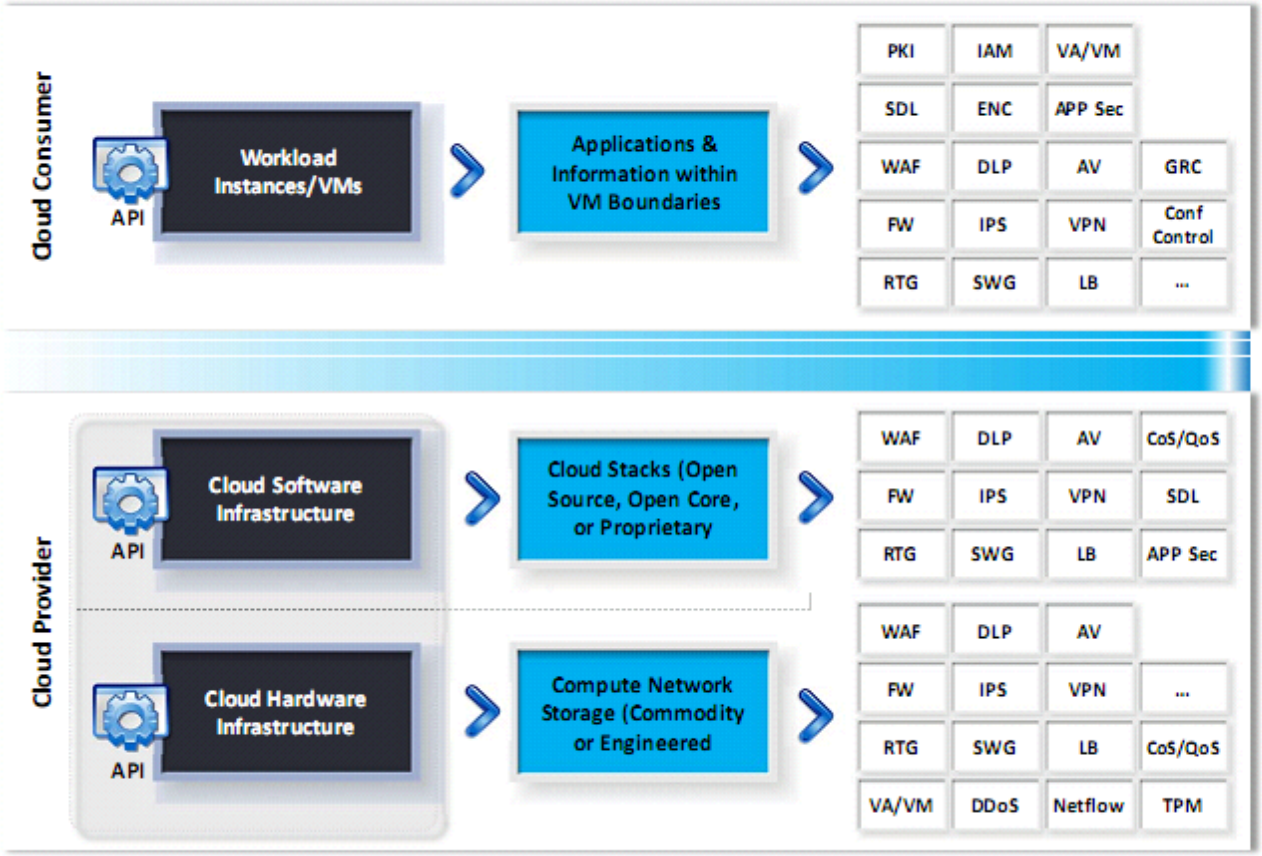
Module Flow



Cloud Security Control Layers

01	Applications	❯	SDLC, Binary Analysis, Scanners, Web App Firewalls, Transactional Sec
02	Information	❯	DLP, CMF, Database Activity Monitoring, Encryption
03	Management	❯	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
04	Network	❯	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
05	Trusted Computing	❯	Hardware and software RoT and API's
06	Computer and Storage	❯	Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
07	Physical	❯	Physical Plant Security, CCTV, Guards

Cloud Security is the Responsibility of both Cloud Provider and Consumer



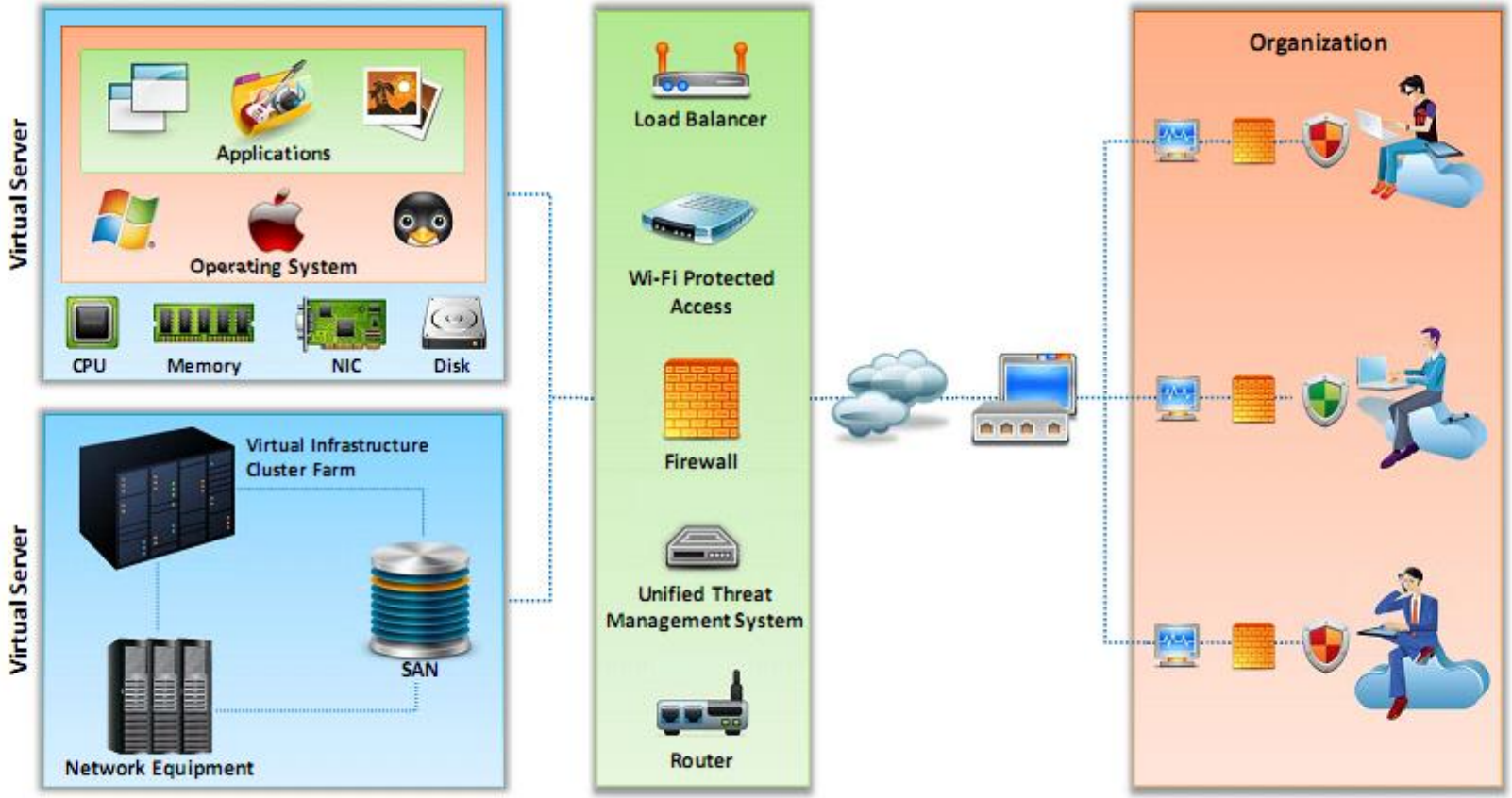
Security Controls

- **PKI:** Public Key Infrastructure
- **SDL:** Security Development Lifecycle
- **WAF:** Web Application Firewall
- **FW:** Firewall
- **RTG:** Real Traffic Grabber
- **IAM:** Identity and Access Management
- **ENC:** Encryption
- **DLP:** Data loss prevention
- **IPS:** Intrusion Prevention System
- **SWG:** Secure Web Gateway
- **VA/VM:** Virtual Application/Virtual Machine
- **App Sec:** Application security
- **AV:** Anti-virus
- **VPN:** Virtual Private Network
- **LB:** Load Balancer
- **GRC:** Governance, Risk, and Compliance
- **Config Control:** Configuration Control
- **CoS/QoS:** Class of Service/ Quality of Service
- **DDoS:** Distributed denial of service
- **TPM:** Trusted Platform Module
- **Netflow:** Network protocol by Cisco

Cloud Computing Security Considerations

- Cloud **computing services should be tailor made** by the vendor as per the given security requirements of the clients
- Cloud service providers should provide higher **multi tenancy** which enables optimum utilization of the cloud resources and to secure data and applications
- Cloud services should implement **disaster recovery plan** for the stored data which enables information retrieval in unexpected situations
- Continuous monitoring on the **Quality of Service** (QoS) is required to maintain the **service level agreements** between consumers and the service providers
- Data stored in the cloud services should be implemented securely to ensure **data integrity**
- Cloud computing service should be **fast**, **reliable**, and need to provide **quick response** times to the new requests
- Symmetric and **asymmetric cryptographic algorithms** must be implemented for optimum data security in cloud computing
- Operational process of the cloud based services should be **engineered**, **operated**, and **integrated** securely to the organizational security management
- **Load balancing** should be incorporated in the cloud services to facilitate networks and resources to improve the response time of the job with maximum throughput

Placement of Security Controls in the Cloud



Best Practices for Securing Cloud

- Enforce **data protection**, **backup**, and **retention** mechanisms
- Implement strong **authentication**, **authorization** and **auditing** mechanisms
- Enforce **SLAs** for patching and vulnerability remediation
- Check for **data protection** at both design and runtime
- Vendors should regularly undergo **AICPA SAS 70 Type II audits**
- Implement **strong key generation**, storage and management, and destruction practices
- Verify one's own cloud in **public domain blacklists**
- Monitor the **client's traffic** for any malicious activities
- Enforce **legal contracts** in employee behavior policy
- Prevent unauthorized server access using **security checkpoints**
- Prohibit **user credentials sharing** among users, applications, and services
- Disclose applicable **logs** and **data** to customers

Best Practices for Securing Cloud (Cont'd)

- Analyze **cloud provider security policies** and SLAs
- Assess security of **cloud APIs** and also log customer **network traffic**
- Ensure that cloud undergoes regular **security checks and updates**
- Ensure that physical security is a **24 x 7 x 365** affair
- Enforce **security standards** in installation/ configuration
- Ensure that the memory, storage, and network access is **isolated**
- Leverage strong **two-factor authentication** techniques where possible
- Baseline **security breach notification** process
- Analyze **API dependency chain software** modules
- Enforce stringent **registration and validation process**
- Perform vulnerability and configuration **risk assessment**
- Disclose infrastructure information, **security patching**, and firewall details

Best Practices for Securing Cloud (Cont'd)

1. Enforce stringent **cloud security compliance**, SCM (Software Configuration Management), and management practice transparency
2. Employ security devices such as IDS, IPS, firewall, etc. to guard and stop **unauthorized access** to the data stored in the cloud
3. Enforce strict **supply chain** management and conduct a comprehensive supplier assessment
4. Enforce stringent **security policies and procedures** like access control policy, information security management policy and contract policy
5. Ensure **infrastructure security** through proper management and monitoring, availability, secure VM separation and service assurance
6. Use **VPNs** to secure the clients data and ensure that data is **completely deleted** from the main servers along with its replicas when requested for data disposal
7. Ensure **Secure Sockets Layer** (SSL) is used for sensitive and confidential data transmission
8. Analyze the **security model** of cloud provider interfaces
9. Understand terms and conditions in **SLA** like **minimum level of uptime** and **penalties** in case of failure to adhere to the agreed level
10. Enforce basic information security practices namely strong **password policy**, **physical security**, device security, **encryption**, data security, network security, etc.

NIST Recommendations for Cloud Security

Assess risk posed to client's data, software and infrastructure

Select appropriate **deployment model** according to needs

Ensure **audit procedures** are in place for data protection and software isolation

Renew SLAs in case **security gaps** found between organization's security requirements and cloud provider's standards

Establish appropriate **incident detection** and **reporting mechanisms**

Analyze what are the **security objectives** of organization

Enquire about **who is responsible** of data privacy and security issues in cloud

Organization/Provider Cloud Security Compliance Checklist

Management	Organization	Provider
Is everyone aware of his or her cloud security responsibilities?		
Is there a mechanism for assessing the security of a cloud service?		
Does the business governance mitigate the security risks that can result from cloud-based "shadow IT"?		
Does the organization know within which jurisdictions its data can reside?		
Is there a mechanism for managing cloud-related risks?		
Does the organization understand the data architecture needed to operate with appropriate security at all levels?		
Can the organization be confident of end-to-end service continuity across several cloud service providers?		
Does the provider comply with all relevant industry standards (e.g. the UK's Data Protection Act)?		
Does the compliance function understand the specific regulatory issues pertaining to the organization's adoption of cloud services?		

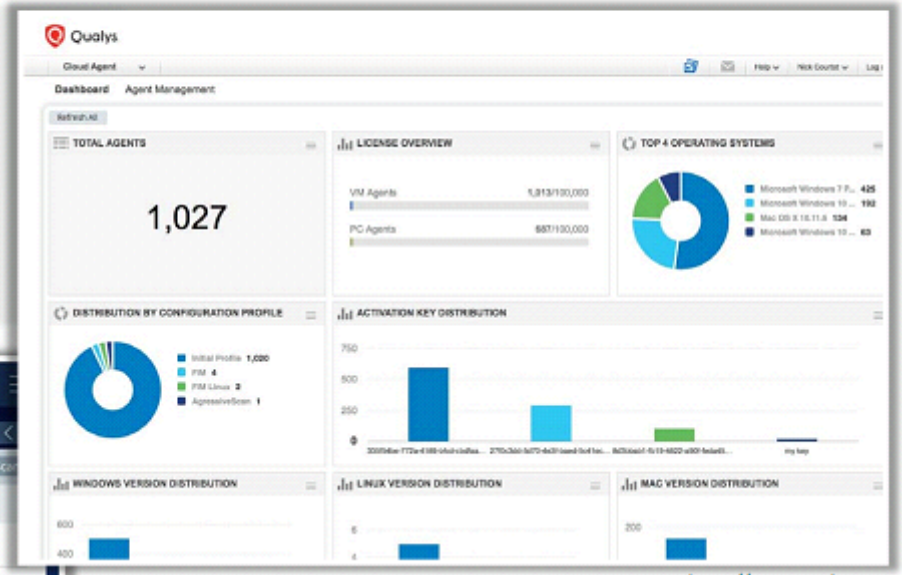
Module Flow

1. Cloud Computing Concepts
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

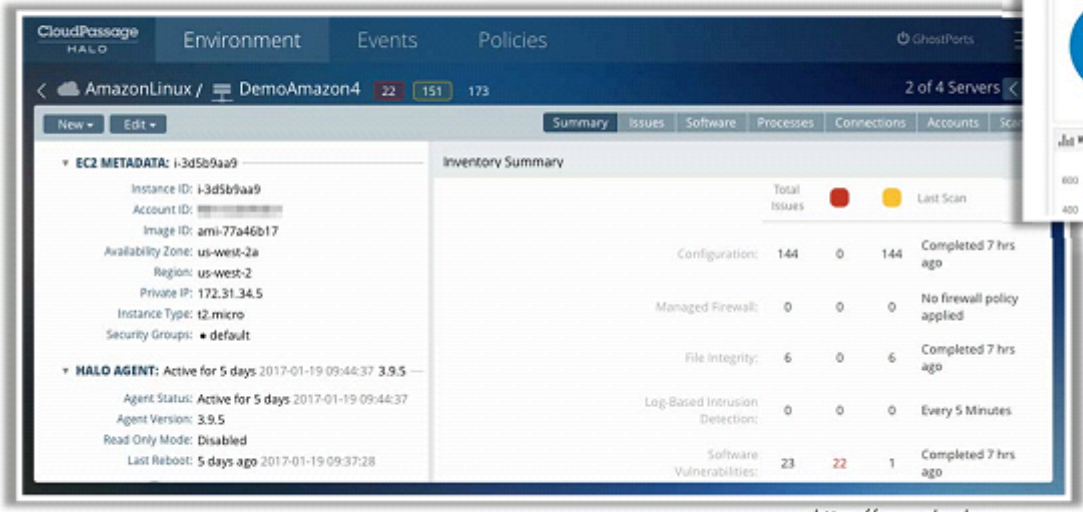
Cloud Security Tools

Qualys Cloud Platform

- Qualys Cloud Platform is a **end-to-end IT security solution** that provides a continuous, always-on **assessment of the global security** and compliance posture, with visibility across all IT assets irrespective of where they reside



https://www.qualys.com



https://www.cloudpassage.com

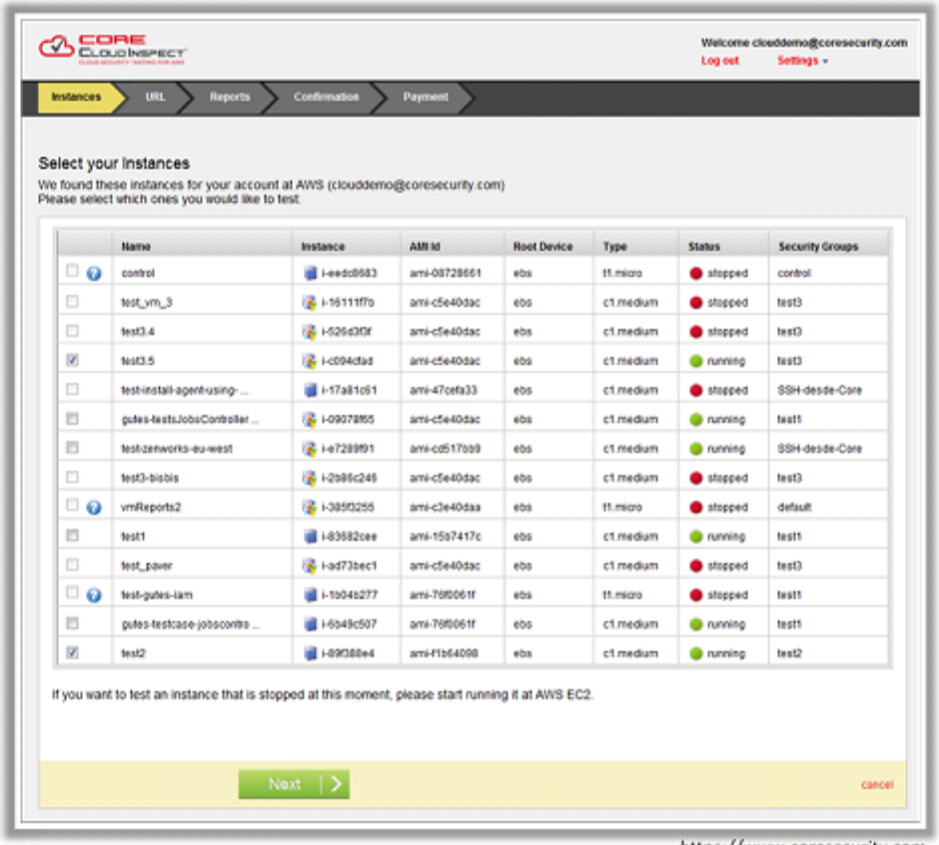
CloudPassage Halo

CloudPassage Halo is the **cloud server security platform** with all the security functions you need to safely deploy servers in public and hybrid clouds

Cloud Security Tools (Cont'd)

Core CloudInspect

- Core CloudInspect **helps validate** when cloud deployment is secure—and gives **actionable remediation information** when it is not secured
- The service conducts proactive, **real-world security tests** using the techniques employed by attackers seeking to **breach your AWS cloud-based systems** and applications



https://www.coresecurity.com

Nessus Enterprise for AWS
https://www.tenable.com

Symantec Cloud Workload Protection
https://www.symantec.com

Alert Logic
https://www.alertlogic.com

Deep Security
https://www.trendmicro.com

SecludIT
https://secludit.com

Module Flow

1. Cloud Computing Concepts
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

What is Cloud Pen Testing?

- Cloud pen testing is a method of actively evaluating the security of a cloud system by **simulating an attack from a malicious source**
- Security posture of cloud should be monitored regularly to determine the presence of **vulnerabilities** and the **risks** they pose
- Cloud security is based on the shared responsibility of both **cloud provider** and the **client**

Scope of Cloud Pen Testing

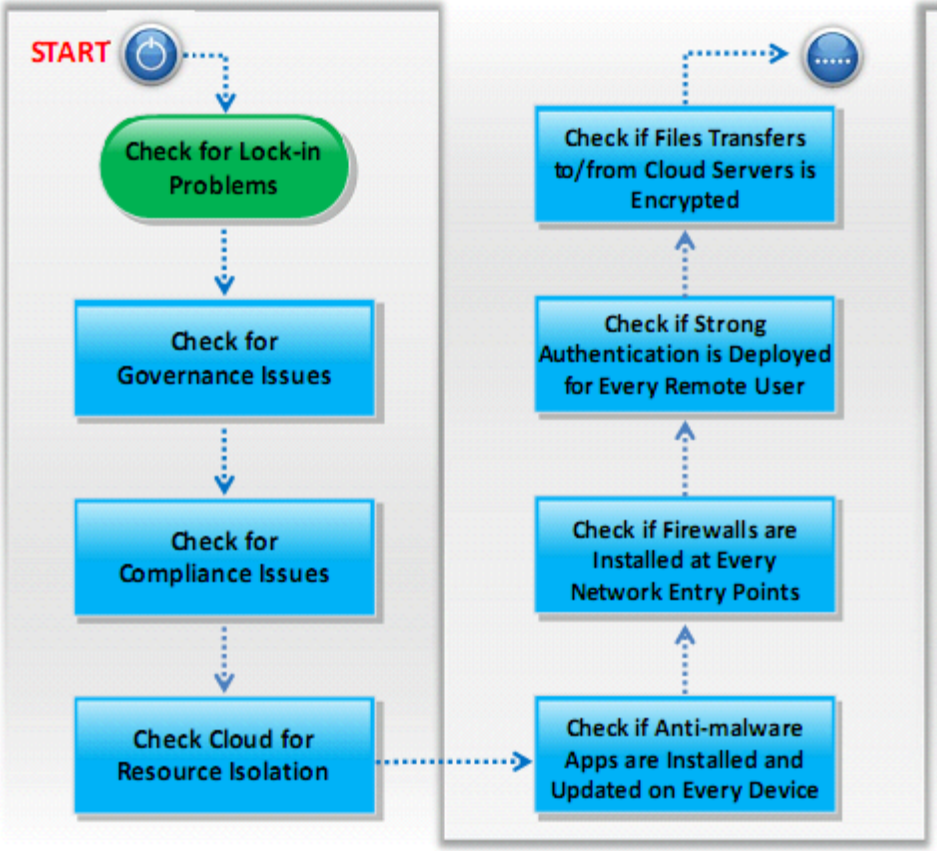
The scope of cloud pen testing depends on the type of cloud service used by the client

- **Infrastructure-as-a-Service (IaaS) –** virtualization security, solution stack, application layer, APIs, etc.
- **Platform-as-a-Service (PaaS) –** application and API layers
- **Software-as-a-Service (SaaS) –** usually **third party pen testing** is not allowed by SaaS vendors until unless it is explicitly mentioned in the Service Level Agreement (SLA)

Key Considerations for Pen Testing in the Cloud

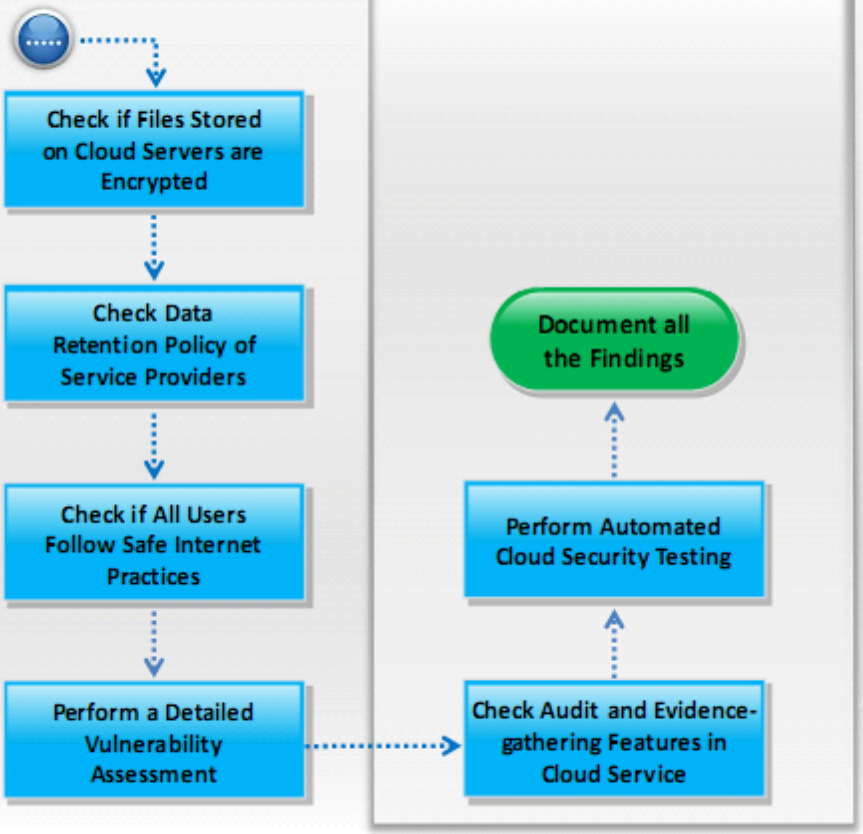
- Determine the **type of cloud**; PaaS, IaaS or SaaS
- Obtain **written consents** for performing pen testing
- Ensure every aspect of the Infrastructure (IaaS), Platform (PaaS), or Software (SaaS) are included in the **scope of testing** and **generated reports**
- Determine **how often and what kind of testing** is permitted by Cloud Service Provider (CSP)
- Prepare **legal** and **contractual** documents
- Perform both **internal** and **external pen testing**
- Perform pen tests on the **web apps/services** in the cloud without web application firewall (WAF) or reverse proxy
- Perform **vulnerability scans on host** available in the cloud
- Determine how to coordinate with the CSP for **scheduling** and **performing the test**

Cloud Penetration Testing



1. Check the service level agreement (SLA) between subscriber and cloud service, and determine the provisions to switch over to other CSPs
2. Check SLA document and track record of CSP to determine Roles and responsibilities of the CSP and subscribers in managing the cloud resources
3. Check the responsibilities of the CSP and subscribers in maintaining compliance, and check if the SLA provides transparency on this issue
4. Check if activity of one subscriber affect the other
5. Check if each component of the cloud infrastructure, i.e. data center, access points, devices, and suppliers is protected using appropriate security controls
6. Unused ports, protocols, and services should be blocked
7. Two-factor authentication should be used to validate those using OTP (One Time Password) for accessing the network to ensure security
8. Check the cloud services for SSL encryption in the access URL, security certificates from reputed vendors, and security pad locks

Cloud Penetration Testing (Cont'd)



9. Check if data stored in cloud servers is encrypted by default and determine the encryption algorithms used to encrypt the data
10. Determine if service providers are bound by the law of the land to disclose the data to third parties
11. Check if a documented computer and Internet usage policy exists and is implemented properly
12. Perform pen testing of each component as for the normal physical machines (check previous modules for more details)
13. Check if the cloud service provider offers features for cloning of virtual machines when required
    - Cloning of virtual machines helps minimize the down time as affected machines and evidence can be analyzed offline, facilitating investigation of a suspected security breach
14. Automated cloud security testing solutions can proactively verify the security of cloud deployments against real, current attack techniques

Recommendations for Cloud Testing

1. Find out whether the cloud provider will **accommodate** your own **security policies** or not
2. Compare the provider's **security precautions** to the present levels of security to ensure the **provider** is achieving better security levels for the user
3. Ensure that the cloud computing partners suggest **risk assessment** techniques and information on how to reduce the **uncovered security** risks
4. Make sure that a cloud **service provider** is capable of providing their policies and procedures for any **security agreement** that an agency faces
5. **Pay attention** to the service provider's **agreement** so that the **coding policies** can be secured
6. **Authenticate** users with a user name and password
7. Ensure that all **credentials** such as accounts and **passwords** assigned to the **cloud provider** should be changed regularly by the organization
8. **Strong password** policies must be advised and employed by the **doud pen testing** agencies

Recommendations for Cloud Testing (Cont'd)

9	Ensure that the existing business IT **security protocols** are up-to-date and flexible enough to handle the risks involved in cloud computing
10	Make sure that IT support can be offered and use more **stringent layers** of security to prevent potential data breaches
11	Make sure that the access to **virtual environment** management interfaces is highly restricted
12	**Password encryption** is advisable
13	Protect the **information** which is uncovered during the penetration testing
14	Pay special attention to cloud **hypervisors**, the **servers** that run multiple operating systems
15	Use a **centralized authentication** or single sign on for the firms that use SaaS applications
16	Make sure that the workers are provided with the best training possible to comply with these **security parameters**

Module Summary

- Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network
- Cloud services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)
- Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying resources such as a server, a storage device or a network
- Attackers create anonymous access to cloud services and perpetrate various attacks such as password and key cracking, building rainbow tables, CAPTCHA-solving farms, launching dynamic attack points, etc.
- Cloud service providers should provide higher multi-tenancy which enables optimum utilization of the cloud resources and to secure data and applications
- Cloud pen testing is a method of actively evaluating the security of a cloud system by simulating an attack from a malicious source