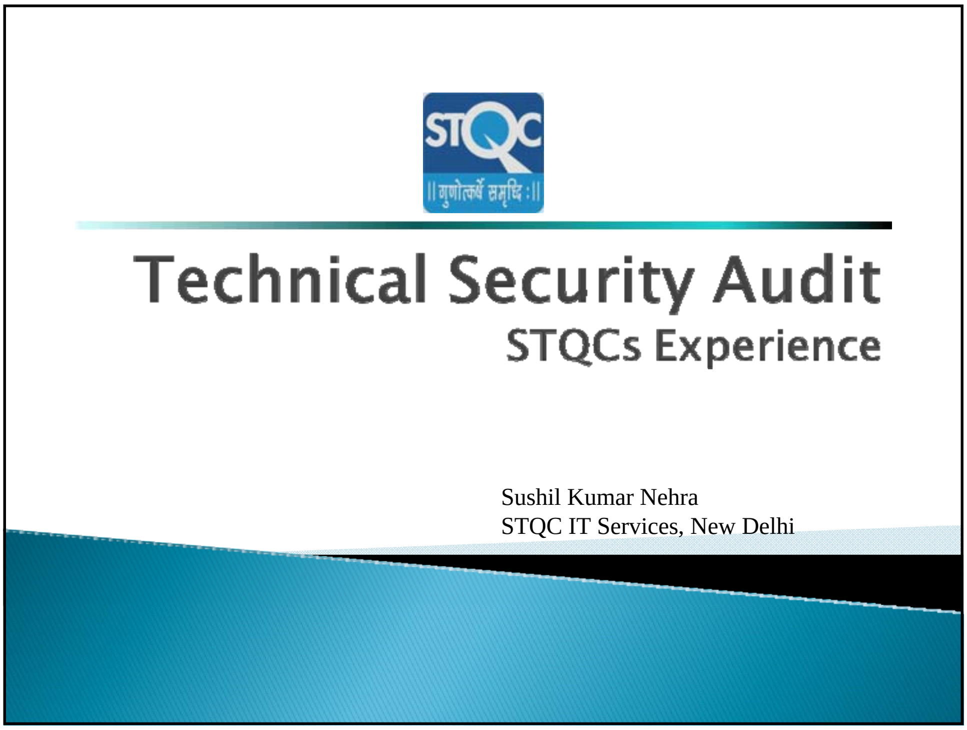
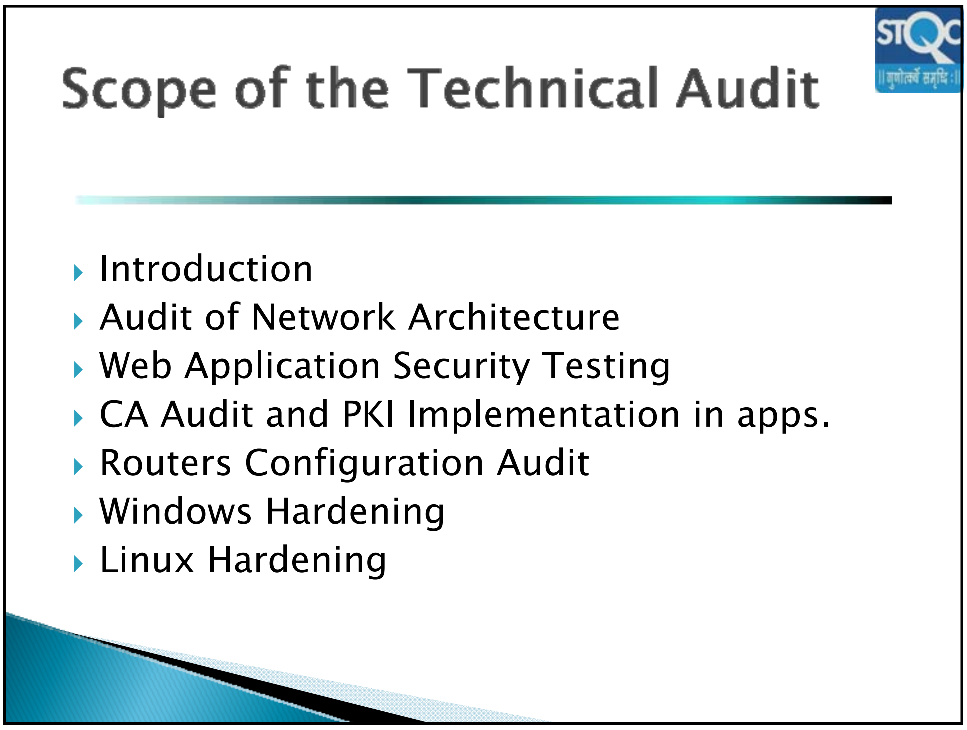


Technical Security Audit

STQCs Experience

Sushil Kumar Nehra
STQC IT Services, New Delhi



Scope of the Technical Audit

- Introduction
- Audit of Network Architecture
- Web Application Security Testing
- CA Audit and PKI Implementation in apps.
- Routers Configuration Audit
- Windows Hardening
- Linux Hardening

Challenges w.r.t Security Implementation

Multiple hats:

•Network Designer.

•Infrastructure

•Developer.

•Database Admin.

•System Admin.

•Security Admin.

•On time delivery of the solution.

And

•Security Analyst.

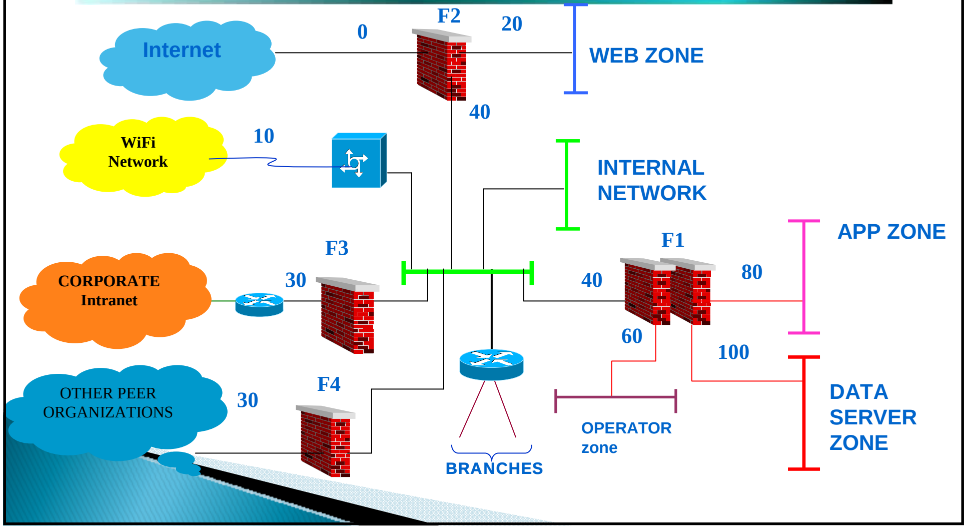
Security Analysis:
Wear a different Hat !

- Security Starts in your mind.
  - When doing Security Analysis use the internal system knowledge but not limit to being:-
    - Network Designer.
    - Developer.
    - Database Admin.
    - System Admin.
    - Security Admin managing firewall, IDS, IPS etc
- Expected to obtain information by studying, interviewing, discussing, referring to standards .

Complexity of Network

- Local Area Networks
- Wide Area Networks
- Wireless Networks
- Radio Networks
- Virtual Private Networks
- Voice Networks
- IP Convergence
- Web Hosting
- Internet E-Mail
- Routed Access to Third Party

Network Segregation based on Security Zones



Network Architecture

- Issues
  - Identification of Information Assets needing protection.
  - Understanding of Environment & Possible threats.
  - Proper segregation of Network, Suitable Access controls.
  - Placement of IDS sensors
  - Monitoring and analysis of Access Logs (syslog)
  - Time synchronized logs using Network Time Protocol

Network Architecture – Major Issues

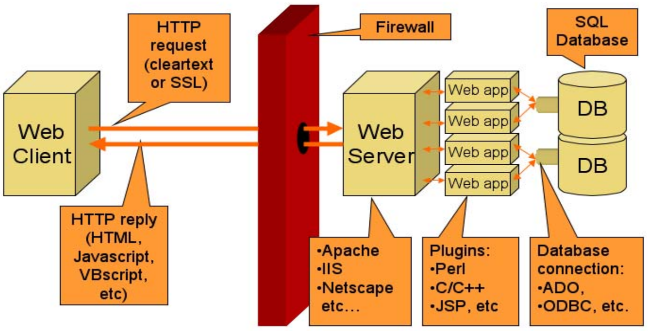
- Issues
  - Improper identification of threats especially internal threats.
  - Placing few servers/PC, placed in outside zone of firewalls, having access to internal network via firewall.
  - Not Segregating the WAN based on security levels. (assuming no threat then not connected to Internet)

Network Architecture

- Issues:
  - Application with 2 tier architecture accessed over WAN.
  - Use of Custom made firewall and improper configuration.
  - Designing complex network but using allow all firewall rules.

Application Hosting Components

Web based application being accessed from Internet



(c) net-square

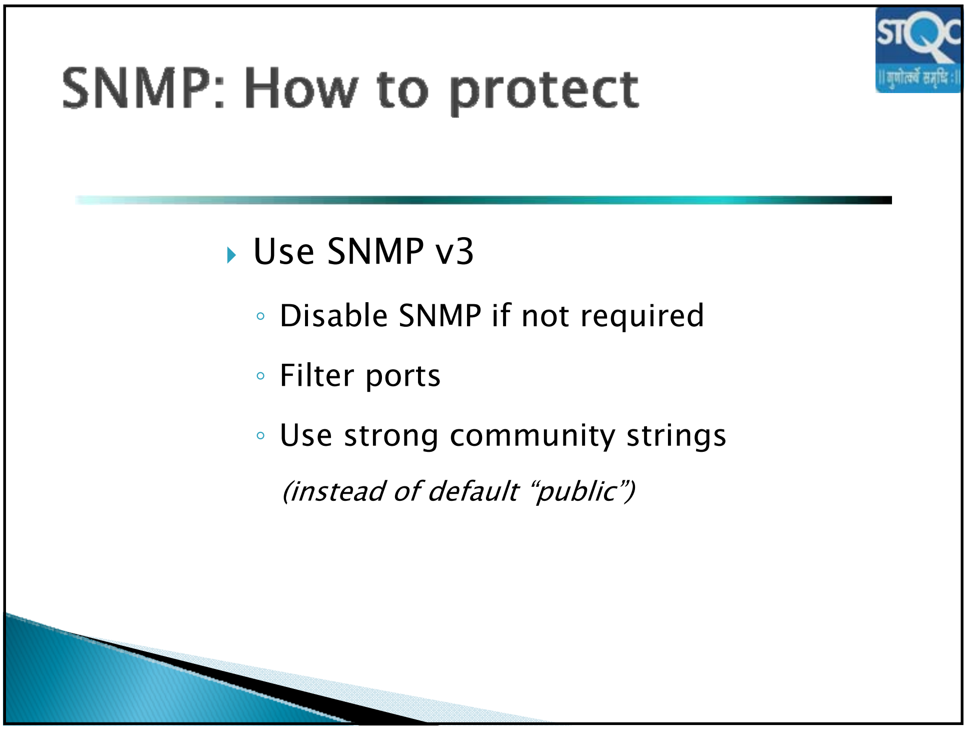
Database & Web server should be in different Zones.

Managing Networks

- Software to monitor and manage big Network
  - CISCOWorks,
  - Tivoli,
  - HP NNM,
  - MRTG,
  - PRTG,
  - WhatsUpGold etc
- Protocol
  - SNMP: Simple Network Management Protocol
    - Used in network management
      - Components
        - Manager, Agents and MIB
    - Works as an application protocol running over UDP
    - One manager can handle hundreds of agents

SNMP: Vulnerabilities

- Unencrypted password
- Default password
- Handling of trap messages
- Mapping of network
- Denial of service



SNMP: How to protect

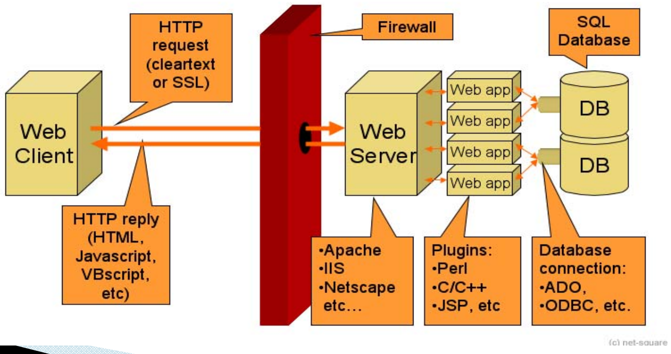
- Use SNMP v3
  - Disable SNMP if not required
  - Filter ports
  - Use strong community strings

    (instead of default "public")

Application Security Testing

Need of Application Security

Application Security – Firewall, IDS, IPS will not be able to stop misuse of the web Application



OWASP Top 10 Vulnerabilities

- A1 – Injection
- A2 – Cross Site Scripting (XSS)
- A3 – Broken Authentication and Session Management
- A4 – Insecure Direct Object References
- A5 – Cross Site Request Forgery (CSRF)
- A6 – Security Misconfiguration
- A7 – Insecure Cryptographic Storage
- A8 – Failure to Restrict URL Access
- A9 – Insufficient Transport Layer Protection
- A10 – Unvalidated Redirects and Forwards

www.owasp.org

Website Penetration Test

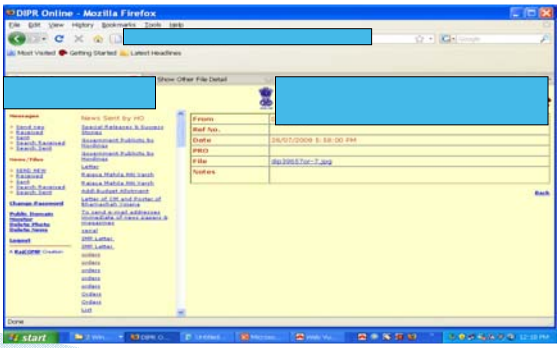
- SQL injection flaw.

By exploiting SQL injection flaw a hacker can delete, modify, insert some data in the database.

Reason: Improper input validation

Using SQL Injection to enter an web applicaiton.

- http://ABCDEFDJFD/Index.asp.
- Able to login to the site with test user and bypassing password with SQL injection.



DIPR Online - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
Show Other File Detail
News Sent by HO
Back
Done
start

[redacted]

[redacted]

[redacted]

From	
Ref No.	
Date	26/07/2008 5:58:00 PM
PRO	
File	dip39657or-7.jpg
Notes	

Cross site scripting

- This vulnerability if present on any page on the website :-
  - users of the website can be misguided to another site or
  - a malicious script can send hijacked session to hacker without the knowledge of user.

Application issues

- Business logic Security
  - Roles and responsibility
  - Designing for convenience
  - Scenario:
    - What if an administrator creates another admin user in the application for few days.
    - Second admin user deletes the original admin.
    - And later on second admin deletes his own account.
    - Leads to Denial of Service and application can not be administered.

C A Audit

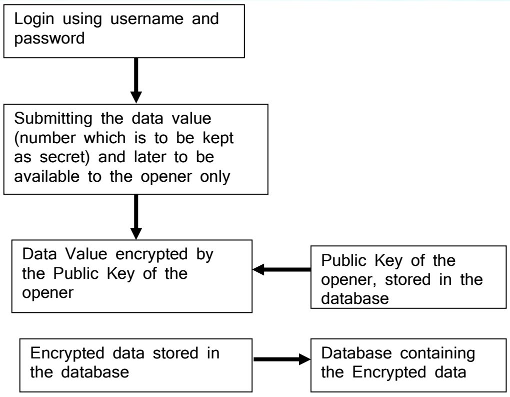
PKI Implementation

- PKI uses a pair of mathematically related encryption keys to secure data.
- One key is kept private while the other is made public, allowing communications between individuals without exchanging secret keys.
- Encryption: Using a public key of receiver, messages can be sent that can only be read by someone possessing the corresponding private key (by receiver having his private key).
- Signing: Informations hash encrypted using private key of sender can be decrypted using that individual's (senders) public key, thus validating the sender and 'signed' the message.

Certification Authority Challenge

- The tricky part of PKI is the infrastructure, a system for generating and managing keys and digital certificates that contain them.
- CA Need to protect its private key, because all the “user keysets” (public -private) are signed by the private key of CA. Other CAs also trust it.
- Need to keep the copy of private key. In case of disaster the system need to be build again and same private key restored.
- Security of the backup copy of private key as important as the original copy. (threat – stealing)

PKI implementation in an application: Scenario one



Login using username and password

Submitting the data value (number which is to be kept as secret) and later to be available to the opener only

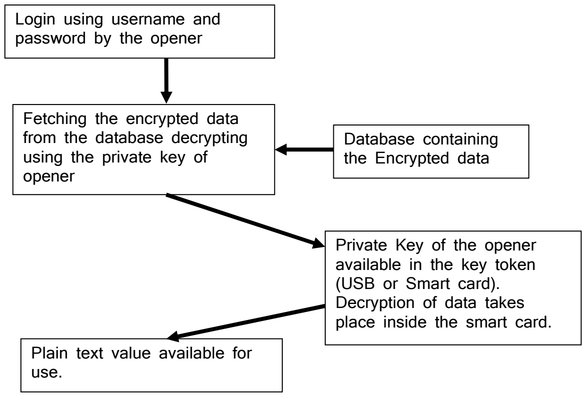
Data Value encrypted by the Public Key of the opener

Public Key of the opener, stored in the database

Encrypted data stored in the database

Database containing the Encrypted data

Decrypting in the PKI based application: Scenario one



Login using username and password by the opener

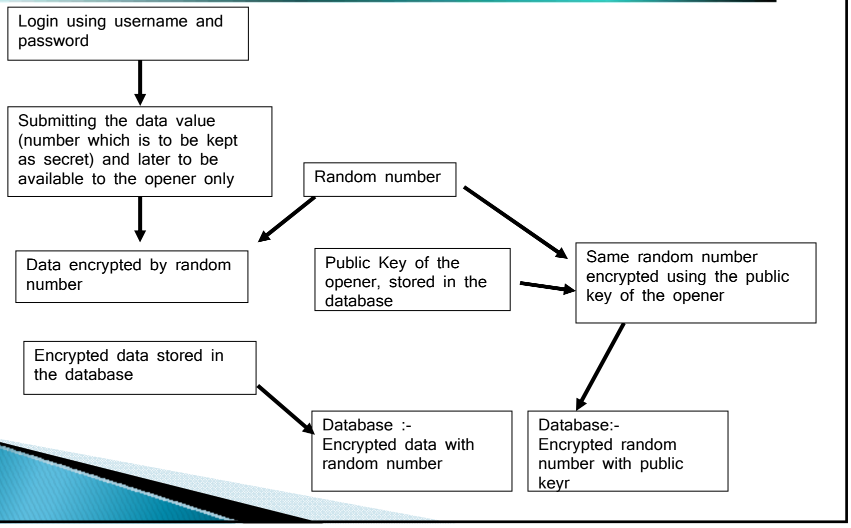
Fetching the encrypted data from the database decrypting using the private key of opener

Database containing the Encrypted data

Private Key of the opener available in the key token (USB or Smart card). Decryption of data takes place inside the smart card.

Plain text value available for use.

PKI implementation in an application: second Scenario



Login using username and password

Submitting the data value (number which is to be kept as secret) and later to be available to the opener only

Random number

Data encrypted by random number

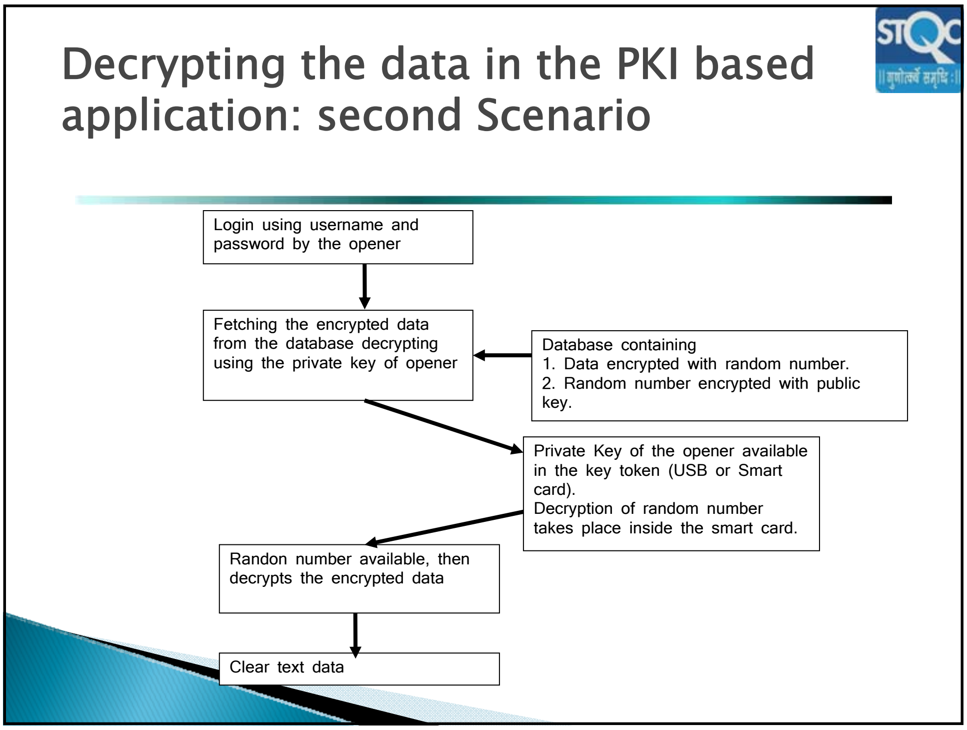
Public Key of the opener, stored in the database

Same random number encrypted using the public key of the opener

Encrypted data stored in the database

Database :- Encrypted data with random number

Database:- Encrypted random number with public keyr



Decrypting the data in the PKI based application: second Scenario

Login using username and password by the opener

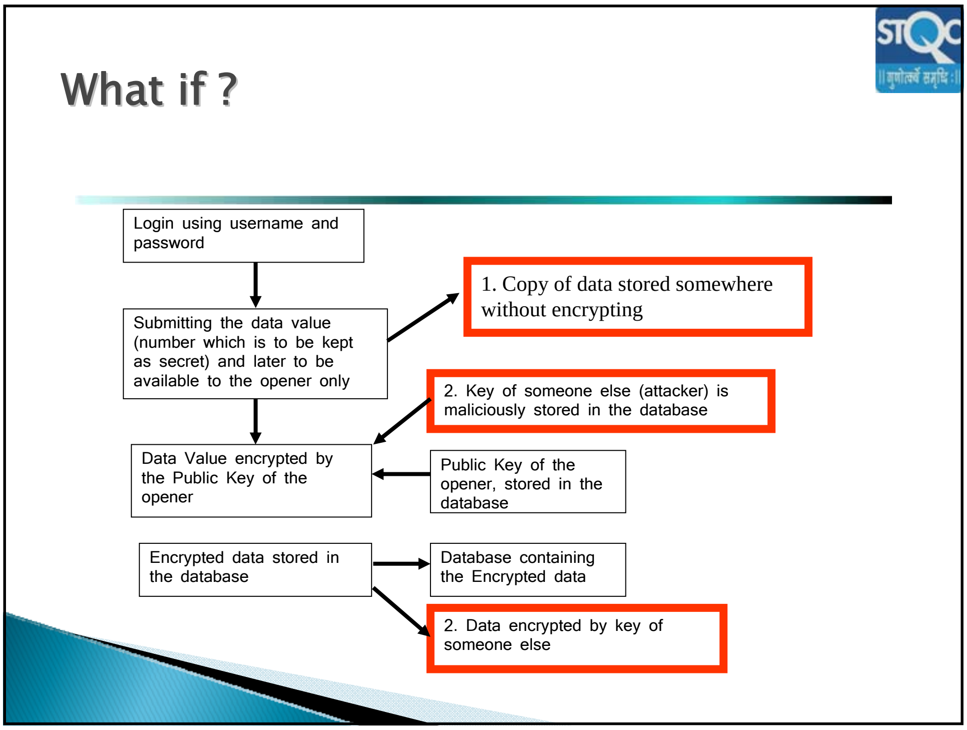
Fetching the encrypted data from the database decrypting using the private key of opener

Database containing
1. Data encrypted with random number.
2. Random number encrypted with public key.

Private Key of the opener available in the key token (USB or Smart card).
Decryption of random number takes place inside the smart card.

Randon number available, then decrypts the encrypted data

Clear text data



What if ?

Login using username and password

Submitting the data value (number which is to be kept as secret) and later to be available to the opener only

1. Copy of data stored somewhere without encrypting

2. Key of someone else (attacker) is maliciously stored in the database

Data Value encrypted by the Public Key of the opener

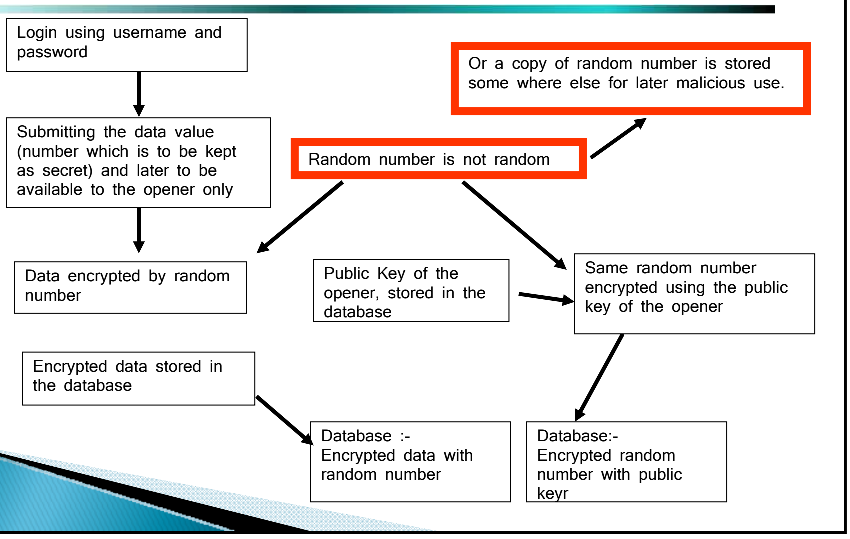
Public Key of the opener, stored in the database

Encrypted data stored in the database

Database containing the Encrypted data

2. Data encrypted by key of someone else

What if ?



Login using username and password

Submitting the data value (number which is to be kept as secret) and later to be available to the opener only

Data encrypted by random number

Encrypted data stored in the database

Database :- Encrypted data with random number

Random number is not random

Or a copy of random number is stored some where else for later malicious use.

Public Key of the opener, stored in the database

Same random number encrypted using the public key of the opener

Database:- Encrypted random number with public keyr

Threats

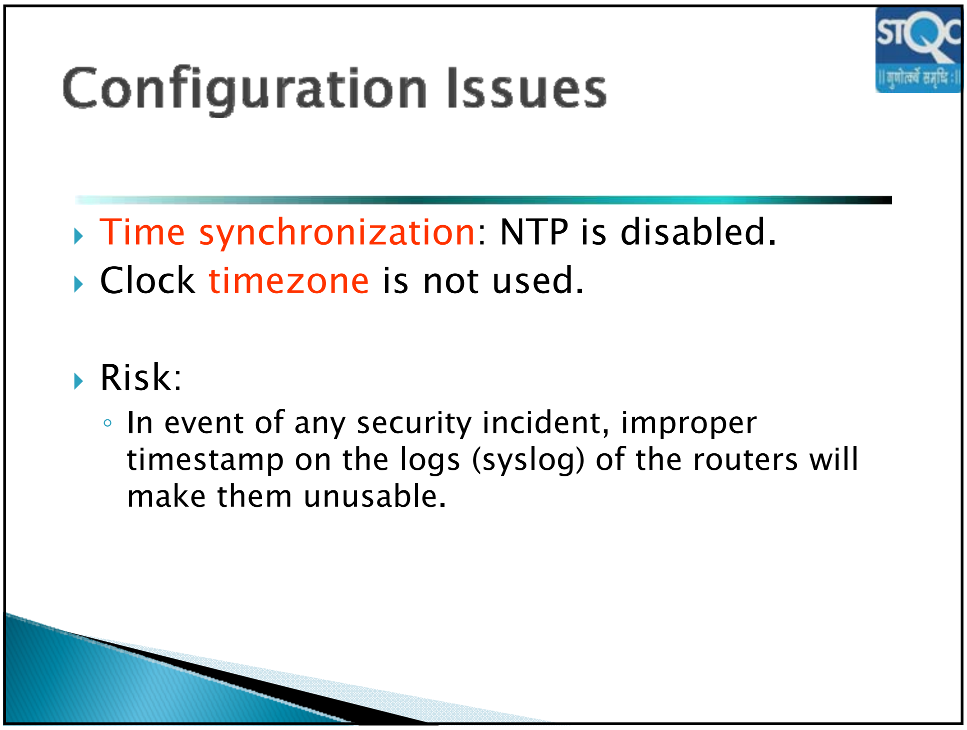
- Apart from insecure coding.

- Developers having access to operational source code on the production server.
- Organisation unable to detect change in code.
- Misuse of backup data for restoration elsewhere and extracting data.

VA & Configuration Audit

- Devices
  - Routers
  - Firewalls
  - Switches
  - Servers

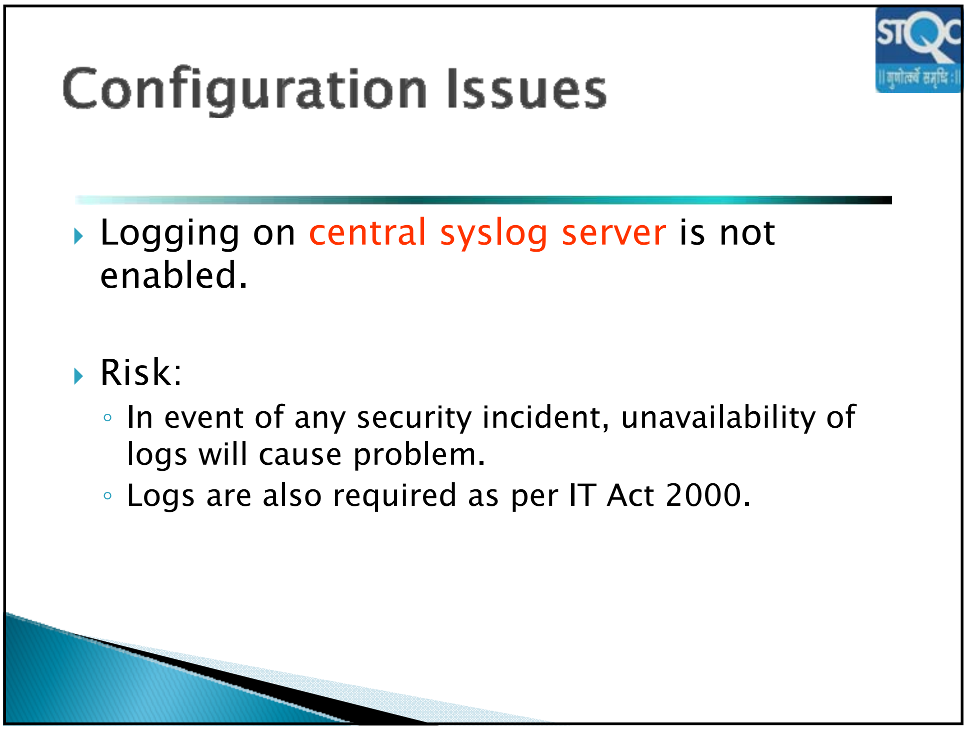
VA, Conf Audit of Routers, Switches, Firewall Issues



Configuration Issues

- Time synchronization: NTP is disabled.
- Clock timezone is not used.

- Risk:
  - In event of any security incident, improper timestamp on the logs (syslog) of the routers will make them unusable.



Configuration Issues

- Logging on central syslog server is not enabled.

- Risk:
  - In event of any security incident, unavailability of logs will cause problem.
  - Logs are also required as per IT Act 2000.

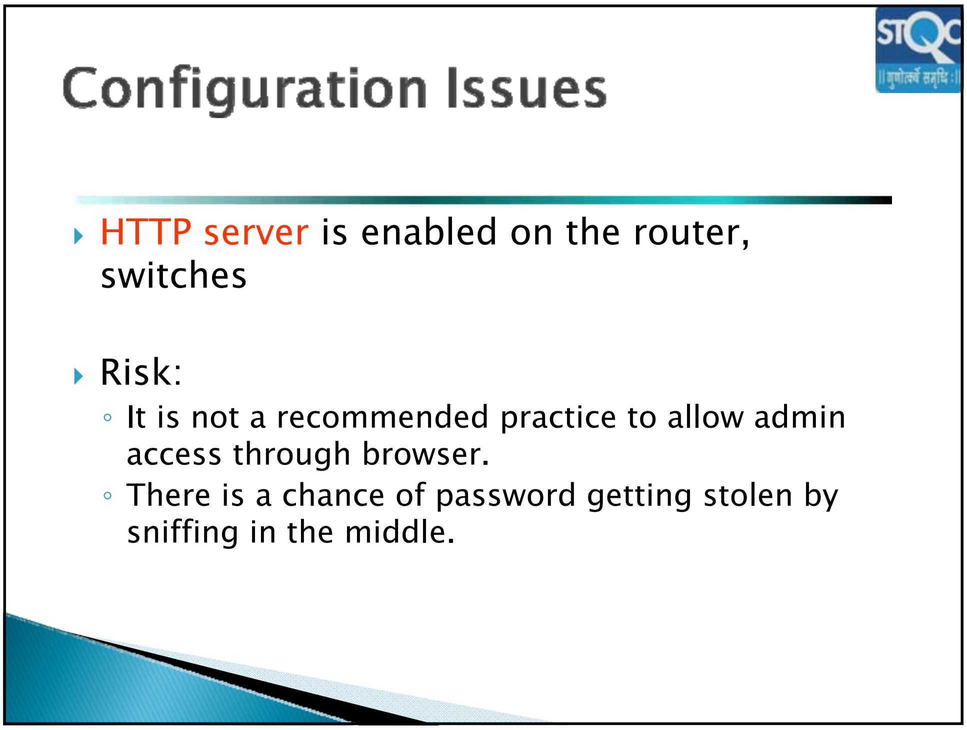
Configuration Issues

- Line console and line aux password is not set.

- Risk:
  - Person with a physical access to the router can login through a PC/Laptop without any console password.
  - If telephone modem is connected to the router/switch, any person can login by dialing the phone number remotely without any access control. It is possible due to absence any Aux Password.

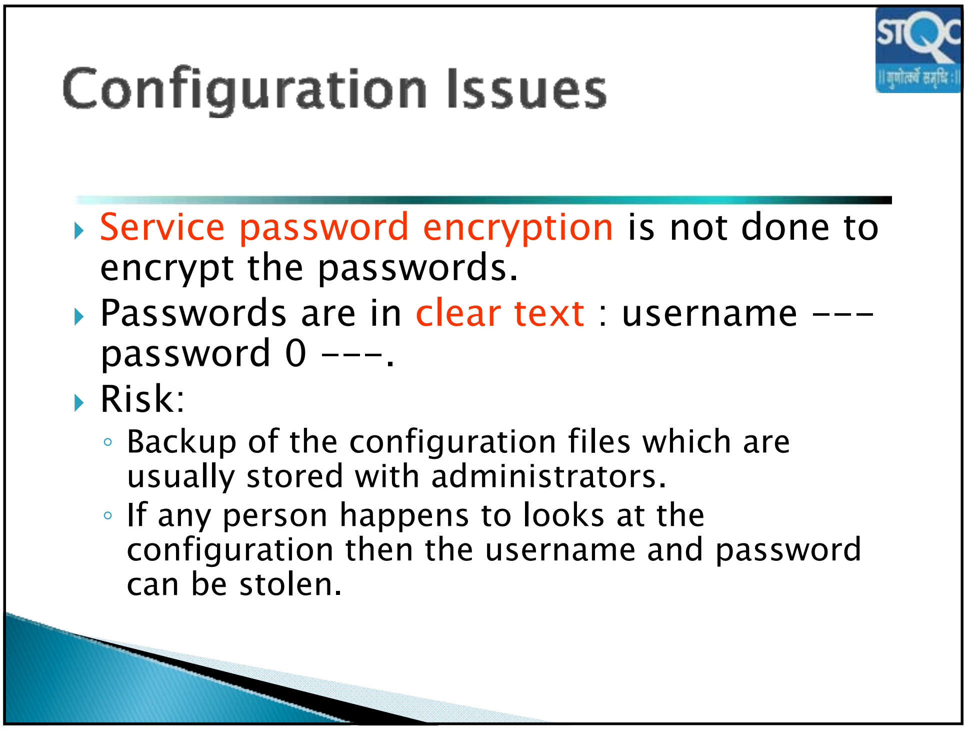
Configuration Issues

- Access list is not used to restrict use of telnet.
- Telnet is being used for remote login instead of SSH (Secure Shell).
- Risk:
  - Telnet is used for login to router for admin purpose. Access to telnet is not restricted from a set of IPs used by router administrators.
  - Telnet should not be used for remote access administration, instead ssh should be used for remote access for administration as ssh encrypts the password.



Configuration Issues

- HTTP server is enabled on the router, switches
- Risk:
  - It is not a recommended practice to allow admin access through browser.
  - There is a chance of password getting stolen by sniffing in the middle.



Configuration Issues

- Service password encryption is not done to encrypt the passwords.
- Passwords are in clear text : username --- password 0 ---.
- Risk:
  - Backup of the configuration files which are usually stored with administrators.
  - If any person happens to looks at the configuration then the username and password can be stolen.

Configuration Issues

- CDP is not disabled.
- Risk:
  - CDP (Cisco discovery protocol) is enabled in CISCO routers/switch by default. Administrator of neighbor network eg., ISP admin, may get undesirable information about your router.

Configuration Issues

- Simple Network Management Protocol (SNMP) version 1 is being used.
- Risk:
  - In SNMP version 1, community name (equivalent of password in SNMP) is sent in clear text which can be captured by a hacker.
  - Once SNMP community is with the hacker, then he can get detailed information from router and also modify settings in the router/switch if write access is allowed.

Configuration Issues

- SNMP RW (Read/Write) is being used.
- Risk:
  - If the hacker is able to get the SNMP community name then he can shutdown or change the settings in the router, it can lead to denial of service attack.

Routers/switch – Configuration Issues

- No access list is applied on SNMP polling.
- Risk:
  - Detailed information can be extracted as well as setting can be modified on the router from any PC/Laptop.

Routers/switch – Configuration Issues

- Source routing is not disabled.
  - By Source routing it is possible for a attacker to send packet from one network to other network (internet) through the pre-defined path as desired by attacker, instead of path defined by the routing policy implemented by the administrator.

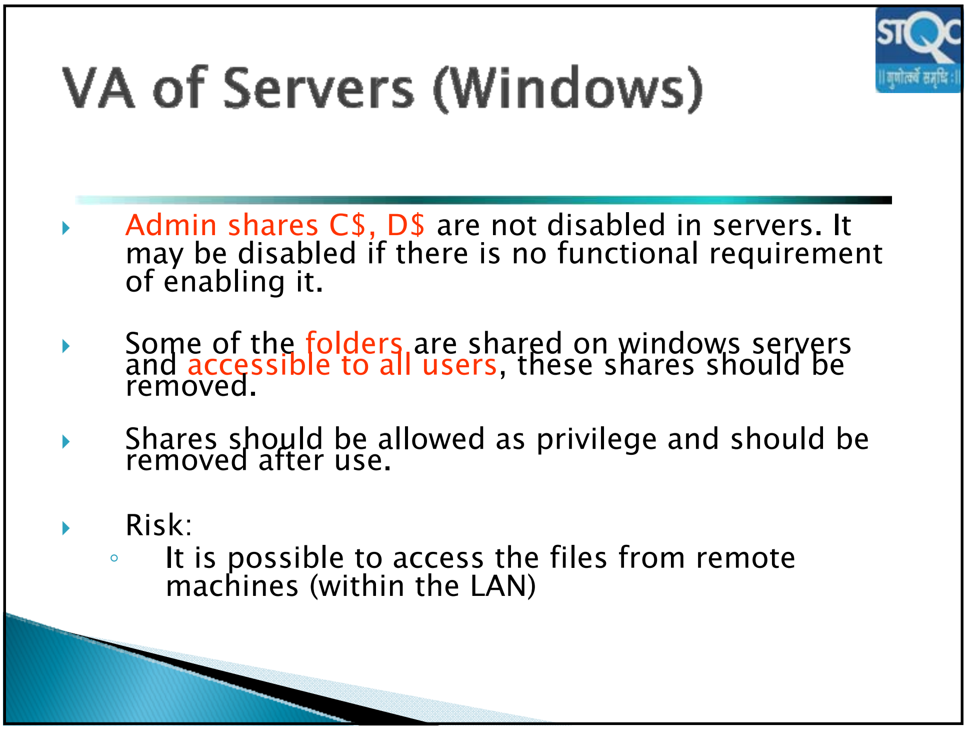
VA of Servers

VA of Servers (Windows)

- Password policy is not implemented on windows servers, including minimum length, max age, lockout threshold and duration.
- Risk:
  - Hacker can run a brute force attack to guess the password. In absence of limit on length of password it is possible to crack the password in short time period.

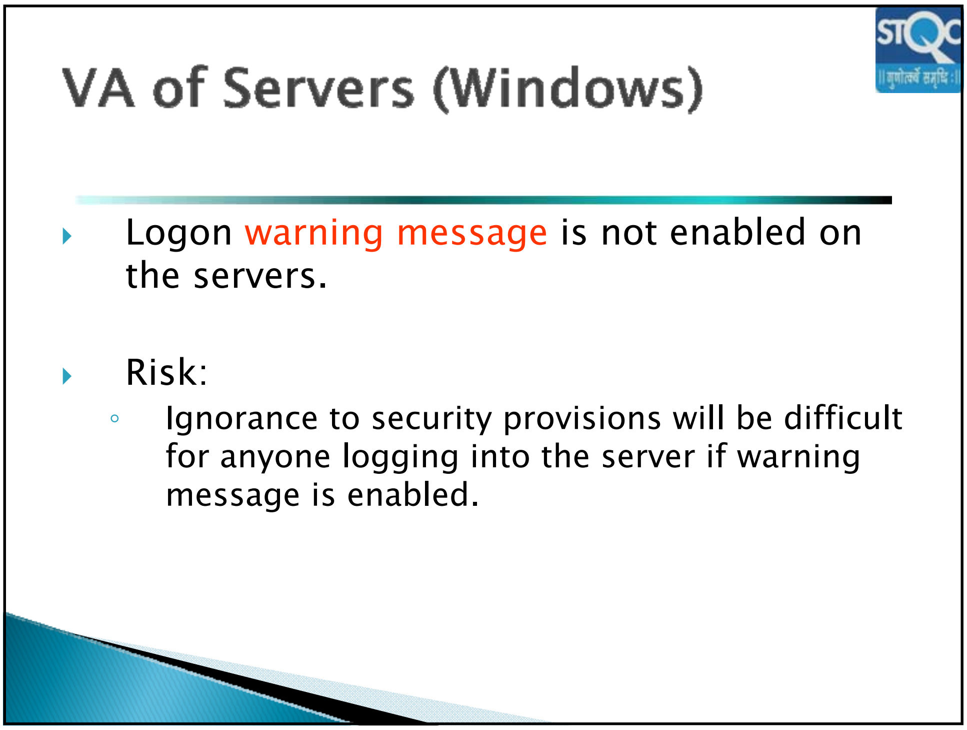
VA of Servers (Windows)

- Security events like startup, shutdown, logins failures are not being logged.
- Risk:
  - Anybody can change security settings without any chance of getting caught.



VA of Servers (Windows)

- Admin shares C$, D$ are not disabled in servers. It may be disabled if there is no functional requirement of enabling it.
- Some of the folders are shared on windows servers and accessible to all users, these shares should be removed.
- Shares should be allowed as privilege and should be removed after use.
- Risk:
  - It is possible to access the files from remote machines (within the LAN)



VA of Servers (Windows)

- Logon warning message is not enabled on the servers.
- Risk:
  - Ignorance to security provisions will be difficult for anyone logging into the server if warning message is enabled.

Windows – Checkpoints

Service Packs and Hotfixes

- Major service pack and Hotfix Requirements
- Minor service pack and Hotfix Requirements
  - As detected by **HFNetChk** or **mbsacli** /**hf** or mbsa (Microsoft baseline analyzer) GUI through comparison with the current version of **mssecure.xml**

Account Policy

Password History	: 24 passwords
Maximum Password Age	: 20 days to 60 days
Minimum Password Age	: 1 day
Minimum password length	: 8 char to 20 char

Password Policy

Minimum Password Length

- Blank passwords and shorter-length passwords are easily guessed by password cracking tools. To lessen the chances of a password being cracked, passwords should be longer in length.

Attacks on password are based on

- blank,
- username,
- dictionary words,
- hybrid dictionary words like Goog13 can be cracked with setting common replacement.

and

- Lastly the brute force attack trying all combinations.

Account lockout Policy an example

Account Lockout Duration: **15 Minutes** (minimum)

Sets the number of minutes an account will be locked out

Account Lockout Threshold: **3 Bad Login Attempts** (maximum)

Prevents brute-force password cracking/guessing attacks on the system. This option specifies the number of invalid logon attempts that can be made before an account is locked out

Reset Account Lockout After: **15 Minutes** (minimum)

The period of time the account will remain locked. If an account is locked out, it refuses to authenticate that account, until the locked out account is reset – either automatically, or by an administrator.

Logging Policy for the Account

Application Log

- Maximum Event Log Size: **80 Mb** (minimum)
- Restrict Guest Access to Logs: **Enabled**
- Log Retention Method: **“Overwrite Events As Needed”**
- Log Retention: **Not Defined**

Security Log

- Maximum Event Log Size: **80 Mb** (minimum)
- Restrict Guest Access to Logs: **Enabled**
- Log Retention Method: **“Overwrite Events As Needed”**
- Log Retention: **Not Defined**

System Log

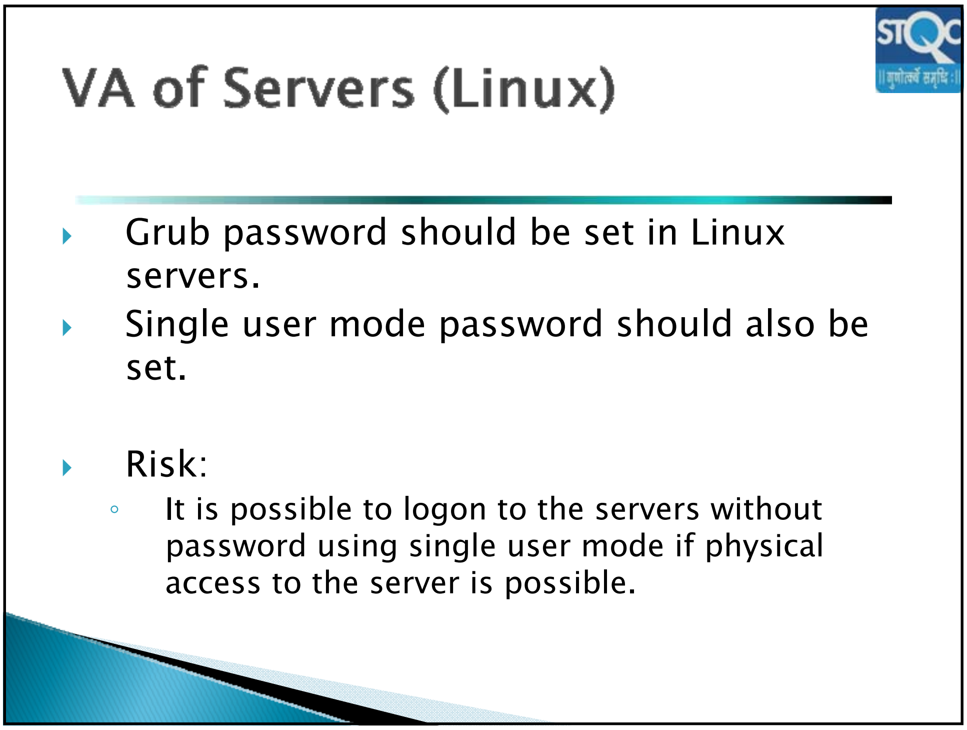
- Maximum Event Log Size: **80 Mb** (minimum)
- Restrict Guest Access to Logs: **Enabled**
- Log Retention Method: **“Overwrite Events As Needed”**
- Log Retention: **Not Defined**

Account Policy

Audit Logon Events: **Success and Failure**

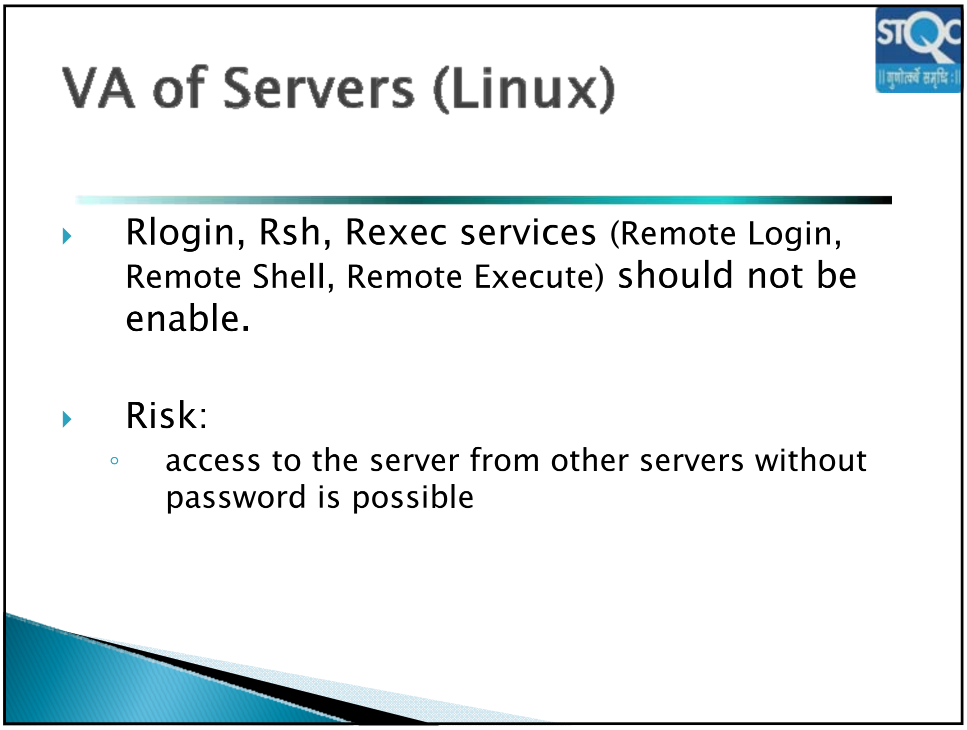
Auditing logon events will track successful and failed logon attempts from the local console, the network, or batch or service accounts using local machine logon credentials. If a user attempts to log on and fails, the only way to know will be to have this auditing enabled, and to periodically check the local machine’s Security Event Log.

VA –Linux



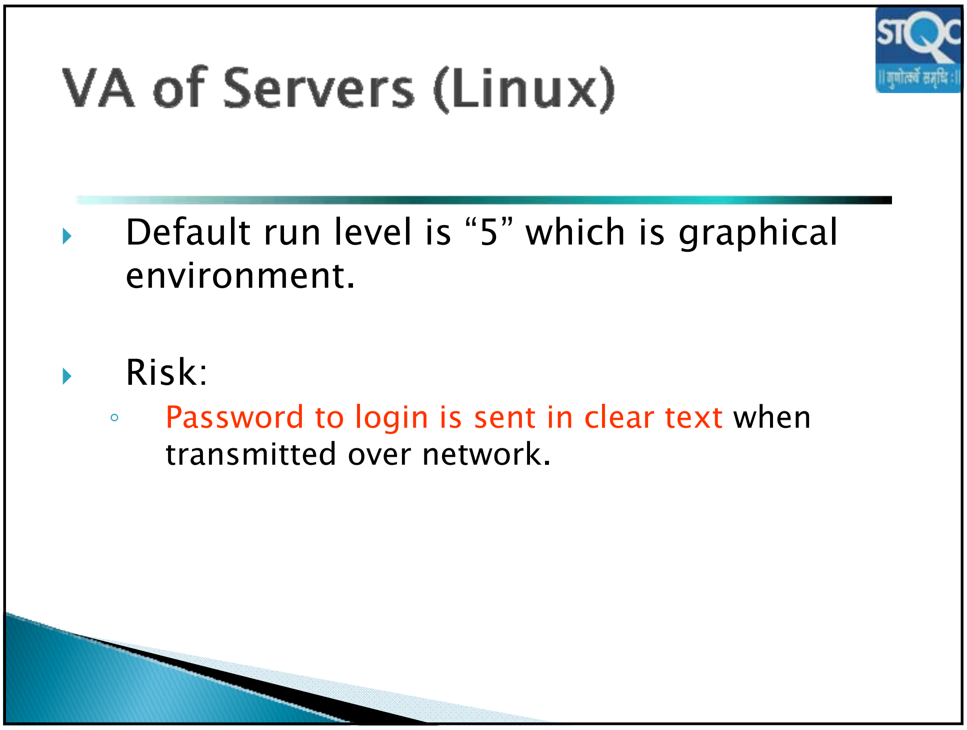
VA of Servers (Linux)

- Grub password should be set in Linux servers.
- Single user mode password should also be set.
- Risk:
  - It is possible to logon to the servers without password using single user mode if physical access to the server is possible.



VA of Servers (Linux)

- Rlogin, Rsh, Rexec services (Remote Login, Remote Shell, Remote Execute) should not be enable.
- Risk:
  - access to the server from other servers without password is possible



VA of Servers (Linux)

- Default run level is “5” which is graphical environment.
- Risk:
  - Password to login is sent in clear text when transmitted over network.

VA of Servers (Linux)

- Webmin is used to manage the servers.
- Risk:
  - Password of Webmin is send in clear text which can be sniffed.
  - Also the vulnerabilities of the application should also be managed.

VA of Servers (Linux)

- Remote login to root account should not be permitted via telnet/ssh.
- *Only individual administrators should login from their account and should access “root” account via “SU”.*
- Risk:
  - For more than one administrators in a organization. If they login to the server via root account, it is not possible to differentiated between the action of individual admin in case of any incident.

VA of Servers (Linux)

- Password policy “max password age”, “min password age” and “min password length” is not enforced by the systems.
- Risk:
  - It is possible to successfully crack brute force attack to crack.

VA of Servers (Linux)

- A number of files are present in the system with SUID=0 and SGID=0. These files when executed runs with roots right. These files should be reviewed and permissions be removed if not required by application.
- Risk:
  - Among numerous files it is possible to hide a malicious file which when executed runs with roots right.
  - If the malicious file is run without roots access then the damage to system will be minimum.

VA of Servers (Linux)

- Warning banner before login (etc/issue) & after login (motd) is not customized.
- Risk:
  - Attacker may claim to be unaware about ownership of the server.

Question ?