Kerberoasting

Roasting the Three-Headed Guard of Windows Active Directory

whoami (@shahrukhiqbal24)

- Petroleum Engineer turned into an InfoSec Enthusiast
- Wannabe Ethical Hacker, Penetration Tester and Red Teamer
- Seasonal Bug Bounty Hunter
- Cyber Security Analyst @ Datacell Solutions Private Limited
- Advocate for “Hacking Is NOT A Crime”
- FIFA & Football (Soccer) aficionado – Manchester United Fan

Agenda

- How it all started
- Kerberoasting overview
- Explaining the Kerberos Authentication Protocol
- Explaining where the vulnerability lies
- Practical Demonstration

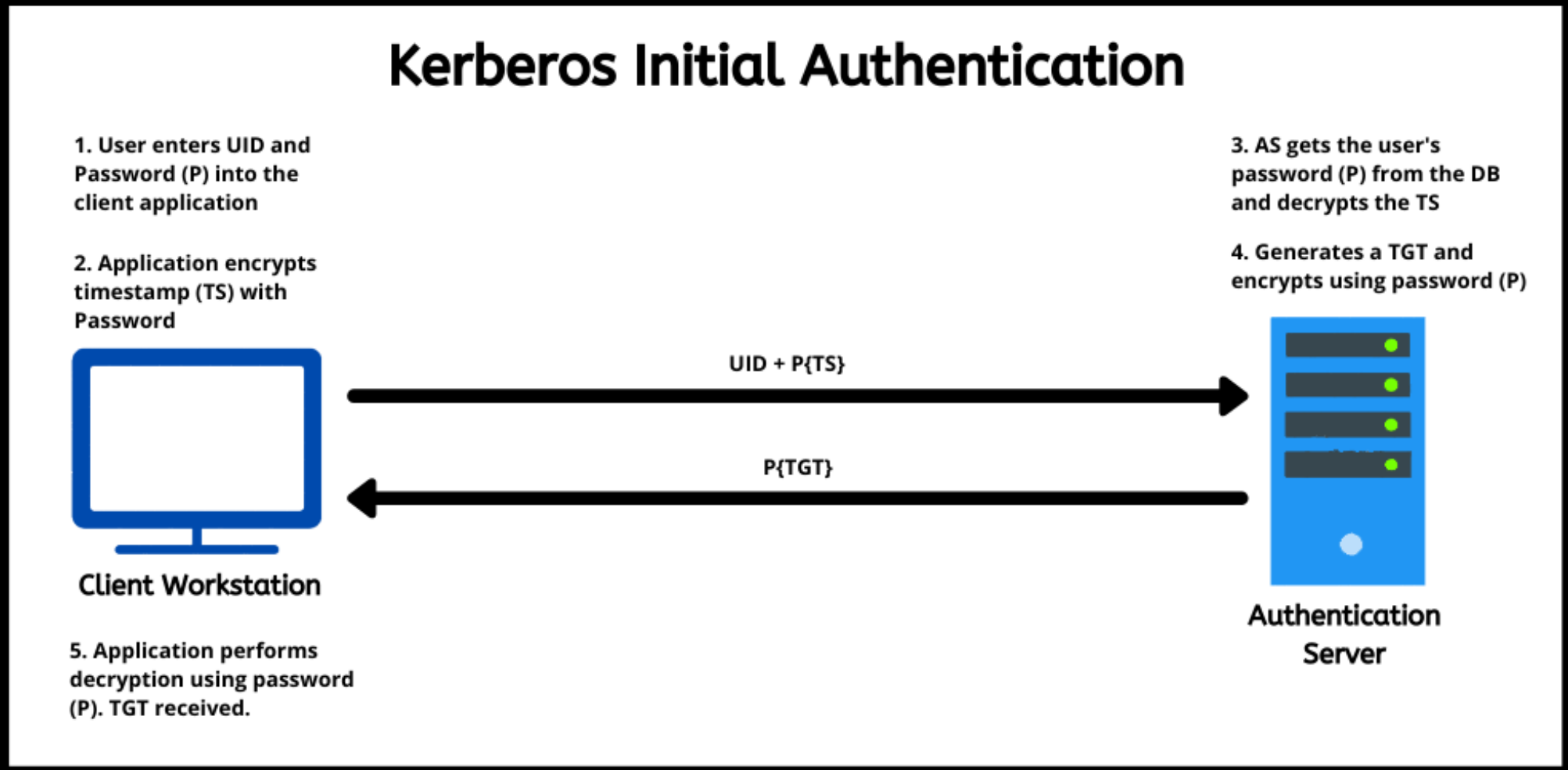
How it all began?

- DerbyCon 4.0 (2014)
- Discovered by Tim Medin (SANS 560 Lead Author / Principal Consultant @ Red Siege Information Security)

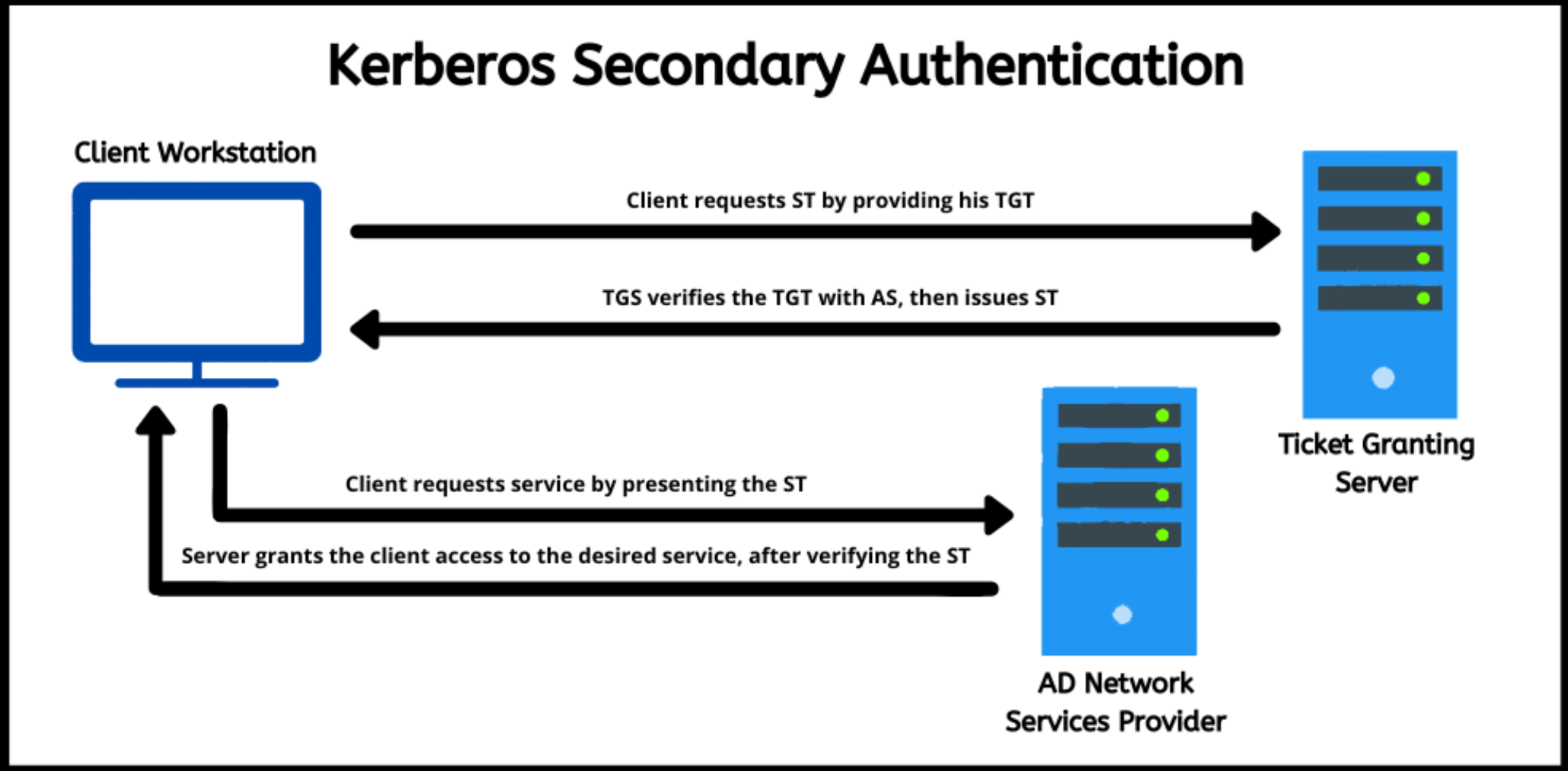
Kerberoasting Overview

- Credential Dumping/Privilege Escalation Technique
- Enterprise ATT&CK (T1558.003)
- How it works?
  - Identify User/Service Accounts with SPNs
  - Request Service Tickets using SPNs
  - Use credential dumping techniques to get the Service Tickets
  - Crack the Service Tickets offline

Kerberos Authentication Protocol

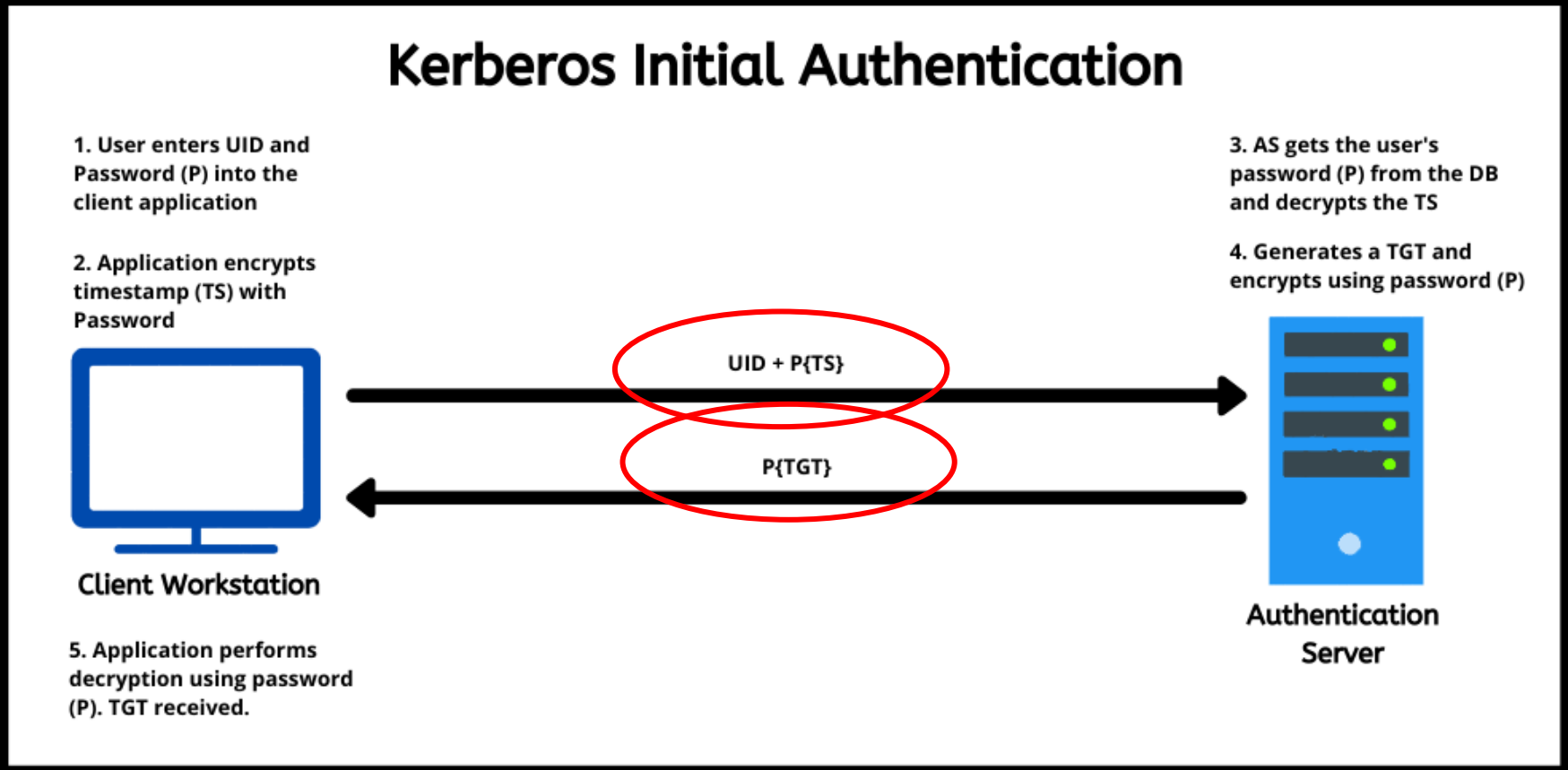


Kerberos Authentication Protocol



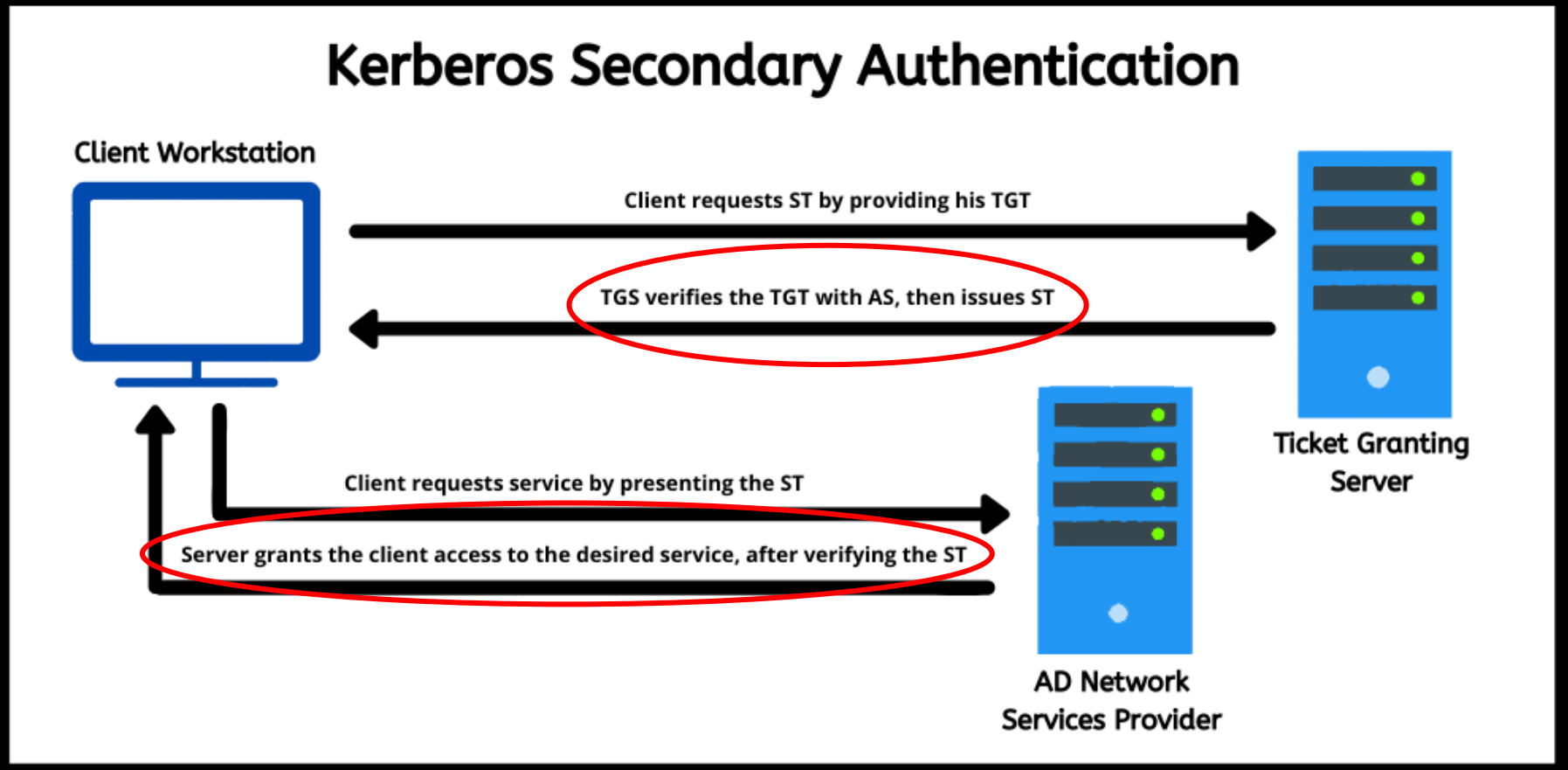
Where the Vulnerability Lies?

- Kerberos uses shared secrets for authentication



Where the Vulnerability Lies?

- Kerberos uses shared secrets for authentication



Where the Vulnerability Lies?

- Kerberos uses shared secrets for authentication
- Users’ passwords are used to encrypt everything
- Does not verify whether the user requesting service tickets has permissions to use that service or not
- Any user can request service tickets for any service

Demo (Assumed Breach Approach)

Detection & Mitigation

- Detection:
  - Enable Audit Kerberos Service Ticket Operations (Event ID 4769)
  - Honey SPNs
- Mitigation:
  - Ensure strong and complex password policies
  - Limit service accounts from administrative privs

Credits / References

- Tim Medin – for discovering the attack
- Benjamin Delpy – for Mimikatz
- SecureAuthCorp – for the Impacket Toolkit
- Active Directory Security
- Mitre ATT&CK
- Red Team Experiments

Thank You!

Socials:

Twitter: @shahrukhiqbal24 / @dcellsolutions

LinkedIn: Shahrukh Iqbal Mirza / Datacell Solutions Private Limited

Website/Blog: www.datacellsolutions.com