Cisco CCNA (200-301)

Identify Elements of Password Policy

Learning Objectives: Define elements of a password policy.

Description: In business, security begins and ends with policy. You will learn about one example of a pervasive policy dealing with end-users and how they access resources across the network.

Q: What do you mean by password management on Cisco Devices?

- Management
    - How are passwords managed on Cisco Devices?
        - enable password
        - Username/password database
        - Line console password
        - line vty password
    - Locally stored on router in startup-config
    - Can use Remote Authentication
        - RADIUS/TACACS+
    - password-recovery 0x2142

Q: Can you remind about password complexity?

- Complexity
    - Passwords should not be easy
    - Should involve level of complexity
        - No names, dates, sequence of numbers
        - Should include alphabetic, numbers, special characters
        - Min of 8 characters
        - e.g. NOT: Password1. but P4t@2B9$7VJb%xYt

Q: Is it possible to have some password complexity on Cisco devices?

- ```
  NYEDGE1#
  NYEDGE1#show passwords configuration
  NYEDGE1#configure terminal
  NYEDGE1(config)#security password min length 8
  NYEDGE1#show passwords configuration
  ```

Q: What alternatives do we have than just relying on passwords?

- Password Alternatives
    - multifactor authentication (2 of 3)
        - Something you know (PIN, Pattern or Password)
        - Something you have (e.g. Yubikey)
        - Something you are
            - biometrics (Fingerprint, FaceID, Iris ID)
    - certificates (digital)
        - `crypto key generate rsa`

Endnotes, External and Etc.

- 5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
  ```