Backup and Password Recovery

Take Backup of OS And Config File

Networkerde kullanılan cihazların işletim sistemlerinde sorunlar oluşabilir. Bu işletim sistemine gelen bir güncellemede bulunan bir bug kaynaklı olabilirken, bir netwok yöneticisi tarafından gerçekleştirilen yanlış yapılandırmalardan da kaynaklanabilmektedir (flash ünitesinde bulunan işletim sistemi dosyalarını silebilir veya NVRAM üzerinde kaydedilen konfigürasyon dosyası silebilir vs.). Bu gibi durumlar için işletim sisteminin ve kullanılan konfigürasyon dosyasının yedekleri alınıyor. Yedekleme sürecinde **uzak bir TFTP sunucusuna işleltim sistemi ve konfigürasyon dosyalarının nasıl yedeklendiği "CCNA 3.09 – Network Management" notlarında detaylıca açıklanmıştır**. İşletim sistemi ve konfigürasyon dosyası gibi kritik öneme sahip dosyaların yedeklerini almak kadar bu yedeklerin güncelliğini korumak da önemlidir. Bir problem yaşandığında en az düzenleme gerektiren en güncel konfigürasyona geçilmek istenir. Bu nedenle yedekler de belirli aralıklarla güncellenmelidir.

Pasword Recovery

Cihazlara giriş için tanımlanan parola bilgilerinin unutulması veya yanlış yapılandırılması sonucunda parola kurtarma işlemi gerçekleştirilebiliyor (**Password Recovery konusu "CCNA 2.4 – Password Recovery" notunda detaylıca açıklanmıştır)**. Bu işlem için fiziksel olarak cihazı yanında olunması ve Console portundan bağlanılması gerekiyordu. Console portundan bağlandıktan sonra cihaz yeniden başlatılarak Rom Monitor moduna giriliyordu (Boot sürecine ilişkin konfigürasyonlar burada yapılıyordu). Bu süreçte cihaza erişen ve parola sıfırlayan kişin bir saldırgan olduğu düşünülürse saldırgan cihazdaki parola bilgilerini sıfırlayarak cihaz kontrolünü ele geçirebilmektedir. Her ne kadar gerçekleşme ihtimali düşük olan bir ihtimal olsa da bu duruma önlem olarak "**no service password-recovery**" komutuyla cihazın Rom Monitor moduna girişler engellenebiliyor. Bu sayede parola kurtarma işlemiyle parola bilgilerinin sıfırlanması önlenebiliyor.