**SENARYO 1**

**NMAP kullanılarak port taraması gerçekleştirilir. Firewall yüzünden gösterilmeyen açık portlar nmap parametreleri kullanarak bypass edilir. NMAP taraması sonucunda sistemde ftp, http ve ssh portlarının açık olduğu gözlenir. NMAP’ in -O parametresi kullanılarak işletim sistemi ve sürümü tespit edilir. Daha sonra ftp üzerinden anonymous login zafiyeti kullanılarak paylaşıma açık olarak unutulan dosyalar(sshconfig vs ) get komutuyla çekilir ve üzerinde değişiklik yapılarak istenilen hale getirilir. Bu dosyalar sayesinde sisteme ssh ile yetkisiz erişim sağlanır. Sisteme erişim sağlandıktan sonra veri tabanı backup dosyası tespit edilir. Backup dosyası okunarak kullanıcı adı, parola, TC Kimlik No, Telefon No gibi hassas veriler görüntülenir. Parolalar veri tabanına herhangi hash algoritmasına sokulmadan kaydedildiği için açık bir şekilde görüntülenir.**

**SENARYO 2**

**Yurt sisteminde https protokolü yerine güvensiz olan http protokolü kullanıldığından dolayı ağ dinlendiğinde veriler şifresiz olarak görüntülenecektir. Bu sebeple ağ içerisinde Man in The Middle atak yapılarak yurt sistemine ait kullanıcı adı ve parolalar elde edilir. Elde edilen kullanıcı adı ve parolalar sistem üzerinde kullanılarak admin paneline erişim sağlanır. Panel incelendikten sonra server üzerine dosya eklemek için bir alan keşfedilir. Dosya ekleme alanında yeterli güvenlik önlemlerinin alınmamasından dolayı buraya bir reverse shell dosyası eklenir. Server’a eklediğimiz dosyada belirttiğimiz ip adresi ve portu dinlemeye başladıktan sonra eklediğimiz dosyayı browser üzerinden çalıştırarak sistemde bir arka kapı açılır ve sisteme erişim sağlanır. Sistem üzerinde araştırma yapılarak backup dosyası ve server a bağlı bir ip kamera tespit edilir. Backup dosyası okunarak içeriği görüntülendi. Tc Kimlik No gibi hassas veriler elde edildi ancak parolalar bir hash algoritmasından geçirilerek veri tabanına keydedildiği için parolalar elde edilemez. Daha sonra ip kameraya erişilerek görüntü alınır. İstenirse kamera kapatılabilir.**

**SENARYO 3**

**Web sitesi üzerinde brute force ile admin paneline erişilerek file upload üzerinden Shell ile sisteme erişim sağlanması.**

**SENARYO 4**

**Server üzerinde port taraması gerçekleştirilerek bu portlar üzerinde bulunan açıklar exploit edilerek sistemin ele geçirilmesi**

**(işletim sistemi zafiyeti Windows Server 2008)**

**SENARYO 5**

**Kartlar üzerinden sisteme sql injection atak denemesi yapılması.(Bu konuda araştırma yapılacak.)**