

## Ek-1 Kullanılan Araçlar

- Nmap
  - Nmap ilgili IP adreslerine yönelik açık portların, servislerin, versiyon tespitlerinin veya işletim sistemi bilgisilerinin keşfedilmesine yaramıştır.
- gobuster
  - gobuster URL adreslerine yönelik deneme yanılma yöntemine dayalı dizinleri dosyaları alt alan adlarını keşfetmemize yarayan araçtır.
- ffuf
  - ffuf'da aynı şekilde dizinleri, dosyaları alt alan adlarını keşfetmemize hızlı bir sonuç alabilmemize yarayan araçtır.
- Burp Suite
  - Burp Suite bir proxy işlevi görerek incelemek istediğimiz web sayfasına gönderdiğimiz istekleri düzenlememize olanak tanıyan bu sayede farklı güvenlik testleri gerçekleştirmemizi mümkün kılan araçtır. Test sürecinde sunuya farklı istekler gönderip sunucunun ne gibi davranışlar sergilediğini görmüş olduk.
- dirsearch
  - dirsearch gizli dosyaları, klasörleri bulmamıza yarayan araçtır.
- arjun
  - arjun URL'lerdeki uç noktaları, parametreleri keşfetmemize yarayan araçtır.
- Netcat
  - Netcat ağ bağlantıları üzerinden veri okuma yazma gibi işlemleri gerçekleştirmemize yarayan araçtır. Test sürecinde karşı web sunucusundan kendi saldırı makinemize bir bağlantı almamıza yararlı.
- John the Ripper
  - John the Ripper parola saldırıları yapabilmemize yarayan araçtır. Test sürecinde kullanıcı adı ve parola hash'ini yakaladığımız kullanıcıya yönelik john ile kaba kuvvet saldırısı gerçekleştirdik.
- wget
  - wget aracı test sürecinde kendi saldırı makinemizde bir sunucu başlattıktan sonra hedef sunucuda yerleşik olarak bu aracı kullanarak dosya aktarımına yarayan araçtır.
- Nessus
  - Nessus gelişmiş bir zafiyet tarama aracıdır. Yukarıki araçların yaptığı bir çok işlevi otomatize hale getirebilen bir araçtır. (Örn dizin keşifleri, işletim sistemi bilgisini edinmek gibi..)
- Zap Proxy
  - Zap Proxy istemci ile sunucu arasına girerek hem manuel hem otomatize testler yapmamıza yarayan bir araçtır. Test sürecinde web siteleri üzerinde taramalar gerçekleştirildi.
- Kerbrute
  - Kerbrute kaba kuvvet saldırısı uygulamak ve bilgi toplamaya yarayan bir araçtır. Test sürecinde kerboras'a yönelik kimlik bilgilerini tespit edebilmek amacıyla kaba kuvvet saldırısı gerçekleştirildi.
- Nuclei
  - Nuclei içerisinde bulundurduğu template'ler ile zafiyet taramaları gerçekleştiren bilgi toplamamıza yarayan bir araçtır.