ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/beyaz-sapkali-hacker-egitimi-yardimci-ders-notlari/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Beyaz%20%C5%9Eapkal%C4%B1%20Hacker%20E%C4%9Fitimi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1. DNS Spoof islemi

-> DNS spoof için önce arp spoof yapılabilir. Böylece kurbanin trafigi üzerimizden geçirilmis olur (arpspoof tool'u kullanilir).

-> Sonra seçilen web siteleri adi karsiligina kendi istedigimiz web sitelerinin yazildigi bir dns dosyasi olusturulur ve dns spoof ile bu dosya iliskilendirilir.
(dnsspoof tool'u kullanilir)

-> Ardindan kurban ilgili web sitesine erismek istediginde sahte DNS dosyasindan yanlis web sitesini alacaktir ve kurban böylece yanlis siteye yönlendirilecektir.

[215. Sayfa]

2. SSLStrip'ten bahsediyor.

[230.Sayfa]

3. Mac Flooding saldirisi ile switch'i hub olmaya zorlamis oluyoruz.

[248.Sayfa]

4. Agdaki ArpSpoof yapan makineleri bulmanin en kolay yolu.

> arp -an | awk'{print $4}' | sort | uniq -c

1 00:13:64:22:39:3F

2 00:19:D2:38:6E:45

Birden fazla makine ayni mac adresine sahip ise içlerinden biri MAC'ini diğeri gibi yapmış demektir. 00:19:D2:38:6E:45 MAC adresi iki bilgisayarda da olduğuna göre bu bilgisayarlardan birisi potansiyel saldırgandır tespitinde bulunabiliriz.

[258.Sayfa]

5. Nmap ile tarama çesitleri ve bu tarama çesitlerinin çalisma

mantiklari anlatiliyor:

[275.Sayfadan itibaren]

6. Bayrak kavrami bir TCP baglantisi icin iletisimin her adimini belirler. Yani baglantinin baslamasi, veri aktarimi, aniden kesilmesi ve sonlandirilmasi tamamen bayraklar araciligi ile yapilir.

[297.Sayfa]

7. Nmap ile yapilan taramalar hping ile de yapilabilir. Hping ile o taramalarin nasil yapilabileceginden bahsediyor:

[303.Sayfa]

8. Isletim sistemi belirleme yazilimlari:

-> Nmap

-> P0f

-> Xprobe

[314.Sayfa]

9. OpenBSD isletim sistemi için kendisine karsi yapilan isletim sistemi belirleme taramalarini yaniltarak farkli bir isletim sistemi kullaniliyor seklinde kandirma özelligi olan scrub'dan bahsediyor.

[312.Sayfa]

10.Nessus gibi bir zaafiyet tarama yazilimi olan Nikto'yu

> perl nikto.pl -update

ile güncelleyebiliriz.

[356.Sayfa]

11.Metasploit'te exploit seçildikten sonra payload seçilirse ek olarak set edilecek OPTIONS'lar belirir. Onlari da set etmek gerekir.

[369.Sayfa]

12.Metasploit'in alternatifleri:

-> Core Impact

-> Canvas

(!) Bunlar ticari yazilimlardir.

13.Hedef sisteme exploit göndermek sistemin çökmesine neden olabilir. Dolayisiyla kesinlikle gerçek sistemler üzerinde bu denenmemelidir.