ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/penetrasyon-testlerinde-acik-kod-yazilimlarin-kullanimi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Pentest%20Sunumu.pdf

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

1)

Pentest Vulnerability Assessment'i kapsar.

(Sayfa 9)

2)

Türkiye’deki pentest projelerinin %99’u vuln. Asses. olarak degerlendirilmektedir.

(Sayfa 10)

3)

Meslek Olarak Pentester

- > Bitmek bilmeyen bir okuma ve deneme serüveni

  Sistem/ağ admini = %20 arastirma %80 operasyon

  Pentester = %80 arastirma %20 operasyon

-> En az bir konuda uzmanlik (Networking, DB, development, system adm. …) gerektirir.

-> Perl, Python, Ruby gibi programlama dillerinden birine hakimiyet.

(Sayfa12)

4)

Açik port güvenlik açigi demek degildir!

Açik port güvenlik açigi barindirabilecek muhtemel ag servisidir!

(Sayfa 32)

5)

Nmap sistemlerin ayakta olup olmadigini nasil anlar?

Kapali sistemlere yapilacak port tarama islemi zaman kaybidir.

6)

Klasik ping programi ICMP üzerinden hedef sistemin ayakta olup olmadigini anlamaya yarar. Günümüz sistemlerinde icmp kapalidir!

7)

Nmap kullanarak hedef sisteme TCP üzerinden ping paketleri gönderip sistemin açik olup olmadigini anlayabiliriz.

> nmap –PS 80 www.microsoft.com

> nmap -PA 80 www.google.com

8)

TCP protokolü kullanarak port tarama islemi TCP bayraklari kullanilarak gerçeklestirilir

–SYN Scan(-sS)

–TCP Connect Scan (-sT)

–FIN, ACK, Null SCAN (-sF, -sA, -sN)

TCP RFC'sine göre dönen cevaplardan portun açik, kapali veya filtrelenmis oldugunu belirler. -p parametresi kullanilarak hangi portlarin taranacagi belirlenir.

9)

Adim adim bir sistemi ele geçirme

-Web açikligi bulunur.

-Açiklik kullanilarak reverse_shell yerlestirilir.

-Reverse_shell+nc kullanilarak sistemde komut satirina ulasilir.

- Kernel yamalari eksikse(%80) uygun exploit bulunarak sistemde root haklari elde edilir. (Privilage Escelation)

Benim NOT: Hedef sistemdeki Reverse shell payload'u bizim sisteme bağlantı sunar. nc ile de kendi makinamızdaki ilgili portu tıpkı metasploit'in multi/handler'ı gibi dinleyerek hedef sistemden gelen bağlantıyı yakalarız ve bir bakmışız komut satırımız nc iken hedef sistemin komut satırı haline gelivermiş olur. Komut satırından hedef sisteme attığımız hak yükseltme payload dosyasını ise ./priv_esc şeklinde çalıştırarak komut satırımız deneme@hedef_sistem iken root@hedef_sistem oluverir ve böylelikle root izni elde etmiş oluruz.

Detaylı bilgi için *Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elde Geçirdiğim Notlar/Netcat ile Sistem Ele Geçirme.docx* dosyasına bakılabilir.

(Page 65)

10)

Güvenlik üç bilesenden olusur: C.I.A.

-Confidentility (Gizlilik saglanmasi)

-Integrity (Gelen giden veride manipulasyonun yasanmamasi)

-Availability (Iletisimde Online kalma)

(Sayfa 74)

11)

DDoS saldirilari güvenligi tehdit eden en önemli unsurlardandir.

(Sayfa 74)

12)

DDOS Test Yöntemleri

- Syn Flood
- UDP Flood
- DNS Flood
- TCP Flood(ACK, FIN flood)
- DNS Amplification
- HTTP GET, POST Flood
- SMTP Flood

Her bir baslik için detayli testler yapilmali ve raporlanmalidir.

13)

DDOS Test Araçlari

- Hping
- Netstress
- Isic
- Nmap
- Ab, Jmeter
- Nemesis

14)

Linux sistemler paket olustururken TTL degerini 64 yaparak gönderirken Windows sistemleri ise 128 degerini kullanir. Penetrasyon testlerinde hedef sisteme yönelik kesif çalismalarinda TTL degeri önemli rol oynamaktadir. TCP/IP bilgisi iyi bir güvenlikçi basit paketlerle hedef sistem önünde Firewall, IPS ve benzeri sistemler olup olmadigini TTL degerine bakarak anlayabilir.

Örnek Çalisma:

Microsoft.com'a ait ip adreslerinden birisi hedef olarak seçilir.

> ping www.microsoft.com

Gelen sonuçlardan ip adresi belirlendikten sonra ilgili IP adresine bir adet SYN bayrakli TCP paketi gönderilir.

> hping -p 80 -S IPADRESI -c 1

Peki sonucu nasil yorumluyacagiz?

(Sayfa 78)

15)

IPS ne ise yarar?

- Gelen saldiri içerikli paketleri engellemeye

16)

IPS var mi yok mu anlamanin en kolay yolu:

- Hedef sistemde IPS'î kizdiracak saldiri içerikli paketlerin gönderilmesi
- GET ../../../etc/passwd HTTP/1.0
- GET ../../../cmd.exe HTTP/1.0 gibi...

Dönen cevaplara göre arada IPS var mi yok mu anlasilabilir.

(Sayfa 79)

17)

Nmap Tarama Çesitleri resmine bak : Sayfa 30'da.