ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/guvenlik-testlerinde-bilgi-toplama/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/G%C3%BCvenlik%20Testlerinde%20Bilgi%20Toplama.pdf

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

1)

Bilgi toplama esnasında bu gerekli mi değil mi diye sorulmadan alınabilecek tüm bilgiler alınmalı ve bu bilgiler sonraki aşamalarda kullanılmak üzere sınıflandırılmalıdır.

(Page 2)

2)

Bilgi toplama; hedef sistemle doğrudan iletişime geçerek ve hedef sistemden bağımsız olmak üzere iki türdür. Bu türler aktif bilgi toplama ve pasif bilgi toplama olarak adlandırılmaktadır.

3)

DNS Sorgu Türleri

A	Host Address	32-bit IP address
CNAME	Canonical Name	Canonical Domain Name for an alias
HINFO	CPU & OS	Name of CPU and Operating System
MINFO	Mailbox Info	Information about a Mailbox or Mail List
MX	Mail Exchanger	16-bit Preference and Name of Host that acts as Exchanger for the Domain
NS	Name Server	Name of Authoritative Server for Domain
PTR	Pointer	Pointer from IP address to Domain Name
SOA	Start of Authority	Multiple fields that specify which parts of the naming hierarchy a server implements
TXT	Arbitrary Text	Uninterpreted string of ASCII text

DNS'te MX sorgusu ile bir "mail sunucusunun" domain-IP çözümlemesi yapılır. MX mail exchanger'ın kısaltılmışıdır.

```
$ nslookup
> set querytype=mx
> bankofengland.co.uk
```

Output:

```
Server: 213.228.193.145
Address: 213.228.193.145#53

Non-authoritative answer:
```

bankofengland.co.uk mail exchanger = 10 cluster2.eu.messagelabs.com.
bankofengland.co.uk mail exchanger = 20 cluster2a.eu.messagelabs.com.

4)

SMTP protokolü mail istemcisi yazılımlarının ve mail sunucusu yazılımlarının kullandığı protokole denir. Nasıl bir browser HTTP protokolünü kullanıyorsa bir Outlook da SMTP protokolünü kullanır. SMTP sunucusu ile kastedilen şey Mail Sunucusudur.

5)

Hedef sistemin saati HTTP protokolü ile ya da SMTP protokolü ile öğrenilebilmektedir.

a) telnet ile 80 portuna bağlantı kurup ardından HEAD /HTTP/1.0 tuşlanarak dönen sonuçtan zaman bilgisi edinilebilir.

```
$ telnet mail.lifeoverip.net 80

Trying 80.93.212.86...
Connected to mail.lifeoverip.net.
Escape character is '^]'.

HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Mon, 28 Jan 2008 17:49:06 GMT
Server: Apache/2.2.4 (FreeBSD) DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.7e-p1
Connection: close
Content-Type: text/html; charset=iso-8859-1
Connection closed by foreign host.
```

b) Hedef sistemin üzerinde bir SMTP sunucusu, yani mail sunucusu çalışıyorsa o sunucuda kayıtlı olmayan bir mail adresine mail gönderip dönen hata mesajının başlıkları incelenerek hedef sistemin saati öğrenilebilir.

6)

Hedef sistemin uptime süresi hping3 tool'u ile öğrenilebilmektedir. Uptime süresi ile kastedilen şey hedef sistemin ne kadar süredir açık kaldığı bilgisidir. Aşağıda bir sistemin uptime süresini öğrenme yöntemini görmektesiniz.

```
$ hping3  -S  --tcp-timestamp -p 80 -c 2  www.ubys.net
```

Output:

HPING 1.2.3.488 (eth0 1.2.3.488): S set, 40 headers + 0 data bytes

len=56 ip=1.2.3.488 ttl=56 DF id=28012 sport=80 flags=SA seq=0 win=65535 rtt=104.5 ms

TCP timestamp: tcpts=55281816
len=56 ip=1.2.3.488 ttl=56 DF id=28013 sport=80 flags=SA seq=1 win=65535 rtt=99.1 ms

TCP timestamp: tcpts=55281917 HZ seems hz=100

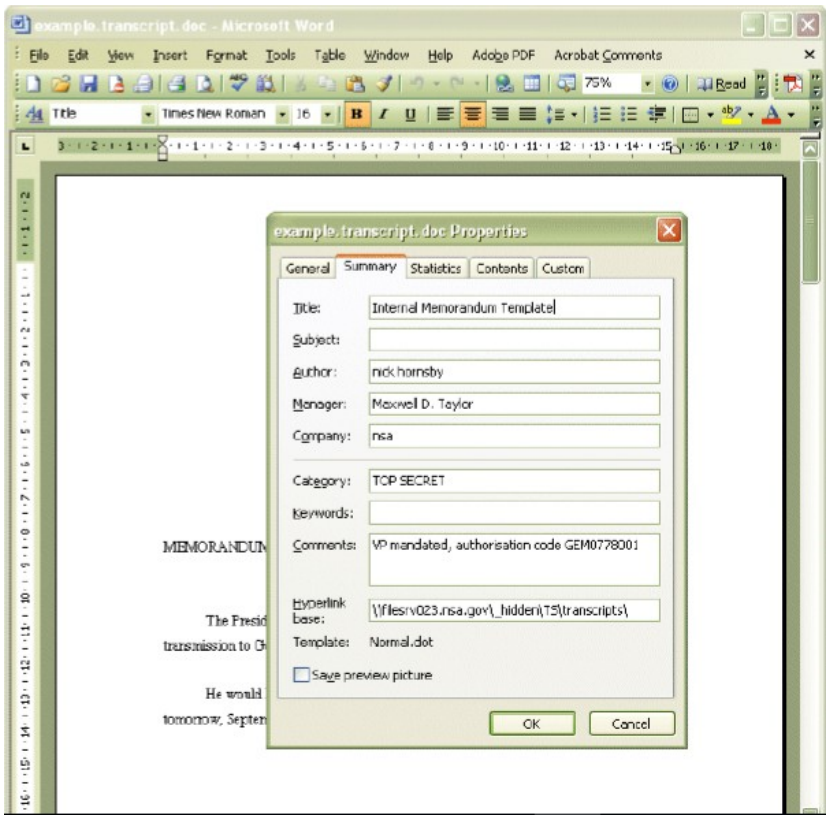
System uptime seems: 53 days, 7 hours, 31 minutes, 6 seconds

--- 1.2.3.488 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
Round-trip min/avg/max = 99.1/101.8/104.5ms

Görüldüğü üzere www.ubys.net sitesinin barındığı sunucu 53 gündür aralıksız açık bilgisini hping3 tool'u ile edinmiş olduk.

7)

Hedef sistemin internette paylaşıma açtığı word, pdf, ppt gibi dosyaların metadata diye adlandırılan döküman hakkındaki bilgilerine erişerek eğer boş bulunmuşlarsa sistem hakkında hassas bilgiler toplanılabilmektedir.



8)

DNS sunucusunun versiyonu dig tool'u ile saptanabilmektedir.

$ dig @10.180.8.115 version.bind chaos txt

Output:

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6 <<>> @10.180.8.115
version.bind chaos txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37376
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;version.bind. CH TXT

;; ANSWER SECTION:
version.bind. 0 CH TXT "9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6"
```

;; AUTHORITY SECTION:
version.bind. 0 CH NS version.bind.

;; Query time: 2 msec
;; SERVER: 10.180.8.115#53(10.180.8.115)
;; WHEN: Fri Oct 18 16:20:20 2013
;; MSG SIZE rcvd: 95