ÖN BİLGİ

Bu belge

- https://www.slideshare.net/slideshow/backtrack-linux101-eitimi/27613256

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Backtrack%20Linux%20E%C4%9Fitimi.pdf

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

1)

// Belgenin son üç satırını yazdırır.

tail -n 3 belge.txt

// Belgenin son üç satırını yazdırır. Fakat her iki saniyede bir bu olayı yeniler. Log
// takip işlemlerinde sık kullanılır.

tail -n 3 -f belge.txt

// String arama motoru grep “bilgi” kelimesini bga.txt içinde arar ve bulduğu
// satırları ekrana basar

grep "bilgi" bga.txt

grep Parametreleri

- -i : Büyük küçük harf duyarsız davran
- -r : Bu parametre ile regexp ifadeleri kullanılabilir.
- -c : Aranan metin parçasının geçtiği satırların gösterilmesine yerine metin parçasının bulunduğu satır sayısının gösterilmesini sağlar.
- -n : Bulunulan satırın dosyadaki satır numarasının gösterilmesini sağlar.

// Bir komutun çıktısı bir dosyaya yazılır

echo "BGA" > kayit.txt

// Makina adı öğrenilir.

hostname

// Makine adı BGA olarak değiştirilir. Değişikliği görmek için terminali kapatıp tekrar açmak gerekir.

echo "BGA" > /etc/hostname

// Linux kernel sürümü öğrenilir.

uname -a

Pipe (|)

Bir komutun output'unu başka komuta input olarak verebiliriz. Peşpeşe Pipe kullanılabilmektedir.

// BGA.txt dosyası cat komutu ile okunur ama çıktısı ekrana değil, grep komutuna
// aktarılır. Grep komutu ise “Bilgi” kelimesinin geçtiği satırları ekrana basar.

```
cat BGA.txt | grep "Bilgi"
```

// ps aux’un ürettiği process’ler çıktısından ilk 10 satırı gösterir.

```
ps aux | head -n 10
```

// ps aux’un ürettiği process’ler çıktısından son 10 satırı gösterir.

```
ps aux | tail -n 10
```

// -p parametresi kaynak dosyanın haklarınının aynısını kopyalanan dosyaya da
// uygular.

```
cp –p mehmet.txt Desktop/
```

// Belirtilen dizinde (/root/Desktop) 777 iznine sahip dosya ve klasörler aranır ve
// bulunanlar ekrana basılır.

```
find /root/Desktop -perm 777
```

// Belirtilen dizinde (/root/Desktop) tipi directory olanlar aranır ve bulunanlar ekrana
// basılır.

```
find /root/Desktop -type d
```

// Belirtilen komutun kullanımını anlatır.

```
man komutAdi
```

// man komutu ile aynı işleve sahiptir. Fakat daha detaylı bilgi verir (man’a göre
daha az tercih edilir).

```
Info komutAdi
```

// Anlık olarak çalışan process'leri görüntüler.

top

// Çalıştırılan bir process'in komut ekranını işgal etmemesi için arkaplana atılması
// işlemi komut çalıştırıldıktan sonra CTRL+Z ile askıya alınıp bg komutunun giril
// mesiyle gerçekleşir.

> nc -lvp 90 // 90'ncı portu dinler….

listening on [any] 90… // CTRL+Z ile askıya alınır.

[1]+ Stopped nc -lvp 90

> bg // Askıya alınan process arkaplanda başlatılır.

bash: bg: job 1 already in background

> jobs // Arkaplandaki process'leri gösterir.

[1]+ Running nc -lvp 90

> fg 1 // [1] nolu arkaplanda çalışan process ön
// plana, yani komut ekranına getirilir.
// Böylece komut ekranını işgal eder ve
// başka komut girilemez. Ta ki sonlana
// kadar…

// Süreçleri sonlandırmak için önce process id öğrenilmelidir. Sonra kill ile process sonlandırılır.

> ps aux | grep "tcpdump"

root 2518 0.0 0.7 …. tcpdump

> kill -9 2518 // 9 numarası process'i tamamen
// öldürmek için kullanılır.

2)

Backtrack Servisleri

Backtrack bir güvenlik dağıtımı olmasına rağmen üzerinde klasik Linux dağıtımlarında bulunabilecek bazı servisleri içermektedir. Bunların amacı çeşitli güvenlik testlerinde ek bileşen olarak kullanabilmektir. Mesela bir sisteme sızma denemesi gerçekleştirildi ve başarıldı. Sızılan sistemden tftp ile veri alınması

gerekiyor. Bu durumda Bakctrack üzerinde ftp servisi çalıştırılarak gerekli bilgiler sunucudan kolaylıkla transfer edilebilir.

• Apache httpd servisini başlatmak için;

> service apache2 start

ya da

> /etc/init.d/apache2 restart

• SSH Servisinin başlatılması için ilk olarak ssh anahtarları oluşturulur:

> sshd-generate

Servisi çalıştırmak için aşağıdaki komutlar kullanılır:

> service ssh start

ya da

> /etc/init.d/ssh start

(!) Bu işlemler grafik arabirimindeki menüler aracılığıyla da yapılabilir

Eğer ssh'i başlatırken aşağıdaki gibi bir hata alırsanız

Could not load host key: /etc/ssh/ssh_host_dsa_key

Could not load host key: /etc/ssh/ssh_host_rsa_key

aşağıdakileri girmeniz gerekir:

ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key

ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key

(Page 46-48)

3)

Kullanıcı Hesapları Dosyaları

•Linux işletim sisteminde kullanıcı bilgileri /etc/passwd dosyasında tutulmaktadır.

•Gruplar hakkındaki bilgiler /etc/group dosyası içerisinde bulunmaktadır.

•/etc/shadow dosyası, kullanıcı şifrelerinin hash'lerinin bulunduğu dosyadır.

•/etc/passwd’i tüm kullanıcılar görebilir.

•/etc/shadow dosyasını sadece root görebilir.

(Page 49)

4)

/etc/passwd Dosya Formatı

passwd'deki satırlardan biri:

bga:x:11807:100:Bilgi Güvenliği Akademisi:/user/bga:/bin/sh

Anlamı:

kullanıcı_ismi:şifre:user_id:group_id:gecos(kullanıcının kişisel bilgileri):kullanıcı_dizini:kabukdizini

(Page 50)

5)

/etc/group Dosya Formatı

group dosyasının satırlarından biri:

root:x:0:bga

Anlamı:

grup_ismi:grup_şifresi:grup_id:üye

(Page 51)

5)

/etc/shadow Dosya Formatı

Shadow’daki satırlarından biri:

root:6TBYsLimb$/25lp7/
UZzjI124JKgHVrg7yVQc.YWF2TPhe25WSaNjcqilbTO/
Cndg.CSIr7shka4TxHwzUP2DTvmssVptLJ/:15400:0:99999:7:::

Anlamı:

kullanıcı_ismi:şifre:sp_lastchg:sp_min:sp_max:sp_warn:sp_inact:sp_expire:sp_flag

• **sp_lastchg:** Kullanıcının şifresini değiştirdiği en son zaman bilgisini saklar. Bu bilgiyi 1 ocak 1970 tarihinden itibaren kaç gün olduğu bilgisi ile gösterir.

• **sp_min:** Kullanıcının şifresini değiştirebilmesi için geçmesi gereken minimum zamandır. Eğer -1 değeri varsa herhangi bir zaman değiştirilebilir.

• **sp_max:** Kullanıcı şifresini kullanabileceği azami gün sayısıdır. 999999 değeri varsa herhangi bir kısıtlama söz konusu değildir

• **sp_warn:** Şifrenin geçerliliğinin dolmadan kaç gün önce uyarı verileceğini bildirir. -1 değeri varsa herhangi bir uyarı verilmez.

• **sp_inact:** Şifre geçerliliği dolduktan sonra kaç gün içerisinde kullanıcı hesabının pasifleştirileceği bilgisidir. -1 değeri varsa pasifleştirilme yapılmaz

• **sp_expire:** Kullanıcı hesabının sona ereceği gün bilgisidir. 1 ocak 1970 tarihinden sonra kaç gün olduğunu gösterir

•**sp_flag:** Sonradan kullanım için düşünülen ve şuan aktif olmayan bir bölümdür

(Page 51-53)

6)

Linux sistemler tuzlu hash kullandıklarından dolayı klasik parola kırma araçları ile kırılamazlar. John The Ripper ve hashcat gibi araçlar kullanarak Linux sistemlerin parola güvenliği test edilebilir.

(Page 53)

7)

Sisteme Yeni Kullanıcı Ekleme

• Useradd veya adduser komutları kullanılabilir

> useradd deneme // useradd [kullanıcıIsmi]

Output:

Adding user ‘deneme’ ...

Adding new group ‘deneme’ [1000] ...

Adding new user ‘deneme’ (1080) with group ‘deneme’ ...

Creating home directory ‘/home/deneme’ ...

Copying files from ‘/etc/skel’ ...

Enter new UNIX password:

Retype new UNIX password:

Passwd: password updated successfully.

- -G parametresi ile eklenecek kullanıcının grubu da belirtilebilir

  > useradd -g friends ziyaretci // useradd -g [grupIsmi] [kullanıcıIsmi]

- Oluşturulan kullanıcının parolası passwd komutu ile güncellenir.

  > passwd ziyaretci

  Output:

  Enter new UNIX password:

  Retype new UNIX password:

  Passwd: password updated successfully.

(Page 54)

8)

Linux dağıtımlarında sistem hesaplarının parolaları /etc/shadow dosyasında hash+salt şeklinde saklanır. Salt her seferinde değişken olarak atanan bir değerdir. Bu şekilde aynı parola iki kere girildiğinde hash değerleri farklı çıkacaktır.

Parola formatı:

root:6GkfJ0/H/$IDtJEzDO1vh8VyDG5rnnLLMXwZl.cikulTg4wtXjq98Vlcf/PA2D1QsT7VHSsu46B/od4IJlqENMtc8dSpBEa1

Anlamı:

➔ root kullanıcı adını temsil eder.
➔ İlk $ ile ikinci $ arasındaki sayı hangi şifreleme (hash) algoritmasının kullanıldığını belirtir. Buradaki değer

- 1 ise MD5
- 2 ise BlowFish (OpenBSD)
- 5 ise SHA256
- 6 ise SHA512

algoritması kullanılmış demektir.

➔ İkinci $ ile üçüncü $ arasındaki karakterler parolanın rainbow table kullanılarak kırılmasını zorlaştırma amaçlıdır. Salt değeri olarak bilinir.

(Page 55-56)

9)

Dosyalar

• Linux işletim sisteminde her şey bir dosyadan oluşur.

➔ Çalıştırılabilir komutlar
➔ USB Disk
➔ Ses kartı
➔ Ethernet kartı sürücüsü
➔ Mp3 dosyası

• Dosya ismi nokta ile başlıyorsa gizli dosyadır (e.g. .htaccess).

• Dosya isimleri case sensitive'dir.

• Linux işletim sistemlerinde dosyalar hiyerarşik bir yapıyla oluşturulmuştur. Hiyerarşik yapının en üstündeki dosyaya root denir.

• Root dizini bütün dosyaları bünyesinde barındırır. '/' dizini ile '/root' dizini aynı değildir. '/root' dizini root kullanıcına ait bir dizindir.

• Linux dizinlerinin anlamları şöyledir:

➔ /bin : Kullanıcı ve sistem yöneticisine ait çalıştırılabilir dosyaları barındırır.
➔ /dev : Donanımlara erişebilmek için gerekli dosyaları barındırır.
➔ /etc : Sistem konfigürasyonları için gerekli dosyaları barındırır.
➔ /lib : Sistem kütüphanelerini barındırır.
➔ /sbin : Sistem yöneticisine ait çalıştırılabilir dosyaları barındırır. Böylece terminale çalıştırılabilir tool'un direk adını yazarak, yani yüklü olduğu dizine gitmeden çalıştırabiliriz.
➔ /home : Kullanıcılara ait dizindir.
➔ /mnt : Sisteme dışarıdan bağlanacak olan donanım aygıtlarının, bağlantı noktalarını belirten dizindir. Windows'un yüklü olduğu partition gibi…
➔ /root : Bir sistemde en yetkili kullanıcı olan "root" kullanıcısına ait dizindir.
➔ /tmp : Geçici dosyaların yer aldığı dizindir.
➔ /usr : Paylaşılan dosyaların barındığı dizindir. Burada çalışabilen dosyalar bulunmakla beraber, döküman ve programlara ait dosyalar da yer almaktadır.
➔ /var : Sistem ve programlara ait log mesajları, email, website projelerinin bulunduğu dizindir.

➔ /proc : Sistem hakkında gerekli bilgilerin bulunduğu sanal dizindir.

(Page 59)

10)

Sayısal Olarak Dosya İzinleri

Read,write,execute birer bitle temsil edilir. 1 ise true, 0 ise false'tur.

Read, Write, Execute

e.g. 1 0 1 => 101

0: 000 -> ---

1: 001 -> --x

2: 010 -> -w-

3: 011 -> -wx

4: 100 -> r--

5: 101 –> r-x

6: 110 -> rw-

7: 111 -> rwx

> chmod 777 dosyaIsmi

(Page 62)

11)

Dosya İzinlerini detaylı izleme komutu :

> ls –l

Output:

```
-rwxrwxr-x    1 rapsodi   rapsodi    5224 Dec 30 03:22 hello
-rw-rw-r--    1 rapsodi   rapsodi     221 Dec 30 03:59 hello.c
-rw-rw-r--    1 rapsodi   rapsodi    1514 Dec 30 03:59 hello.s
drwxrwxr-x    7 rapsodi   rapsodi    1024 Dec 31 14:52 posixuft
[Permissions]  [Owner]    [Group]
```

```
- rwxrwxrwx
|  |    |    |
|  |    |    |---------- other permissions
|  |    |--------------- group permissions
|  |-------------------- owner permissions
|----------------------- directory flag
```

Owner
Bu kısımda dosyanın sahibinin dosya üzerindeki hakları tanımlanır.

Group
Bu kısımda dosyanın dahil olduğu grubun dosya üzerindeki hakları tanımlanır.

Other
Sistemde bulunan tüm kullanıcıların dosya üzerindeki hakları tanımlanır.

(Page 62, 64)

12)

Paket, programın işletim sistemine uygun kurulacak hale getirilmiş versiyonuna denir. Mesela Red hat linux'u için hazırlanmış paketler Pardus için uygun değildir.

(Page 92)

13)

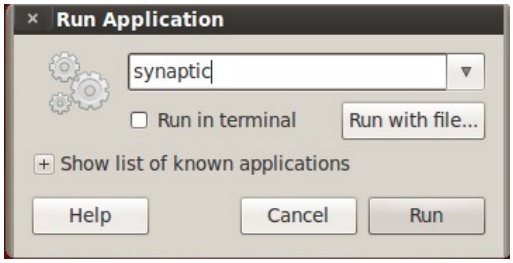
Linux/UNIX sistemlerde temelde iki çeşit paket kurulumu gerçekleştirilir:

- Kaynak kod derlenerek
- Paket yönetim sistemi kullanarak

(Page 93)

14)

ALT+F2 tuşu ile çalıştırmak istenilen herhangi bir programın sistemdeki adını yazıp Run butonuna basmamız yeterlidir.



(Page 95)

15)

#Paket yüklemek için

apt-get install PaketAdı

#Paket aramak için

apt-cache search PaketAdı

#Paket güncellemek için

apt-get update

apt-get upgrade

#Paket kaldırmak için

apt-get remove PaketAdı

(Page 98)

16)

Kaynak Koddan Program Kurulumu

• Kaynak kodun bulunduğu dizine geçilir ve sırasıyla aşağıdakiler terminale girilir:

./configure

make

make install

• Veyahut README, INSTALL gibi dosyalar okunur ve oradaki yönergeler uygulanarak kurulum yapılır.

(Page 98)

17)

#Ağ durumunun özetini verir. Daha doğrusu IP, ICMP, TCP ve UDP için alınan verilen #paketler gibi istatistikleri verir.

> netstat -s // -s : statistic

#Sistemdeki açık tcp bağlantılarını sıralar.

> netstat -t // -t : tcp

Output:

Proto	Recv-Q	Local Address	Foreign Address	State
tcp	0	192.168.2.2:36763	91.190.216.66:12350	ESTABLISHED
tcp	0	192.168.2.2:34019	157.56.52.27:40003	ESTABLISHED

.

.

.

[böyle sıralar]

#Açık tcp portlarını kullanan yazılımların isimlerini öğrenmek için -p parametresi #eklenir.

> netstat -t -p // ya da netstat -tp

Output:

e.g.

tcp 0 0 192.168.2.2:36763 91.190.216.66:12350 ESTABLISHED 2777/skype

#Trafik İzleme

#En temel tcpdump kullanımı

> tcpdump -i dinlenecekEthernetAdi // e.g. tcpdump -i eth0

Sık kullanılan tcpdump parametreleri

-i : ağ arabirimi seçmeye yarar

-nn : domain çözme işlevi ekler

-tcp port : belirli bir portun paketlerini dinletmeye yarar

-w : trafiği kaydetmeye yarar.

#Belirli IP adresine (ya da domain'e) giden ve gelen trafiği göstertir.

> tcpdump -i eth0 host www.includekarabuk.com

#Belirli ip adresinin SMTP portu dinlenilir ve trafik dosyaya kaydedilir.

> tcpdump -i eth0 tcp port 25 and host www.includekarabuk.com -w smtp.pcap

(Page 106-109)

18)

Wireshark yazılımı tcpdump yazılımı ile aynı görevi yapmaktadır. Wireshark, grafiksel arayüz olarak kullanılır. Bu yüzden paketlerin takibi daha kolaydır.

(page 109)

19)

Privilege Escalation

Hedef sisteme sızıldıktan sonra sisteme daha etkili hükmedebilmek için yetki yükseltmemiz gerekir. Bunun için passwd gibi dosyalardaki şifreleri kırıp uzak sistemde root olarak oturum açabiliriz.

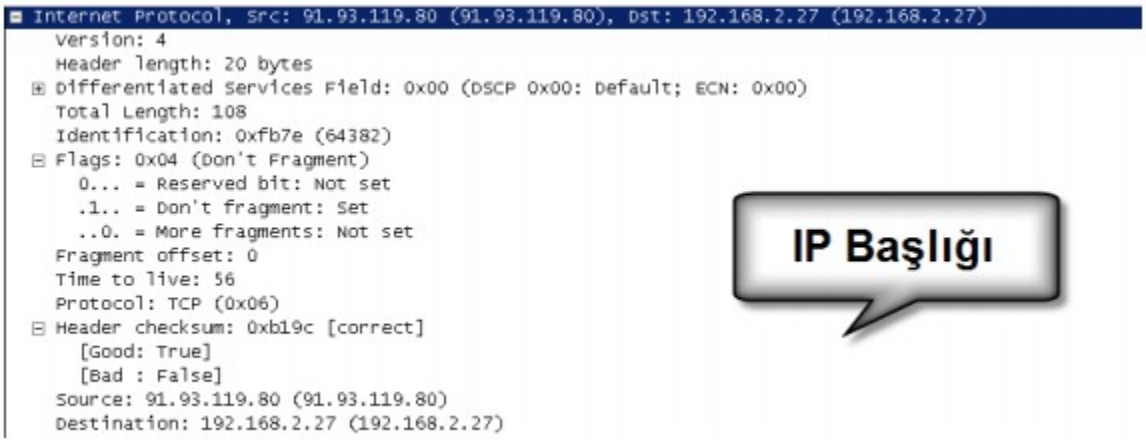
- hashcat

(Page 127)

20)

Network Stress Testing

Hping ile IP paketlerine ait istenilen alanlar düzenlenebilir. IP başlığına bakılırsa en önemli alanların kaynak_ip adresi, hedef_ip adresi, paket parçalama opsiyonu ve ip id numarası olduğu görülecektir.



Hping kullanarak ilk paketimizi gönderelim. Öntanımlı olarak hping icmp yerine TCP paketlerini kullanır. Boş (herhangi bir bayrak set edilmemiş) bir tcp paketini hedef sistemin 0 portuna gönderir.

```
root@BGA:~# hping3 192.168.2.1
HPING 192.168.2.1 (eth1 192.168.2.1): NO FLAGS are set, 40 headers + 0 data byte
s
^C
--- 192.168.2.1 hping statistic ---
8 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Varsayılan durumda TCP paketleri üretir fakat kabiliyeti sadece bunla sınırlı değildir. İstenirse tamamen özelleştirilebilen Raw IP paketleri, icmp ve udp paketleri de oluşturulabilir.

Hping Çalışma Modları

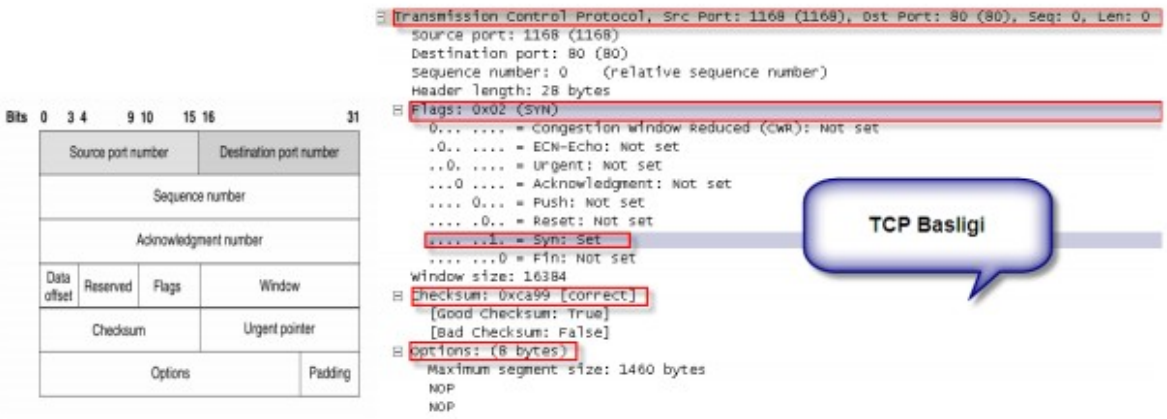
-0 ya da --rawip	:	Raw ip paketleri kullanmak için
-1 ya da --icmp I	:	icmp Paketi oluşturmak için.
-2 ya da --udp	:	UDP Paketleri oluşturmak için.

-8 ya da –scan : Klasik Tarama modu.

-9 ya da –listen : Dinleme modu

TCP Paketleri ile Oynamak

Bir TCP paketinde hangi alanlar vardır, öncelikle buna biraz değinelim sonra hping ile tcp başlığındaki alanları oynayarak neler yapabiliyoruz görelim.



TCP oturumunda en önemli bileşen bayrak(flags)lardır. Oturumun kurulması, veri aktarımı, bağlantının koparılması vb gibi işlerin tamamı bu bayraklar aracılığı ile yapılır. İnceleyeceğimiz diğer protokollerde(IP, ICMP, UDP) bayrak tanımı yoktur. İlk oluşturacağımız paket her TCP oturumunun kurulmasında ilk adımı oluşturan SYN bayraklı bir paket . Hping’e -S parametresi vererek SYN bayraklı paketler gönderebiliriz.

```
root@BGA:~# hping3 -S 192.168.2.1 -c 3
HPING 192.168.2.1 (eth1 192.168.2.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.2.1 ttl=255 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=5.3 ms
len=46 ip=192.168.2.1 ttl=255 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=2.5 ms
len=46 ip=192.168.2.1 ttl=255 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=2.6 ms

--- 192.168.2.1 hping statistic ---
3 packets tramitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.5/3.4/5.3 ms
root@BGA:~#
```

-c parametresi kullanılmazsa hping durdurulana kadar (CTRL^c) paket göndermeye devam eder. –c ile kaç adet paket göndereceği belirtilir.

> hping3 -R 192.168.1.1 -c 3

Benzer şekilde -R yerine diğer TCP bayrak tipleri konularak istenilen türde TCP paketi oluşturulabilir.

Port Belirtimi

•-p parametresi kullanılarak hedef sisteme gönderilen paketlerin hangi porta gideceği belirtilir. Default olarak bu değer 0 dır.

•-s parametresi ile kaynak TCP portu değiştirilebilir, öntanımlı olarak bu değer rastgele atanır.

1000. porta RST, FIN, PUSH ve SYN bayrakları set edilmiş paket gönderimi şu şekildedir:

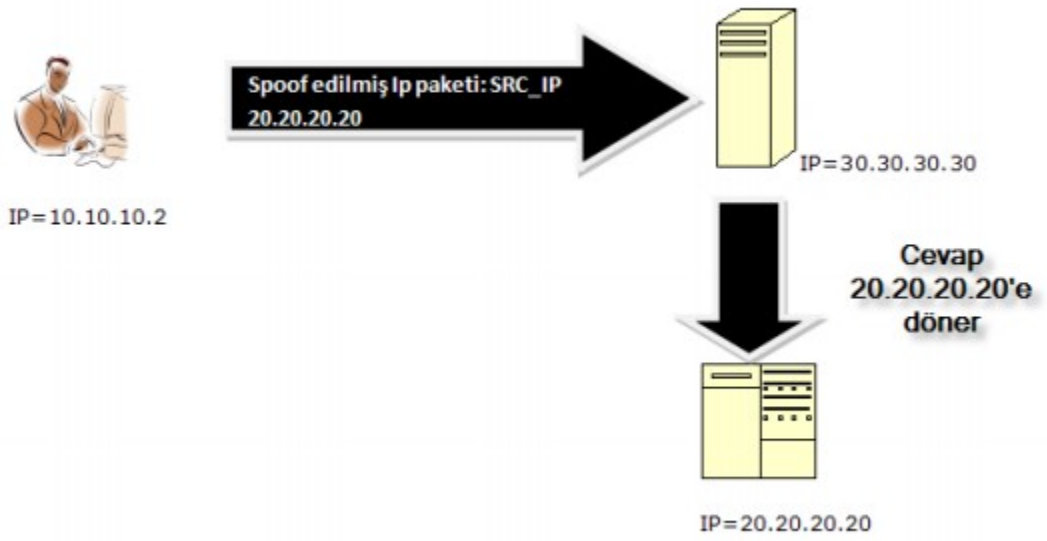
```
root@BGA:~# hping3 -RFPS -c 3 192.168.2.1 -p 1000
HPING 192.168.2.1 (eth1 192.168.2.1): RSFP set, 40 headers + 0 data bytes

--- 192.168.2.1 hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

(RFPS => R: RST, F: FIN, P: PUSH, S: SYN)

Hping kullanarak istenilen ip adresinden geliyormuş gibi paketler üretilebilir. Burada dikkat edilmesi gereken husus kaynak ip adresini spoof ederek gönderdiğimiz

paketler hedefe ulaştıktan sonra dönecek cevabın bize değil spoof edilmiş ip adresine döneceğidir.



Örnek: www.bga.com.tr adresine 10.10.10.10 ip adresinden geliyormuş gibi SYN paketleri gönderelim.

```
root@BGA:~# hping3 -a 10.10.10.10 -S -p 80 www.bga.com.tr
HPING www.bga.com.tr (eth1 199.27.135.47): S set, 40 headers + 0 data bytes
^C
--- www.bga.com.tr hping statistic ---
6 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Ekrandaki sonuç incelenirse geriye hiç paket dönmediği(100% packet loss) görülecektir. Bunun sebebi gönderdiğimiz paketlere dönen cevapların 10.10.10.10 ip adresine gitmesidir. 10.10.10.10 ip adresi de –eğer varsa böyle bir adres- kendisine gelen bu paketlere RST bayraklı TCP paketleriyle cevap dönecektir.

Paket oluştururken ip seviyesinde belirlenebilecek diğer bir özellik de paketlerin yaşam süresini belirleyen TTL değeridir. Hping ile istediğimiz ttl değerini pakete atayabiliriz. Burada dikkat edilmesi gereken husus TTL değerleri düşükse paketimizin hedefe ulaşamadan zaman aşımına uğramasıdır.

```
root@BGA:~# hping3 -t 10 www.google.com.tr -p 80 -S
HPING www.google.com.tr (eth1 173.194.35.152): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.60 name=UNKNOWN
TTL 0 during transit from ip=209.85.255.70 get hostname...^C
```

Çıktıdan da görüleceği gibi ttl değerini 10 yapıp gönderdiğimiz paketler Google.com'a ulaşamadan aradaki bir Router tarafından düşürülüyor ve bize bilgi mesajı olarak icmp paketleri dönüyor.

Hedef sisteme milyonlarca farklı ip adresinden geliyormuş gibi istek gönderilebilir. Özellikle DOS/DDOS saldırılarının simulasyonlarında faydalı olan bir özelliktir.

> hping3 --rand-source -S -p 80 www.bga.com.tr

```
root@BGA:~# hping3 --rand-source -S -p 80 192.168.2.1
HPING 192.168.2.1 (eth1 192.168.2.1): S set, 40 headers + 0 data bytes
^C
--- 192.168.2.1 hping statistic ---
5 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@BGA:~#
```

(Page 136-141)

21)

Bu sekme altında sisteme bulaşmış rootkit'lerin tespiti, image recovery, network forensic gibi ihtiyaçları karşılayabilecek araçlar bulunmaktadır.

- chkrootkit

Chkrootkit (check rootkit) aracı linux/unix sistemlere yerleşmiş rootkitleri tespit etmek için geliştirilmiştir. Chkrootkit aracı bilinen rootkit yazılımlarını tespit edebilmektedir.

// ps ve ls binary komutlarına (dosyalarına) trojan bulaşmış mı diye

// kontrol eder.

> chkrootkit ps ls

Output:

Checking `ps'... not infected

Checking `ls'... not infected

Görüldüğü üzere ps ve ls komutlarına (dosyalarına) trojan bulaşmamış.

// Kök dizinden itibaren recursive olarak dosyalara trojan bulaşmış mı

// kontrolü yapar.

> chkrootkit -r /

// Binary programların içerisindeki şüpheli string'leri tespit eder.

> chkrootkit -x

Trojan bulaştığı tespit edildiğinde *not infected* yazısı yerine *vulnerable* gibi bir yazı yazar. Bu ifade trojan'ın dosyaya bulaştığını ve trojan'ın root yetkisine sahip olduğunu söyler. Bu ihlalden kurtulmanın yolu sistemi temiz bir CD'den tekrar yüklemekten geçer.

http://www.chkrootkit.org/README

(Page 143)

22)

Bulguların Raporlanması

Yapılan sızma çalışmaları videoya kaydedilmek istenirse

Kali Linux->Reporting Tools->Media Capture->recordmyscreen uygulaması kullanılabilir.

(page 144)