C0R3 Bilişim Güvenliği Grubu

Ateş Duvarı Geçme Teknikleri

<evrim@core.gen.tr>

Ateş Duvarı

- Sistemin girişinde yer alır
- Sistemin yapısına göre ayarlanır
- Ağ üzerindeki paketleri inceler
- İçerideki sistemlerin güvenliğini sağlar
- Gerektiğinde hareketleri kaydedebilir

Ateş Duvarı Geçme Teknikleri

- Ateş Arkasındaki bilgisayarların portlarının taranması:
  1. Ateş Üzerinde Yürüme Tekniği (Firewalking)
  2. Şahit İle Tarama Metodu (Witness Scanning)

Ateş Üzerinde Yürüme Metodu

- Ateş duvarı tarafından filtrelenmiş bilgisayarların portlarını taramak için kullanılır
- Aynı isimle bu metodu uygulayan bir yazılım da mevcuttur (www.packetfactory.net)
- IP TTL alanından istifade eder

IP TTL Alanı

- İngilizce açılımı: Time To Live
- Herhangi bir IP paketinin kaynaktan hedefe ulaşıncaya kadar katedebileceği maksimum zamanı saniye cinsinden ifade eder
- 8 bit'tir. 2^8-1 = 255 saniye
- IP başlığı her işlendiğinde en az 1 azaltılır.
- Paket hedefe ulaşmadan sıfırlanırsa, ICMP TTL Exceeded mesajı ile kaynak uyarılır

IP TTL Alanı

- Öngörülen TTL başlangıç değerleri:
  - Linux 2.4.x, 2.2.x -> 255
  - Solaris 2.6 -> 255
  - Win95 -> 32
  - Win98 -> 128
  - Win2k -> 128

ICMP TTL Exceeded Mesajı

- Type: 11
- Code: 0 (Code 1, Fragment Reassembly Time exceeded)
- Hatayı oluşturan paketin 64 bit'i sona eklenir (RFC)

/usr/sbin/traceroute

- Kaynak ile hedef arasındaki güzergahı belirlemek için kullanılır
- İlk olarak TTL'i 1 olan paketler yaratır.
- Gelen mesajlara göre bu alanı her 3 pakette bir arttırır
- TTL alanı 255 olana veya hedef bilgisayara ulaşıncaya kadar bu işlem sürdürülebilir

/usr/sbin/traceroute

- 2 tip paket üretir:
    1. UDP paketi
    2. ICMP Echo Request Paketi

/usr/sbin/traceroute

- 2 tip paket üretir:
    1. UDP paketi
    2. ICMP Echo Request Paketi

/usr/sbin/traceroute

```
[root@drew /]# traceroute www.me.metu.edu.tr
traceroute to www.me.metu.edu.tr (144.122.169.2), 30 hops max, 38
byte packets
 1  212.45.90.66 (212.45.90.66)  1.701 ms  2.068 ms  1.693 ms
 2  212.45.90.100 (212.45.90.100)  193.992 ms  13.824 ms  109.005
 3  212.45.65.17 (212.45.65.17)  312.384 ms  400.341 ms  109.610 ms
 4  212.45.65.51 (212.45.65.51)  15.803 ms  15.602 ms  16.776 ms
 5  195.175.16.1 (195.175.16.1)  21.765 ms  109.050 ms  105.127 ms
 6  195.175.16.38 (195.175.16.38)  240.324 ms  613.278 ms  392.902
 7  1.asn9000.atm.metu.edu.tr (144.122.155.1)  497.011 ms  483.626
ms  83.046 ms
 8  exchange.me.metu.edu.tr (144.122.169.2)  98.565 ms  32.134 ms
30.381 ms
[root@drew /]#
```

/usr/sbin/traceroute

```
tcpdump: listening on all devices
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33435: udp 10 [ttl
1]
eth0 < 212.45.90.66 > evrim.envy.com.tr: icmp: time exceeded in-transit [tos
0xc0]
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33436: udp 10 [ttl
1]
eth0 < 212.45.90.66 > evrim.envy.com.tr: icmp: time exceeded in-transit [tos
0xc0]
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33437: udp 10 [ttl
1]
eth0 < 212.45.90.66 > evrim.envy.com.tr: icmp: time exceeded in-transit [tos
0xc0]
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33438: udp 10
eth0 < 212.45.90.100 > evrim.envy.com.tr: icmp: time exceeded in-transit
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33439: udp 10
eth0 < 212.45.90.100 > evrim.envy.com.tr: icmp: time exceeded in-transit
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33440: udp 10
eth0 < 212.45.90.100 > evrim.envy.com.tr: icmp: time exceeded in-transit
eth0 > evrim.envy.com.tr.33174 > exchange.me.metu.edu.tr.33441: udp 10
```

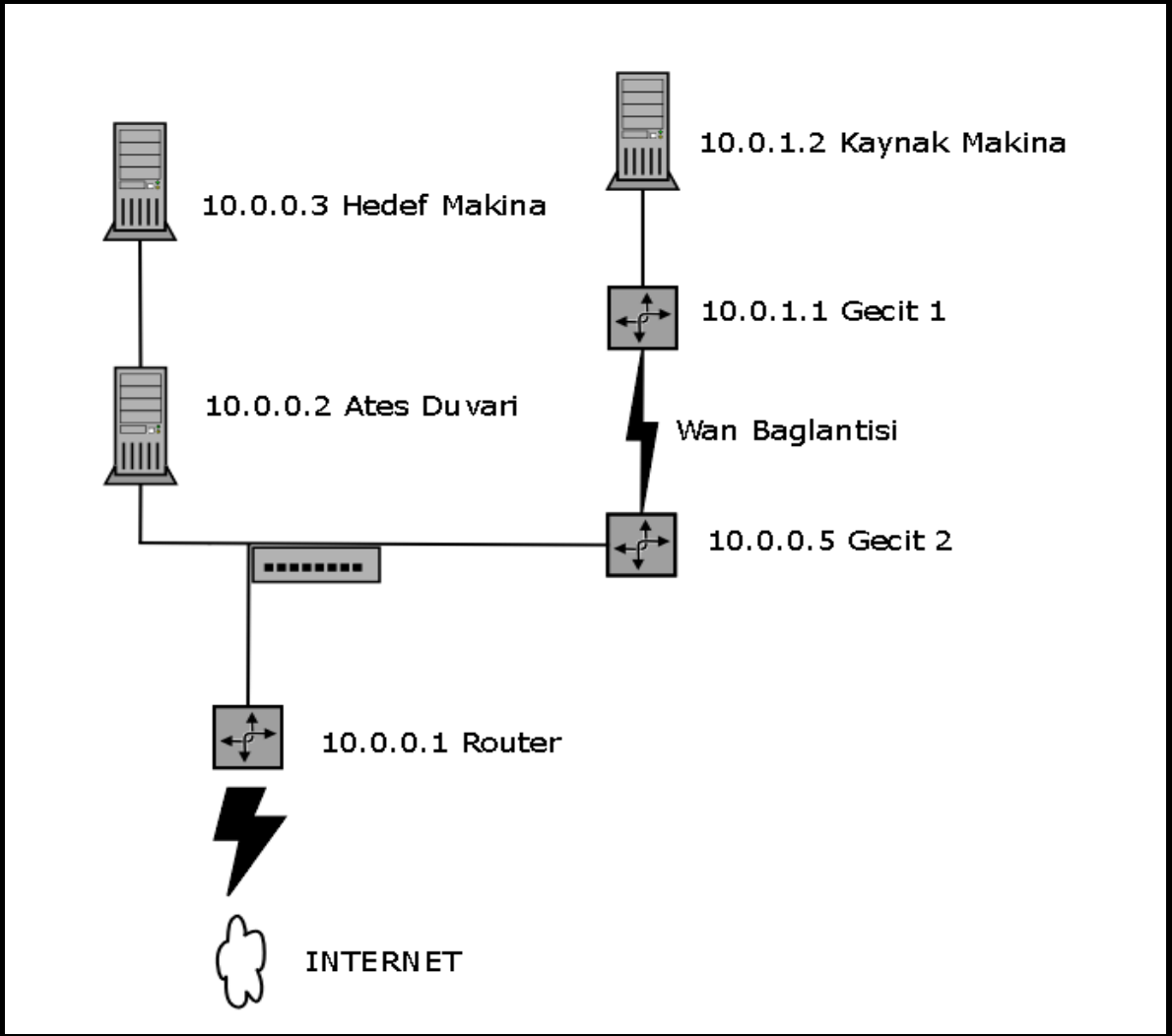
/usr/sbin/traceroute

```
[root@drew /]# traceroute www.me.metu.edu.tr -I
traceroute to www.me.metu.edu.tr (144.122.169.2), 30 hops max, 38
byte packets
 1  212.45.90.66 (212.45.90.66)  6.966 ms  1.551 ms  1.635 ms
 2  212.45.90.100 (212.45.90.100)  1247.278 ms  410.565 ms  395.974
ms
 3  212.45.65.17 (212.45.65.17)  627.535 ms  240.710 ms  857.604 ms
 4  212.45.65.51 (212.45.65.51)  516.441 ms  306.949 ms  493.033 ms
 5  195.175.16.1 (195.175.16.1)  178.596 ms  394.434 ms  322.868 ms
 6  195.175.16.38 (195.175.16.38)  344.103 ms  593.531 ms  509.578
ms
 7  1.asn9000.atm.metu.edu.tr (144.122.155.1)  450.677 ms  496.985
ms  1148.606 ms
 8  exchange.me.metu.edu.tr (144.122.169.2)  809.592 ms  1094.848 ms
 962.074 ms
[root@drew /]#
```

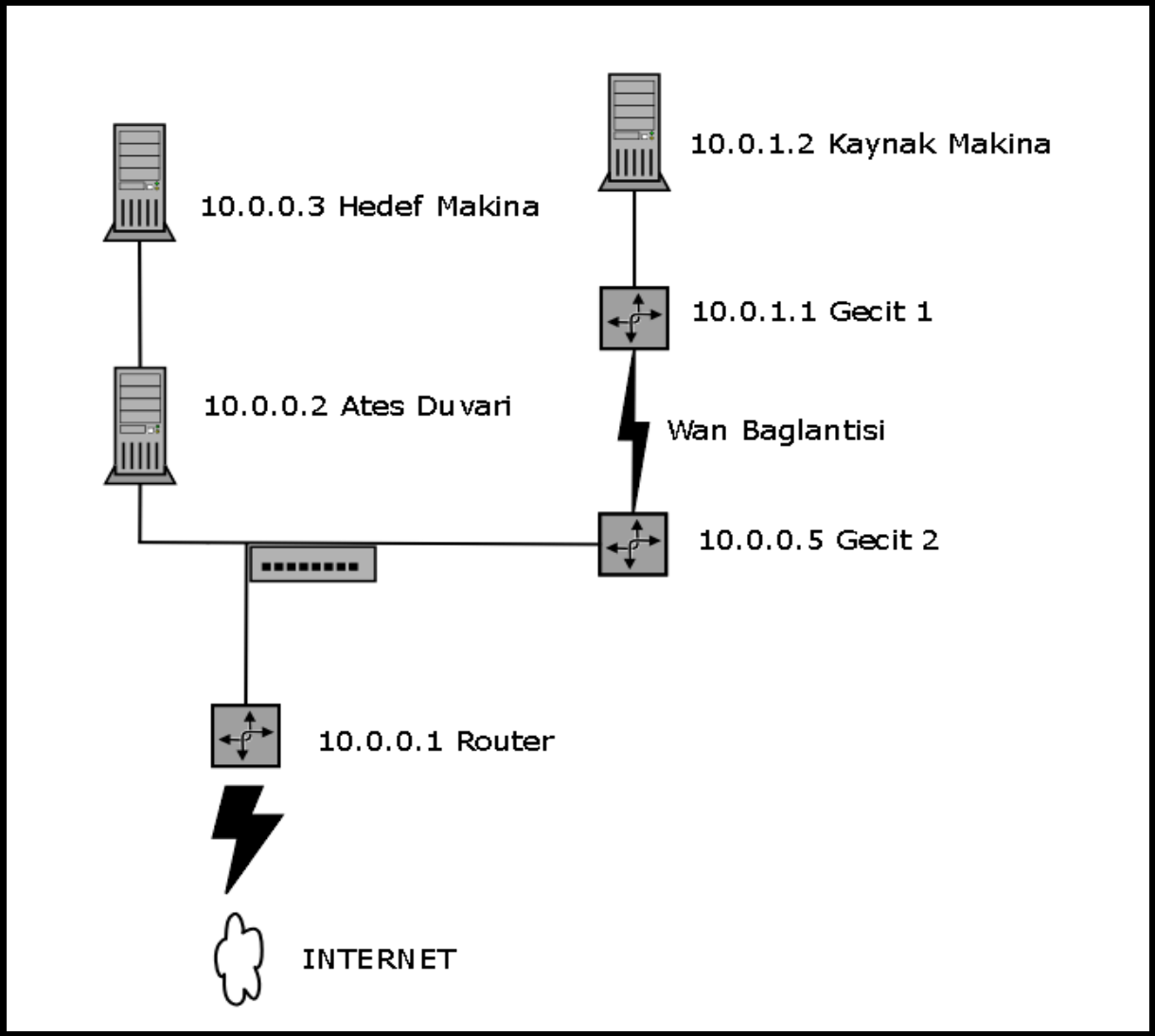
/usr/sbin/traceroute

```
eth0 < 212.45.65.17 > evrim.envy.com.tr: icmp: time exceeded in-
transit [tos 0xc0]
eth0 > evrim.envy.com.tr > exchange.me.metu.edu.tr: icmp: echo
request
eth0 < 212.45.65.17 > evrim.envy.com.tr: icmp: time exceeded in-
transit [tos 0xc0]
eth0 > evrim.envy.com.tr > exchange.me.metu.edu.tr: icmp: echo
request
eth0 < 212.45.65.17 > evrim.envy.com.tr: icmp: time exceeded in-
transit [tos 0xc0]
eth0 > evrim.envy.com.tr > exchange.me.metu.edu.tr: icmp: echo
request
eth0 < 212.45.65.51 > evrim.envy.com.tr: icmp: time exceeded in-
transit [tos 0xc0]
eth0 > evrim.envy.com.tr > exchange.me.metu.edu.tr: icmp: echo
request
eth0 < 212.45.65.51 > evrim.envy.com.tr: icmp: time exceeded in-
transit [tos 0xc0]
eth0 > evrim.envy.com.tr > exchange.me.metu.edu.tr: icmp: echo
request
```

Ağ Şeması


10.0.1.2 Kaynak Makina
10.0.0.3 Hedef Makina
10.0.1.1 Gecit 1
10.0.0.2 Ates Duvari
Wan Baglantisi
10.0.0.5 Gecit 2
10.0.0.1 Router
INTERNET

Ağ Şeması


10.0.1.2 Kaynak Makina
10.0.0.3 Hedef Makina
10.0.1.1 Gecit 1
10.0.0.2 Ates Duvari
Wan Baglantisi
10.0.0.5 Gecit 2
10.0.0.1 Router
INTERNET

/usr/sbin/traceroute

```
[root@drew /]# traceroute 10.0.0.3
traceroute to 10.0.0.3 (10.0.0.3), 30 hops max, 40 byte
packets
 1  10.0.1.1 (10.0.1.1)  7.333 ms  3.745 ms  4.600 ms
 2  10.0.0.5 (10.0.0.5)  24.859 ms  43.169 ms  63.847 ms
 3  10.0.0.2 (10.0.0.2)  45.621 ms  39.363 ms  40.371 ms
 4  10.0.0.3 (10.0.0.3)  41.867 ms  61.479 ms  51.631 ms
[root@drew /]#
```

/usr/sbin/traceroute

```
[root@drew /]# iptables -A OUTPUT -p icmp --icmp-type time-
exceeded -j DROP
[root@drew /]# iptables -L
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere
icmp time-exceeded
```

/usr/sbin/traceroute

```
[root@drew /]# traceroute 10.0.0.3
traceroute to 10.0.0.3 (10.0.0.3), 30 hops max, 40 byte
packets
 1  10.0.1.1 (10.0.1.1)  10.915 ms  4.397 ms  3.988 ms
 2  10.0.0.5 (10.0.0.5)  29.039 ms  39.540 ms  41.029 ms
 3  * * *
 4  10.0.0.3 (10.0.0.3)  44.753 ms  41.061 ms  40.043 ms
[root@drew /]#
```

/usr/sbin/traceroute

```
[root@drew /]#
eth1 < 10.0.1.1 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.1.1 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.1.1 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.5 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.5 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.5 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.3 > 10.0.1.2: icmp: 10.0.0.3 udp port 33444
unreachable
```

/usr/sbin/traceroute

```
[root@drew /]#
eth1 < 10.0.1.1 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.1.1 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.1.1 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.5 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.5 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.5 > 10.0.1.2: icmp: time exceeded in-transit
eth1 < 10.0.0.3 > 10.0.1.2: icmp: 10.0.0.3 udp port 33444
unreachable
```

Firewalking

- Uygulanabileceği durumlar:
  - Hedef bilgisayarın gerçek IP'si olması gereklidir
  - Ateş duvarı paketleri yönlendirmelidir. (Routing)
  - Bridge modülü ile ayarlanmış bir geçitte uygulanması mümkü değildir

Firewalking

- Amaç:

  Ateş duvarı arkasında yer alan bilgisayarların filtrelemeye rağmen portlarının taranması

- Uygulama:

  Aradaki güzergah belirlenir

  TTL'i geçite geldiğinde 1 olacak paketler yaratılır

  ICMP TTL Exceeded mesajları dinlenir

Firewalking

```
[root@drew hax]# ipchains -V
ipchains 1.3.10, 1-Sep-2000
[root@drew hax]# ipchains -L
Chain input (policy ACCEPT):
target     prot opt     source               destination
  ports
DENY       udp  ------  anywhere             10.0.0.3
any ->   http
DENY       tcp  ------  anywhere             10.0.0.3
any ->   http
Chain forward (policy ACCEPT):
target     prot opt     source               destination
  ports
DENY       tcp  ------  anywhere             10.0.0.3
any ->   http
DENY       udp  ------  anywhere             10.0.0.3
any ->   http
Chain output (policy ACCEPT):
```

Firewalking

```
[root@drew Firewalk-1.0]# ./firewalk 10.0.0.5 10.0.0.3 -i eth1 -p
TCP -S 23,80
Ramping up hopcounts to binding host...
probe:  1  TTL:  1  port 33434:  expired from [10.0.1.1]
probe:  2  TTL:  2  port 33434:  Bound scan at 2 hops [10.0.0.5]
port  23: open
port  80:  *
1 ports open, 0 ports unknown
4 probes sent, 3 replies received
[root@drew Firewalk-1.0]#
```

Firewalking

```
[root@drew hping2]# ./hping2 -S -c 1 -t 3 -p 80 -s 53 10.0.0.3
HPING 10.0.0.3 (eth1 10.0.0.3): S set, 40 headers + 0 data bytes

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

[root@drew hping2]# ./hping2 -S -c 1 -t 3 -p 23 -s 53 10.0.0.3
HPING 10.0.0.3 (eth1 10.0.0.3): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=10.0.0.2 name=UNKNOWN

--- 10.0.0.3 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@drew hping2]#
```

Firewalking

```
[root@drew /]# iptables -V
iptables v1.2.1a
[root@drew /]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       udp  --  0.0.0.0/0            10.0.0.3       udp dpt:80
DROP       tcp  --  0.0.0.0/0            10.0.0.3       tcp dpt:80

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  0.0.0.0/0            10.0.0.3       tcp dpt:80
DROP       udp  --  0.0.0.0/0            10.0.0.3       udp dpt:80

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       udp  --  0.0.0.0/0            10.0.0.3       udp dpt:80
DROP       tcp  --  0.0.0.0/0            10.0.0.3       tcp dpt:80
[root@drew /]#
```

Firewalking

```
[root@drew Firewalk-1.0]# ./firewalk 10.0.0.5 10.0.0.3 -i eth1 -p TCP -S
23,80
Ramping up hopcounts to binding host...
probe:  1  TTL:  1  port 33434:  expired from [10.0.1.1]
probe:  2  TTL:  2  port 33434:  Bound scan at 2 hops [10.0.0.5]
port  23: open
port  80: open
2 ports open, 0 ports unknown
4 probes sent, 4 replies received
[root@drew Firewalk-1.0]#
```

Firewalking

```
[root@drew hping2]# ./hping2 -S -c 1 -t 3 -p 80 -s 53 10.0.0.3
HPING 10.0.0.3 (eth1 10.0.0.3): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=10.0.0.2 name=UNKNOWN

--- 10.0.0.3 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@drew hping2]# ./hping2 -S -c 1 -t 3 -p 23 -s 53 10.0.0.3
HPING 10.0.0.3 (eth1 10.0.0.3): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=10.0.0.2 name=UNKNOWN

--- 10.0.0.3 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@drew hping2]#
```

Şahit İle Tarama Metodu

- Amaç:

  Ateş duvarı arkasında bulunan makinaların portlarını taramak

- Özellikler:

  Tarama için hedefin bulunduğu ağdaki diğer bir bilgisayar kullanılır

  IP ID alanından istifade eder

  Tarayan kaynağın bulunması zordur

  Şahit bilgisayarın yükü çok az olmak zorundadır

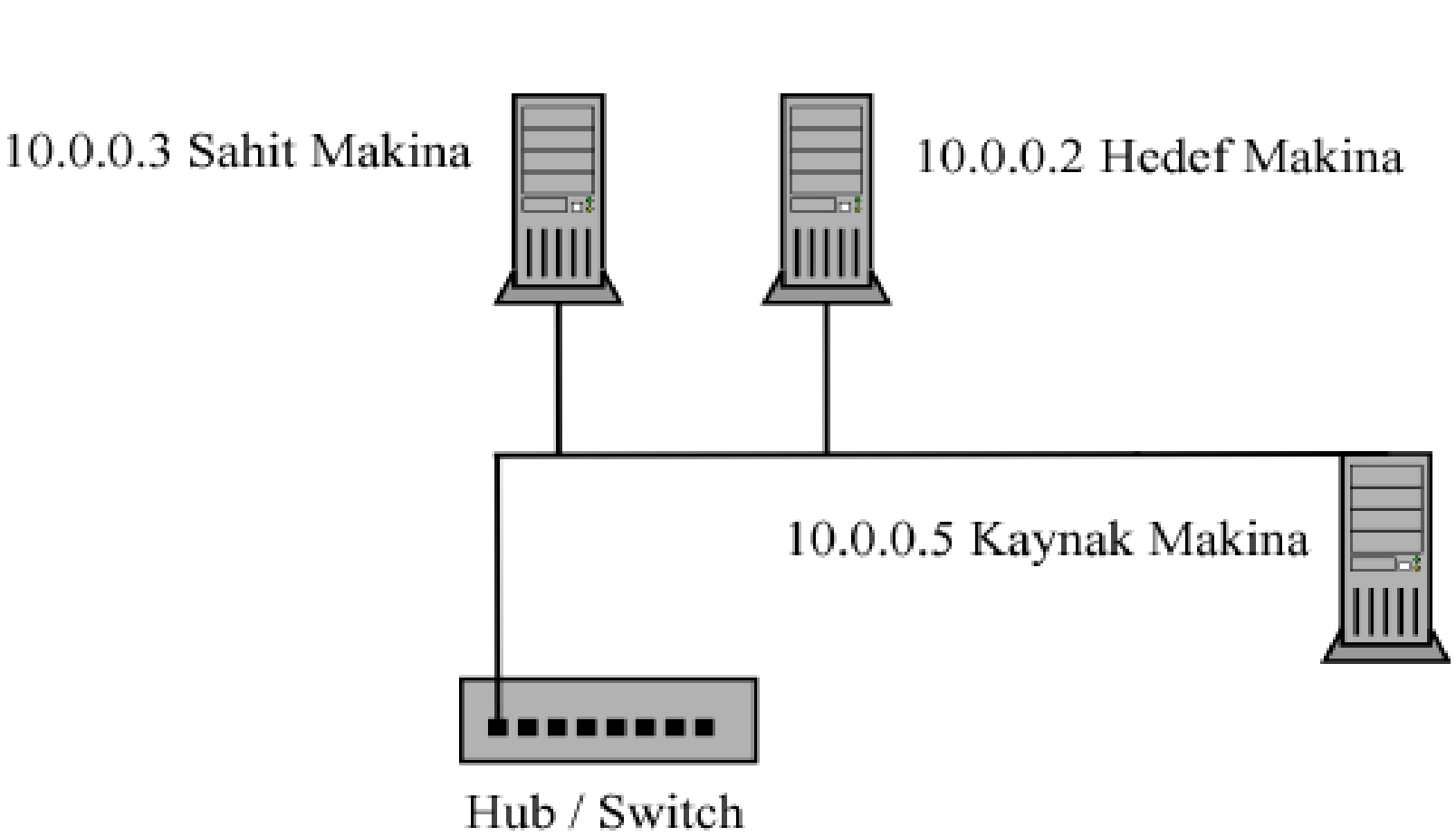
IP ID Alanı

- Parçalara ayrılmış paketlerin yeniden birleştirilmesinde kullanılır
- 16 bit'tir
- RFC'ye rağmen birçok işletim sisteminde farklı uyarlanmıştır

IP ID Alanı ve İşletim Sistemleri

- Ard arda üretilen paketler için Win98, Win2k ID alanını sabit olarak 256 arttırır.
- Bazı unix'ler bu değeri 1 arttırırlar.
- Eski Linux çekirdeklerinde getpid() fonksiyonunun cevabı atanırdı
- Linux 2.4.x bu değeri 0 olarak ayarlar

Ağ Şeması


10.0.0.3 Sahit Makina
10.0.0.2 Hedef Makina
10.0.0.5 Kaynak Makina
Hub / Switch

Teori

- Hedef: 10.0.0.2, Şahit: 10.0.0.3, Kaynak: 10.0.0.5
- Şahit bilgisayara idle konumda iken SYN bayraklı paketler gönderilerek ID değerlerinin değişimi gözlenir ve kaydedilir. (Muhtemelen ID değeri 1 yada 256 kadar artacaktır.)
- Asıl tarama işlemi sırasında sonuçlar bu süreç içersindeki ID değerlerinin değişimi gözlenerek elde edileceğinden bu süreç tarama sonuna kadar devam edecektir.
- Kaynak bilgisayardan kaynak adresi şahit olarak atanmış yalancı SYN paketleri hedef bilgisayarın taramak istenilen portuna gönderilir.
- Eğer port kapalı ise, hedef bilgisayar “ICMP Port Unreachable” ile şahit bilgisayara cevap verecektir.

Teori

- Eğer port açık ise, normal bağlantı prosedürünü yerine getirerek ACK/SYN paketi ile şahit bilgisayara geri dönecektir.
- Şahit bilgisayar “ICMP Port Unreachable” mesajını alır ise kaynak bilgisayara verdiği cevaplardaki ID değerlerinde herhangi bir değişme gözlenmeyecektir.
- Eğer hedeften ACK/SYN paketi alırsa birinci seçenekteki sürece verdiği cevaplardaki ID değeri bir seferlik ya bir, ya da belli bir oranda artacaktır.

Uygulama

```
[root@drew hping2]# ./hping2 -S -r -W 212.45.90.68 -c 4
HPING 212.45.90.68 (eth1 212.45.90.68): S set, 40 headers + 0
data bytes
len=1500 ip=212.45.90.68 flags=RA seq=0 ttl=124 id=397 win=0
rtt=42.6 ms
len=1500 ip=212.45.90.68 flags=RA seq=1 ttl=124 id=+1 win=0
rtt=27.3 ms
len=1500 ip=212.45.90.68 flags=RA seq=2 ttl=124 id=+1 win=0
rtt=28.0 ms
len=1500 ip=212.45.90.68 flags=RA seq=3 ttl=124 id=+1 win=0
rtt=27.6 ms

--- 212.45.90.68 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 27.3/31.3/42.6 ms
[root@drew hping2]#
```

Uygulama

```
[root@drew hping2]# ./hping2 -a 212.45.90.68 -S -p 23
212.45.90.66 -c 4
HPING 212.45.90.66 (eth1 212.45.90.66): S set, 40 headers + 0
data bytes

--- 212.45.90.66 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@drew hping2]#
```

Uygulama

```
[root@drew hping2]# nmap -sI 212.45.90.68:139 -P0 212.45.90.66
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Idlescan using zombie 212.45.90.68 (212.45.90.68:139); Class:
Broken little-endian incremental
Interesting ports on  (212.45.90.66):
(The 1545 ports scanned but not shown below are in state:
closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
80/tcp     open        http
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
631/tcp    open        cups
852/tcp    open        unknown
3306/tcp   open        mysql
6000/tcp   open        X11
Nmap run completed -- 1 IP address (1 host up) scanned in 16
seconds
[root@drew hping2]#
```

Şahit İle Tarama Metodunun Engellenmesi

- ID alanını doğru yorumlayan işletim sistemleri kullanılmalı
- Yalancı kaynak adresli paketleri ağdan ayıklamak

C0R3 Bilişim Güvenliği Grubu
<evrim@core.gen.tr>