

Bunyamin Demir, <bunyamindemir at gmail dot com>, webguvenligi.org, 20/01/2011

ORACLE VERİTABANI TRAFİĞİNİN GÜVENLİĞİ

Oracle veritabanında, veritabanına yetkili erişim olmadan verinin elde edilebilmesi için çeşitli yollar mevcuttur. Çünkü veri hem trafik olarak bilgisayar ağları üzerinden geçmektedir hem de dosya sisteminde saklanmaktadır. Bilgisayar ağları üzerinden geçen trafik üçüncü şahıslar tarafından izlenebilir ve hassas veriler çalınabilir. Aynı zamanda hassas veri içeren bilgiler, işletim sistemi üzerinde dosya olarak tutulmaktadır. Bu dosyalara yapılan yetkisiz erişimler hassas verinin çalınmasına sebep olabilir.

Bu bölümde sadece trafiğin şifrenmesi konusunu incelenmiştir.

1. Oracle Veritabanı Trafiğinin Şifrenmesi

Oracle veritabanı bağlantılarının çoğu, bilgisayar ağları üzerinden yapılan (uzaktan) bağlantılardır. Dolayısıyla veritabanı trafiği bilgisayar ağları üzerinden geçmektedir. Veritabanı trafiği TNS protokolünü kullanarak TCP/IP paketleri halinde bilgisayar ağları üzerinden iletilir. Trafiği daha iyi analiz edebilmek adına oluşan veritabanı trafiği üç genel başlık altında sınıflandırılmıştır.

- 1.Oturum bilgisini içeren, veritabanına bağlantıyı oluşturan trafik,
- 2.Bağlantı oluşturulduktan sonra çalıştırılan SQL trafiği,
- 3.Çalıştırılan SQL cümleciklerine karşın geri dönen sorgu cevapları.

Oracle veritabanı kurulumu da belirtmediğiniz sürece ön tanımlı olarak yapılan yapılandırma ile, veritabanı üzerine gelen ve giden tüm trafik düzmetin şeklindedir. Dolayısıyla araya girebilecek üçüncü şahıslar tarafından trafik dinlenebilir ve hassas bilgiler çalınabilir.

Düz metin trafiğin içeriğine bakabilmek için Wireshark uygulamasını kullandım. Bu uygulama ile alınmış olan oturum bilgisi trafiği Şekil 4.1 de gösterildiği gibidir.

```

0000 00 0c 29 23 46 52 00 50 56 c0 00 08 08 00 45 00 ..)#FR.P V.....E.
0010 00 dd f6 ff 40 00 80 06 dc 7c 0a 0a 09 01 0a 0a ....@... .|.....
0020 09 8a 11 d7 05 f1 34 37 84 30 ff 74 4a a3 50 18 .....47 .0.tJ.P.
0030 fb 7c 69 4e 00 00 00 b5 00 00 01 00 00 00 01 34 .|iN.... .....4
0040 01 2c 0c 01 08 00 7f ff 4f 98 00 00 00 01 00 93 ..... O.....
0050 00 22 00 00 00 00 01 01 28 44 45 53 43 52 49 50 .". (DESCRIP
0060 54 49 4f 4e 3d 28 43 4f 4e 4e 45 43 54 5f 44 41 TION=(CO NNECT_DA
0070 54 41 3d 28 53 49 44 3d 6f 72 61 74 65 73 74 29 TA=(SID= oratest)
0080 28 43 49 44 3d 28 50 52 4f 47 52 41 4d 3d 29 28 (CID=(PR OGRAM=)(
0090 48 4f 53 54 3d 5f 5f 6a 64 62 63 5f 5f 29 28 55 HOST=__j dbc__)(U
00a0 53 45 52 3d 62 75 6e 79 61 6d 69 6e 20 64 65 6d SER=buny amin dem
00b0 69 72 29 29 29 28 41 44 44 52 45 53 53 3d 28 50 ir)))(AD DRESS=(P
00c0 52 4f 54 4f 43 4f 4c 3d 74 63 70 29 28 48 4f 53 ROTOCOL= tcp)(HOS
00d0 54 3d 31 30 2e 31 30 2e 39 2e 31 33 38 29 28 50 T=10.10. 9.138)(P
00e0 4f 52 54 3d 31 35 32 31 29 29 29 ORT=1521 ))

```

Şekil 4.1: Düzmetin veritabanı trafiği (Oturum bilgisi)

Veritabanı trafiğinin elde edilmesinden önce, örnek bir tablo oluşturup, bu tabloya veriler girelim.

```

CREATE TABLE KREDI_KARTI
("RECORDID" NUMBER NOT NULL ENABLE,
"AD" VARCHAR2(50 BYTE),
"SOYAD" VARCHAR2(50 BYTE),
"KARTNO" VARCHAR2(50 BYTE),
CONSTRAINT "KREDI_KARTI_PK" PRIMARY KEY ("RECORDID"));

```

Ardından tablo içine kayıtları ekleyelim.

```

INSERT INTO KREDI_KARTI (RECORDID, AD, SOYAD, KARTNO) VALUES ('1', 'bunyamin',
'demir', '1111111111111111')

```

```

INSERT INTO KREDI_KARTI (RECORDID, AD, SOYAD, KARTNO) VALUES ('2', 'ahmet',
'ordu', '2222222222222222')

```

```
INSERT INTO KREDI_KARTI (RECORDID, AD, SOYAD, KARTNO) VALUES ('3', 'ebru', 'demir', '333333333333333')
```

İstemcinin IP adresi 10.10.9.1 ve Oracle veritabanı sunucumuzun IP adresi ise 10.10.9.138 olarak atayalım. Wireshark yardımı ile 10.10.9.1 ve 10.10.9.138 arasındaki 1521 portlu veritabanı trafiğini dinlemeye alalım.

İstemci tarafından aşağıdaki SQL cümlecığı çalıştırıldığında

```
SQL> SELECT AD, SOYAD, KARTNO FROM bunyamin.KREDI_KARTI;
```

```
00000000 00 73 00 00 06 00 00 00 00 00 11 69 00 01 01 02 .s.....l....
00000010 01 2a 01 29 03 5e 00 02 80 21 00 01 01 29 01 01 (*).^...l...).
00000020 0d 00 00 04 ff ff ff ff 01 32 04 7f ff ff ff 00 .....2.....
00000030 00 00 00 00 00 00 00 00 00 00 01 53 45 4c 45 43 .....SELEC
00000040 54 20 41 44 2c 20 53 4f 59 41 44 2c 20 4b 41 52 T AD, SO YAD, KAR
00000050 44 4e 4f 20 46 52 4f 4d 20 4b 52 45 44 49 5f 4b DNO FROM KREDI_K
00000060 41 52 54 49 01 01 00 00 00 00 00 00 01 01 00 00 ARTI....
00000070 00 00 00 .....
```

Şekil 4.2: Düzmetin veritabanı trafiği (SQL)

```
00000000 01 51 00 00 06 00 00 00 00 00 10 17 37 9e d5 c1 .Q.....7...
00000010 3b 53 da a4 0e 1c 52 ca 2c c4 d9 99 78 6e 04 0e ;S...R.,...xn..
00000020 16 21 2e 01 96 01 03 3d 01 80 00 00 01 32 00 00 .!.....= .....2..
00000030 00 00 01 b2 01 01 32 01 02 01 02 02 41 44 00 00 .....2. ....AD..
00000040 00 01 80 00 00 01 32 00 00 00 00 01 b2 01 01 32 .....2. ....2
00000050 01 05 01 05 05 53 4f 59 41 44 00 00 01 01 01 80 ....SOY AD.....
00000060 00 00 01 32 00 00 00 00 01 b2 01 01 32 01 06 01 ...2.... ....2...
00000070 06 06 4b 41 52 44 4e 4f 00 00 01 02 01 07 07 78 ..KARDNO .....x
00000080 6e 04 0e 16 22 21 00 02 1f e8 01 0a 01 0a 06 22 n...!.. ...."
00000090 01 03 00 01 32 00 00 00 07 08 62 75 6e 79 61 6d ....2... ..bunyam
000000A0 69 6e 05 64 65 6d 69 72 10 31 31 31 31 31 31 31 in.demir .1111111
000000B0 31 31 31 31 31 31 31 31 31 07 05 61 68 6d 65 74 11111111 1..ahmet
000000C0 04 6f 72 64 75 0f 32 32 32 32 32 32 32 32 32 .ordu.22 22222222
000000D0 32 32 32 32 32 15 01 03 07 07 04 65 62 72 75 05 22222... ..ebru.
000000E0 64 65 6d 69 72 10 33 33 33 33 33 33 33 33 33 33 demir.33 33333333
000000F0 33 33 33 33 33 33 08 01 06 03 0d ff 8c 00 01 0a 333333.. ....
00000100 01 01 00 00 00 00 00 04 02 03 50 01 03 02 05 7b .....P....{
00000110 00 00 01 0a 01 1e 03 00 01 20 00 00 00 03 01 23 .....#
00000120 94 01 04 00 02 02 0b 00 00 00 00 00 01 01 00 00 .....
00000130 00 00 1e 4f 52 41 2d 30 31 34 30 33 3a 20 68 69 ...ORA-0 1403: hi
00000140 e7 20 76 65 72 69 20 62 75 6c 75 6e 6d 61 64 69 . veri b ulunmadi
00000150 0a .
```

Şekil 4.3: Düzmetin veritabanı trafiği (Cevap)

Şekil 4.2, Şekil 4.3 de yakalanan trafiklerden de görüldüğü gibi hem çalıştırılan SQL cümlecığı hem de bu cümlecığe karşın geri dönen cevap kümesi, ağ trafiğinin içinden düz metin olarak geçmekte ve üçüncü şahıslar tarafından görüntülenebilmektedir.

Bu problemi çözmek için veritabanı trafiğinin şifrenmesi gerekmektedir. Dolayısıyla araya girip trafiğı dinleyen üçüncü şahısların eline sadece şifreli trafik geçmiş olacaktır ve bu da anlamlı bir veri kazanmalarına engel olacaktır.

Oracle veritabanı bu tür istismarlar için Advanced Security Option (Oracle ASO) uygulaması yardımıyla veri güvenliğı çözümlerini sunmaktadır. ASO yardımıyla veritabanı trafiğı şifreli hale getirilebilir, veritabanında bulunan hassas verilerin şifreli halde saklanması sağlanabilir. Bu çalışma sırasında veritabanı trafiğinin şifrenmesi için hem Oracle ASO çözümlerini hem de SSH tünelleme yöntemini kullanılmıştır. Oracle ASO çözümlerini, Oracle ile geldiğı için, kurulum ve kullanımı nispeten daha basittir. Fakat özellikle internet (dış) bağlantılar için SSH tünelleme modeli de kullanılabilir.

1.1. Oracle ASO İle Veritabanı Trafığının Şifrenmesi

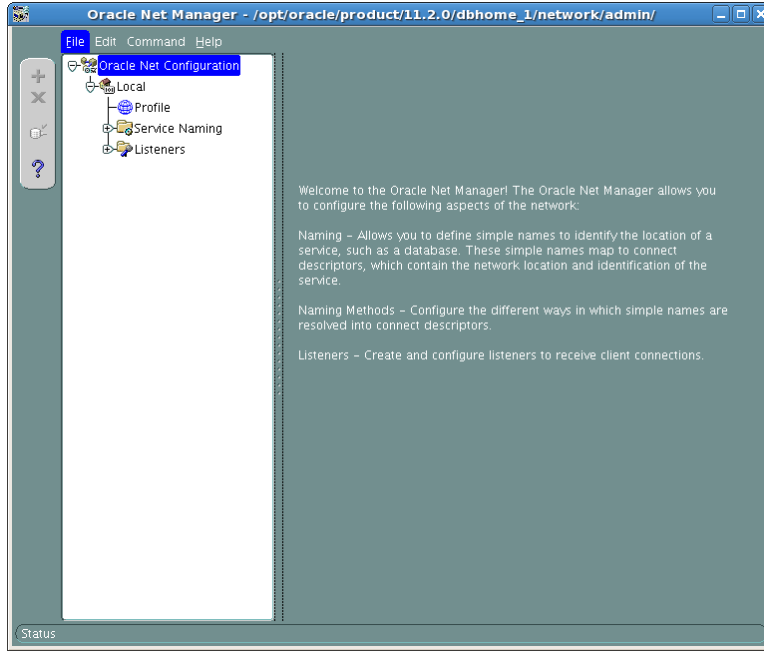
Veritabanı üzerinde tutulan verilerin güvenliğini sağlamak amacıyla ağ katmanındaki kısıtlamalar (güvenlik duvarı gibi) ve veri tabanı erişim kontrolleri ile birçok önlem alınmaktadır. Bu önlemler veriye erişimin güvenli bir şekilde gerçekleştirilmesini sağlamakta ve dış tehditlerin veriye erişimini engellemektedir. Ancak, veritabanı dosyaları disk üzerinden kopyalandığında, bilgisayar ağları üzerinden geçtiğinde ya da veritabanı yedeklerinin bulunduğu teyp'ler ele geçirildiğinde hassas veriler yetkisi olmayan kişilerin erişimine açık hale gelmektedir. Bunu önlemenin en güvenli yolu bu verilerin şifrelenerek tutulması veya aktarılmasıdır.

Oracle veritabanı tarafından sunulan ASO uygulaması ile verilerin hem ağ katmanında hem de disk katmanında şifrelenerek taşınması ve saklanması sağlamaktadır. Oracle ASO bazı Oracle dağıtımlarında beraber gelmektedir, bazılarında ise sonradan ilave edilebilmektedir. Bu çalışmamızda öncelikle yapılandırması hakkında bilgi verip, düz metin trafik ile şifreli trafiğın kıyaslanabilmesi için daha önce istismar edilen trafiğın aynısı elde edilmeye çalışacağız. Bu durumda Oracle ASO için

“Oracle Net Manager” kullanılarak yapılandırma, arayüz yardımı ile yapılabilir. Oracle Net Manager`i çalıştırmak için

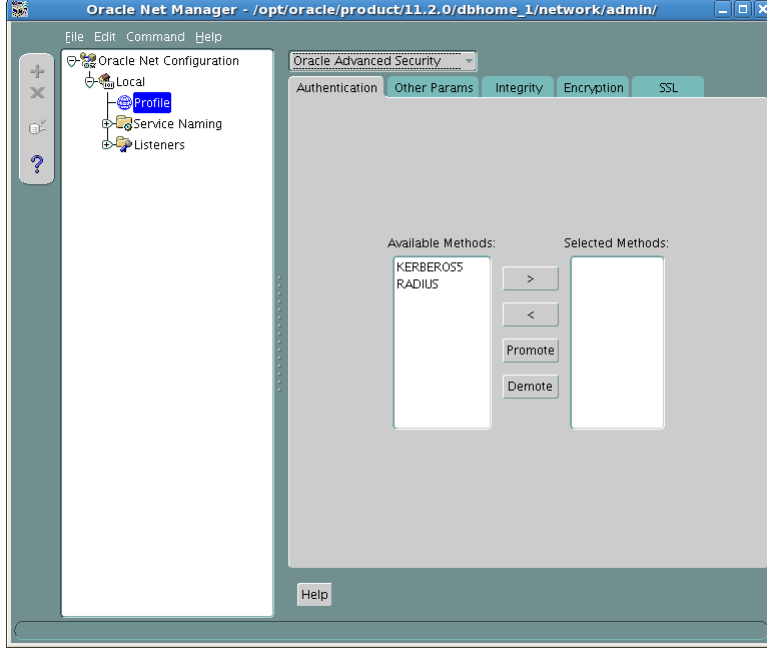
\$ORACLE_HOME/bin/netmgr

komutu kullanılır ve Şekil 4.4 de görüntülenen arayüz gelmektedir



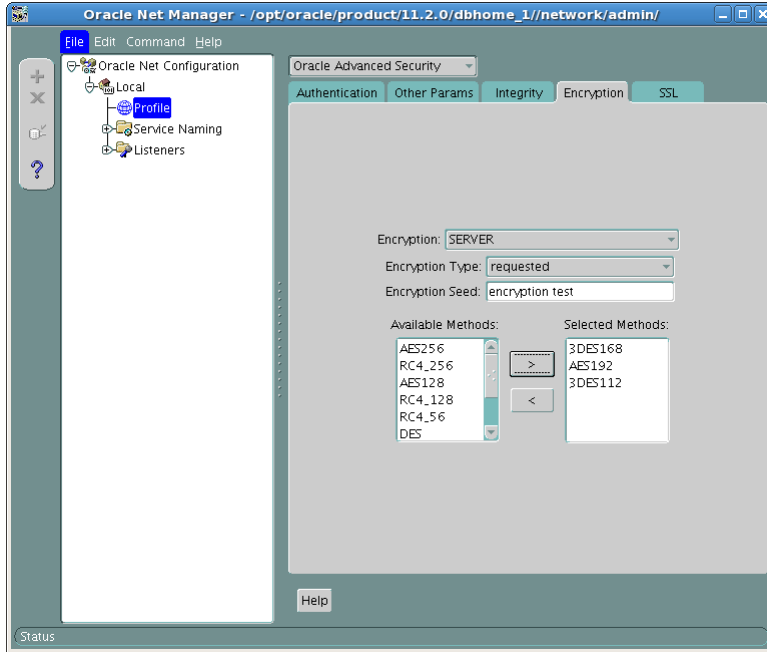
Şekil 4.4: Oracle net manager – I

Profile kısmından Advanced Security Option seçilir.



Şekil 4.5: Oracle net manager - II

Trafiğin şifrelenmesi için Şekil 4.5 de “Encryption” seçeneği seçilir ve sunucu tarafı için gerekli yapılandırma Şekil 4.6 da görülen alanlarda yapılır.



Şekil 4.6: Oracle ASO sunucu yapılandırması

“Encryption Type” için dört seçenek bulunmaktadır:

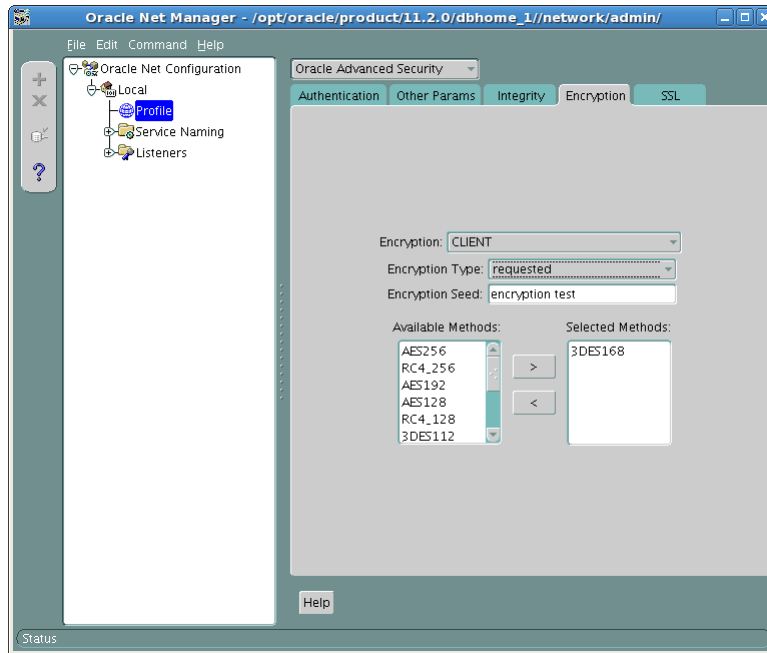
REQUIRED: Şifrelemenin gerekli olduğunu belirtir. Oracle şifrelenmemiş bağlantılara izin vermeyecektir.

REQUESTED: İsteğe bağlı olarak trafik şifrelenecektir. Hem sunucu hem istemci tarafında bu şekilde seçilmiş ise trafik şifrelenir, aksi durumda şifrelenmez.

ACCEPTED: Oracle`ın “accepted”, istemci tarafının “required” ve “requested” ayarlaması ile trafik şifreli olacaktır. Burada karar karar istemciye bırakılmıştır.

REJECTED: Şifreli trafiğe izin verilmeyeceği anlamına gelir.

İstemci tarafı için yapılması gereken değişiklikler de Şekil 4.7`de görüldüğü gibi yapılır.



Şekil 4.7: Oracle ASO istemci yapılandırması

Değişiklikler kaydedildiğinde \$ORACLE_HOME/network/admin/sqlnet.ora dosyası içine aşağıdaki bilgiler eklenecektir.

```
SQLNET.ENCRYPTION_CLIENT = requested
SQLNET.ENCRYPTION_SERVER = requested
NAMES.DIRECTORY_PATH = (TNSNAMES, EZCONNECT)
SQLNET.CRYPTO_SEED = 'encryption test'
SQLNET.ENCRYPTION_TYPES_CLIENT = (3DES168)
SQLNET.ENCRYPTION_TYPES_SERVER = (AES192, 3DES168, 3DES112)
```

Daha önce düzmetin olarak gördüğümüz trafiğin aynısı oluşturulup, tekrar yakalamak denendiğinde ise;

```
SQL> SELECT AD, SOYAD, KARTNO FROM bunyamin.KREDI_KARTI;
```

SQL cümleciğinin şifrelenmiş hali;

```
00000000 00 7c 00 00 06 00 00 00 00 00 18 d3 ad 30 98 77 .|..... ..0.w
00000010 fd 62 d7 61 df d9 b8 70 ae 25 eb 54 ad 0a 60 ba .b.a...p .%.T..`.
00000020 2e d2 59 e7 89 ad 72 54 61 b6 5c e5 bf ca 91 bf ..Y...rT a.\.....
00000030 45 fd 1c 35 41 e8 3d 6f 99 b8 30 f6 5c d2 8c e7 E..5A.=o ..0.\...
00000040 f6 2b 98 14 ca 39 07 68 a1 f4 ff e9 ae 9d 12 90 .+...9.h .....
00000050 56 ed 22 11 56 1c 5c ff da 0c 5c 7f 4d ef 26 49 V."V.\. ..\M.&I
00000060 e8 cf 03 87 9c a2 f1 b7 5d 01 c7 40 4a a6 1a ba ..... ]..@J...
00000070 7e b9 1b 75 b6 50 89 8b 50 e4 09 00 ~...u.P.. P...
```

Şekil 4.8: Şifreli veritabanı trafiği (SQL) – I

SQL sorgusu sonucu dönen verinin şifrelenmiş hali;

```
00000000 01 4c 00 00 06 00 00 00 00 00 0b 18 5d ee ad 59 .L.....].Y
00000010 3c 22 e7 7a 4b d0 36 06 d4 43 e6 59 6c 63 48 5f <".zK.6..C.YlcH_
00000020 84 c0 dd 7c 00 5c b0 49 c2 ab c6 9c 2c 9c f7 5f ...|\I....._
00000030 09 75 7b 1b fd 5b 64 68 8b 35 f8 08 33 6e 66 61 u{.[dh.5..3nfa
00000040 e5 7e c2 20 26 09 f0 37 f0 2f 34 e9 55 b9 51 08 ~. &.7./4.U.Q.
00000050 81 8e 49 2a 06 4b 5d 26 d1 54 13 03 a4 3b 46 50 ..I*K]&T...;FP
00000060 c2 7e d3 b9 ca 0a b3 e9 50 4e 14 d1 e4 ba 31 41 ~.....PN...1A
00000070 a1 47 a4 6c ca 2a 96 b1 f0 ff 2a f7 b7 55 52 1f .G1*...*.UR.
00000080 60 ee ef be cb a8 d2 46 80 5a 97 bf 1d 77 b5 ea `.....F.Z...w.
00000090 e4 f5 7b 0b 8d 19 55 d4 47 16 32 18 24 1c 80 da ..{...U.G.2.$...
000000A0 4b 63 65 86 0f 81 56 b7 71 72 7e c2 f2 b8 6d 3f Kce...V.qr~...m?
000000B0 30 a1 cc ce 2c dd ee 3a 69 25 93 97 5e ea 7d 85 0.....i%..^).
000000C0 5a 4b 95 51 8f a7 21 15 d9 5a ba cc a1 9e 88 c2 ZK.Q..l.Z.....
000000D0 8c 73 7e 3d cb f8 da 7e 26 d8 df 32 ef e1 c0 f4 .s~...~&..2....
000000E0 19 a0 18 bf b8 00 e2 6e 87 d9 64 6c 24 68 c4 ba .....n..dl$h..
000000F0 0d 3f 45 ea 88 38 1a 46 8f 91 91 aa 8d 35 48 59 .?E..8.F.....5HY
00000100 dd c5 11 12 b5 64 67 c2 40 93 61 20 93 fa 12 0f .....dg.@.a....
00000110 ee 11 f1 3a 96 8d ec 0d 65 da 53 c7 a0 2e d4 44 .....e.S...D
00000120 17 7b 80 a0 63 23 99 14 e3 01 e4 66 ed 3a 1a 50 ..{.c#.....f:P
00000130 40 b3 45 16 35 ab a6 85 37 03 1e 8b e7 e6 d1 c8 @.E.5...7.....
00000140 f5 1c 58 61 af 4e 54 70 44 97 03 00 ...Xa.NTp D...
```

Şekil 4.9: Şifreli veritabanı trafiği (Cevap) – I

Oracle ASO kullanımıyla bilgisayar ağları üzerinden geçen veritabanı trafiği şifrelenmiş olup (Şekil 4.8, Şekil 4.9), trafiği dinleyen üçüncü şahıslar tarafından elde edilen bilgilerin düz metin olmaması sağlanmıştır.

1.2. SSH Tünelleme İle Veritabanı Trafiğinin Şifrelenmesi

SSH protokolü, uzak sunuculara güvenli bağlantı kurmak için kullanılır. Normalde bir istemci ile sunucu arasındaki trafik şifreli değildir ve düz metin olarak görüntülenebilir. Fakat SSH protokolü kullanılır ise trafik güvenli hale gelmektedir. Bu yöntem SSH protokolünün üzerinden geçirdiği tüm trafiği şifreli olarak aktarmasından kaynaklanmaktadır. Tünelleme ise şu şekilde olmaktadır; istemci yerel bir port'a trafiğini gönderir. Tünelleme aracı bu port'u uzak sunucu IP adresi ve portuna yönlendirir. Fakat istemcinin yerel port'a trafiğini göndermesinden önce istemci-sunucu arasından SSH tünelleme işlemi yapılmış olmalıdır.

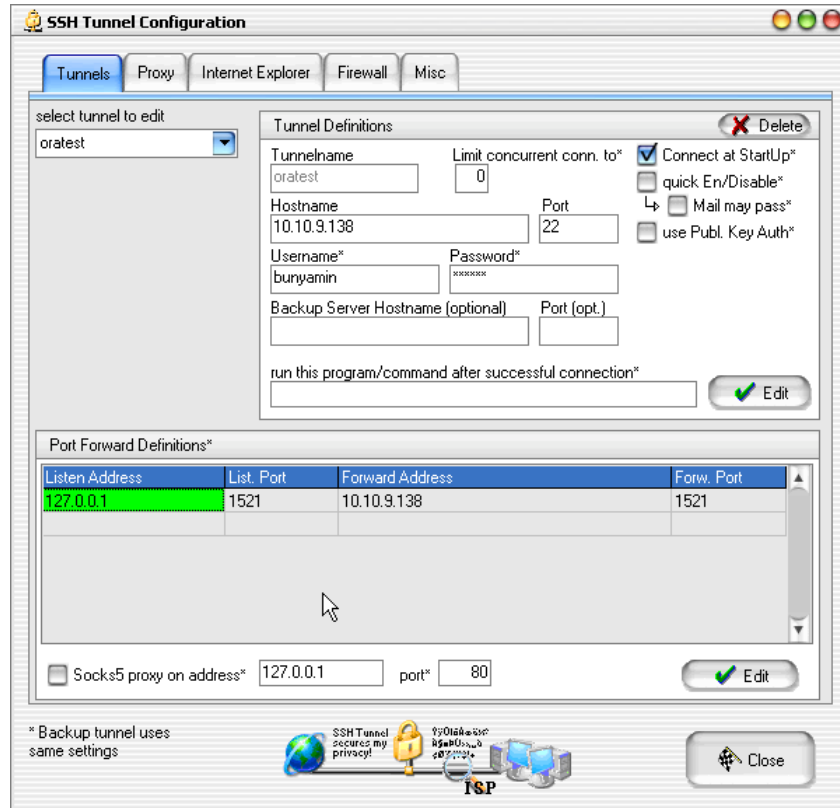
Örnek çalışma için tanımlar aşağıdaki gibi olabilir:

İstemci IP adresi 10.10.9.1

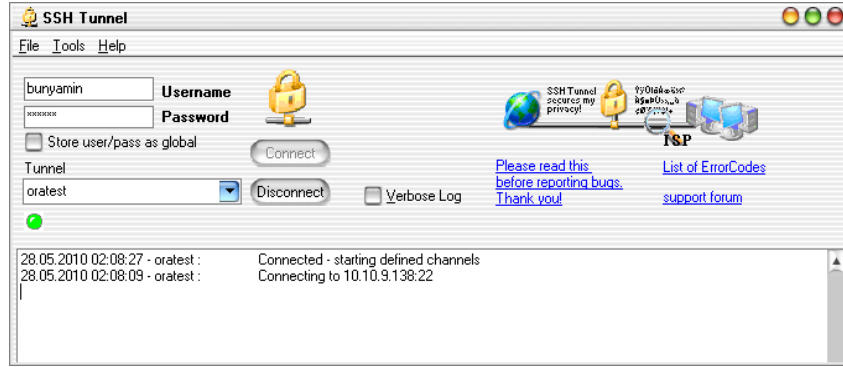
Sunucu IP adresi 10.10.9.138

Veritabanının çalıştığı port: 521

SSH bağlantısı kurulacak veritabanı üzerinde “bunyamin” adında bir işletim sistemi kullanıcısı oluşturduğum. Ardından “SSH Tunnel” uygulaması yardımı ile veritabanına bağlantı kuracak uygulama için 127.0.0.1 IP adresinin, 1521 portuna tanım yaptım. Bu port, tünelleme ile hedef veritabanı olan 10.10.9.138 sunucusunun, 1521 portuna yönlendirilmiştir. Dolayısıyla veritabanına bağlanacak olan istemcimiz artık kendi üzerine trafiği gönderecek ama kendi üzerine trafiği gönderdiği port, veritabanı sunucusuna yönlendirilmiş olacaktır. Örnek arayüz Şekil 4.10 ve Şekil 4.11’de gösterilmiştir.

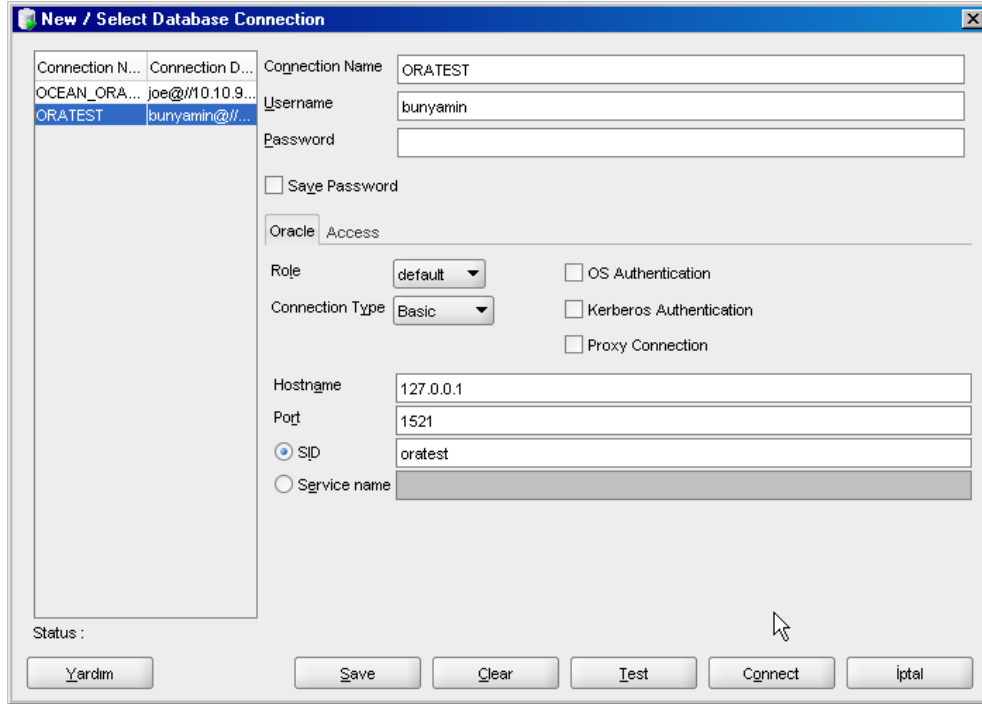


Şekil 4.10: SSH Tunnel yapılandırma arayüzü



Şekil 4.11: SSH Tunnel bağlantı arayüzü

Ardından veritabanına bağlanacak uygulama, veritabanına doğrudan bağlanmak yerine kendi üzerinde bulunduğu istemcinin 1521 nolu portuna bağlanacaktır (Şekil 4.12).



Şekil 4.12: SQL Developer bağlantı arayüzü

Diğer örneklerde olduğu gibi yine bir SQL cümlecği çalıştırıp, trafiği izleyelim.

SQL> SELECT AD, SOYAD, KARTNO FROM bunyamin.KREDI_KARTI;

SQL cümlecığının şifrelenmiş hali:

```
00000000 b2 30 62 20 c1 46 38 57 fb 14 ec 58 9b 62 20 af .0b .F8W ...X.b .
00000010 06 cb 40 47 72 39 e9 9a 07 d5 61 3f 54 1c b7 45 ..@Gr9...a?T..E
00000020 48 f8 25 b3 0a 3e 12 e3 ea 50 31 06 0f 6b 79 99 H.%...>..P1..ky.
00000030 65 cb 23 26 d8 00 ca 85 94 f4 67 87 06 28 5b 58 e.#&....g..([X
00000040 59 32 d4 61 c2 ba 76 55 10 52 c9 47 39 ca 4f 50 Y2.a..vU .R.G9.OP
00000050 94 57 0a 5f 31 61 c7 5b ff 9c aa 89 12 c4 4d 56 .W._1a.[ .....MV
00000060 f9 df 75 95 e2 c9 c6 a3 e3 92 ef b6 51 c0 28 7f ..u.....Q.(.
00000070 c9 27 be af 90 d7 f4 60 35 ff b4 44 0f 9d 93 c6 .'.....`5..D....
00000080 23 37 67 70 a6 96 fe fa e8 fb 69 f5 6b ad 9b 56 #7gp....i.k..V
00000090 f3 7f a3 bf 2f 10 ea ff d2 a7 91 8f e0 34 50 03 ..../. ....4P.
000000A0 55 e0 9e 4a U..J
```

Şekil 4.13: Şifreli veritabanı trafiği (SQL) - II

SQL sorgusu sonucu dönen verinin şifrelenmiş hali:

```
00000000 d2 31 38 ed e4 29 f6 65 be 72 00 13 9e 7e 4a 4d .18..)e .r...~JM
00000010 1a fe 4f 30 92 25 a8 ef 4e 18 08 be 57 0b 1e 0a ..00.%.. N...W...
00000020 b9 17 9d 32 7d 2e e5 e5 6b 7f 73 ef 19 93 a8 e3 ...2}... k.s.....
00000030 da 2c fa dc e6 d3 73 c1 3e f3 ac f2 c8 7d 44 5c ,.....s. >....}D\
00000040 5e 89 56 57 e8 84 af 61 4a 4b 39 e4 8c d4 34 0f ^.VW...a JK9...4.
00000050 7d 45 47 27 ad 2a c4 ab 17 2c 82 36 50 4e d4 fa }EG'.*... ,6PN..
00000060 ba 18 66 d4 e3 74 c3 cc 0b ab ac c4 e2 89 0b d6 ..f..t.. ....
00000070 0d 4f 1c 00 8c 30 91 dd d5 1f 4b 17 cf 70 d9 d9 .O...0.. ..K..p..
00000080 c9 d8 9e c6 02 43 b4 1a cb 2f 18 45 2b 19 a8 90 .....C.. /..E+...
00000090 29 45 ef 4f 3d fd d0 59 b1 08 f5 ea d3 e4 99 93 )E.O=..Y .....
000000A0 46 3d 6e bd f0 2e 27 81 4b 0a ec 4c e5 33 74 26 F=n...'. K..L.3t&
000000B0 fd 94 b6 ed 64 db 50 b4 dd d3 be 2d 24 d7 3f 51 ....d.P. ...-$.?Q
000000C0 2e e5 79 ad 09 da 63 f6 a2 62 76 35 50 ec 49 99 ..y...c. .bv5P.I.
000000D0 8f 7c d6 82 1a 1c e9 0f 88 b8 ce d5 6c a7 e3 30 .).....l..0
000000E0 53 bd 35 30 78 b2 24 36 80 82 73 78 3e 2e 8d f9 S.50x.$6 ..sx>...
000000F0 ab f9 f0 03 dd 96 7b dc 00 c7 1e 2c 9d 1d db c0 .....{. ....
00000100 c1 ae fa 33 93 93 e1 60 3a 40 24 ad b9 84 22 8c ...3...` :@$...".
00000110 84 dd 6d c7 03 5a 17 a7 5a 8d ac d9 c8 1b 2c 89 ..m..Z.. Z.....,
00000120 5d 8f 8f 9e 8f 1e 53 e1 d5 0b 9d 36 a1 a2 37 6d ]....S. ...6..7m
00000130 2b 31 fa b0 41 4b eb dd d5 ac 2f 35 0e 57 8c c0 +1..AK.. .. /5.W..
00000140 99 11 b5 b4 90 27 50 ef 8e 07 ea 0c 51 e0 35 30 .....P. ....Q.50
00000150 3e e8 bb 6b f0 30 b1 51 09 72 21 3b 43 3b 76 05 >..k.O.Q .r!;C;v.
00000160 62 28 14 9d 8e 13 ef 99 7d 69 10 3f 9f 0b b1 f1 b(..... }i.?....
00000170 14 d3 43 07 ..C.
```

Şekil 4.14: Şifreli veritabanı trafiği (Cevap) – II

Şekil 4.13 ve Şekil 4.14 de görüleceği gibi trafik şifreli hale gelmiştir.

Dolayısıyla Oracle ASO ve SSH Tunnel yardımıyla düzmetin olan veritabanı trafiğini şifreli hale getirmiş olduk. Benim tecrübelerim; iç ağ'da Oracle ASO, dış bağlantılar için ise SSH Tunnel yönteminin kullanılması yönünde. Tabii istemci sayısı gibi parametreler de performansı etkileyen unsurlar olacaktır.