ÖN BİLGİ

Bu belge

• https://www.bgasecurity.com/makale/internet-ve-yerel-ag-sizma-testleri/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

 https://www.includekarabuk.com/kitaplik/indirmeDeposu/ Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/%C4%B0nternet%20ve %20Yerel%20A%C4%9F%20S%C4%B1zma%20Testleri.pdf

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

1)

iodine ile DNS Tünelleme

iodine adlı tool kullanılarak DNS protokolü üzerinden internet erişiminin engellendiği bir yerel ağda engellerin aşılıp internete çıkılabilmektedir. Böylece ilgili ağda bulunan bilgilerin dışarıya çıkartılması mümkün hale gelmektedir. Bu tool Kali'de yüklü olarak gelmektedir. Ubuntu'da ise aşağıdaki şekilde yüklenebilir:

> sudo apt-get install iodine

Benim NOT: Kullanımı hakkında bazı bilgiler verilmiş, ama somutlaşmadığından buraya not alınmamıştır.

(Page 3)

2)

Cain & Abel Kullanarak ARP Cache Poisoning Saldırısı

// Denendi, Başarılı Olundu.

Gereksinimler

~/Downloads/Windows 7 Professional SP1 x64 - Cain _ Abel Materyaller.zip

Zip İçeriği:

- Windows 7 Professional SP1 ISO

- Cain and Abel exe

Local ağda bulunan bir bilgisayarın ağ trafiğini dinleyebilmek için Cain & Abel yazılımı ile ARP Cache Poisoning yöntemini kullanalım. Diyelim ki IP adresleri şöyle olsun:

Gateway : 192.168.2.1 Saldırgan: 192.168.2.2 Kurban : 192.168.2.6

Saldırı öncesi kurbanın ARP tablosuna bir göz atalım. Zira ARP Cache Poisoning saldırısı ile kurbanın ARP tablosunu değiştireceğimiz için farkı gözümüzle görebilelim:

C:\Windows\system32>ar	р —а	
Interface: 192.168.2.6 Internet Address 192.168.2.1	0xc Physical Address 00-1c-a8-59-5e-25	Type dynamic

(Resim Temsili)

Görüldüğü üzere kurban gateway'i (192.168.2.1'i) 00-1c-a8-59-5e-25 olarak görüyor. Şimdi saldırıya başlayalım.

Öncelikle Cain and Abel programının düzgün çalışabilmesi için şu gereksinimlerin karşılanması gerekiyor:

Cain and Abel programı çalışmak için şu adımların uygulanmasını ister:

i) Windows 7 işletim sisteminde çalışmak.

ii) Windows Güvenlik Duvarını devredışı bırakmak.

iii) Gelişmiş Güvenlik ile Birlikte Windows Güvenlik Duvarı'nda Windows Güvenlik

Duvarı Özellikleri'ni On'dan Off'a çevirmek.

iv) Yönetici olarak CMD çalıştırmak ve şu kuralı girmek:

netsh int ip set global taskoffload=disable

v) Kuralı girdikten sonra windows 7'de ethernet adaptörünü devre dışı bırakıp tekrar etkinleştirmek.

vi) Cain and Abel programını kapatıp yönetici olarak tekrar başlatmak.

Bu adımlar neticesinde Cain and Abel programında sıradaki saldırı adımları sorunsuzca uygulanabilir ve başarılı sonuç alınabilir.

Cain & Abel programı başlatılır ve saldırı yapılacak ağ arayüzünü seçmek için menudeki Configure seçilir.

File View Configure	Fools Help	Configuration Dialog ×	
Becoders Cached Passwords	iffer 🥑 😡 I	Challenge Spoofing Filters and ports HTTP Fields Traceroute Certificate Spoofing Certificates Collector Sniffer APR (Arp Poison Routing) APR-SSL Options	
Protected Storage By Protected Storage By LSA Secrets By Wireless Passwords By Trike Passwords Windows Mail Passwords	Press the + button	Adapter Fraduess Solvie Wask W Device \NPF_{08566 0.0.0 0.0.0 Device \NPF_{0957C2 192.168.0.12 255.255.0 Device \NPF_{098651 0.0.0.0 0.0.0.0 Device \NPF_{098651 0.0.0.0 0.0.0.0 Device \NPF_{098651 0.0.0.0 0.0.0.0	
		Winpcap Version 4.1.0.2980 Current Network Adapter \Device\NPF_{809F7C2C-A16A-4D0B-A701-31F73D326EAD}	
	💣 Protected Stor	WARNING !!! Only ethemet adapters supported Options Image: Start Sniffer on startup Image: Start APR on startup OK Cancel Apply Help	
http://www.oxid.it			1

Kendi adaptörümüzü (interface'imizi) seçtikten sonra Options altındaki "Start Sniffer on startup" ve "Start APR on startup" tick'lenir, ve OK butonuna basılır. Ardından sniffer işlemi aşağıdaki belirtilen butonla enable edilir.

												- • ×
File	View Configure	Tools Help										
🔄 🛃 🗞 謙 聯 🖳 🕇 ⊗ 😼 🤽 🕙 🚥 🖼 🖬 📾 📾 வ 🕼 🖇 / 1												
& Decc Start/Sto	💰 Dece Start/Stop Sniffer rk 🙀 Sniffer 🥑 Cracker 🔕 Traceroute 💷 CCDU 💖 Wireless 🚯 Query											
IP address	MAC address	OUI fingerprint	Host name	B	В	B 8	Gr	M0	M1	M3		
🖳 Hosts 😽 A	PR 🕂 Routing	👫 Passwords 🔏 VolP		_	_			_	_	_		
Activate / Deactiva	te the Sniffer											1.

Daha sonra Sniffer sekmesine gelinir.

aín											
File	/iew Configure	Tools Help									
🔄 🚳 🚱 g	CHALL CHALL	🕇 🕹 😼 🖥 🕻	m 📟 🔀 📼 🗖 % 🖉		01	2]	ī.				
🖉 Decoders	Network	Sniffer 🥑 Cracker 🔯 Trace	eroute 🔝 CCDU 🞇 Wirel	ess	🖒 Q	uery					
IP address	MAC address	OUI fingerprint	Host name	B	B	B8	Gr	M0	M1	M3	
L											
		Scan MAC Addres	ses	-							
		Resolve Host Nam	e								
		Remove	Delete								
		Remove All									
		Clear Promiscuou	s-Mode Results								
		Export									
🖳 Hosts 🗔 A	PR 🕂 Routing	Passwords 🔏 VolP									
Lost packets: 0%	•										

Sniffer ekranı gelince ekrana sağ tıklanır ve Scan MAC addresses seçilir. Sonra gelen ekrandaki pencereye OK denir.

File	View Configure	Tools Help		
🔄 🙀 🕹	NTLM SPODF SPODF AUTH RESET NTLM	🛛 🕂 🞯 😼 📴 🎦 🌆	MAC Address Scanner X	
Decoders	🔮 Network 😫	Sniffer 🥑 Cracker 🔕 Tracero	Target	
IP address	MAC address	OUI fingerprint H	F C All hosts in my subnet Gr M0 M1 M3	
192.168.0.1	001018DEAD05	BROADCOM CORPORATION	O Range	
			From 192.168.0.1 To 192.168.0.254	
			Promiscuous-Mode Scanner	
			ARP Test (Broadcast 31-bit)	
			ARP Test (Broadcast 16-bit)	
			ARP Test (Group bit)	
			ARP Test (Multicast group 0)	
			ARP Test (Multicast group 1)	
			OK Cancel	
📑 Hosts 😽	APR 🕂 Routing	👫 Passwords 🔏 VolP		
Lost packets: 09				1.

Böylece yerel ağdaki aktif bilgisayarların keşfi yapılır. Keşif işlemi bittikten sonra aşağıdaki gibi aktif cihazlar sıralanır.

Ζ										- • ×
File	View Configure	Tools Help								
🛛 🗠 😰 🕹	NTLM SPOOF SPOOF		🎫 🚾 📼 🔽	0	1 9	L				
🎉 Decoders 🙎 Network 🏟 Sniffer 🥑 Cracker 🔯 Traceroute 🔤 CCDU 💖 Wireless 🚯 Query										
IP address	MAC address	OUI fingerprint	Host name	B	B E	38 G	r M0	M1	M3	
192.168.0.1	001018DEAD05	BROADCOM CORPORATION								
192.168.0.10	3CC2435EEDC8	Nokia Corporation								
192.168.0.16	6C71D9D894D3	AzureWave Technologies, Inc								
192.168.0.11	10A5D00B98AA	Murata Manufacturing Co.,Ltd.								
📙 Hosts 😽	APR 🕂 Routing	<table-of-contents> Passwords 🛛 🔏 VolP</table-of-contents>								
Lost packets: 0	%									li.

Şimdi sıra geldi router'la kurban arasına girmeye. Bunun için öncelikle alt tarafta yer alan APR sekmesine tıklanılır. Sonra ekrandaki boş içerikli tabloya birkez tıklanılır ve böylece + butonu tıklanabilir olacağından +'ya basılır.

File View Con	figure Tools 2										
🎉 Decoders 🔮 Network 🗐 Sniffer 🥑 Cracker 🔯 Traceroute 🛄 CCDU 💖 Wireless 🚯 Query											
APR	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
APR-DNS											
APR-SSH-1 (0)											
APR-HTTPS (0)											
APR-ProxyHTTPS (0)											
APR-FTPS (0)											
APR-POP3S (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	[
APR-LDAPS (0)	Status	in uddress	mixe address	T denets +	- Tuckets	mine dualess	in dudiess				
APR-SIPS (0)											
1											
< _ >	🚱 Configuratio	on / Routed Packet	s								
🖳 Hosts 🚱 APR 🕂 Re	, puting 🚯 Passw	ords 🔏 VolP									
http://www.oxid.it									1.		

Bu tıklamalar sonucu ekrana gelen iki textarea'dan birinde gateway seçilir, diğerinde ise kurban seçilir.

		T 1 111								
	ligure	I cois Heip	LB 🕥 📷	an 🔂 📾 🖪	-	90 pa sa 4	2	×		
Decoders Network APR APR-Cert APR-ONS APR-SSH-1 (0) APR-HTTPS (0)	Stat	APR enables you directions. If a se machine has not all other hosts or	u to hijack IP traffic bet lected host has routing the same performance your LAN.	W. ween the selected capabilities WAN of a router you co	ARN traffi uld c	ING III t on the left list and a ic will be intercepted ause DoS if you set	all selected hosts on the as well. Please note th APR between your De	e right list in both nat since your sfault Gateway and		
→ R + R-RDP (0) → APR-RDP (0) → APR-FTPS (0) → APR-POP3S (0) → APR-IMAPS (0) → APR-LDAPS (0) → APR-SIPS (0)	Stat	IP address 192.168.0.1 192.168.0.10 192.168.0.16 192.168.0.11	MAC 001018DEAD05 3CC2435EEDC8 6C71D9D894D3 10A5D00B98AA	Hastname		IP address 192.168.0.11 192.168.0.16 192.168.0.10	MAC 10A5D00B98AA 6C71D9D894D3 3CC2435EEDC8	Hostname 2	-	
< >> > >> >> >> >> >> >> >> >>> >>> >>>	outing	Comparation / In Passwords	VoIP		>	<	OK	Cancel		
http://www.oxid.it										1.

NOT: Yukarıdaki ekran ilk göründüğünde sağ taraftaki textarea boş içerikle gelecektir. Ne zaman sol taraftaki textarea'dan bir hedef seçersen o zaman sağ taraftaki textarea doluverecektir.

Hedefler seçildikten sonra OK butonuna basılır ve Nükleer alarma benzeyen simgeye tıklanır.

NOT: En baştaki Configure aşamasında ayarda "başlangıçta otomatik sniff'le" dediğimiz için bu aşamada birkaç saniye içerisinde sniffing işlemi nükleer butona basmadan kendiliğinden başlayabilir ve "Idle" status'ündeki işlem "Sniffing" status'üne geçebilir.

File_View Con	figure Tools He	lp							- • •		
🎉 Decoders Start/Stop APR 🗐 Sniffer 🥑 Cracker 🔯 Traceroute 🛤 CCDU 💖 Wireless 🚯 Query											
APR	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
APR-Cert	着 Idle	192.168.0.1	001018DEAD05			6C71D9D894D3	192.168.0.16				
APR-DINS											
APR-HTTPS (0)											
APR-ProxyHTTPS (0)											
APR-RDP (0)											
APR-POP3S (0)											
APR-IMAPS (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address				
APR-LDAPS (0)											
APR-SIPS (0)											
Configuration / Routed Packets											
📕 Hosts 🕹 APR 🕂 Ro	outing 👫 Passw	ords 🔏 VolP									
Activate / Deactivate ARP Pois	on Routing								1.		

Böylece zehirleme işlemi başlar. Zehirleme işlemi ile önce kurbanın makinasına gateway olarak saldırganın MAC'i yollanır. Bunu kurbanın ARP tablosuna tekrar bakarak görebiliriz.

C:\Windows\system32>ar	p -a		
Interface: 192.168.2.6 Internet Address 192.168.2.1	0xc Physical Address 00-1a-73-fb-09-8a	Type dynamic	

(Resim Temsili)

Görüldüğü üzere kurbanın ARP tablosunda 192.168.2.1 IP adresli gateway önceden 00-1c-a8-59-5e-25 adresine sahipken şimdi 00-1a-73-fb-09-8a adresine sahiptir. Yani MAC adresi olarak kurbanın tablosuna gateway diye saldırganın makinası yerleşmiştir. Bu manipulasyon gateway'in ARP tablosunda da gerçekleştirilir ve gateway'e kurban diye saldırganın MAC'i yollanır. Böylelikle kurban paketlerini gateway'e yolluyorum diye saldırgana yollayacaktır ve saldırgan da bu paketleri gateway'e forward edecektir. Aynı zamanda gateway dışarıdan gelen paketleri kurbana yolluyorum diye saldırgana yollayacaktır ve saldırgan da bu paketleri kurbana forward edecektir. Yani kurbanın trafiği ortada yer alan saldırganın üzerinden kusursuzca geçecek ve internet erişimi forward'lar sayesinde sekteye uğramayacaktır.

Cain & Abel uygulamasında bu zehirleme işlemi sonrası yapılan dinlemelerde sniff'lenenler FTP, SMTP, HTTP, şeklinde parse edilerek sınıflandırılacaklardır. Bu sınıflandırmaları ve sniff'lenenleri görmek için programın alt sekmelerindeki Passwords'e tıklanılır.

Ξίη					
File View Confi	igure Tools Hel	р			
🗏 🛳 🐼 🐼 nữm địệ từn	🖳 🕂 🕲	B 8 54		I 🗖 😻 💋	1 ? O
Decoders 🔮 Network	🔹 Sniffer 🥑	Cracker 🔕 Tra	ceroute 🔝 CCD	U 😗 Wireless	Duery
🐴 Passwords 🔷	HTTP server	Client	Username	Password	URL
🤷 FTP (0)	46.45.187.221	192.168.0.15	hefese	deneme123*!	http://www.includekarabuk.com/
LDAP (0)					
POP3 (0)					
sqb SMB (0)					
Telnet (0)					~
		/			
MSKerb5-DreAuth					
Radius-Keys (0)					
Radius-Users (0)					
23 IKE-PSK (0)					
MySQL (0)			,		
SNMP (0)					4
	🗐 НТТР				
🗏 Hosts 🚱 APR 🕂 Ro	uting <u> </u> Passw	ords 🛛 💰 VoIP			

Lost packets: 0%

Yukarıda sniff'lenen bir HTTP hesabını görmektesiniz.

(Page 5-8)

3)

DHCP Spoofing ve DHCP Resource Starvation Denemeleri

Amacımız yerel ağda bulunan bir DHCP sunucusunun dağıtacağı IP havuzunu tüketmek ve böylece DHCP sunucusunu IP isteklerine cevap veremez hale getirmektir. Sonrasında ise saldırgan olarak biz bir DHCP sunucusu gibi davranarak kurbanlara IP dağıtmaya çalışacağız. Böylelikle yerel ağdaki başkalarının trafiğini üzerimizden geçirmiş olacağız. Öncelikle pig.py adlı tool'u kullanarak ağdaki DHCP sunucusunun tüm IP havuzunu tüketelim:

> pig.py eth0 // pig.py tool'u Kali'de yüklü olarak gelmektedir.

Betik yukarıdaki gibi çalıştırıldığında aşağıdaki gibi ardı ardına IP talep çıktıları üretecektir.

root@kali:~# pig.py eth0	
WARNING: No route found for IPv6 destination :: (no default route?)	
Sending DHCPDISCOVER on eth0	
DHCPOFFER handing out IP: 2.2.2.50	
sent DHCP Request for 2.2.2.50	
waiting for first DHCP Server response on eth0	

Sending DHCPDISCOVER on eth0	
DHCPOFFER handing out IP: 2.2.2.90	
sent DHCP Request for 2.2.2.90	
Sending DHCPDISCOVER on etho	

Havuz tükendiğinde betiğin istekleri cevapsız kalacaktır. O an geldiğinde DHCP sunucusu gibi davranalım ve başkalarının trafiğini üzerimizden geçirelim. Bunun için ettercap'i başlatalım:

> ettercap -G

Kullanacağım ağ arayüzünü seçelim ve ardından sırayla aşağıdaki resimlerin gösterdiği işlemleri yapalım.



IP Pool (optional) 5.5.5.1 Netmask 255.255.255.0 DNS Server IP 5.5.5.1	2	Server Information		
Netmask 255.255.255.0 DNS Server IP 5.5.5.1	U	IP Pool (optional)	5.5.5.1	
DNS Server IP 5.5.5.1		Netmask	255.255.2	55.0
		DNS Server IP	5.5.5.1	

Bu son resim için "saldırıda kullanılacak alanlar doldurulur" denmiş. Fakat neye göre kime göre anlaşılamadı. Bu değerler rasgele mi veriliyor?

Benim NOT: PDF bu aşamada bırakmış. Tahminimce bu son resimdeki OK butonuna basarak local ağdaki istemciler IP'yi bizden almaya başlayacaklar ve biz de bir şekilde istemcilerin trafiğini dinleyebilir konuma geleceğiz. Böylece kritik bilgileri sniff'leyebileceğiz.

(Page 9-10)

4)

Wireshark Kullanımı

Eski adı Etheral olan Wireshark açık kaynak kodlu bir sniffer aracıdır. İki tür filtreye sahiptir:

- a. Capture Filter
 - Yakalanacak paketleri belirli kriterlere (tipine, portuna, protokolüne) göre yakalatmaya capture filter denir.
- b. Display Filter
 - Yakalanmış paketler içerisinde belirlenen özelliklere sahip olanları ayıklamaya da display filter denir.

Yani capture filter ile hangi paketlerin yakalanması gerektiğini Wireshark'a söylerken display filter ile yakalanmış bir yığın paket içerisinden hangisinin gösterilmesi gerektiğini belirtiyoruz.

(Page 11) 5)

Herhangi bir pakete sağ tıklayıp "Follow TCP Stream" diyerek tıklanılan paketin içeriği okunabilmektedir. Aşağıda ip.src == 93.89.224.247 filtresi kullanılarak includekarabuk'ün paketleri sıralanmıştır ve içlerinden POST yazan HTTP paketine sağ tıklayıp Follow TCP Stream denmiştir.

Wire	shark				🏚 📅 🖇 📧 🜒 08:57 🔱
0	😣 🖻 🗈 Capturing from eth0 [Wireshark	1.10.6 (v1.10.6 from maste	r-1.10)]		
	File Edit View Go Capture Analyze Statis	tics Telephony Tools Inter	nals Help		
	🖲 🗿 🔏 📕 🙇 🚞 🕷	C Q < > 3			3 🔀 🛛 🔞
9	Filter: ip.src == 93.89.224.247	▼ Expre	ssion Clear	Apply Save	
	No. Time Source	Destination	Protocol	Length Info	
	815 11.667556000 192.168.0.12	93.89.224.247	TCP	54 49853 > http [ACK] Seq=1 Ack=1 Win=29	9200 Len=0
	816 11.667788000 192.168.0.12	93.89.224.247	HTTP	481 GET /adminPaneli/index.php HTTP/1.1	
	831 11.737640000 93.89.224.247	192.168.0.12	TCP	60 http > 49853 [ACK] Seq=1 Ack=428 Win=	=27740 Len=0
	833 11.771267000 93.89.224.247	192.168.0.12	HTTP	1176 HTTP/1.1 200 OK (text/html)	
	834 11.771296000 192.168.0.12	93.89.224.247	TCP	54 49853 > http [ACK] Seq=428 Ack=1123 V	Win=31416 Len=0
	840 11.87/396000 192.168.0.12	93.89.224.247	HITP	484 GET /TAVICON.1CO HTTP/1.1	dia-27740 Lan-0
	845 11.942001000 93.89.224.247	192.108.0.12	ICP	1028 HTTP/1 1 404 Not Found (toxt/html)	Mark Packet (toggle)
	847 11 943277000 192 168 0 12	93 89 224 247	TCP	54 49853 > http [ACK] Seg=858 Ack=2097	Ignore Packet (toggle)
	1155 17.673075000 192.168.0.12	93.89.224.247	HTTP	770 POST /adminPaneli/index.php HTTP/1.1	Set Time Reference (toggle)
<u>e</u>	1156 17.737178000 93.89.224.247	192.168.0.12	TCP	60 http > 49853 [ACK] Seg=2097 Ack=1574	Time Chift
	1157 17.856755000 93.89.224.247	192.168.0.12	HTTP	1373 HTTP/1.1 200 OK (text/html)	nine sinc
S	1158 17.856788000 192.168.0.12	93.89.224.247	TCP	54 49853 > http [ACK] Seq=1574 Ack=3416	Packet Comment
	1236 62.866555000 192.168.0.12	93.89.224.247	тср	54 [TCP Keep-Alive] 49853 > http [ACK]	Manually Resolve Address
6					Apply as Filter
	▶ Frame 1155: 770 bytes on wire (6160 bi	its), 770 bytes captured	(6160 bits)	on interface 0	
Fz	Ethernet II, Src: Asustekt_64:a9:d5 (A Internet Protocol Version 4, Src, 192)	20:CT:30:64:89:05), DST:	Broadcom_de:	ad:05 (00:10:18:de:ad:05)	Prepare a Filter
	Transmission Control Protocol Src Po	rt · 49853 (49853) Det D	ort http (86	a) Seg: 858 Ack: 2007 Len: 716	Conversation Filter
	Hypertext Transfer Protocol	(45055), bst h	ore. heep (or	, seq. 650, Ack. 2057, Een. 710	Colorize Conversation
	▶Line-based text data: application/x-w	w-form-urlencoded			SCTP 🕨
e.					Follow TCP Stream
					Follow UDP Stream
2					Follow SSL Stream
لت	0000 00 10 18 de ad 05 20 cf 30 64 ag	0 d5 08 00 45 00	0dE.		
\square	0010 02 14 30 7a 40 00 40 00 08 83 Co	44 59 e1 50 18	P :=DY.P.		Protocol Preferences •
-	0030 83 7c 01 ec 00 00 50 4f 53 54 20	2f 61 64 6d 69	PO ST /admi		Decode As
1	0040 66 50 61 66 65 6c 69 2f 69 66 64	65 78 2e 70 68 nPanel	li/ index nh		Print
	Ready to load or capture	Packets: 4539 · Displayed:	Profile: De	efault	Show Packet in New Window



Böylece includekarabuk'ün admin panelinden POST'lanan kullanıcı adı ve şifre paket içerisi açılarak okunabilmiştir.

(Page 14-15)

6)

Ziyaret Edilen Web Sitelerini Listeleme ve DOS Tespiti

Wireshark'ın Statistics menüsünden dinlenen trafikten geçen ziyaret edilmiş web sitelerini dökümünü anlık etkileşimli olarak alabilirsiniz. Bu işlem için aşağıdaki seçenekleri işaretleyin.



Ve ekrana gelen filtre kutucuğunu boş geçip Ok deyin.

Wire	Wireshark	ti, Tr 🖇 📧 ৰn) 09:05 ⊀‡
0	👩 🛯 🖙 Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]	
	File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	
- 🔁		8 5 2
9	Filter: Filter: Fxpression Clear Apply Save	
	No. Time Source Destination Protocol Length Info	0
	1679 243.22251000 192.168.0.12 93.89.224.247 TCP 54 [TCP Keep-Alive] 49853 > htt	p [ACK] Seq=1573 Ack=3416 Win=35613 Len=0
	[680 243.28613800 93.89.224.247 192.168.0.12 TCP 60 [TCP Keep-Alive ACK] http >	49853 [ACK] Seq=3416 Ack=1574 Win=8190 Len=0
	1681 246.30768800 172.217.16.99 192.168.0.12 TLSv1.2 109 Application Data	
	1682 246.30772900 192.168.0.12 172.217.16.99	Ack=4608 Win=40832 Len=0
	1083 246.300/3000 1/2, 217, 16, 99 192, 168, 6, 12	=4608 ACK=446 W1n=90112 Len=0
A	1685 246 30998204 192 168 A 12 172 217 16 99 Filter:	Ack=4607 Win=40832 Len=0
	1686 246.30998800 172.217.16.99 192.168.0.12	=4607 Ack=446 Win=90112 Len=0
~~	1687 246.31619700 172.217.16.99 192.168.0.12 Cancel Create Stat	
	1688 246.31622600 192.168.0.12 172.217.16.99 101 37.000 Seq=446	Ack=4606 Win=40832 Len=0
-	1689 246.31623200 172.217.16.99 192.168.0.12 TCP 60 https > 34518 [FIN, ACK] Seq	=4606 Ack=446 Win=90112 Len=0
	1690 246.32023900 216.58.214.227 192.168.0.12 TLSv1.2 109 Application Data	
S	S 1691 246.32026800 192.168.0.12 216.58.214.227 TCP 54 66299 > https [ACK] Seq=448	Ack=4609 Win=40832 Len=0
	1692 246.3202/600 216.58.214.22/ 192.168.0.12 TCP 60 NTTps > 60299 FFIN, ACKI Seq	=4609 ACK=448 W1n=90112 Len=0
1	▶ Frame 1679: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0	
	Ethernet II, Src: AsustekC_64:a9:d5 (20:cf:30:64:a9:d5), Dst: Broadcom_de:ad:05 (00:10:18:de:ad:05)	
12	Internet Protocol Version 4, Src: 192.168.0.12 (192.168.0.12), Dst: 93.89.224.247 (93.89.224.247)	
	▶ Transmission Control Protocol, Src Port: 49853 (49853), Dst Port: http (80), Seq: 1573, Ack: 3416, Len: 0	
\leq		
es!		
2		
Ľ	0000 00 10 18 de ad 05 20 cf 30 64 a9 d5 08 00 45 00 0dE.	
	0010 00 28 30 80 40 00 40 06 0b 4b c0 a8 00 0c 5d 59 . (0.0.0	
100		
W		
	🗧 😌 🗹 eth0: <live capture="" in="" progress=""> Packets: 5216 · Displayed: Profile: Default</live>	

Böylece ekrana ziyaret edilen web siteleri gelecektir.

Eğer dinlenilen trafikteki sadece belirli bir istemcinin ziyaret ettiği web sitelerini görmek istersek o zaman az önce gelen filtre kutucuğuna

ip.src == istemciIP

filtresi girilerek arzulanan sonuca ulaşılabilir.

Bunların yanısıra ziyaret edilen web sitelerinin görüntülendiği ekrandan bir DOS atağı yapılıp yapılmadığı da tespit edilebilir.

HTTP Requests by HTTP Host 1232 0,000 ▶ 239.255.255.250:1900 1204 0,000 ▶ www.includekarabuk.com 5 0,000 ▶ askubuntu.com 5 0,000 ▶ cdn.sstatic.net 6 0,000 ▶ istack image com 1 0.000	0747 0730 97,73% 0003 0,41% 0003 0,41%
▶ 239.255.255.250:1900 1204 0,000 ▶ www.includekarabuk.com 5 0,000 ▶ askubuntu.com 5 0,000 ▶ cdn.sstatic.net 6 0,000 ▶ istack image com 1 0.000	0730 97,73% 0003 0,41% 0003 0,41%
▶www.includekarabuk.com 5 0,000 ▶askubuntu.com 5 0,000 ▶cdn.sstatic.net 6 0,000 ▶istask image com 1 0,000	0003 0,41% 0003 0,41%
> askubuntu.com 5 0,000 > cdn.sstatic.net 6 0,000 > bictack image com 1 0,000	003 0,41%
Cdn.sstatic.net 6 0,000	
histockimaus.com 1 0.000	0004 0,49%
	0,08%
▶b.scorecardresearch.com 1 0,000	0,08%
▶ pixel.quantserve.com 1 0,000	0001 0,08%
▶engine.adzerk.net 4 0,000	0002 0,32%
▶ area51.stackexchange.com 1 0,000	0,08%
▶archive.ubuntu.com 4 0,000	002 0,32%

Görüldüğü üzere ziyaret edilen web siteleri yanında ziyaret edilme sayısı da yer almaktadır. Bu sayı aşırıya kaçtığı takdirde bu ekran bir DOS atağının habercisi olabilir.

(Benim Notum)

Network Miner ile Trafik Analizi // Denendi ve başarıldı.

Network Miner programı sniff'lenen trafik dosyaları içerisinde parse işlemi yaparak kritik bilgilere ulaşmamızı sağlayan bir madencilik programıdır. Şimdi az önce elle yaptığımız şifre bulma işini bu sefer Network Miner'a otomatize bir şekilde yaptıralım. Öncelikle az önce dinlenilen eth0 interface'inden elde edilen paketleri pcap uzantılı bir dosyaya toplayalım. Bunun için Wireshark'ın paket sniff akışını durdurman gerekir.



Ardından File -> Save As diyelim. Ekrana gelecek ayarlardan dosya ismi olarak herhangi bir şey, dosya uzantısı olarak ise wireshark/tcpdump/ – pcap diyelim.

e in folder:	home hefese		Create Folde
laces	Name	▲ Size	Modified
ft Home	Android		15-09-2015
Desktop	🚞 android-studio		19-08-2015
befese	androidStudioProjects		17-12-2015
	🚞 arachni-1.4-0.5.10		09-02-2016
evices	backports-3.16-1		30-04-2016
Computer	CodeBlocksProjects		03-05-2016
D4D8-1 📤	crunch-3.4		19-01-2016
TOSHIBA 🔺	Desktop		09:09
	Documents		05-04-2016
	Downloads		Yesterday at 01:29
	a dwhelper		30-04-2016
	EclipseProjects		07-09-2014
	a genymotion		30-09-2015
	hashcat-2.00		29-02-2016

pcap dosyamızı oluşturduktan sonra Network Miner'ı Ubuntu'ya kurmak için aşağıdaki kodları sırasıyla terminale girelim.

> sudo apt-get install libmono-winforms2.0-cil

- > wget www.netresec.com/?download=NetworkMiner -O /tmp/nm.zip
- > sudo unzip /tmp/nm.zip -d /opt/
- > cd /opt/NetworkMiner*
- > sudo chmod +x NetworkMiner.exe
- > sudo chmod -R go+w AssembledFiles/
- > sudo chmod -R go+w Captures/
- > mono NetworkMiner.exe

NOT: Eğer program zaten kuruluysa programı başlatmak için şu iki satırı girmen gerekir:

> cd /opt/NetworkMiner* > mono NetworkMiner.exe

Son kod ile NetworkMiner programı başlayacaktır.



Wireshark'tan elde ettiğimiz pcap dosyasını NetworkMiner'a verelim.





Pcap dosyası aşağıdaki gibi NetworkMiner'a yüklenecektir.

Loading PCAP file Dosvo	🗱 HAVELSAN İş 🖸 BG🏦 fınavı 🗋 myo.karabuk.edi. 🗋 Linux Yaz Kampı 🕌 H4cktimes 🔳 Siber Dergi 💽 Tu
includekarabuk.pcap	STEP 1: Install Mono 44% Ubuntu (also other Debis based distros like Xubuntu and 200 root/@hefese-N611g: (opt/Network Miner 2-0
	🛿 🖨 🗉 NetworkMiner 2.0
	File Tools Help
	Keywords Anomalies Case Panel Data Hosts (26) Files (76) Images Messages Credentials (2) Sessions (31) DNS (49) Parameters (84) File MD5 Include 29ac2
	■ 192.168.0.11 ■ 192.168.0.12 ■ 192.168.0.12 ■ 192.168.0.12 ■ 176.233.140.108 ■ 176.240.150.250 ■ 176.240.150.0250 ■ 172.217.16.100 [lous.l.google.com] ■ 172.217.18.60 [puss.l.google.com] ■ 172.217.18.60 [puss.l.google.com] ■ 172.217.18.60 [puss.l.google.com] ■ 216.58.20.20.60 [puss.l.google.com] ■ 216.58.214.225 [googlehosted.l.googleusercontent.com] ■ 216.58.214.226 [www.google.com] ■ 216.58.214.226 [googleapis.l.google.com] ■ 31.13.937.[gocgleuser.com] ■ 31.13.937.[gocgleuser.com] ■ 31.13.93.36 [star-mini.cl0r.facebook.com] ■ 93.89.2242.427 [includekarabuk.com] ■ 91.20.160.1

File Loois Help			
Keywords Anomalies		Case Panel	
Hosts (91) Files (127) Image	s (6) Messages Credentials (1) Sessions (60) DNS (197) Parameter	Filename	MD5
Show Cookies 🛛 🔽 Show N	TLM challenge-response 🔽 Mask Passwords	includekarab	29ac
Client	Server		
192.168.0.12 [HEFESE-N61]Q] 192.168.0.12 [HEFESE-N61]Q]	54.235.146.142 [engine3-774595980.us-east.1.elb.amazonaws.com] 151.101.65.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchar 151.101.65 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchan 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchanç 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchanç 104.16.112.18 [stack.imgur.com.cdn.cloudflare.net] [i.stack.imgur.co 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchanş 95.172.94.39 [anycast-europe.quantserve.com.akadns.net] [akamai- g3.89.224.247 [includekarabuk.com] [www.includekarabuk.com] 80.239.149.17 [a1294.w20.akamai.net] [b.scorecardresearch.com.ed 93.89.224.247 [includekarabuk.com] [www.includekarabuk.com]		
<	اد	Reload Case	

Paket yüklenmiştir ve parse işlemi de son bulmuştur. Credentials sekmesine geçildiğinde aşağıdaki ekran gelecektir.

😣 🗐 🗊 NetworkMiner	2.0		
File Tools Help			
Keywords Anomalies		Case Pan	el
Hosts (91) Files (127) Image	es (6) Messages Credentials (11) Sessions (60) DNS (197) Paramete	File	MD5
V Show Cookies V Show I	NTLM challenge-response J Mask Passwords	Include	29402
Client	Server		
192.168.0.12	93.89.224.247 [includekarabuk.com] [www.includekarabuk.com]		
192.168.0.12	93.89.224.247 [includekarabuk.com] [www.includekarabuk.com]		
192.168.0.12	151.101.65.69 [askubuntu.com]		
192.168.0.12	151.101.1.69 [askubuntu.com] [cdn.sstatic.net]		
192.168.0.12	104.16.112.18 [stack.imgur.com.cdn.cloudflare.net] [i.stack.imgur.com		
192.168.0.12	80.239.149.17 [a1294.w20.akamai.net] [b.scorecardresearch.com.edg		
192.168.0.12	95.172.94.39 [anycast-europe.quantserve.com.akadns.net] [akamai-pi:		
192.168.0.12	151.101.65.69 [askubuntu.com] [cdn.sstatic.net]		
192.168.0.12	54.235.146.142 [engine3-774595980.us-east-1.elb.amazonaws.com] [ε		
192.168.0.12	151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchange		
192.168.0.12 [HEFESE-N61JQ]	151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchange		
	<u>•</u>	Reload (Case Files
Running NetworkMiner with Mo	no		

Görüldüğü üzere 11 tane credential tespit edildiği söylenmiştir. Bunlardan çoğu çerez olacağı için çerezleri ayıklayalım. Bunun için Show Cookies tick'ini kaldıralım.

😣 🖨 💷 NetworkMiner 2.0	
File Tools Help	
Keywords Anomalies Hosts (91) Files (127) Images (6) Messages Credentials (1) Sessions (60) DNS (197) Paramete	Case Panel Filename MD5
Show Cookies 🔽 Show NTLM challenge-response 🛛 🗆 Mask Passwords	includekarab 29ac2
Client Server	
192.168.0.12 [HEFESE-N61]Q] 93.89.224.247 [includekarabuk.com] [www.includekarabuk.com]	Reload Case Files
Running NetworkMiner with Mono	

Geriye bir tane credential kalmıştır. İşte o bizim includekarabuk'ün admin panelinden POST ettiğimiz kullanıcı adı ve şifreyi tutmaktadır. Kullanıcı adı ve şifreyi çekmek için sırasıyla ilgili satıra sağ tıklanır ve bir Copy username denir, bir de Copy Password denir. Böylece admin hesap bilgileri elimize geçmiş olur.

😣 🗐 🗊 Network Miner 2	2.0	
File Tools Help		
Keywords Anomalies Hosts (91) Files (127) Images	s (6) Messages Credentials (1) Sessions (60) DNS (197) Parameter TLM challenge-response	Case Panel Filename MD5 includekarab 29ac2
Client	Server	
192.168.0.12 [HEFESE-N61JQ]	93.89.224 A 7 Te ductores to an intermediate dekarabuk.com]	
Running NetworkMiner with Mon	0	

😣 🖱 🗊 NetworkMiner 2.0	
File Tools Help	
Keywords Anomalies Hosts (91) Files (127) Images (6) Messages Credentials (1) Sessions (60) DNS (197) Parametr	Case Panel Filename MD5
J Show Cookies M Show NTLM challenge-response J Mask Passwords	
Client Server 192.168.0.12 [HEFESE-N61JO] 93.89.224.247 [includ Copy Username Copy Password Auto-resize all columns	4
	Keload Case Files
Running NetworkMiner with Mono	

Sonuç olarak fark ettiysen Wireshark'ta kullanıcı adı ve şifreyi bulmak için onca paket yığını içerisinde boğuşuyorduk ve elimizle filtreler girerek sonuca ulaşmaya çalışıyorduk. NetworkMiner'da ise bu filtreleme işini bizim yerimize NetworkMiner yapıyor ve şıp diye trafik içerisinde bulduğu kullanıcı adı ve şifreyi önümüze sunuyor.

(Page 17-20)