

LAB – Sử dụng công cụ Cain & Abel



Mô tả

Cain & Abel là chương trình tìm mật khẩu hoạt động trên hệ điều hành Windows. Nó cho phép dễ dàng tìm ra nhiều loại mật khẩu bằng cách dò tìm trên mạng, giải mã các mật khẩu đã mã hóa bằng các phương pháp Dictionary, Brute-force and Cryptanalysis, ghi âm các cuộc đàm thoại qua đường VoIP, giải mã các mật khẩu đã được bảo vệ dựa trên các kỹ thuật lưu trữ mật khẩu, phát hiện mật khẩu có trong bộ đệm và phân tích các giao thức định tuyến.

Chương trình này không khai thác những lỗ hổng chưa được vá của bất kỳ phần mềm nào. Nó tập trung vào những khía cạnh/điểm yếu hiện có trong các chuẩn giao thức, các phương pháp đăng nhập và các kỹ thuật đệm. Mục đích chính của công cụ này là tìm ra mật khẩu và những thông tin cần thiết từ nhiều nguồn.

Trong bài Lab này ta dùng Cain & Abel để làm thay đổi bảng ARP hay giả mạo địa chỉ MAC của những thiết bị được giám sát và từ đó có thể phân tích nội dung của lưu lượng, có được các thông tin nhạy cảm từ một số giao thức cụ thể.

Cấu hình trên Router

```
Router#show run
Building configuration...
Current configuration : 1174 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
```



no service password-encryption ! hostname Router 1 memory-size iomem 15 ip subnet-zero ! ip cef 1 interface FastEthernet0/0 ip address dhcp ip nat outside ip virtual-reassembly duplex auto speed auto ! interface FastEthernet0/1 ip address 192.168.1.1 255.255.255.0 ip nat inside ip virtual-reassembly I. ip classless ip http server no ip http secure-server ip nat inside source list 1 interface FastEthernet0/0 overload access-list 1 permit 192.168.1.0 0.0.0.255

Cấu hình CAIN

Bật tính năng Sniffer (hình 1).

Chọn tab Sniffer \rightarrow chọn vào dấu "+" để quét các host đang tồn tại trong mạng tấn công. Trong cấu hình này ta chọn quét tất cả các host trong subnet (192.168.1.x/24) \rightarrow chọn "OK" (hình 2). Xem kết quả ở hình 3.

Trong tab Sniffer -> chọn tab APR (hình 4).

Start ARP Poisoning \rightarrow bấm chuột vào dấu "+" để chọn host cần tấn công (bên trái) và Default Gateway Router (bên phải) \rightarrow bấm "OK" \rightarrow xem kết quả hình 5.

CÔNG TY TNHH TƯ VÁN VÀ DỊCH VỤ CHUYÊN VIỆT TRUNG TÂM TIN HỌC VNPRO



ĐC: 276 - 278 Ung Văn Khiêm, P.25, Q.Binh Thạnh, Tp Hồ Chí Minh **Đ**T: (028) 35124257 | **Hotline:** 0933427079 **Email:** vnpro@vnpro.org

		Sniffer 🔐 Cracker	Traceroute	Wireless	D Q	uery				
ress	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	MO M	11 M3	
				1			_			
					-				-	
					_					
					_			_	-	
					-				-	

Hình 1: Bật Sniffer

lress	MAC address	OUI fingerprint	Host name	B31	B16 B8	3 Gr	MO	M1 M	43	
			MAE Address Scanner		2	4				
			Target • All hosts in my subn • Range From 192:.168 To 192:.168 Promiscuous-Mode Sca ARP Test (Broadca ARP Test (Mulicast AIT Test	et 1	4					
					Cancel					

Hình 2: Quét các Host

CÔNG TY TNHH TƯ VÁN VÀ DỊCH VỤ CHUYÊN VIỆT TRUNG TÂM TIN HỌC VNPRO

DC: 276 - 278 Ung Văn Khiêm, P.25, Q.Bình Thạnh, Tp Hồ Chí Minh DT: (028) 35124257 | Hotline: 0933427079 Email: vnpro@vnpro.org



ddress	MAC address	OUI fingerprint	Host name	B	1 816	B8	Gr	MO	M1	M3	
168.1.1	001F6C6E90A1	Cisco Systems									
168.1.50	001A803D141D	Sony Corporation			_						
						-	-				
						_		-			
						-					
										-	
						_	-				
					-			-			
					-	-					
						_	-	-		_	
							-				
					-		-	-		-	
						-					
						-		-		-	
					_	_					
					-	-	-	-			
					_	-					
						-	-	-			
					-						

Hình 3: Kết quả

Tile View Config	ire Tools Help								<u>- 8 ×</u>
	H + 0 I	B 64 🕤 🔤	I 📟 🔀 🖃 🕻	3 📽 💋	0 ?	i			
🖉 Decoders 🔮 Network	📓 Sniffer 🥑	Cracker 🧕 T	raceroute 🔝 CC	DU 😗 Wire	eless 🚯 Q	juery			
APR APR-Cert (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address		
APR-DNS									
APR-HTTPS (0)									
APR-RUP (0)									
APR-POP35 (0)									
APR-LDAPS (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address		
	-								
	• • • • •			<u> </u>		1			
	Configurat	on / Routed Packet:	<u> </u>						
Hosts 🚱 APR 🕁 Ri	outing 🦷 Passi	vords 🌠 🌾 VoIP]						
🛃 Start 🛛 🚱 🧶 »		1	3 - Paint					🛃 🌒 -	4:01 PM

Website: www.vnpro.vn | Forum: www.vnpro.org | Video: https://www.youtube.com/@vnpro149

- 0



Hình 4: Chọn APR



Hình 5

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
Idle	192.168.1.50	001A803D141D	0	0	001F6C6E90A1	192.168.1.1	
Chabue	TD addrocc	MMC addrard	Darkete	- Dackate	MAC address	10 address	
Didids	Tr ddio55	I nime address	- duots * 2	- roundls	mine address		
						-	



Hình 6:

addracc	MAC address	OUIT fingerprint	Host name		B14	89	Gr	MO	MI	MB	
2.168.1.1	001F6C6E90A1	Cisco Systems	nuscriane	65.	010	DO	l or	MO	1 141	Pla	
2.168.1.50	001A803D141D	Sony Corporation									
					_						
					-	-					
					-	-					
					-						

Hình 7









ĐC: 276 - 278 Ung Văn Khiêm, P.25, Q.Binh Thạnh, Tp Hồ Chí Minh **Đ**T: (028) 35124257 | **Hotline**: 0933427079 **Email**: vnpro@vnpro.org

_ 8 ×

V mPro
YnPro

	Statur		Mac address	Dacketr ->	eless Ep c	Mac address	ID address	
PR-Cert (0) PR-DN5 PR-SSH-1 (0) PR-HTTPS (0) PR-RDP (0) PR-FTPS (0) PR-POP35 (0)	Idle	192.168.1.50	001A803D141D	0	0	001F6C6E90A1	192.168.1.1	
PR-IMAPS (0) PR-LDAPS (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
				-				
	L							
	L							
	L							
					-		-	
	-							
	Castin	wation / Dauted Dasks			<u>.</u>		10 A	



Kiểm tra

Đến bước này bạn đã hoàn tất việc chuẩn bị bắt gói và thu thập các thông tin. Bước tiếp theo tiến hành kiểm tra xem khi một máy tính nằm trong mạng, truy cập vào hộp thư Yahoo mail có độ bảo mật rất cao có thể bị lấy mất username và password không?

1. Đăng nhập vào hộp thư Yahoo (hình 10).

2. Sau khi nhập username và password \rightarrow chọn "Đăng Nhập".

Bình thường sau khi bấm "Đăng Nhập" ta sẽ vào ngay hộp thư của mình nhưng nhìn hình ta thấy trình duyệt IE 7.0 thông báo "*There is a problem with this website's security certificate*" như vậy là có vấn đề xảy ra và thông tin username và password của user đã bị mất (hình 11).

3. Bấm chuột vào hàng chữ "*Continue to this website (not recommended)*" khi đó ta sẽ vào được hộp mail của mình.

4. Giờ ta sẽ kiểm tra trước và sau khi bật tính năng ARP Poisoning đã tác động như thế nào đến máy VICTIM (hình 12, 13)?

CÔNG TY TNHH TƯ VĂN VÀ DỊCH VỤ CHUYÊN VIỆT TRUNG TÂM TIN HỌC VNPRO



DC: 276 - 278 Ung Vân Khiêm, P.25, Q.Binh Thạnh, Tp Hồ Chí Minh DT: (028) 35124257 | Hotline: 0933427079 Email: vnpro@vnpro.org



Hình 10: Đăng nhập Yahoo



Hình 11: Cảnh báo bảo mật

Trước

	Pro			CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT TRUNG TÂM TIN HỌC VNPRO ĐC: 276 - 278 Ung Văn Khiểm, P.25, Q.Binh Thạnh, Tẹ Hồ Chí Minh ĐT: (028) 35124257 Hotline: 0933427079 Email: vnpro@vnpro.org
	C:\Users\quocle>arp -a			
	Interface: 192.168.1.50 Internet Address 192.168.1.1	0x9 Physical Address 00-1f-6c-6e-90-a1	Type dynamic	
	C:\Users\quocle>_			
		Hình I	12	
Sau				

C:\Users\quocle>arp -a		
Interface: 192.168.1.50 Internet Address 192.168.1.1 192.168.1.40	0x9 Physical Address 00-1f-c6-06-ad-2b 00-1f-c6-06-ad-2b	Type dynamic dynamic

Hình 13

Kết quả: Máy 192.168.1.50 đã bị giả mạo địa chỉ MAC khiến cho các gói tin đi từ 192.168.1.50 ra Gateway giờ bị chuyển tiếp sang ATTACKER (192.168.1.40).

5. Kiểm tra CAIN để lấy thông tin username và password đã bắt được. Xem kết quả hình 2.16 phần được tô màu xanh đậm

File View Configu	ure Tools <u>H</u> elp					
🛛 🖾 🕼 🥹 ATAM REBER AN	₩ + ♥ № '		8 🖬 🔲 🐇	8 💴 🕐 😵		
😤 Decoders 🔮 Network	🕻 🎒 Sniffer 🥑 Crac	ker 🧟 Traceroute	CCDU	🖞 Wireless 🚯 🤇	Query	
Passwords	Timestamp	HTTP server	Client	Username	Password	URL
- 🙅 FTP (0)	12/02/2009 - 16:03:08	203.84.204.124	192.168.1.50	13ea3n5th/N=	6f0kWHxsfevSj	http://vn.yahoo.com/?p=us
- 🔄 HTTP (22)	12/02/2009 - 16:03:41	124.108.125.235	192.168.1.50	1	0	vn.yahoo.com
	12/02/2009 - 16:03:42	203.84.204.124	192.168.1.50	13e3e605u/N=	RXbu6nxsfeu09	http://vn.yahoo.com/?p=us
- 📴 LDAP (0)	12/02/2009 - 16:03:45	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/?p=us
	12/02/2009 - 16:03:45	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com//p=us
որի SMB (0)	12/02/2009 - 16:03:45	124.100.125.235	102 169 1 50	1	0	nicup://vin.yanoo.com//p=us
Telnet (0)	12/02/2009 - 16:03:51	200.72.142.74	192,160,1,50	I ITSoiffor122	122454	https://logip.upbog.com/config/mpi28.cvc-um8.inth-up
	12/02/2009 - 16:04:12	203.84.204.124	192 168 1 50	13edi2po2/N-	9cbPEpyscem09	http://wp.mc766.mail.vaboo.com/mc/welcome2action=8VV=1546
TDS (0)	12/02/2009 - 16:04:12	124 108 103 241	192 168 1 50	http://wp.mc76	1234436388/	http://www.weidemanager.com/st2ad_type=iframe&ad_size=180x15
TNS (0)	12/02/2009 - 16:04:13	124,108,103,241	192,168,1.50	http://www.mc76	1234436388/1	http://ad.vieldmanager.com/st?ad_type=iframe&ad_size=300x25
	12/02/2009 - 16:05:16	124,108,125,235	192,168,1.50	1	0	http://doi.yolananagoricon/scrod_cypo-inanodad_size-ocosec
SMIP (U)	12/02/2009 - 16:05:18	203.84.204.124	192,168,1,50	13er3ic46/N=k	b4XiRnxsfeu09	http://vn.vahoo.com/
NNIP (U)	12/02/2009 - 16:05:20	124.108.125.235	192.168.1.50	1	0	http://vn.vahoo.com/
DCE/RPC (0)	12/02/2009 - 16:05:20	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/
MSKerb5-PreAuth (0)	12/02/2009 - 16:05:20	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/
🛛 🤲 Radius-Keys (0)	12/02/2009 - 16:05:27	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/
Radius-Users (0)	12/02/2009 - 16:05:41	124.108.125.235	192.168.1.50	1	0	vn.yahoo.com
	12/02/2009 - 16:05:43	203.84.204.124	192.168.1.50	13e4eg0gj/N=	8EOwW3xsfeu	http://vn.yahoo.com/?p=us
- 5 IKE-PSK (0)	12/02/2009 - 16:05:46	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/?p=us
- Ro MySOL (III)	12/02/2009 - 16:05:46	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/?p=us
SNMP (0)	12/02/2009 - 16:05:47	124.108.125.235	192.168.1.50	1	0	http://vn.yahoo.com/?p=us
GRE/PPP (0)	-					
PPPOE (U)						
				-		
					-	
	-					
	1082.5					
	 ∢					Þ
	📑 НТТР					
Harte 🔿 ADD 🛧 D	outing B Decouverde					
	odding 17 Passwords	100 VOLP				
Lost packets: 0%		Transferrer Constant	1			
🕂 Start 🛛 🚱 🎒 🍣 😵]]	🦉 7 - Paint				🛃 🎒 4:06 PM

Hình 14

