## Labo Hacking (90 min)

0	Introduction s	udo ./c 2
	<ul> <li>Ce travail pratique sous Windows 7 illustre les attaques suivantes : <ol> <li>Crack d'un mot de passe avec l'outil Cain – 20 min</li> <li>\$1.7 à \$1.9 → excel (privé ou AAI)</li> </ol> </li> <li>Man-in-the-Middle pour voler username-password d'une session telnet – 20</li> <li>Man-in-the_Middle pour voler username-password d'une session https – 30</li> <li>Forger un paquet ARP malicieux afin de produite l'attaque ARP poisoning -</li> </ul>	) min ) min - 10 min
Important	<b>Ce travail exige une préparation</b> Etudier les paragraphes 2.1, 3.1.1, 3.1.2, 3.1.4, 4.4, 5.3 et 5.4 du document <u>http://www.tdeig.ch/windows/Authentification_LM_NTLM.pdf</u>	
Action	Ouvrir une session utilisateur Username=albert password=admin sous Windows7 Copier le dossier <u>\\10.2.1.1\doc1abo\Secu\Hacking</u> sur le bureau	
1	Username – Password	20 min
Objectif	Tester la résistance d'un mot de passe	
But 1.1	Créer 2 comptes utilisateur	
Action	Ouvrir une <b>session administrateur</b> Clic-droit sur Computer (bureau) – Manage – Continue Sélectionner Local Users and Groups Clic-droit sur le dossier Users – New User Décocher User must change password at next logon Cocher Password never expires Create – Close User=alice Pass=jensen	
	User=bob Pass=qawsed	
But 1.2	Afficher le contenu du fichier SAM avec pwdump	
Action	Clic-droit sur Command Prompt (bureau) – Run as administrator – Yes Dans le dossier C:\Users\albert\Desktop\Hacking ,exécuter pwdump7 –h pour connaître les possibilités de cette commande pwdump7 pour afficher le contenu du fichier SAM	
Résultat Administrat Guest:501:N albert:1001	Chaque ligne correspond à un compte Les divers champs d'une ligne sont séparés par : for:500:NO PASSWORD************************************	0C089C0::: **::: E634:::
But 1.3	Mots de passe d'un dictionnaire	

Action Clic sur dictionary.txt pour afficher la liste des mots de passe de ce dictionnaire

## But 1.4 Lire le fichier SAM

# Action Clic-droit sur Cain (bureau) – Run as administrator – Yes Clic sur l'onglet **Cracker** (barre d'outils)

Clic dans la zone blanche puis la touche « Insert » du clavier - Next

🎉 Decoders 🔮 Network 關 Snit	ffer 🥑 Cracker 🔇	Traceroute	CC	DU 😗 Wirel	ess	
💰 Cracker 🖌	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
IM & NTLM Hashes (6)	Administrator	* empty *	*	* empty *	AAD3B435B	31D6CFE0D16AE931B73C59D7E0C089C0
MTLMv2 Hashes (0)	🗙 albert	* empty *	*	•	AAD3B435B	209C6174DA490CAEB422F3FA5A7AE634
MS-Cache Hashes (0)	X alice	* empty *	*		AAD3B435B	7CB1264F4D1CE6C93A1611369337CB08
PWL files (0)	🗙 bob	* empty *	*		AAD3B435B	B235C9712FA566E6B6432935FB51C8D9
Cisco IOS-MD5 Hashes (0)	Guest	* empty *	*	* empty *	AAD3B435B	31D6CFE0D16AE931B73C59D7E0C089C0
Cisco PIX-MD5 Hashes (0)	🗙 ursula	* empty *	*		AAD3B435B	57D583AA46D571502AAD4BB7AEA09C70

Cain affiche le contenu du fichier SAM

But 1.5	Cracker le mot de passe d'alice avec le dictionnaire
Action	Sélectionner la ligne alice – clic droit – Dictionary Attack – NTLM hashes Clic droit dans la zone « Dictionary » - Add to list – C:\\Dictionary.txt Start
But 1.6	Cracker le mot de passe de bob avec la méthode dictionnaire puis brute-force
Action	Refaire l'opération précédente (attaque par dictionnaire) avec bob mais ne pas oublier de faire un « reset » avec clic droit sur la zone « Dictionary » - Reset initial file position
	Pour l'attaque en brute force, clic droit sur bob – Brute-Force-Attack – NTLM Hashes Limiter le jeu de caractères utilisés aux lettres Start
	Observer la valeur affichée pour Current password
Question 1a	Quelle est la valeur moyenne du Key Rate
Question 1b	Appuyer simultanément sur Ctrl Maj Esc pour répondre à la question Quelle est la charge CPU affichée par le Task Manager – onglet Performance ?
Action	Utiliser la calculette CryptMe pour effectuer les §1.7 à 1.9 à domicile Elle se trouve sur le site web www.tdeig.ch dans le dossier contenant les documents du cours
But 1.7	Puissance de calcul de Charly
	Utiliser la calculette CryptMe – onglet Attaques pour estimer la puissance de calcul de votre ennemi
	Comparer les valeurs affichées avec votre mesure 1a
But 1.8	Résistance du mot de passe
Action	Utiliser la calculette CryptMe – onglet Résistance
But 1.9	Longueur du mot de passe
Action	Utiliser la calculette CryptMe – onglet Longueur du mot de passe

2	Charly vole username	& password donnant a	accès au serveur 10.2.1.3	<b>20 min</b>		
Réseau	PC1 (victime Alice), PC2 utilisé par Charly et le serveur 10.2.1.3 (Bob) sont reliés par un commutateu Ethernet. Le serveur DHCP fournit des adresses en 10.2.2.X					
	PC1 Alice Victime DHCP	PC2 Charly Hacker	Bob Serveur Telnet			
			10,2,1,3			
		Switch Ethernet 1Gbit/s				
But 2.1	Trouver les adresses E	thernet & IP d'Alice et	Charly			
	Noter ces valeurs <ul> <li>Alice (PC1) :</li> <li>Charly (PC2) :</li> <li>Bob</li> </ul>	Ethernet = Ethernet = Ethernet =	IP = IP = IP = 10.2.1.3			
Question 2a	Comment avez-vous pro Expliquer votre méthodo	océdé ? logie				
But 2.2	Utiliser l'outil Cain pou	r effectuer l'attaque A	RP poisoning			
Action	Suivre les étapes décrite	es dans les <mark>pages 7 à 9</mark>	de ce document			
	Alice établit une connex password = <mark>123</mark>	on <b>telnet</b> (Command P	rompt) sur le serveur 10.2.1	.3 avec username = <mark>test</mark> et		
Question 2b	Lors de l'attaque ARP p	pisoning, quelle est l'ent	rée erronée présente dans	le cache ARP d'Alice ?		
Question 2c	Cain a-t-il récupéré les p	paramètres username-p	assword? Si oui pourquoi	?		
But 2.3	Analyse Wireshark telr	net_10.2.1.3				
Action	Ouvrir l'acquisition telne	t_10.2.1.3.pcap				
<u> telnet_10.2</u> .	1.3.pcapng [Wireshark 1.4	3.3 (SVN Rev 45256 from	/trunk-1.8)]			
<u>File E</u> dit <u>V</u> iev	w <u>G</u> o <u>C</u> apture <u>A</u> nalyze	Statistics Telephony Too	ols <u>I</u> nternals <u>H</u> elp	······································		
	NN BBX	224 9	🔊 🖓 🕹 🛛 🔳 🖪			



-

Expression... Clear Apply

Save

Filter: telnet



#### Installer ce certificat

ertificate
General Details Certification Path
Certificate Information
Windows does not have enough information to verify this certificate.
Issued to: localhost.localdomain
Issued by: VMware Installer
Valid from 21. 03. 2013 to 19. 09. 2024
Install Certificate Issuer State
ext – Next – Finish
onfirmer
ertificate Import Wizard
The import was successful.
ОК
<u> </u>
<b>`</b>
Install Certificate
arn more about <u>certificates</u>
OK
nore
Currie warning
Certificate Warnings
guaranteed. Depending on your security policy, this issue might not represent a security con You may need to install a trusted SSL certificate on your server to prevent this warning from appearing.
The certificate received from "10.2.1.4" was issued for "localhost.localdomain". Secure communication with "10.2.1.4" cannot be guaranteed. Ensure that the fully-qualified domain name on the certificate matches the address of the server you are trying to connect to.

Click Ignore to continue using the current SSL certificate. View Certificate Ignore Cancel  $\boldsymbol{<}$ □ Install this certificate and do not display any security warnings for "10.2.1.4".

Documents	Aidez-vous au besoin des documents ci-dessous pour répondre aux questions http://www.oxid.it/ca_um/topics/apr-https.htm
	http://www.oxid.it/ca_um/topics/certificates_collector.htm
	http://www.oxid.it/ca_um/topics/sniffer_related_taqs.htm
	<u>Intp://www.oxid.it/ca_diff/topics/api_felated_faqs.ntm</u>
Question 3a	Qui a généré le certificat reçu par Alice ?
Question 3b	Contrôler avec un navigateur la présence du certificat
Question 3c	Quelles sont les différences entre ce certificat et celui envoyé par Bob ?
Question 3d	Quelle est la procédure pour retrouver le username-password dans Caïn ?
Question 3e	Comment contrer cette attaque ?
4	Forger un paquet ARP malicieux afin de produite l'attaque ARP poisoning10 min
Introduction	L'outil Colasoft permet de forger (construire) un paquet. Il est très utile lors de tests spécifiques et lors d'attaques.
Rappel	Le cache ARP est mis à jour dynamiquement grâce au couple d'adresses source Ethernet – IP présentes dans l'en-tête ARP (voir ex 1)
Configuration	<ul> <li>Vous avez besoin de 2 PC sous Windows 7 pour les scénarios suivants :</li> <li>Alice = Victime = PC1</li> <li>Bob = 10.2.1.1</li> <li>Charly = Hacker = PC2</li> </ul>
But 4.1	Afficher le contenu du cache ARP de la victime Alice
Remarque	Par défaut, PC1 et PC2 obtiennent leur configuration IP par DHCP. Le service DHCP, fourni par le firewall pfSense, attribue l'adresse IP 10.2.2.X en fonction de l'adresse Ethernet reçue dans la demande selon une liste blanche qui sera étudiée au prochain labo.
Action	Sur PC1 (Alice),
	arp -a Pour connaître le contenu du cache ARP
Q_4a	Quelle est l'adresse Ethernet du serveur 10.2.1.1 ?
But 4.2	<b>Corrompre la table ARP de la victime Alice</b> Forger le paquet <b>ARP response</b> capable de créer l'entrée IP=10.2.1.1 : Eth = aa:bb:cc:dd:ee:ff dans le cache ARP de <b>PC1</b>
Action	Sur <b>PC2 (Charly)</b> , Exécuter <b>pktbuilder_1.0.1.177.exe</b> avec les droits admin Bouton Add Select Template: ARP Packet – Ok
Q_4b	Quelles valeurs donner aux divers champs ?
Test	Clic droit sur le paquet n°1 à droite – Send Selected Packet Contrôler l'effet dans le cache ARP d'Alice

## Utilisation du logiciel Cain 4.9.36

## 1) Activer la vue Sniffer

Eile View Configure	Tools <u>H</u> elp		•	- 1	
Decoders Network	+ W Ba Per M	reroute 🕅 CCDU % Wirele	Ø °		
IP address MAC address	OUI fingerprint	Host name	B31	B16	B8
	$\mathbf{X}$				
4					
🖳 Hosts 🐼 APR 🕂 Routing	g 🕅 Passwords 🔏 VoIP				
ttp://www.oxid.it					

## 2) Sélection ner l'interface réseau avec Configure

Filters and b		Tracemute	Cartificata Specifica
Sniffer	APR (Arp Poisor	Routing) C	Centificate Spoofing
Adapter		IP address	Subnet Mask
Devic	e\NPF_{CE14504 e\NPF_{AACAB0	10.1. <mark>40.9</mark> 4 192.168.1.46	255.255.0.0 255.255.255.0
Winpcap 4.1.0.200	Version		
Current N	etwork Adapter	themet adapters of	innoted
Options -	Sniffer on startup APP on startup	Don't use Prom	iscuous mode

3) Activer le Sniffer

🔄 🙀 🕹	CHALL CHALL NTLM SPOOF SPOO AUTH RESET NTLH		B B 64
😤 Decoders	🔮 Network	Sniffer	G Cracker
4) Ajouter les é	éléments 🦯		W

## 5) Sélectionner l'adresse IP d'Alice = 10.1.40.26

ange.					
All h	iosts in	my su	bnet		
Han	ige				
Fro	m				2
	10 .	1	40	8	26
To	-				
	10 .	1	40	æ	26
ARF ARF ARF	PTest ( PTest ( PTest ( PTest ( PTest (	Broad Broad Broad Group Multic	cast 3 cast 1 cast 8 (bit) ast gr	31-Е 16-Е 3-Бі оцр	oit) oit) ;) o O)

6) idem pour l'adresse IP de **Bob** Dans mon cas

IP address	MAC address
10.2.2.7	E0CB4E252FB1
10.2.2.26	5404A6D18CDB

## 7) Activer la vue APR (Arp Poison Routing)

			acercuita 🛄 CCC				
APR APR-Cert	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
APR-POP3S (0) APR-IMAPS (0) APR-LDAPS (0) APR-LDAPS (0)	🕉 Configur	ation / Routed Packets					
Hosts APR + R	outing 💦 Pas	sswords 🔏 VoIP					

8) Sélectionner la zone puis Ajouter

### 9) Dans mon cas . Alice = 10.2.2.26 et Bob = 10.2.2.7

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
de Ide	10.2.2.26	5404A6D18CDB	1		E0CB4E252FB1	10.2.2.7	

## Appelez le prof pour qu'il valide cette attaque !

10) Lancer I'ARP Poisoning



### 11) Observer le changement d'état

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.2.2.26	5404A6D18CDB	0	0	E0CB4E252FB1	10.2.2.7

## 12) Alice établit une session telnet

## 13) Observer le résultat dans la vue Passwords/

Passwords	Started	Closed	Telnet server	Client	Status	File
FTP (0) HTTP (0)	08/03/2013 - 16:27:33		10.2.2.7	10.2.2.20	Reco View	
IMAP (0) LDAP (0)					Remo	ove Delete
0 POP3 (0) 1 SMB (0)					-	
VNC (0)						

## 14) Extraire Username & Password

Telnet-201338152733531-49212 - Notepad	
File Edit Format View Help	
Telnet server could not log you in using NTLM authentication. Your password may have expired. Login using username and password Welcome to Microsoft Telnet Service login: tteesst password: 123	sniffer generated file =====
-[1;1HMicrosoft Telnet Server. 23'364'864 bytes free-[25;1HC:\Users\test>	+[2;1H*======
	-

#### Liens

http://www.oxid.it/ca\_um/ http://www.oxid.it/ca\_um/topics/promiscuous-mode\_scanner.htm

User Manual

http://www.oxid.it/ca\_um/topics/mac\_scanner.htm

http://www.oxid.it/ca\_um/topics/configuration.htm

http://www.oxid.it/ca um/topics/route table manager.htm

http://www.oxid.it/ca um/topics/apr.htm

http://www.oxid.it/ca\_um/topics/apr-https.htm