#### Zakład Systemów Złożonych

#### Politechnika Rzeszowska

# BEZPIECZEŃSTWO SYSTEMÓW I SIECI KOMPUTEROWYCH

#### Laboratorium zdalne nr 9:

Metody łamania haseł na przykładzie Windows 8.1

## 1. Uzyskiwanie dostępu do konta lokalnego.

Aby uzyskać dostęp do konta lokalnego z zapomnianym lub nieznanym hasłem potrzebujemy tylko płyty z zainstalowanym systemem operacyjnym.



Windows 8.1 z utworzonymi użytkownikami

Następnie należy w ustawieniach BIOS (w tym przypadku w ustawieniach programu) bootowanie z płyty, pendrive, obrazu płyty w zależności od tego jakim nośnikiem z systemem dysponujemy.

9	Oracle VM VirtualBox Manager	+ _ 🗆 ×
File Machine Help	Windows 8.1 - Settings	? ×
New Se System Display Storage Audio Network Serial Ports USB Shared Folders Storage Network	e Attributes Information Kore Information Kore Ko	E Primary Master  Choose a virtual CD/DVD disk file pl_windows_7_professional_with_sp1_x64_dvd_u_676944.iso ubuntu-14.04-desktop-amd64.iso pl_windows_8_1_x64_dvd_2707401.iso debian-live-7.7.0-amd64-standard.iso Remove disk from virtual drive
SAIA PORT U: SAIA PORT U: Mational Host Driver: Mational Controller: In	Indows DirectSound tel HD Audio	Cancel Help

Dodawanie obrazu ISO do bootowania systemu który atakujemy

Po wybraniu kolejności bootowania w BIOS (zmianie ustawień w systemie wirtualnym). Należy zapisać zmiany i ponownie uruchomić system.

	Windows 8.1 [Running] - Oracle VM VirtualBox	↔	-		×
Machine View Devices Help					
	k				
	🖆 Instalator systemu Windows 🕞 🗉 💌				
	Windows <sup>®</sup> 8				
	Język, który chcesz zainstalować: Polski (Polska) 🗸 🗸				
	Format godziny i waluty: Polski (Polska)				
	Mawatura lub metoda wprowadzama: Polski (programisty)				
	Wprowadź język i inne preferencje, a następnie kliknij przycisk Dalej, aby kontynuować.				
	© 2013 Microsoft Corporation. Wszelkie prawa zastrzeżone. Dalej				
		ļ .			
		🗀 🖷 🔘 🕻	👌 Ŧ Rigi	ht Contr	rol

Menu wyboru języka

Gdy po zaakceptowaniu bootowania instalacji systemu pojawi się powyższe menu należy wybrać odpowiadające nam języki i klikamy przycisk "Dalej"



Menu wyboru instalacji lub naprawy systemu.

Po pojawieniu się powyższego okna należy wybrać opcję "Napraw komputer".



Menu wyboru dalszych czynności.

Następnie wybieramy opcję **Rozwiąż problemy** → **Opcje zaawansowane** → **Wiersz polecenia**.



Uruchomiony wiersz poleceń

Po przejściu przez wybrane opcje powinnyśmy uzyskać okno konsoli (cmd).

📸 Windows 8.1 [Running] - Oracle VM VirtualB	ox 🗢 🗆 🗙
Machine View Devices Help	
Administrator: X:\windows\SYSTEM32\cmd.exe	
Microsoft Windows [Version 6.3.9600]	<u>^</u>
X:\Sources>c:	
C:∖>dir Uslume in drive C is Zastrzeżone przez system Uslume Sarial Number is 6400-5188	
Directory of G:	
2015-01-08 19:43 0 Recovery.txt 1 File(s) 0 bytes 0 Div(s) 92 450 816 bytes free	
C:∖>e:	
E:\>dir Volume in drive E is IRM_CCSA_X64FRE_PL-PL_DU5 Volume Serial Number is FEA7-9557	
Directory of E:\	
2013-08-23         00:37         128         autorun.inf           2013-08-23         00:37         427         600           2013-08-23         00:37         427         600           2013-08-23         00:37         12128         hockneys.efi           2013-08-23         00:37         12128         hockneys.efi           2013-08-23         00:37         77         42         setup.exe           2013-08-23         00:37         77         742         setup.exe           2013-08-23         00:37         CDTA         sources         sources           2013-08-23         00:37         CDTA         sources         sources	
E: \>d:	
D:∖>dir Volune in drive D has no label. Volune Serial Number is A002-9E67	
Directory of D:\	
2013-08-22       16:22       (D1R)       PerfLogs         2015-01-08       18:38       (D1R)       Program Files         2013-08-22       16:36       (D1R)       Program Files         2015-01-07       2015-40       (D1R)       Ulars         2015-01-07       16:59       16:948       979       36         2015-01-07       16:948       979       36       bytes	
D:\>	
	🙍 💿 🤌 🖶 🥅 📾 🔟 🛛 🐼 💽 Right Control 🔬

Wyszukiwanie dysku z atakowanym systemem operacyjnym.

Następnie za pomocą poleceń "**c**:", "**dir**", "**dir**" itd. odnajdujemy dysk zawierający zainstalowany system operacyjny na którym próbujemy zmienić zapomniane hasło.



Podmiana pliku Utlman.exe na plik cmd.exe.

Gdy odnaleźliśmy atakowany system następnie musimy przejść do folderu System32 poleceniem: *cd Windows/System32*. Po poprawnym przejściu do folderu musimy utworzyć kopie 2 plików: *cmd.exe (copy cmd.exe cmdKOPIA.exe), Utilman.exe (copy Utilman.exe UtilmanKopia.exe)*. Program *cmd.exe* to nic innego jak nasz konsola systemowa. Program *Utilman.exe* jest to Centrum ułatwień dostępu. Dlaczego wybieramy ten program zobaczycie w następnych krokach. Po utworzeniu kopii plików wykonywalnych programów należy usunąć plik *Utilman.exe* (del Utilman.exe), a następnie zmienić nazwę plikowi *cmdKOPIA.exe* na Utilman.exe (rename cmdKOPIA.exe Utilman.exe). Po zakończeniu tych czynności wpisujemy polecenie exit aby wyjść z konsoli. Następnie w menu klikamy "*Kontynuuj*".



Uruchomienie konsoli z poziomu logowania do systemu.

Po uruchomieniu się systemu podczas gdy wygląd ekranu logowania nie uległ zmianie, należy kliknąć na ikonę zaznaczoną czerwonym kółkiem. Jest to podmieniony program Centrum ułatwień dostępu na konsole systemową.



Zmiana hasła atakowanego konta lokalnego.

Następnie wpisujemy polecenie: **net user**, które wyświetla wszystkich użytkowników komputera. Gdy zobaczymy listę użytkowników należy wybrać z niej użytkownika któremu chcemy zmienić hasło poleceniem (konto: Alojzy): **net user Alojzy Test1**. (Nazwa konta: Alojzy, nowe hasło dla konta: Test1). Następnie poleceniem **exit** wychodzimy z konsoli. Hasło na naszym koncie zostało zmienione i już uzyskaliśmy dostęp do konta. Aby przywrócić poprzednią funkcję aplikacji Utilman.exe należy wykonać polecenia od Printscreen 2.3 do Printscreen 2.8 do polecenia **cd Windows/System32** włącznie. Następnie należy usunąć plik Utilman.exe (**del Utilman.exe**), następnie zmienić nazwę pliku *UtilmanKOPIA.exe* na *Utilman.exe* (**rename UtilmanKOPIA.exe Utilman.exe**). Wpisać komendę **exit** i następnie wybrać "Kontynuuj".



## 2. Uzyskiwanie dostępu do danych konta Microsoft.

Windows 8.1 z utworzonym użytkownikiem z hasłem (konto Microsoft)

Wszystko robimy w taki sam sposób jak w przykładzie z kontem lokalnym do PrintScreena 3.9., ponieważ nie możemy zmienić w konsoli hasła użytkownika z poziomu konsoli systemowej musimy uaktywnić konto Administratora w systemie (domyślnie jest ono nieaktywne). Jedyne co możemy to uzyskać dostęp do wszystkich plików których używał dany użytkownik aby odzyskać/ukraść najważniejsze dokumenty użytkownika.



PrintScreen 2.2: Uruchomienie konsoli z poziomu logowania do systemu.



Aktywowanie konta Administratora.

Następnie należy uruchomić ponownie komputer.



Wybór konta do zalogowania.

Uzyskujemy dostęp do wszystkich plików systemu, ponieważ mamy uprawnienia Administratora więc także dostęp do folderu Moje dokumentu użytkownika atakowanego.



Dostęp do danych z konta Jan Kowalski (konto Microsoft).

#### 3. Kon-Boot 2.3

Za pomocą programu Kon-Boot można bez znajomości hasła użytkownika dostać się do systemu operacyjnego. Należy przygotować bootowalną płytą lub pendriva i po ponownym uruchomieniu komputera pojawi się poniższe okno. Następnie po załadowaniu systemu każde stworzone konto nie będzie posiadało hasła. Jedynym minusem tego rozwiązania jest brak możliwości zalogowanie się na konto połączone z kontem Microsoft (hasło nie ulega zmianie). Po wyjęciu bootowalnej płyty bądź pendrive wszystko wraca do stanu poprzedniego (o ile nie dokonaliśmy żadnych zmian w koncie na które się logowaliśmy). Jest to bardzo wygodne narzędzie jeżeli potrzebujemy bardzo szybkiego dostępu do każdego konta.



Okno ładowania programu Kon-Boot.

# 4. Windows Password Recorvery

Za pomocą programu Windows Password Recorvery można w sposób bardzo szybki uzyskać hasła wszystkich użytkowników utworzonych na komputerze. Niestety program ten jest programem płatnym, a w wersji testowej program odkrywa tylko pierwsze 3 litery hasła. Jednak na potrzeby laboratorium na utworzonych obrazach jest pełna wersja programu.



Menu start z wyszukaniem programu Windows Password Recorvery.



Uruchomione okno programu Windows Password Recorvery.

Po uruchomieniu programu należy wybrać opcję import aby aplikacja mogła pobrać pliki z zaszyfrowanymi hasłami systemu.

<b>1</b>	Windows 8.1 [Running] - Oracle VM VirtualBox	+ _ 8 ×
Machine View Devices He	le Windows Password Recovery - Empty project	- 5
Project Recovery	Cold     Agent     Totols     Options       Cold     Listers     Agent	jien * Tores = 🗗 -
💡 There may be some things bett	er than sex, and some things worse than sex. But there is nothing exactly like it.	Customize
Recent Projects     Recent Projects     Recent Projects     Paiget     Open a project     Swe the project a     Swe the project a     Create new project a     Create new project a     Create new project     Lads then local computer     Lads then rence computer     Lads then rence computer     Lads then binary friel     Lads then advente rencement     Lads then advente rencement     Lads then advente rencement	Contrage and Agence and Agence A	
Help Great for Updates Help About	Andre song and the song an	
• ****		
2012 - 101 12:50 January 14 2015+	Pogun name - repone Pogun name - repone Recented alower: 100 cm - Application strated Installational course #100(2010) Error 500(2010)	Â
4 ê		- 計量型 () - <sup>10,17</sup> 2015-01-16
		📓 🕓 🖉 🚍 📾 🚺 🔞 🖲 Right Cantrol

Import plików zawierających hasła.

Madrie Vere Deutse Mei
Windows Recovery - ROLECTIM - 0
Source Series Records and Series
hapot boxt Fourt. Rev Open Pennolo
Passwords Guine
Hathes Project
River must be some thinks where the source than see, but there is nothing reach like it. Curtomer
Project     Y # X { SuitApp. Habes Propers Report Hadaway monitor     S
Receit Projects Common statistics
Project • Time-legand: Omnis Time-left: Inclus
Open a project         Current spand (hit)         13 231 497         Average spand (hit)         13 804 623
Modestal Met 25/24 Curver mode: complex short passwords
■ See the project
Cristiane point Password Statistics
Rober Passworkstal Passworksded. 80.241.143
Last password here to a computer Last password here to the total stepped: 0
s coad how results computer
I not the harp files
Los de na aconte progue
Overall progress
Rep •
Crex or guard
🖏 hep
le Aout
Log window
2 10.1452. Innany 14.2015 Looking for current see's passwords step 4
© 101454 January 14015 - 2 MILM hadre to be recovered
2 MiRS/ analys (M205 – 2 unique tables to be found
10.1853 known yi 42015     Stating recevery (preliminary attack)
© 101857 Invary 14205 Four NTLM personal for user Basic (Inve)
manufacture prefining attack in proper, dated at 101853 January 14
- F G 20 - F

Odzyskiwanie haseł wszystkich użytkowników systemu.

Długość odzyskiwania hasła zależy z ilu i jakich znaków się składa. Najprostsze hasła odszyfrowane są w parę sekund, a te bardziej złożone ze znaków specjalnych są dużo cięższe do rozszyfrowania i może to trwać ok. 10 minut.

				Windows 8.1 [Running] - Oracle VM Virtu	alBox		+	- 8 ×
Machine View Deices Help								
123				Windows Password Recovery - PROJ	EKTMM			- 0 ×
Project Recovery	Edit Report Tools	Utils Options						ilew - Theres - 🕖 -
3 5 3 1	Save							
Inport Export Export New	Open Dave as							
Passwords	Close							
	rogen							
There may be some things better !	than sex, and some things wors	e than sex. But ther	re is nothing exactly like it.					Customize
⊕ ⊕ Project ♥ ₽ X	4 Start Page Hash	es Progress	Report Hardware mo	star	111 back	17 beach	function .	Þ
Recent Projects *	Username	KU LM P	distance ini passa	ora	UM NASH	NINDO	Description	
Project *	Administrator	300	Empty> 🧧 <em< td=""><td>pty&gt;</td><td></td><td>310700400000000016004 44860000 4 PB</td><td>Vibudowane konto do administrowania ko</td><td></td></em<>	pty>		310700400000000016004 44860000 4 PB	Vibudowane konto do administrowania ko	
🙆 Open a project	C Allopy	1004	Empty given	iy-u=s		21F1E0490623210C10F0444630080486 85DEEEC3013E0177828680AE04008776		
	Coric	501	Employ Excert	the second s		CONTRACTOR DE LA CONTRACTORIZICA DE LA CONTRACTOR DE LA C	Whistoware konto do dortero do komost	
🚽 Save the project	HomeGroupUserS	1003	Empty> C/N	*** idle6+ChKC^dGA8>M0/*?A/REAT+pmC<_Po6-Wso9EvielMv5*1A-Y**@5*Htl8/P8157V		1022C886224AA91863C8509CC88873A9	Wbudowane konto dostepu do komputera	
🛃 Save the project as	an Kowalski	1001 🧧 <	Empty> 🙀 proje	ial		EA58E256776D0AF9259F2874EB178D18		
Create new project	-							
Hashes *								
Load from local computer								
Solution and from remote computer								
Inport from binary files								
Load from another program								
South the second								
Help *								
Check for Updates								
🛟 Help								
About								
Lonwindow								a ×
10:18-54 January 14:20155	2 unique hashes to be found							4
10:10:54 January 14 2015>	Stating recovery (preliminary	attacki						~
10:18:57 January 14 2015>	Found NTLM password for use	er Basia: (love)						
2 10:20:02 January 14 2015>	Stopping recovery (preliminan	v attack)						
10:20:02 January 14 2015>	Found NTLM password for use	er Alojzy: (gwerty/@	(#\$)					
10:20:02 January 14 2015>	Recovery stopped							_
www.passcape.com Users: 6, Sel	ected users: 0, Passwords four	nd: 6 (100.0%)					Pesswards found durin	g last session: 2 (33.)
📢 🙆 🚞 📗	3							2 (0 10.21 2015-01-14
							0 0 p = a (	🛯 👔 🖲 Right Control

Odszyfrowane wszystkie hasła systemu Windows.