Lab 3: Hash Methods

You will be assigned a folder in vCentre. Navigate to Production->crypto->netxx and then startup your Kali instance.

Demo: http://youtu.be/Xvbk2nSzEPk

1 Hashing

No	Description	Result

1	On Kali, login and get an IP address using:
	`sudo dhclient eth0`
	
	Next, download an update to hashcat with:
	`sudo apt-get install hashcat`	

2	Using (either on your Windows desktop or on Kali):
	
	`http://asecuritysite.com/encryption/md5`
	
	Match the hash signatures with their words ("Falkirk", "Edinburgh", "Glasgow" and "Stirling").
	
	`03CF54D8CE19777B12732B8C50B3B66F`
	`D586293D554981ED611AB7B01316D2D5`
	`48E935332AADEC763F2C82CDB4601A25`
	`EE19033300A54DF2FA41DB9881B4B723`
		`03CF5:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?
		
		`D5862:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?
		
		`48E93:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?
		
		`EE190:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?

3	Using (either on your Windows desktop or on Kali): `http://asecuritysite.com/encryption/md5` Determine the number of hex characters in the following hash signatures.	MD5 hex chars: SHA-1 hex chars: SHA-256 hex chars:

		SHA-384 hex chars: SHA-512 hex chars: How does the number of hex characters relate to the length of the hash signature:

4	From your Windows desktop or Kali, for the following /etc/shadow file, determine the matching password:
	
	`bill:$apr1$waZS/8Tm$jDZmiZBct/c2hysERcZ3m1`
	`mike:$apr1$mKfrJquI$KxOCL9krmqhCuOSHKqp5Q0`
	`fred:$apr1$Jbe/hCIb$/k3A4kjpJyC06BUUaPRKsO`
	`ian:$apr1$OGyPhsLi$jTTzWOHNS4Cl5ZEoyFLjB.`
	`jane: $1$rqOIRBBN$R2pOQH9egTTVN1Nlst2U7.`
		The passwords are password, napier, inkwell and Ankle123.
		[Hint: openssl passwd -apr1 -salt ZaZS/8TF napier]
		
		Bill's password:
		
		Mike's password:
		
		Fred's password:
		
		Ian's password:
		
		Jane's password:

5	From your Windows desktop or Kali, download the following:
	
	`http://asecuritysite.com/files02.zip`
	
	and the files should have the following MD5 signatures:
	
	`MD5(1.txt)= 5d41402abc4b2a76b9719d911017c592`
	`MD5(2.txt)= 69faab6268350295550de7d587bc323d`
	`MD5(3.txt)= fea0f1f6fede90bd0a925b4194deac11`
	`MD5(4.txt)= d89b56f81cd7b82856231e662429bcf2`
		Which file(s) have been modified:

6	From your Windows desktop or Kali, download the following ZIP file:
	
	`http://asecuritysite.com/letters.zip`
	
	View the Postscript files using:
	
	`http://view.samurajdata.se/`
		Outline what the letters contain:
		
		Now determine the MD5 signature for them. What can you observe from the result?

7	Select either Windows or Kali for this part:
	
	On Kali, download the following ZIP file and run the two programs, and run them in a command console:
	
	`http://asecuritysite.com/files01u.zip`
	
	Or on Windows, download the following ZIP file and run the two programs, and run them in a command console:
	
	`http://asecuritysite.com/files01.zip`
		What do the programs do?
		
		Now determine the MD5 signature for them. What can you observe from the result?

2 Hashing Cracking (MD5)

No	Description	Result

1	On Kali, next create a words file (**words**) with the words of "napier", "password" "Ankle123" and "inkwell"
	
	Using hashcat crack the following MD5 signatures (hash1):
	`232DD5D7274E0D662F36C575A3BD634C`
	`5F4DCC3B5AA765D61D8327DEB882CF99`
	`6D5875265D1979BDAD1C8A8F383C5FF5`
	`04013F78ACCFEC9B673005FC6F20698D`
	Command used: `hashcat -m 0 hash1 words`
		`232DD...634C` Is it [napier][password][Ankle123][inkwell]?
		
		`5F4DC...CF99` Is it [napier][password][Ankle123][inkwell]?
		
		`6D587...5FF5` Is it [napier][password][Ankle123][inkwell]?
		
		`04013...698D` Is it [napier][password][Ankle123][inkwell]?

2	Using the method used in the first part of this tutorial, find crack the following for names of fruits (the fruits are all in lowercase): FE01D67A002DFA0F3AC084298142ECCD 1F3870BE274F6C49B3E31A0C6728957F 72B302BF297A228A75730123EFEF7C41 8893DC16B1B2534BAB7B03727145A2BB 889560D93572D538078CE1578567B91A	FE01D: 1F387: 72B30: 8893D: 88956:

3 Hashing Cracking (LM Hash/Windows)

All of the passwords in this section are in lowercase.

No	Description	Result
1	On Kali, and using John the Ripper, and using a word list with the names of fruits, crack the following pwdump passwords: fred:500:E79E56A8E5C6F8FEAAD3B435B51404EE:5EBE7DFA074DA8EE8AEF1FAA2BBDE876::: bert:501:10EAF413723CBB15AAD3B435B51404EE:CA8E025E9893E8CE3D2CBF847FC56814:::	Fred: Bert:
2	On Kali, and using John the Ripper, the following pwdump passwords (they are names of major Scottish cities/towns): Admin:500:629E2BA1C0338CE0AAD3B435B51404EE:9408CB400B20ABA3DFEC054D2B6EE5A1::: fred:501:33E58ABB4D723E5EE72C57EF50F76A05:4DFC4E7AA65D71FD4E06D061871C05F2::: bert:502:BC2B6A869601E4D9AAD3B435B51404EE:2D8947D98F0B09A88DC9FCD6E546A711:::	Admin: Fred: Bert:
3	On Kali, and using John the Ripper, crack the following pwdump passwords (they are the names of animals): fred:500:5A8BB08EFF0D416AAAD3B435B51404EE:85A2ED1CA59D0479B1E3406972AB1928::: bert:501:C6E4266FEBEBD6A8AAD3B435B51404EE:0B9957E8BED733E0350C703AC1CDA822::: admin:502::333CB006680FAF0A417EAF50CFAC29C3:D2EDBC29463C40E76297119421D2A707:::	Fred: Bert: Admin:

Repeat all 3.1, 3.2 and 3.3 using **Ophcrack**, and the rainbow table contained on the instance (rainbow_tables_xp_free).