Chapter five

- What is Social Engineering?
- How social engineering Works?
- Common Social Engineering Techniques
- Social Engineering Counter Measures

60

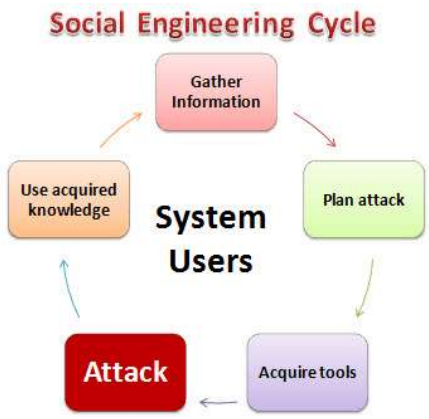
What is social engineering

- **Social engineering** is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system.
- The term can also include activities such as **exploiting human kindness, greed, and curiosity** to gain access to restricted access buildings or getting the users to installing backdoor software.
- Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems

61

- هندسةاجتماعيةهو فن التلاعب بمستخدمي نظام الحوسبة للكشف عن المعلوماتالسرية التي يمكن استخدامها للوصول غير المصرح به إلى نظامالكمبيوتر.
- يمكنأن يشمل المصطلح أيضاً أنشطة مثلاستغلال اللطف والجشع والفضولالبشريللوصول إلى المباني المقيدة الوصول أو حمل المستخدمينعلى تثبيت برامج الباب الخلفي.
- تعدمعرفة الحيل التي يستخدمها المتسللون لخداع المستخدمين لإصدار معلوماتتسجيل الدخول الحيوية من بين أمور أخرى أمراً أساسياً في حماية أنظمةالكمبيوتر

How social engineering Works?



62

- تجميعالمعلومات:هذه هي المرحلة الأولى ، يتعلم بقدر ما يستطيع عن الضحية المقصودة.يتم جمع المعلومات من مواقع الشركة ومنشورات أخرى وأحياناً من خلالالتحدث إلى مستخدمي النظام المستهدف.
- هجومالخطة:يحدد المهاجمون كيف ينوي تنفيذ الهجوم
- اكتسابالأدوات:يتضمن ذلك برامج الكمبيوتر التي سيستخدمها المهاجم عند شنالهجوم.
- هجوم:استغلال نقاط الضعف في النظام المستهدف.
- استخدامالمعرفة المكتسبة:يتم استخدام المعلومات التي تم جمعها أثناء تكتيكاتالهندسة الاجتماعية مثل أسماء الحيوانات الأليفة وتواريخ ميلاد مؤسسيالمؤسسة وما إلى ذلك في هجمات مثل تخمين كلمة المرور

How social engineering Works?-cont.

- **Gather Information:** This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.
- **Plan Attack:** The attackers outline how he/she intends to execute the attack
- **Acquire Tools:** These include computer programs that an attacker will use when launching the attack.
- **Attack:** Exploit the weaknesses in the target system.
- **Use acquired knowledge:** Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing

63

استغلال الألفة: المستخدمون أقل تشككاً في الأشخاص الذين يعرفونهم. يمكن للمهاجم التعرف على مستخدمي النظام المستهدف قبل هجوم الهندسة الاجتماعية. قد يتفاعل المهاجم مع المستخدمين أثناء الوجبات ، وعندما يدخن المستخدمون ، قد ينضم إليهم ، في المناسبات الاجتماعية ، وما إلى ذلك. وهذا يجعل المهاجم مألوفاً للمستخدمين. لنفترض أن المستخدم يعمل في مبنى يتطلب رمز وصول أو بطاقة للوصول ؛ قد يتبع المهاجم المستخدمين عند دخولهم هذه الأماكن. يفضل المستخدمون إبقاء الباب مفتوحاً للمهاجم للدخول كما هو معتاد عليهم. يمكن للمهاجم أيضاً أن يطلب إجابات لأسئلة مثل المكان الذي قابلت فيه زوجتك ، واسم مدرس الرياضيات في المدرسة الثانوية ، وما إلى ذلك. من المرجح أن يكشف المستخدمون عن إجابات لأنهم يثقون في الوجه المألوف.

Common Social Engineering Techniques

- **Familiarity Exploit:** Users are less suspicious of people they are familiar with. An attacker can familiarize him/herself with the users of the target system prior to the social engineering attack. The attacker may interact with users during meals, when users are smoking he may join, on social events, etc. This makes the attacker familiar to the users. Let's suppose that the user works in a building that requires an access code or card to gain access; the attacker may follow the users as they enter such places. The users are most like to hold the door open for the attacker to go in as they are familiar with them. The attacker can also ask for answers to questions such as where you met your spouse, the name of your high school math teacher, etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password.

64

ظروف التخويف: يميل الناس إلى تجنب الأشخاص الذين يخيفون الآخرين من حولهم. باستخدام هذه التقنية ، قد يتظاهر المهاجم بوجود حجة ساخنة على الهاتف أو مع شريك في المخطط. قد يطلب المهاجم بعد ذلك من المستخدمين معلومات يمكن استخدامها لتهديد أمن نظام المستخدمين. من المرجح أن يقدم المستخدمون الإجابات الصحيحة فقط لتجنب المواجهة مع المهاجم. يمكن أيضاً استخدام هذه التقنية لتجنب الفحص عند نقطة تفتيش أمنية.

Common Social Engineering Techniques-cont.

- **Intimidating Circumstances:** People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on the phone or with an accomplice in the scheme. The attacker may then ask users for information which would be used to compromise the security of the users' system. The users are most likely give the correct answers just to avoid having a confrontation with the attacker. This technique can also be used to avoid been checked at a security check point.

65

Common Social Engineering Techniques-cont.

- **Phishing:** This technique uses trickery and deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as Yahoo and then ask the unsuspecting user to confirm their account name and password. This technique could also be used to get credit card information or any other valuable personal data.

- التصيد:تستخدم هذه التقنية الخداع والخداع للحصول على بيانات خاصة من المستخدمين.قد يحاول المهندس الاجتماعي انتحال شخصية موقع ويب حقيقيمثل Yahoo ثم يطلب من المستخدم المطمئن تأكيد اسم حسابه وكلمةالمرور. يمكن أيضاً استخدام هذه التقنية للحصول على معلومات بطاقة الائتمانأو أي بيانات شخصية أخرى ذات قيمة.

66

66

Common Social Engineering Techniques-cont.

- **Tailgating:** This technique involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area.

- الذيل:تتضمن هذه التقنية متابعة المستخدمين خلفهم عند دخولهم مناطق محظورة.من باب المجاملة البشرية ، من المرجح أن يسمح المستخدم للمهندسالاجتماعي بالدخول إلى المنطقة المحظورة.

67

67

Common Social Engineering Techniques-cont.

- **Exploiting human curiosity**: Using this technique, the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus, or the user may be tempted to open a file with a name such as Employees Revaluation Report 2013.docx which may actually be an infected file.

- استغلال فضول الإنسان: باستخدام هذه التقنية ، قد يتعمد المهندس الاجتماعي إسقاط قرص فلاش مصاب بفيروس في منطقة يمكن للمستخدمين التقاطه بسهولة. من المرجح أن يقوم المستخدم بتوصيل قرص الفلاش بالكمبيوتر. قد يقوم قرص الفلاش بتشغيل الفيروس تلقائياً ، أوقد يغري المستخدم بفتح ملف باسم مثل تقرير إعادة تقييم الموظفين 2013.docx والذي قد يكون في الواقع ملفاً مصاباً.

68

68

Common Social Engineering Techniques-cont.

- **Exploiting human greed**: Using this technique, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirm their details using credit card details, etc.

- استغلال الجشع البشري: باستخدام هذه التقنية ، قد يغري المهندس الاجتماعي المستخدم بوعود بجني الكثير من المال عبر الإنترنت عن طريق ملء نموذج وتأكيد تفاصيله باستخدام تفاصيل بطاقة الائتمان ، وما إلى ذلك.

69

69

Social Engineering Counter Measures

- **To counter the familiarity exploit**, the users must be trained to not substitute familiarity with security measures. Even the people that they are familiar with must prove that they have the authorization to access certain areas and information.
- **To counter intimidating circumstances attacks**, users must be trained to identify social engineering techniques that fish for sensitive information and politely say no.
- **To counter phishing techniques**, most sites such as Yahoo use secure connections to encrypt data and prove that they are who they claim to be. Checking the URL may help you spot fake sites. Avoid responding to emails that request you to provide personal information.

70

إجراءاتالهندسة الاجتماعية المضادة

- لمواجهةاستغلال الألفة ،يجب تدريب المستخدمين على عدم الاستعاضة عن الإلمامبالإجراءات الأمنية. حتى الأشخاص الذين هم على دراية بهم يجب أن يثبتوا أنلديهم الإذن بالوصول إلى مناطق ومعلومات معينة.
- لمواجهةهجمات الظروف المخيفة ،يجب تدريب المستخدمين على تحديد تقنياتالهندسة الاجتماعية التي تبحث عن معلومات حساسة ويقولون بأدب لا.
- لمواجهةتقنيات التصيد الاحتيالي ،تستخدم معظم المواقع مثل Yahoo اتصالات آمنة لتشفيرالبيانات وإثبات أنها كما تدعي أنها كذلك. قد يساعدك التحقق من عنوان URL فياكتشاف المواقع المزيفة. تجنب الرد على رسائل البريد الإلكتروني التي تطلب منكتقديم معلومات شخصية.

Social Engineering Counter Measures-cont.

- **To counter tailgating attacks**, users must be trained not to let others use their security clearance to gain access to restricted areas. Each user must use their own access clearance.
- **To counter human curiosity**, it's better to submit picked up flash disks to system administrators who should scan them for viruses or other infection preferably on an isolated machine.
- **To counter techniques that exploit human greed**, employees must be trained on the dangers of falling for such scams.

71

- لمواجهةالهجمات المتخلفة ،يجب تدريب المستخدمين على عدم السماح للآخرين باستخدامتصريحهم الأمني للوصول إلى المناطق المحظورة. يجب على كل مستخدم استخدامتصريح الوصول الخاص به.
- لمواجهةفضول الإنسان ،من الأفضل إرسال أقراص فلاش منتقاة إلى مسؤوليالنظام الذين يجب عليهم فحصها بحثاً عن فيروسات أو أي إصابة أخرىويفضل أن يكون ذلك على جهاز معزول.
- لمواجهةالتقنيات التي تستغل الجشع البشري ،يجب تدريب الموظفين على مخاطرالوقوع في مثل هذه الحيل.

71

Summery

- Social engineering is the art of exploiting the human elements to gain access to un-authorized resources.
- Social engineers use a number of techniques to fool the users into revealing sensitive information.
- Organizations must have security policies that have social engineering countermeasures.

- الهندسةالاجتماعية هي فن استغلال العناصر البشرية للوصول إلى موارد غير مصرحبها.
- يستخدمالمهندسون الاجتماعيون عدداً من الأساليب لخداع المستخدمين للكشفعن معلومات حساسة.
- يجبأن يكون لدى المنظمات سياسات أمنية لها إجراءات مضادة للهندسة الاجتماعية.

72

72

Chapter six

- What is cryptography?
- What is cryptanalysis?
- What is cryptology?
- Encryption Algorithms
- Hacking Activity: Hack Now!

73

73

8. ماهو التشفير؟

- التشفيرهي دراسة وتطبيق التقنيات التي تخفي المعنى الحقيقي للمعلومات عنطريق تحويلها إلى صيغ غير بشرية قابلة للقراءة والعكس صحيح.

- لنفترضأنك تريد إرسال الرسالة "احب التفاح"،يمكنك استبدال كل حرف فيالعبارة بالحرف الثالث على التوالي في الأبجدية. ستكون الرسالة المشفرة"." K NQXG CRRNGVلفك تشفير رسالتنا ، سيتعين علينا العودة بثلاثةأحرف في الأبجدية باستخدام الحرف الذي نريد فك تشفيره. توضح الصورةأدناه كيفية إجراء التحويل.

What is cryptography?

- **Cryptography** is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

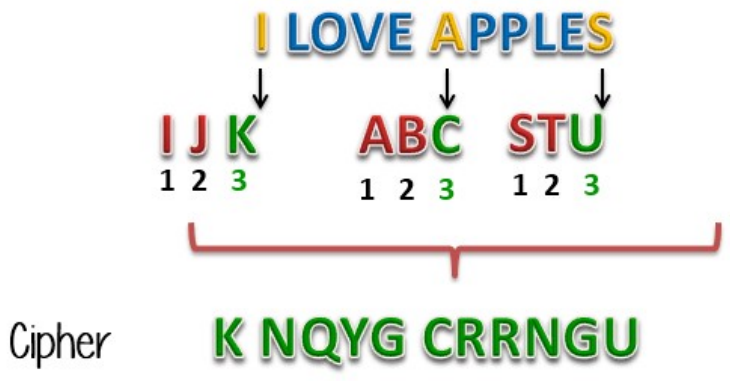
- Suppose you want to send the message "**I LOVE APPLES**", you can replace every letter in the phrase with the third successive letter in the alphabet. The encrypted message will be "**K NQXG CRRNGV**". To decrypt our message, we will have to go back three letters in the alphabet using the letter that we want to decrypt. The image below shows how the transformation is done.

74

74

What is cryptography?-cont.

Key: Replace every letter with 3rd successive letter



75

75

ماهو التشفير؟

- تسمىعملية تحويل المعلومات إلى صيغة غير بشرية قابلة للقراءة التشفير.
- تسمىعملية عكس التشفيرفك التشفير.
- فكالتشفيريتم باستخدام ملفالمفتاح السريالتي لا يعرفها إلا المستلمون الشرعيونللمعلومات. يستخدم المفتاح لفك تشفير الرسائل المخفية. هذا يجعلالاتصال آمناً لأنه حتى إذا تمكن المهاجم من الحصول على المعلومات ،فلن يكون ذلك منطقياً بالنسبة له.
- تعُرفالمعلومات المشفرة بامتدادالشفرة.

What is cryptography?-co

- The process of transforming information into nonhuman readable form is called **encryption**.
- The process of reversing encryption is called **decryption**.
- **Decryption** is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages. This makes the communication secure because even if the attacker manages to get the information, it will not make sense to them.
- The encrypted information is known as a **cipher**.

76

76

What is Cryptanalysis?

- **Cryptanalysis** is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attacks depends
  1. **Amount of time available**
  2. **Computing power available**
  3. **Storage capacity available**

ماهو تحليل الشفرات؟

- تحليلالشفراتهو فن محاولة فك تشفير الرسائل المشفرة دون استخدام المفتاحالذي تم استخدامه لتشفير الرسائل. يستخدم تحليل الشفرات التحليلالرياضي والخوارزميات لفك تشفير الأصفار. يعتمد نجاح هجمات تحليلالشفرات
  1. مقدار الوقت المتاح
  2. قوة الحوسبة المتاحة
  3. سعة التخزين المتاحة

77

77

What is Cryptanalysis?-cont.

- The following is a list of the commonly used Cryptanalysis attacks;
  1. **Brute force attack**– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
  2. **Dictionary attack**– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
  3. **Rainbow table attack**– this type of attack compares the cipher text against pre-computed hashes to find matches.

ماهو تحليل الشفرات؟

- فيمايلي قائمة بهجمات تحليل الشفرات شائعة الاستخدام ؛

1.هجوم القوة الغاشمة -يستخدم هذا النوع من الهجوم خوارزميات تحاول تخمين جميع التركيباتالمنطقية الممكنة للنص العادي والتي يتم بعد ذلك تشفيرها ومقارنتها مع التشفيرالأصلي.

2-هجوم القاموس -يستخدم هذا النوع من الهجوم قائمة كلمات للعثور على تطابق بين النصالعادي أو المفتاح. يتم استخدامه في الغالب عند محاولة اختراق كلمات المرور المشفرة.

3-هجوم طاولة قوس قزح-يقارن هذا النوع من الهجوم نص التشفير مقابل تجزئة محسوبةمسبقاً للعثور على التطابقات.

78

78

What is cryptology?

- Cryptology combines the techniques of cryptography and cryptanalysis.
- يجمععلم التشفير بين تقنيات التشفير وتحليل الشفرات.

79

79

Encryption Algorithms

- **MD5**– this is the acronym for **Message-Digest 5**. It is used to create **128-bit hash values**. Theoretically, hashes cannot be reversed into the original plain text. **MD5** is used to encrypt passwords as well as check data integrity. **MD5** is not collision resistant. **Collision resistance** is the difficulties in finding two values that produce the same hash values.

خوارزميات التشفير

- MD5– هذا هو اختصار لملخص الرسائل 5.يتم استخدامه لخلق قيم تجزئة 128بت.نظرياً ، لا يمكن عكس التجزئة في النص العادي الأصلي.MD5 يستخدملتشفير كلمات المرور وكذلك التحقق من سلامة البيانات.MD5 ليستمقاومة الاصطدام.مقاومة الاصطدامهي الصعوبات في العثور على قيمتينتنتجان نفس قيم التجزئة.

80

Encryption Algorithms-cont.

- **SHA**– this is the acronym for **Secure Hash Algorithm**. SHA algorithms are used to generate condensed representations of a message (**message digest**). It has various versions such as;
  - **SHA-0**: produces 120-bit hash values. It was withdrawn from use due to significant flaws and replaced by SHA-1.
  - **SHA-1**: produces 160-bit hash values. It is similar to earlier versions of **MD5**. It has cryptographic weakness and is not recommended for use since the year 2010.
  - **SHA-2**: it has two hash functions namely **SHA-256** and **SHA-512**. SHA-256 uses **32-bit** words while SHA-512 uses **64-bit** words.
  - **SHA-3**: this algorithm was formally known as **Keccak**.

81

- SHA-هذا هو اختصار لخوارزمية التجزئة الآمنة.تستُخدم خوارزميات SHA لإنشاءتمثيلات مكثفة للرسالة (ملخص الرسالة).لها إصدارات مختلفة مثل ؛
  - SHA-0:ينتج قيم تجزئة 120 بت. تم سحبه من الاستخدام بسبب عيوب كبيرة واستبداله بـ SHA-1.
  - SHA-1:تنتج قيم تجزئة 160 بت. إنه مشابه للإصدارات السابقة من MD5 يحتوي علىضعف في التشفير ولا يوصى باستخدامه منذ عام 2010.
  - SHA-2:لديها وظيفتان هاش وهماSHA-256وSHA-512.يستخدم SHA-256 32بتالكلمات بينما يستخدم SHA-512 64بتكلمات.
  - SHA-3:كانت هذه الخوارزمية معروفة رسمياً باسمكيكاك.

Encryption Algorithms-cont.

- **RC4**– this algorithm is used to create stream ciphers. It is mostly used in protocols such as **Secure Socket Layer** (**SSL**) to encrypt internet communication and **Wired Equivalent Privacy** (**WEP**) to secure wireless networks.
- **BLOWFISH**– this algorithm is used to create **keyed**, **symmetrically blocked ciphers**. It can be used to encrypt passwords and other data.

- RC4– تستُخدم هذه الخوارزمية لإنشاء أصفار دفق. يتم استخدامه في الغالب في بروتوكولات مثل طبقة المقابس الآمنة (SSL) لتشفير اتصالات الإنترنت و الخصوصية المكافئة للشبكات السلكية (WEP) لتأمين الشبكات اللاسلكية.
- بلوفيش- يتم استخدام هذه الخوارزمية في الإنشاء الأصفار المقفلة والمحجوبة بشكل متماثل. يمكن استخدامه لتشفير كلمات المرور والبيانات الأخرى.

82

82

Hacking Activity: Use CrypTool

- In this practical scenario, we will create a simple cipher using the **RC4 algorithm**. We will then attempt to decrypt it using brute-force attack. For this exercise, let us assume that we know the encryption secret key is 24 bits. We will use this information to break the cipher.
- We will use **CrypTool 1** as our cryptology tool. **CrypTool 1** is an open source educational tool for crypto logical studies. You can download it from https://www.cryptool.org/en/ct1-downloads

83

83

Hacking Activity: Use CrypTool-cont.

- **Creating the RC4 stream cipher**
  - We will encrypt the following phrase

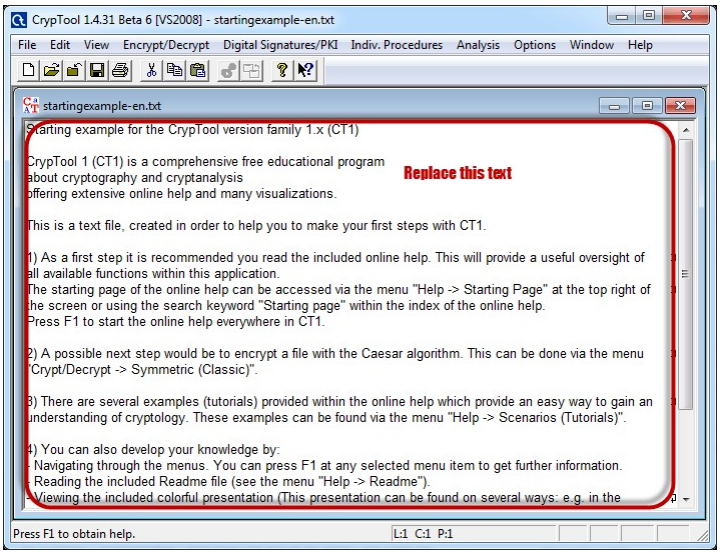
    Never underestimate the determination of a kid who is time-rich and cash-poor

  - We will use **00 00 00** as the encryption key.

84

Hacking Activity: Use CrypTool-cont.

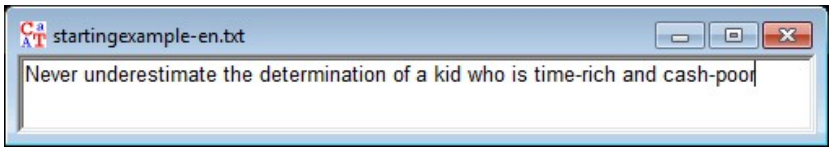
- Open **CrypTool 1**



85

Hacking Activity: Use CrypTool-cont.

- Replace the text with Never underestimate the determination of a kid who is time-rich and cash-poor

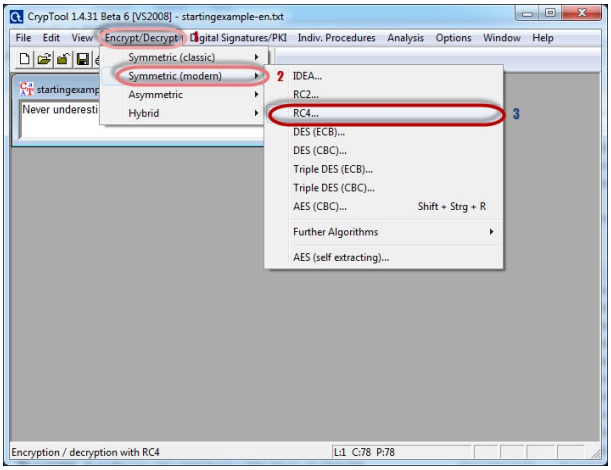


86

86

Hacking Activity: Use CrypTool-cont.

- Click on **Encrypt/Decrypt** menu

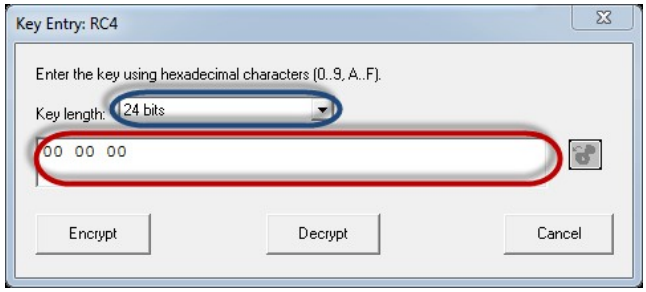


87

87

Hacking Activity: Use CrypTool-cont.

- Point to **Symmetric** (**modern**) then select **RC4** as shown above
- The following window will appear

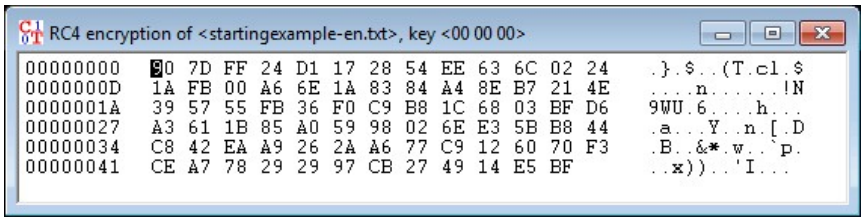


88

88

Hacking Activity: Use CrypTool-cont.

- Select **24 bits** as the encryption key
- Set the value to **00 00 00**
- Click on **Encrypt** button
- You will get the following stream cipher

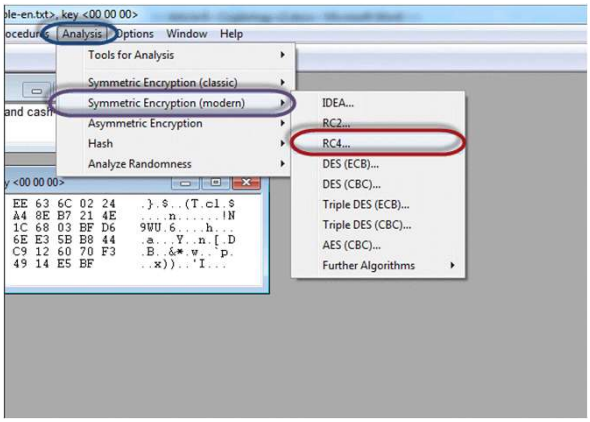


89

89

Hacking Activity: Use CrypTool-cont.

- Attacking the stream cipher
  - Click on **Analysis** menu

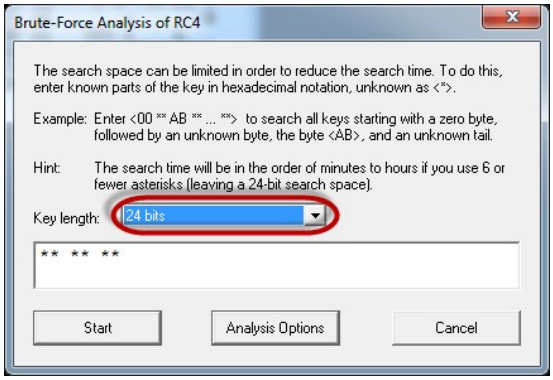


90

90

Hacking Activity: Use CrypTool-cont.

- Point to **Symmetric Encryption** (**modern**) then select **RC4** as shown above
- You will get the following window

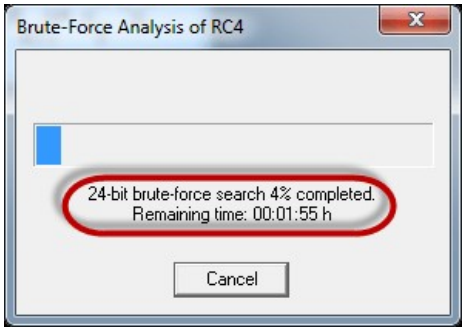


91

91

Hacking Activity: Use CrypTool-cont.

- Remember the assumption made is the secret key is **24 bits**. So make sure you select **24 bits** as the **key length**.
- Click on the **Start** button. You will get the following window

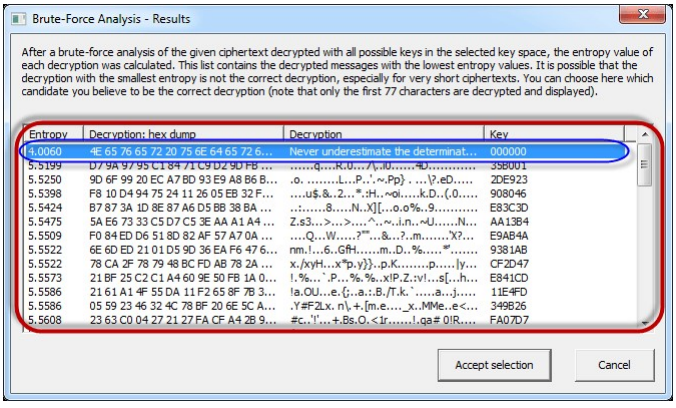


92

92

Hacking Activity: Use CrypTool-cont.

- **Note**: the time taken to complete the **Brute-Force Analysis** attack depends on the processing capacity of the machine been used and the **key length**. The longer the key length, the longer it takes to complete the attack.
- When the analysis is complete, you will get the following results.



93

93

Hacking Activity: Use CrypTool-cont.

- **Note**: a lower **Entropy** number means it is the most likely correct result. It is possible a higher than the lowest found **Entropy** value could be the correct result.
- Select the line that makes the most sense then click on **Accept selection** button when done

Summery

- **Cryptography** is the science of ciphering and deciphering messages.
- A **cipher** is a message that has been transformed into a nonhuman readable format.
- **Deciphering** is reversing a cipher into the original text.
- **Cryptanalysis** is the art of deciphering ciphers without the knowledge of the key used to cipher them.
- **Cryptology** combines the techniques of both cryptography and cryptanalyst.