Information Hiding Techniques Using Network Protocols

Manar Younis Kashmola **Ameera Bibo Sallo**

College of Computer And Math .Sciences *Presidency of Mosul University*

University of Mosul, Iraq

Received on : 28/4/2010 **Accepted on : 21/6/2011**

ABSTRACT

The covert channels of type covert storage channels were used in this research to hide textual data or an (image hiding secrete data) in the transmission protocol layer and the internet protocol layer of TCP/IP module. We use IP protocol in designing covert channel by using Identification field, and use TCP protocol in designing covert channel by using Urgent Pointer field, and UDP by using Source Port field. Finally ICMP protocol by using Echo request message and Message field.

The result of Covert channel after analyzing the protocols (IP, TCP, UDP, ICMP) header depends on the field that used in the designing the Covert channel. The access ratio of hidden data in the two protocols TCP/IP was %100. UDP protocol on the other hand depends on a mechanism of unsafe communication. ICMP protocol provided a good transmission, though unreliable, in that the message structure can be unreliable or clear.

Keywords: Information Hiding, Network Protocols, Covert channel Hiding Information in TCP, UDP,ICMP, IGMP

تقنيات إخفاء المعلومات باستخدام بروتوكولات الشبكة

منار يونس كشمولة **أميرة بيبو سلو**

كلية علوم الحاسوب والرياضيات، جامعة الموصل *رئاسة الجامعة، جامعة الموصل*

تاريخ استلام البحث: 2010/04/28 **تاريخ قبول البحث: 2011/06/21**

الملخص

تم في هذا البحث استخدام القنوات المخفية من نوع قناة الخزن المخفية (Covert Storage Channel) لإخفاء بيانات نصية أو صورة مُخفى فيها بيانات سرية في بروتوكولات طبقة النقل وطبقة الانترنت في نموذج TCP/IP، حيث استخدم بروتوكول الانترنت IP في تصميم قناة مخفية باستخدام حقل التعريف Identification، وكذلك استخدم بروتوكول TCP في تصميم قناة مخفية باستخدام حقل مؤشر الحالة الطارئة Urgent Pointer، وبروتوكول UDP باستخدام حقل رقم منفذ المصدر Source Port، وأخيرا البرتوكول ICMP باستخدام هيكلية رسالة طلب الصدى Echo Request وحقل الرسالة Message.

كانت نتائج القنوات المخفية التي ظهرت بعد تحليل ترويسة البروتوكولات المستخدمة في تصميم القنوات المخفية اعتمدت على الحقل المستخدم في تصميم القناة، ونسبة وصول البيانات المخفية في البروتوكولين IP وTCP 100%، أما بروتوكول UDP فيعتمد على آلية عمله التي لا تؤمن اتصالاً موثوقاً، أما بروتوكول ICMP فأنه وفر إرسالا مقبولا ولكنه يبعث على الشك وذلك لان بنية الرسالة المستخدمة تكون معروفة وواضحة.

الكلمات المفتاحية: إخفاء المعلومات، بروتوكولات الشبكة ، تحويل قناة معلومات مخفية في TCP، UDP، ICMP ، IGMP

1- المقدمة

شبكة الانترنت هي البيئة الجديدة للتعامل مع المعلومات في عصر ثورة المعلومات وازدياد أهميتها، ويتوجب التفكير الجاد في حمايتها وحماية خصوصية الأفراد العاملين عليها، لذلك لم تعد الأمنية موضوعا متعلقا بطرائق التشفير ووضع السياسات الأمنية والبحث عن الثغرات في بروتوكولات الاتصالات وإنما أمنية المرور أيضاً

التي يكون جوهرها موجوداً في القنوات المخفية، وأن غاية التشفير حماية محتوى الرسالة، أما غاية القنوات المخفية فهي أخفاء وجود الرسالة. [6]

يتناول البحث محورين، الأول تضمن تعريفاً لبروتوكولات الشبكة والبنية الهرمية لها والنموذج TCP/IP وشرحاً لمجموعة من بروتوكولات TCP/IP. أما المحور الثاني فقد تضمن مقدمة عن القنوات المخفية وتصنيفها، ثم شرحا للقنوات المخفية في بروتوكولات الشبكة مثل البروتوكولات IP،TCP،UDP،ICMP.

إن علمي الإخفاء والتشفير يستخدمان مع اختلافهما في تأكيد وثوقية البيانات، ففي التشفير يمكن لأي طرف أن يكتشف إن ثمة طرفين يتصلان بطريقة مشفرة، أما في إخفاء المعلومات فيخفى أصلا وجود الاتصال فلا يمكن لأحد أن يلاحظ وجود طرفين يتبادلان الرسائل عبر قنوات الاتصال. وثمة فروقات عديدة بين إخفاء المعلومات والتشفير وهي موضحة في الجدول (1). [1]

جدول (1). الفرق بين أخفاء المعلومات والتشفير

إخفاء المعلومات	التشفير
يعمل على إخفاء وجود المعلومات	يعمل على إخفاء محتويات المعلومات
يحاول إخفاء وجود اتصال	يكون الاتصال دليلا
النتيجة النهائية لإخفاء المعلومات هي عنصر_الإخفاء	النتيجة النهائية للتشفير هي النص المشفر
هدف طرائق الإخفاء ذات الأمنية العالية منع المراقب الوسيط من معرفة وجود البيانات السرية أصلا	هدف طرائق التشفير القوية منع المتطفل من الحصول على أية معلومات عن النص الواضح من النص المشفر الذي هُوجم
ليست ثمة خوارزمية محددة بل يعتمد على الطبيعة البشرية في الإخفاء	يعتمد على خوارزميات معروفة
ليس له بصمة، لكن عند معرفة طريقة الإخفاء يتم استرجاع الرسالة السرية	توجد لكل خوارزمية تشفير نقاط ضعف تسمح للمهاجم باسترجاع الرسالة السرية
من الممكن دمج التشفير مع إخفاء المعلومات للحصول على إخفاء عالي الأمنية	من الممكن دمج طريقتي تشفير للحصول على تشفير مزدوج

2- الدراسات السابقة

حاول الباحثون إيجاد تقنيات إخفاء متطورة تواكب التطور السريع في تقنيات الإخفاء والشبكات، فمنهم من أنجز بحوثا ودراسات واسعة لربط تقنيات إخفاء المعلومات مع تقنيات الذكاء الاصطناعي، وآخرون أنجزوا الاتصال السري في شبكات الحاسوب من خلال القنوات المخفية والكتابة المغطاة في بروتوكولات الشبكة، ومن هذه البحوث:

1. في عام 1989 قدم الباحثان Wolf وGirling بحثاً لإخفاء البيانات في حقل الحشوة padding field، مثلا تحشو الايثرنت حزم الشبكة عندما يكون طولها اقل من 60Bytes، إذ يتم إضافة حشوة لترويسة بروتوكول الانترنت IP وبروتوكول النقل TCP ليصبح حجم الحزمة 64Bytes وهو اقل حجم مسموح به لحزمة الشبكة. [17]
2. في عام 2002 قدم الباحث Ahsan بحثاً تضمن تقنيتين لتصميم القنوات المخفية، الاولى هي إخفاء البيانات في ترويسة البروتوكولات IP و TCP، والثانية هي إعادة ترتيب حزم الشبكة باستخدام بروتوكول IPSec. [7]

3. وفي العام نفسه قدم الباحثان Ahsan وKundur طريقة اقترحا فيها استخدام قيمة العلم Don't fragment (DF) في ترويسة بروتوكول الانترنت IP لإخفاء قيم ثنائية (0) أو (1) وذلك فقط في حالة معرفة المرسل قيمة وحدة النقل العظمى Maximum Transfer Unit (MTU) للطريق إلى المستلم، فيرسل المرسل حزمة بيانات ذات حجم اقل من حجم وحدة النقل العظمى. [Kundur,2002]
4. وقدم في العام نفسه الباحث Fisk بحثاً اقترح فيه طريقة لتصميم قناة مخفية لإخفاء البيانات في مقطع بروتوكول النقل TCP (TCP segment)عندما يكون العلم TCP reset (RST) مشغلا، وهذا العلم يعمل على قطع الاتصال، ولا يحتوي هذا المقطع على بيانات. [17]
5. في عام 2004 قدم الباحث Lliamas بحثا صمم فيه خادم وكيل Server proxy لإخفاء معلومات في القناة المخفية باستخدام حقل التعريف Identification في ترويسة البروتوكول IP عند طلب خدمة معينة من الخادم. [Lliamas,2004]
6. وفي العام نفسه قدم الباحثون Cauich وGomez وWatanabe بحثا لإخفاء المعلومات في ترويسة البروتوكول الانترنت IP في حقل التعريف Identification وحقل انزياح الجزء Fragment Offset في حالة عدم تجزئة الحزمة من قبل الموجهات الموجودة في شبكة الاتصال. [Cauich,2004]
7. في عام 2005 قدم الباحثان Bharti وSnigdh بحثا لإخفاء المعلومات في بروتوكولات IP و TCP واقترحا أفضل حقول في ترويسة هذه البروتوكولات لإخفاء المعلومات السرية فيها في الشبكات المزدحمة. [8]
8. وفي العام نفسه قدم الباحثان Murdoch وLwies بحثا لتصميم قنوات مخفية باستخدام حقل التعريف Identification في ترويسة بروتوكول الانترنت IP، وحقل الرقم التسلسلي Sequence Number في ترويسة بروتوكول النقل TCP في بيئة نظام التشغيل Linux. [13]
9. في عام 2006 قدم الباحثون Zander وArmitage وBranch بحثا لإخفاء البيانات في حقل مدة الحياة Time To Live (TTL) في ترويسة بروتوكول الانترنت IP. [17]

3- البروتوكولات

البروتوكولات مجموعة من القوانين والإجراءات التي تتحكم وتنظم عملية الاتصال والتفاعل بين الأجهزة المختلفة على الشبكة لكي تستطيع هذه الأجهزة الاتصال مع بعضها وفهم كل منها الآخر، ومن الممكن أن تعمل عدة بروتوكولات مع بعضها لتنفيذ أمر معين، وتسمى عندئذ مكدس البروتوكولات Protocol Stack، أو مجموعة البروتوكولات Protocol Suite. [5]

إن وظيفة البروتوكولات في الجهاز المرسل هي:

1. تقسيم البيانات إلى مقاطع .
2. إضافة معلومات العنونة إلى الحزم.
3. تجهيز البيانات للإرسال.

أما وظيفة البروتوكولات في الجهاز المستقبل فهي:

1. التقاط حزم البيانات من وسط الاتصال.
2. إدخال حزم البيانات إلى جهاز المستقبل عبر الشبكة.
3. تجميع كل حزم البيانات المرسلة وقراءة معلومات التحكم المضافة إلى هذه الحزم.

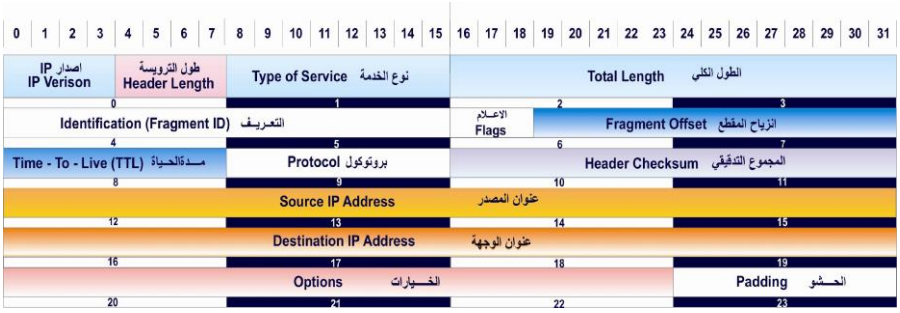
4. نسخ البيانات من الحزم إلى ذاكرة مؤقتة لإعادة تجميعها.
5. تمرير البيانات المعاد تجميعها إلى البرامج في صورة مفهومة قابلة للاستخدام.

1-3 مجموعة بروتوكولاتTCP/IP

هي مجموعة من البروتوكولات التي تمت تسميتها طبقاً لأهم بروتوكولين في المجموعة وهما IP وTCP. ولا يمكن لأي مستخدم أن يتعامل مع احد بروتوكولات TCP/IP بمعزل عن البروتوكولات الأخرى، وذلك لان بروتوكولات TCP/IP تقوم بنقل البيانات من طبقة إلى أخرى وتتعامل سوياً لانجاز عملية النقل. [3]

أ- بروتوكول الإنترنت IP

يعد بروتوكول الإنترنت البروتوكول الرئيس في طبقة الانترنت في مكدس بروتوكولات TCP/IP. وهو مسؤول عن تحديد العنوان المنطقي IP address لمصدر ووجهة كل حزمة تنقل خلال الشبكة. [5] ويمثل الشكل (1) ترويسة بروتوكول انترنيت IP



الشكل (1). ترويسة بروتوكول الانترنت IP

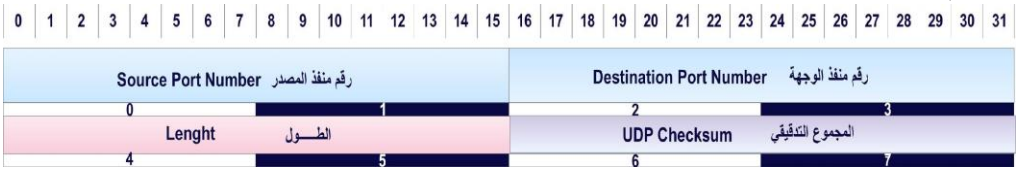
ب- بروتوكول التحكم بالإرسال TCP

بروتوكول TCP هو من بروتوكولات طبقة النقل يهدف إلى توفير خدمة نقل البيانات بموثوقية عالية بين حاسبين متصلين عبر شبكة الاتصال وهو يرتبط دوماً ببروتوكول الإنترنت، ويستخدم من قبل تطبيقات الشبكات التي تتطلب اتصالا آمناً وموثوقاً ويضمن عدم ضياع حزم البيانات [3]. تحتوي ترويسة TCP على حقول تضمن الاتصال الموثوق كما في الشكل (2).

الشكل (2). ترويسة TCP

ج- بروتوكول معطيات المستخدم UDP

هو من بروتوكولات طبقة النقل وهو لا يؤمن اتصالاً موثوقاً، اي لا يضمن وصول البيانات إلى المستقبل بصورة كاملة، ويستخدم في تطبيقات ترسل كميات كبيرة من البيانات وتتطلب سرعة عالية في عملية النقل. كما في الشكل (3). [2]



الشكل (3). ترويسة UDP

د- بروتوكول التحكم بالأخطاء ICMP

يعد ICMP بروتوكولاً يستخدم بشكل أساسي لتشخيص المشاكل التي تحدث بين أجهزة الشبكة [ادريس،2006]. حقول ترويسة هذا البروتوكول متغيرة من رسالة إلى أخرى ولكن جميع الرسائل تتشابه في الحقول الثلاثة الأولى كما في الشكل (4). [10]

الشكل (4). ترويسة ICMP

4- القنوات المخفية Covert Channels

وهي مسارات اتصال لم يتم تصميمها، وكذلك لم تكن غايتها نقل المعلومات أبدا، وتستخدم هذه القنوات من قبل برامج غير موثوق بها من أجل الحصول على المعلومات لصالحها وهي في الوقت ذاته تنجز خدمة لبرامج أخرى. [12]

4-1 تصنيف القنوات المخفية

يمكن التمييز بين صنفين رئيسين للقنوات المخفية وهما: [14]

1- قناة الخزن المخفية Covert Storage Channel

هي قناة مخفية تُضمّن المعلومات بصورة مباشرة وغير مباشرة في موقع خزني وقراءة معلومات ذلك الموقع في عملية الاسترجاع. وهذا يتطلب وجود مصادر مشتركة في النظام، مثلا يتطلب إرسال الحرفين "AB" باستخدام قناة خزن مخفية تضمين قيمة شفرة Unicode لهذين الحرفين في حقل الرقم التسلسلي في ترويسة بروتوكول TCP في طرف المرسل، وفي جهة المستقبل يتم استرجاع قيمة الحرفين "AB" من المكان نفسه الذي خزنت فيه، وفي عملية الإرسال السري تمثل حزمة الشبكة المرسلة والمستقبلة المصدر المشترك. [11] [8]

2- قناة الوقت المخفية Covert Timing Channel

هي قناة مخفية يتم تضمين المعلومات فيها بتضمين فترات زمنية (تأخيرات) على وقوع الإحداث في النظام، مثلا استخدام أزمنة وصول حزم الشبكة لتنفيذ قناة ثنائية (Binary channel). [9]

2-4 مواصفات القناة المخفية الناجحة

ثمة مواصفات يشترط التنبه لها عند تصميم قناة مخفية وهي:

1. يشترط أن تبدو حزمة البيانات التي تضم البيانات المخفية نظامية ومتناسقة.
2. اختيار الحقول غير المناسبة في حزمة البيانات يجعل مرور الشبكة غير طبيعي وشاذاً.
3. اختيار البروتوكول الشائع في بيئة الشبكات يزيد من سرية وقدرة الاختباء للمعلومات المخفية.

3-4 القنوات المخفية في بروتوكولات الشبكة

أ- الإخفاء في IP

من حقول هذا البروتوكول التي تستخدم لتصميم قناة مخفية: [7] [16] [17]

1. **حقل تعريف IP IP Identification**
2. **حقل مدة الحياة Time To Live**
3. **حقل الخيارات IP Option**

ب- الإخفاء في بروتوكول TCP

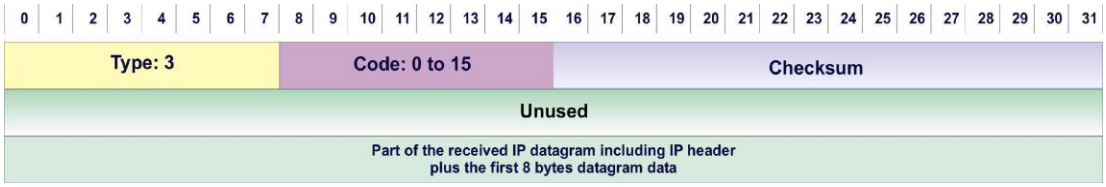
من حقول ترويسة هذا البروتوكول التي تستخدم لتصميم قناة مخفية:[13] [15] [16]

1. **حقل رقم منفذ المصدر Source Port number**
2. **حقل رقم التسلسل TCP sequence number**
3. **حقل رقم الإشعار Acknowledgment number**
4. **حقل مؤشر الحالة الطارئة Urgent Pointer**

ج- الإخفاء في ICMP

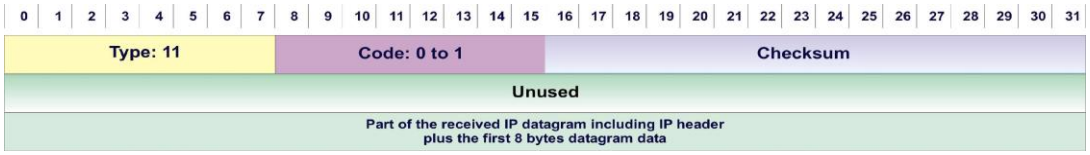
أن كل رسالة من رسائل ICMP لها بنية خاصة تختلف عن الرسائل الأخرى، وفي بعض الحالات تتولد رسائل من ICMP تحتوي على حقول غير مستخدمة يستفاد منها في تصميم القنوات المخفية، ومن أشهر هذه الرسائل المستخدمة في القنوات المخفية : [10] [16]

1. الوجهة لا يمكن الوصول إليها Destination Unreachable



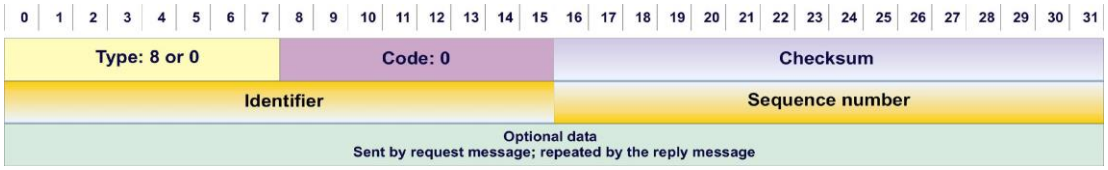
الشكل (5). بنية رسالة الوجهة لايمكن الوصول إليها

2. تجاوز الوقت Time Exceeded



الشكل (6). بنية رسالة تجاوز الوقت

3. رسالة طلب الصدى Echo Request



الشكل (7). بنية رسالة طلب الصدى

5- النظام المقترح لإخفاء المعلومات

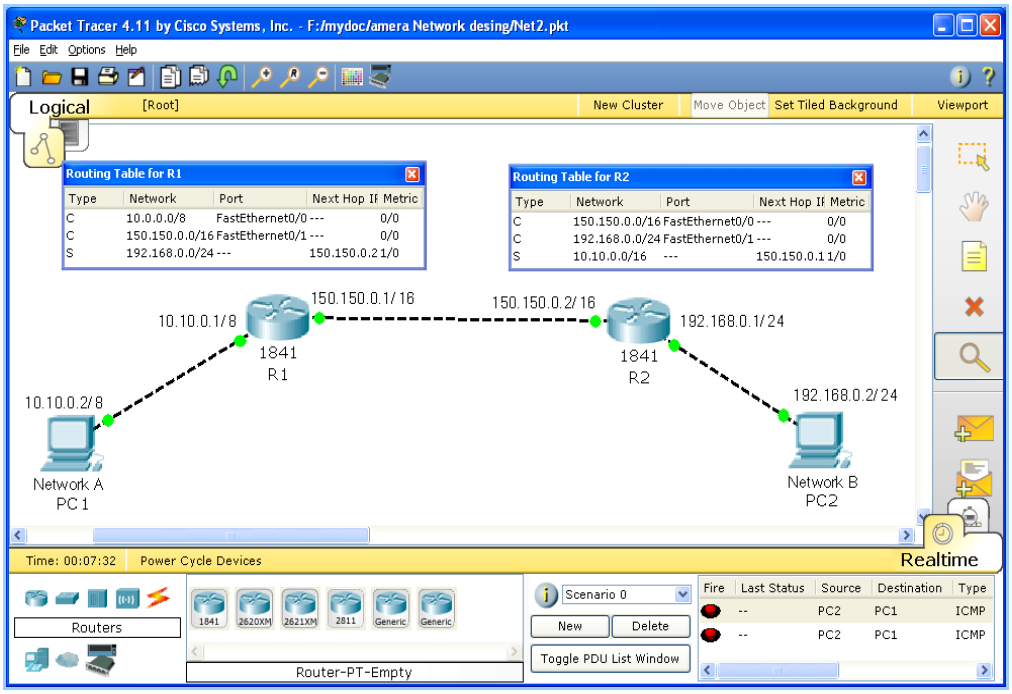
تم اقتراح نظام لإخفاء معلومات سرية (مشفرة) وإرسالها بصورة مخفية عبر شبكة الاتصال، حيث استخدم بروتوكول الانترنت IP في تصميم قناة مخفية باستخدام حقل التعريف Identification، وكذلك استخدام بروتوكول TCP في تصميم قناة مخفية باستخدام حقل مؤشر الحالة الطارئة Urgent Pointer، وبروتوكول UDP باستخدام حقل رقم منفذ المصدر Source Port، وأخيرا البرتوكول ICMP باستخدام بنية رسالة طلب الصدى Echo Request وحقل الرسالة Message. والشكل (8) يبين المخطط الصندوقي للإخفاء باستخدام القنوات المخفية. حيث تقوم جهة الإرسال بإخفاء المعلومات النصية المشفرة الناتجة من مرحلة التشفير أو المخفية في الصورة الملونة الناتجة من مرحلة الإخفاء في الصورة في بروتوكولات شبكة محلية باستخدام القنوات المخفية. [6]

وفي جهة المستقبل يتم استرجاع البيانات السرية المرسلة عبر القنوات المخفية سواء أكانت تلك البيانات نصاً مشفراً أم صورة مُخفية فيها نص مشفر.

5-1 تصميم القنوات المخفية

أ- تصميم شبكة الاتصال المحلية

تتكون الشبكة المحلية من ثلاث شبكات هي 10.10.0.0 و150.150.0.0 و192.168.0.0، وتحتوي على جهازي حاسوب وجهازي موجه، وجهاز الموجه المستخدم هو جهاز حاسوب يحتوي على بطاقتي شبكة وقد استخدم التوجيه الساكن في بناء جدول التوجيه لكل موجه، ويبين الشكل (4-10) تصميم الشبكة المستخدمة باستخدام برنامج Packet Tracer واستخدم هذا البرنامج لرسم وفحص الشبكة المستخدمة في البحث قبل ربطها فيزيائيا.



الشكل (4-10). الشبكة المحلية المستخدمة في تصميم القنوات المخفية

ب- خوارزمية الإخفاء باستخدام القنوات المخفية في بروتوكولات الشبكة

المدخلات: حزم الشبكة (Network Packets)، الملف المراد إرساله بصورة مخفية.

المخرجات: حزم الشبكة المُخفى فيها بيانات سرية.

خطوات الخوارزمية:

1- إدخال اسم ملف الإدخال المراد إرساله عبر القنوات المخفية.

2- حساب حجم الملف.

3- توليد حزم الشبكة.

4- قراءة حزمة شبكة تكون في حالة إرسال.

5- حشر حجم الملف في حقل ID في ترويسة IP.

6- تغيير قيمة الحقل TOS في ترويسة IP .

7- حساب قيمة المجموع التدقيقي IPCHECKSUM لترويسة IP.

8- إرسال حزمة الشبكة بعد التغيير إلى بطاقة الشبكة.

9- قراءة حزمة شبكة تكون في حالة إرسال

10- قراءة كتلتين ثمانيتين من ملف الإدخال في حالة الإخفاء في IP, TCP, UDP و32 كتلة ثمانية في حالة الإخفاء في بروتوكول ICMP.

11- حساب قيمة المجموع التدقيقي IPCHECKSUM لترويسة بروتوكول القناة المخفية.

12- إرسال حزمة الشبكة بعد التغيير إلى بطاقة الشبكة.

13- ارجع إلى 9 في حالة عدم انتهاء البيانات في ملف الإدخال .

14- إنهاء الاتصال.

15- النهاية.

ج- خوارزمية استرجاع البيانات المخفية في بروتوكولات الشبكة

المدخلات: حزم الشبكة (Network Packets) المستقبلة أي قناة الإخفاء.

المخرجات: البيانات المسترجعة من قناة الإخفاء.

خطوات الخوارزمية:

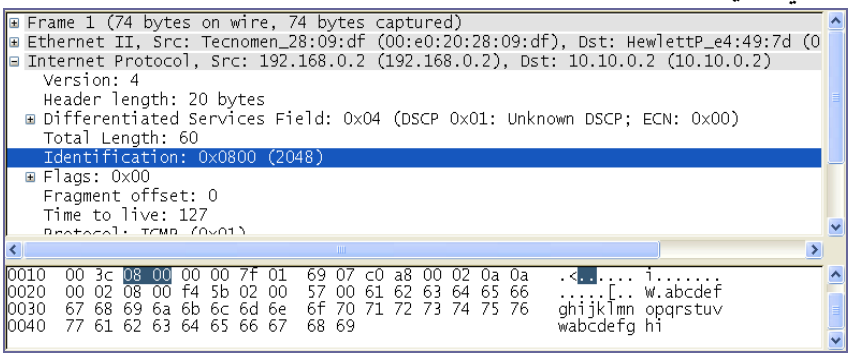
1. إدخال اسم ملف الإخراج.
2. قراءة حزمة شبكة مستقبلة.
3. استرجاع حجم الملف من حقل ID في ترويسة IP .
4. قراءة حزمة شبكة مستقبلة IP.
5. استرجاع البيانات من حقول البروتوكولات IP, TCP, UDP , ICMP و 32 .
6. خزن البيانات المسترجعة في ملف الإخراج.
7. إرسال حزمة الشبكة بعد الاسترجاع إلى نظام التشغيل.
8. ارجع إلى 4 في حالة عدم انتهاء البيانات في ملف الإدخال .
9. إنهاء الاتصال.
10. النهاية.

2-5 نتائج القنوات المخفية

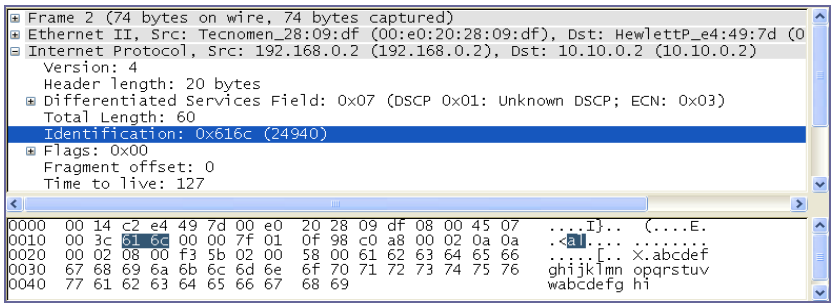
في مجال القنوات المخفية تم إرسال كلمة al_mosul بصورة مخفية باستخدام البروتوكولات IP وTCP وUDP، وإرسال كلمة al_mosul بعد تشفيرها باستخدام البروتوكول IP، وكذلك إرسال ملف بحجم 256 باستخدام بروتوكول ICMP، وسُجلت نتائج القنوات المخفية باستخدام برنامج Ethereal وهو برنامج تحليل بروتوكولات الشبكة.

1- الإخفاء في بروتوكول الانترنت IP

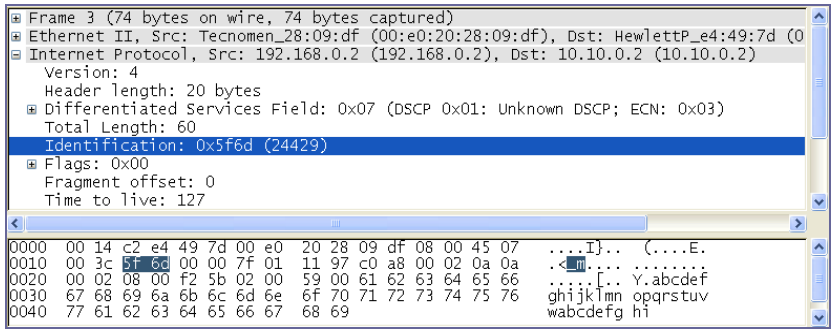
استخدمت أربع حزم لإرسال كلمة **al_mosul** عبر القناة المخفية المصممة باستخدام حقل التعريف Identification في ترويسة بروتوكول الانترنت IP



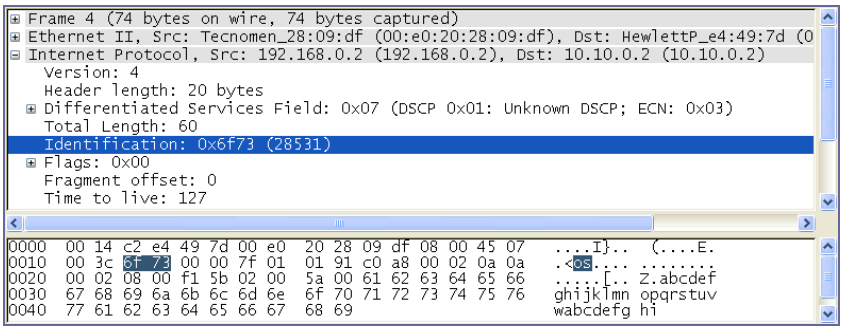
الشكل (10). ترويسة بروتوكول IP مخفى فيها حجم الملف



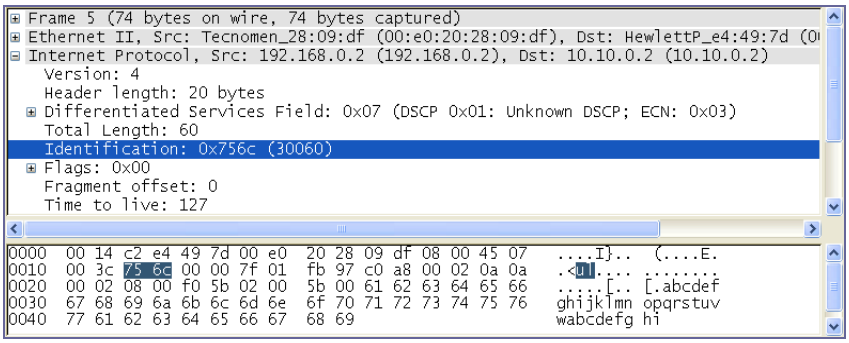
الشكل (11). ترويسة بروتوكول IP مخفى فيها الحرفان al



الشكل (12). ترويسة بروتوكول IP مخفى فيها الحرفان _m



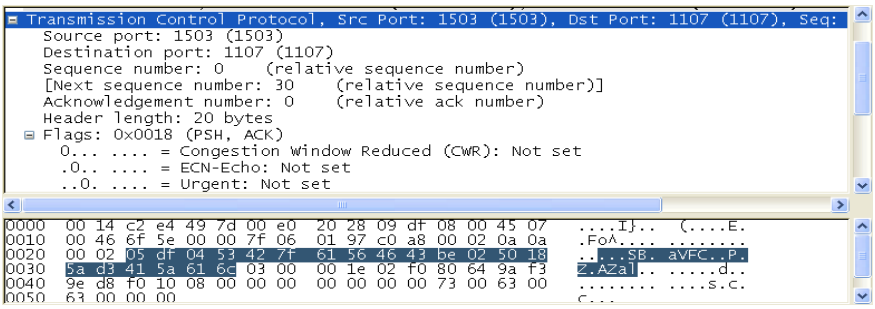
الشكل (13). ترويسة بروتوكول IP مخفى فيها الحرفان os



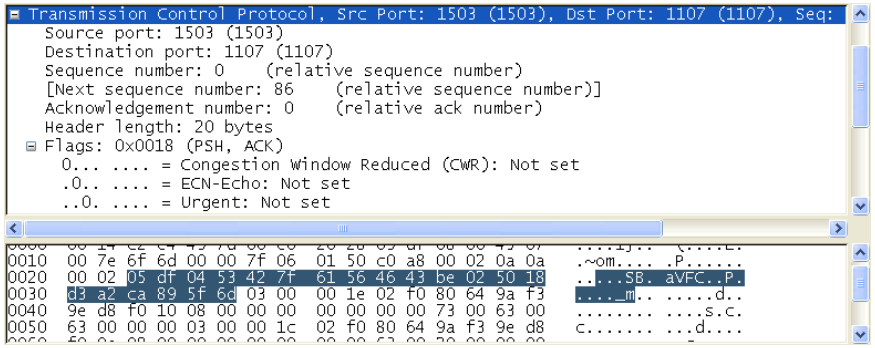
الشكل (14). ترويسة بروتوكول IP مخفى فيها الحرفان ul

2- الإخفاء في بروتوكول النقل TCP

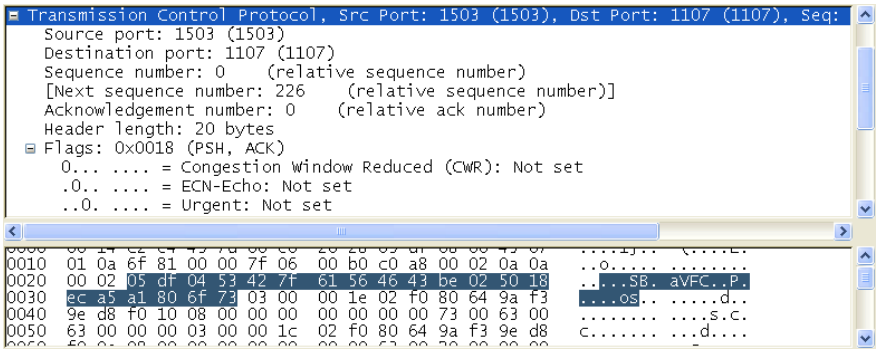
استخدمت أربع حزم لإرسال كلمة **al_mosul** عبر القناة المخفية المصممة باستخدام حقل مؤشر الحالة الطارئة urgent pointer في ترويسة بروتوكول النقل TCP، ويمكن توضيح عملية الإرسال كما في الأشكال:



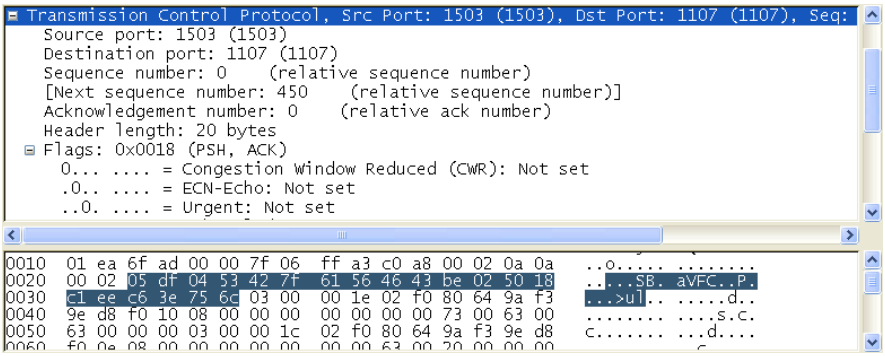
الشكل (15). ترويسة بروتوكول TCP مخفي فيها الحرفان al



الشكل (16). ترويسة بروتوكول TCP مخفي فيها الحرفان m_



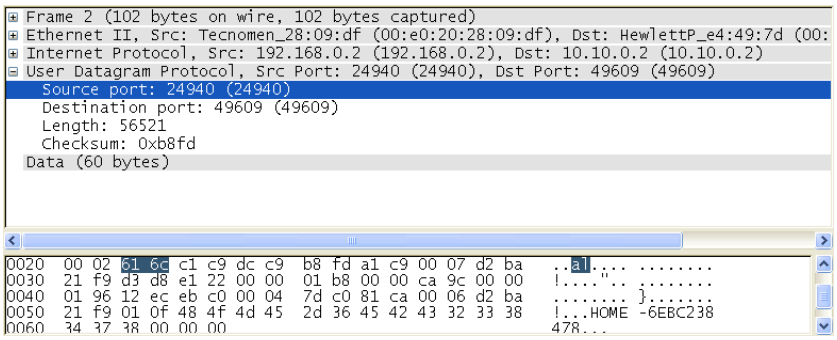
الشكل (17). ترويسة بروتوكول TCP مخفي فيها الحرفان os



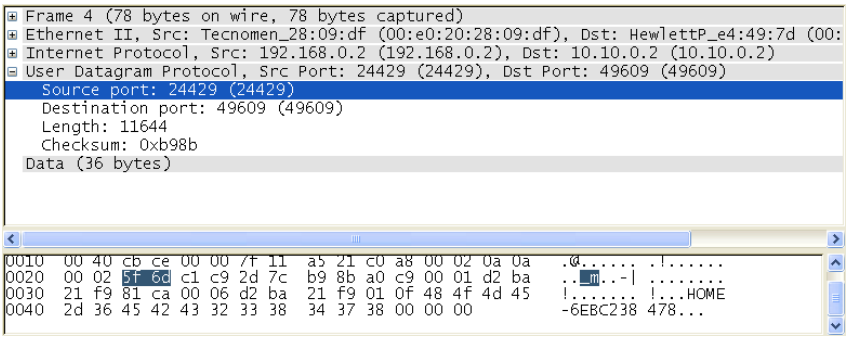
الشكل (18). ترويسة بروتوكول TCP مخفي فيها الحرفان ul

3- الإخفاء في بروتوكول النقل UDP

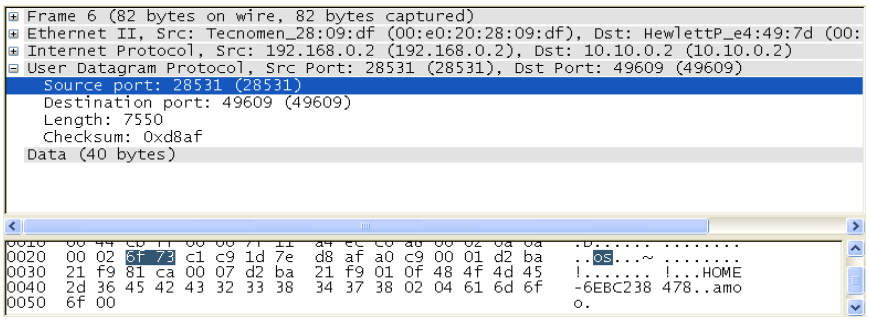
استخدمت أربع حزم لإرسال كلمة **al_mosul** عبر القناة المخفية المصممة باستخدام حقل رقم منفذ المصدر source port في ترويسة بروتوكول النقل، ويمكن توضيح عملية الإرسال كما في الأشكال:



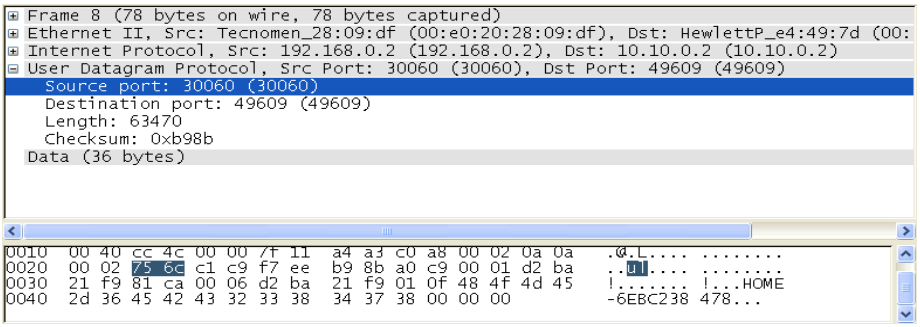
الشكل (19). ترويسة بروتوكول UDP مخفي فيها الحرفان al



الشكل (20). ترويسة بروتوكول UDP مخفي فيها الحرفين m_



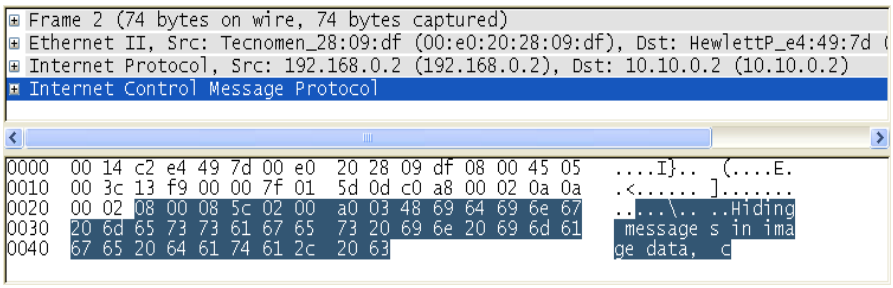
الشكل (21). ترويسة بروتوكول UDP مخفي فيها الحرفان os



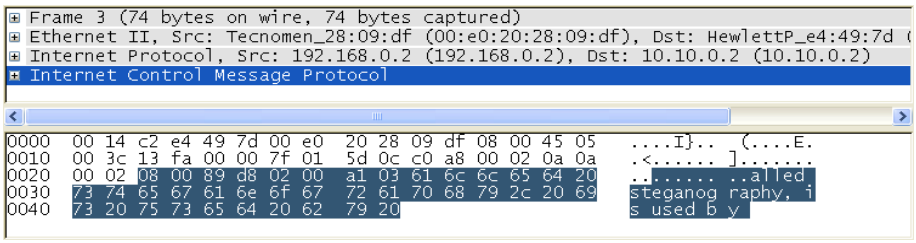
الشكل (22). ترويسة بروتوكول UDP مخفي فيها الحرفان ul

4- الإخفاء في بروتوكول التحكم بالأخطاء ICMP

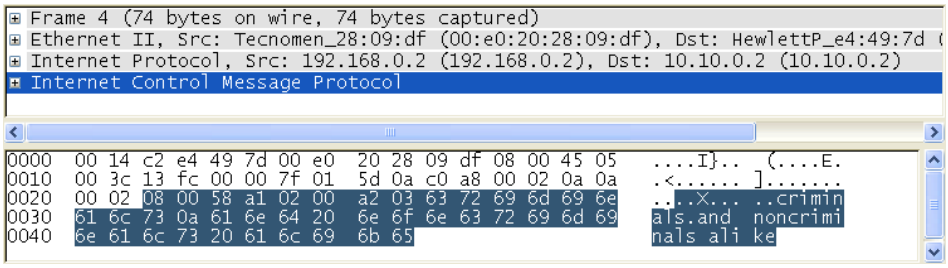
استخدمت ثمان حزم لإرسال ملف حجمه 256 عبر القناة المخفية المصممة باستخدام حقل الرسالة message في ترويسة بروتوكول ICMP، ويمكن توضيح عملية الإرسال كما في الأشكال:



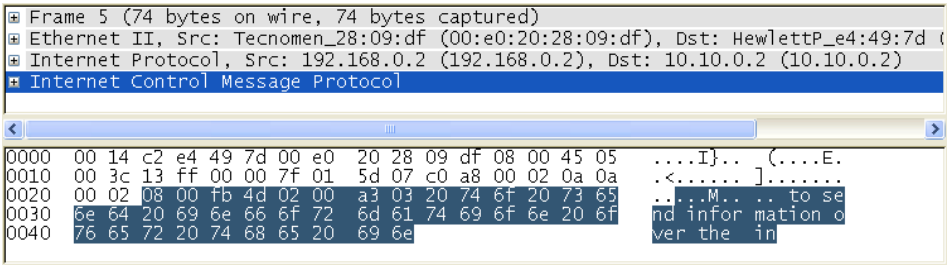
الشكل(23). ترويسة الحزمة الأولى لبروتوكول ICMP



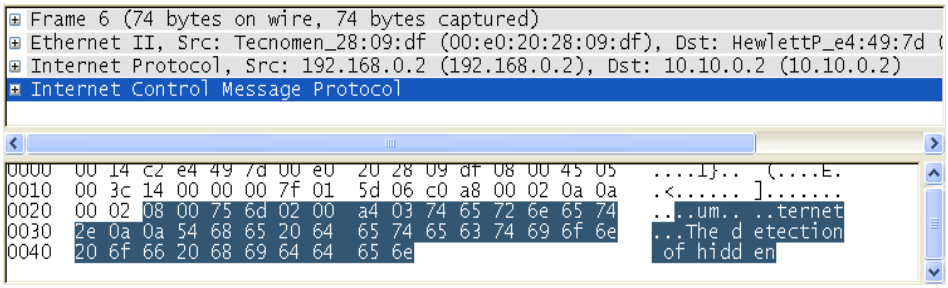
الشكل(24). ترويسة الحزمة الثانية لبروتوكول ICMP



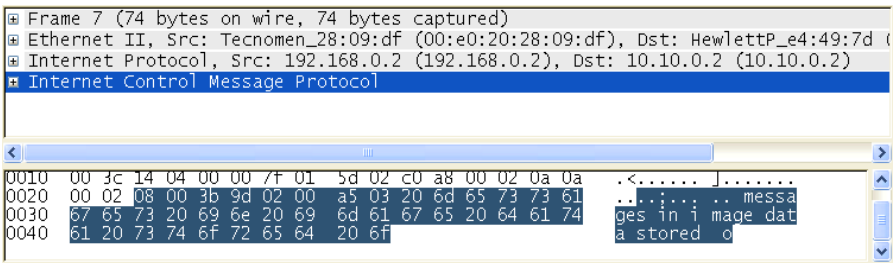
الشكل(25). ترويسة الحزمة الثالثة لبروتوكول ICMP



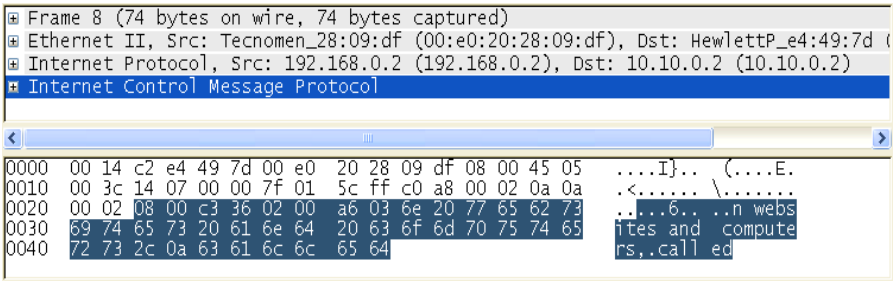
الشكل(26). ترويسة الحزمة الرابعة لبروتوكول ICMP



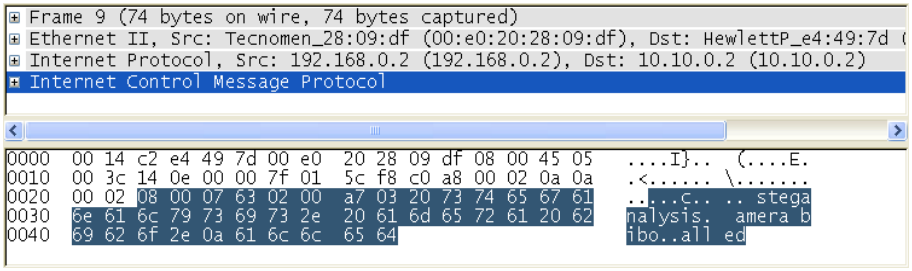
الشكل(27). ترويسة الحزمة الخامسة لبروتوكول ICMP



الشكل(28). ترويسة الحزمة السادسة لبروتوكول ICMP



الشكل(29). ترويسة الحزمة السابعة لبروتوكول ICMP



الشكل(30). ترويسة الحزمة الثامنة لبروتوكول ICMP

6- الاستنتاجات

من خلال تطبيق تقنيات الإخفاء المقترحة لإخفاء معلومات سرية باستخدام تقنية الكتابة المغطاة والقنوات المخفية ومن خلال النتائج التي تم الحصول عليها تم التوصل إلى الاستنتاجات الآتية:

1. إجراء اتصال غير مرئي بين طرق المرسل والمستلم باستخدام القنوات المخفية قلل من مستوى الشك في وجود اتصال سري.
2. يستقبل الموجه حزمة الشبكة ويعيد حساب المجموع التدقيقي لترويسة بروتوكول الانترنت بعد تقليل قيمة TTL بمقدار واحد، وفي حالة اختلافه تهمل الحزمة وكذلك يفحص عنوان الوجهة ,فان كان عنوان بث Broad Cast يمنع إرسالها إلى شبكة أخرى.
3. أظهرت البروتوكولات المستخدمة في تصميم القنوات المخفية النتائج الآتية:

أ- أعطى بروتوكول IP المستخدم في القناة المخفية نتائج جيدة جداً لإخفاء ملف نصي وصورة من غير التأثير على مرور الشبكة.

ب- أعطى بروتوكول TCP المستخدم في القناة المخفية نتائج جيدة لأنه يوفر اتصالا موثوقا.

ج- يوفر بروتوكول UDP المستخدم في القناة المخفية اتصالا مخفيا,ولكن هذا الاتصال غير معتمد عليه وذلك لأن آلية اتصال عمل هذا البروتوكول غير موثوق به.

د- يوفر بروتوكول ICMP المستخدم في القناة المخفية مساحات إخفاء اكبر من مساحات البروتوكولات السابقة ولكنه يبعث على الشك لكثرة استخدامه في التشخيص أخطاء الشبكة.

بالتالي فان حجم البيانات التي يمكن إخفاءها ضمن حزم البروتوكولات يعتمد على المساحة التي توفرها تلك البروتوكولات للإخفاء ويزداد عدد الحزم المطلوبة للإخفاء فيها مع ازدياد حجم الملف المراد إخفاءه.

المصادر

[1] الحمامي، علاء حسين والحمامي، محمد علاء (2008)، "إخفاء المعلومات: الكتابة المخفية والعلامة المائية "، إثراء للنشر والتوزيع، الشارقة.

[2] عبد القادر، فادي، (2006)، "احترف برمجة الشبكات والنظم الموزعة"، أزمنة للنشر والتوزيع، عمان الأردن.

[3] عريان، عمار، (2003)، "المرجع الشامل في الشبكات"، شعاع للنشر والعلوم، حلب، سورية.

[4] ليدن، كانداس ومارشال، ويلينسكي، (2000)، "TCP/IP"، دار الفاروق للنشر والتوزيع، القاهرة، مصر.

[5] معمو، محمد شيخو، (2005)، "مبادئ البروتوكول TCP/IP"، شعاع للنشر والعلوم، حلب، سورية.

[6] بيبو، أميرة، (2009)، "تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة"، رسالة ماجستير ، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

[7] Ahsan, Kamran (2002), "Covert channel analysis and data hiding in TCP/IP", Unpublished M. Sc. Thesis, University of Toronto, Canada.

[8] Bharti, Vishal and Snigdh, Itu (2008), "Practical Development and Deployment of Covert Communication in IPV4", Birla Institute of Technology, India.

[9] Cabuk, Serdar , Brodley, Carla and Shields, Clay (2004), "IP Covert Timing Channels: An Initial Exploration", Washington, USA.

[10] Forouzan, Behrouz A., (2003), "TCP/IP: Protocol Suite", McGraw-Hill, USA.

[11] Kwecka, Zbigniew, (2006), "Application Layer Covert Channel Analysis and Detection", University for the degree of Bachelor of Science with Honours in Networked Computing, Napier University, Edinburgh.

[12] Lampson, Butler W., (1973), "A Note on the Confinement Problem", pp 613-615.

[13] Murdoch, Steven J., (2007), "Covert Channel Vulnerabilities in Anonymity Systems", Unpublished Ph.D. Thesis, University of Cambridge.

[14] Pozo, Rubén Rios del, (2007), "Information Hiding in Networks Covert Channels", Skovde University.

[15] Siddiqui, Kashif Ali, (2003), "Covert Chanaels in TCP/IP & Protocol Steganography".

[16] Smeets, Marc and Koot, Matthijs, (2006), "Covert Channels", Unpuplished M. Sc. Thesis, University of Amsterdam. msmeets,mrkoot}@os3.nl

[17] Zander, Sebastian , Armitage, Grenville and Branch, Philip (2006), "Covert Channels in the IP Time To Live Field", Swinburne University of Technology Australia.