

Information Hiding Techniques Using Network Protocols

Manar Younis Kashmiri

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

أميرة بيبو سلو

منار يونس كشمولة

رئاسة الجامعة، جامعة الموصل

كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ قبول البحث: 2011/06/21

تاريخ استلام البحث: 2010/04/28

المخلص

تم في هذا البحث استخدام القنوات المخفية من نوع قناة الخزن المخفية (Covert Storage Channel) لإخفاء بيانات نصية أو صورة مخفية 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 البروتوكول 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 و TCP 100%، أما بروتوكول UDP فيعتمد على آلية عمله التي لا تؤمن اتصالاً موثقاً، أما بروتوكول ICMP فإنه وفر إرسالاً مقبولاً 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 موضوعاً متعلقاً 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 إخفاء 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 شرحاً للقنوات المخفية في بروتوكولات الشبكة مثل البروتوكولات ICMP، UDP، TCP، IP. 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 أصلاً 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 إخفاء المعلومات والتشفير

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

2- الدراسات السابقة

حاول الباحثون إيجاد تقنيات إخفاء متطورة تواكب التطور السريع في تقنيات الإخفاء والشبكات، فمنهم من أنجز بحوثاً 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، مثلاً 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 و Kundur طريقة اقترحا فيها استخدام قيمة العلم (DF) Don't fragment في ترويسة بروتوكول الانترنت IP لإخفاء قيم ثنائية (0) أو (1) وذلك فقط في حالة معرفة المرسل قيمة وحدة النقل العظمى (MTU) Maximum Transfer Unit 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 segment) TCP عندما يكون العلم (RST) TCP reset مشغلا، وهذا العلم يعمل على قطع الاتصال، ولا يحتوي هذا المقطع على بيانات. [17]
5. في عام 2004 قدم الباحث Lliamas بحثاً 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 و Gomez و Watanabe بحثاً 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 و Snigdha بحثاً 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 و Lwies بحثاً 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 و Armitage و Branch بحثاً لإخفاء البيانات في حقل مدة الحياة (TTL) Time To Live 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 العنوان 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 المرسل 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 بروتوكولات TCP/IP

هي مجموعة من البروتوكولات التي تمت تسميتها طبقاً لأهم بروتوكولين في المجموعة وهما IP و TCP. 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 انترنت IP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP Version إصدار IP		Header Length طول الترويسة		Type of Service نوع الخدمة				Total Length الطول الكلي																							
Identification (Fragment ID) التعريف				Flags الأعلام		Fragment Offset الزياح المقطع																									
Time - To - Live (TTL) مددالحياة				Protocol بروتوكول				Header Checksum المجموع التتقني																							
Source IP Address عنوان المصدر																Destination IP Address عنوان الوجهة															
Options الخيارات																Padding الحشو															

الشكل (1). ترويسة بروتوكول الانترنت IP

ب- بروتوكول التحكم بالإرسال TCP

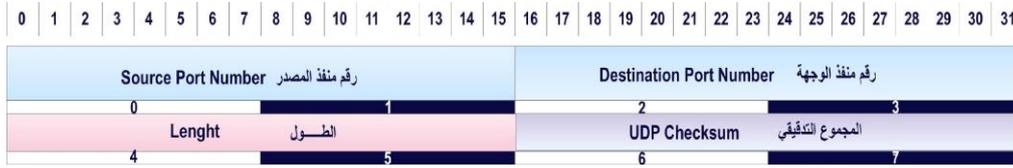
بروتوكول TCP هو من بروتوكولات طبقة النقل يهدف إلى توفير خدمة نقل البيانات بموثوقية عالية بين حاسبين متصلين عبر شبكة الاتصال وهو يرتبط دوماً ببروتوكول الإنترنت، ويستخدم من قبل تطبيقات الشبكات التي تتطلب اتصالاً آمناً وموثوقاً ويضمن عدم ضياع حزم البيانات [3]. تحتوي ترويسة TCP على حقول تضمن الاتصال الموثوق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

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source Port Number رقم منفذ المصدر								Destination Port Number رقم منفذ الوجهة																							
Sequence Number الرقم التسلسلي																Acknowledgment Number رقم الاعتراف															
Reserves محجوز				Flags اعلام				Windows size حجم النافذة																							
TCP checksum المجموع التتقني				Urgent pointer المؤشر العاجل										Options الخيارات																	
Options الخيارات																Padding الحشو															

الشكل (2). ترويسة TCP

ج- بروتوكول معطيات المستخدم UDP

هو من بروتوكولات طبقة النقل وهو لا يؤمن اتصالاً موثقاً، أي 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 أبداً، 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 رئيسيين 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، مثلاً 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 المرسله 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 الأحداث في النظام، مثلاً 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 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

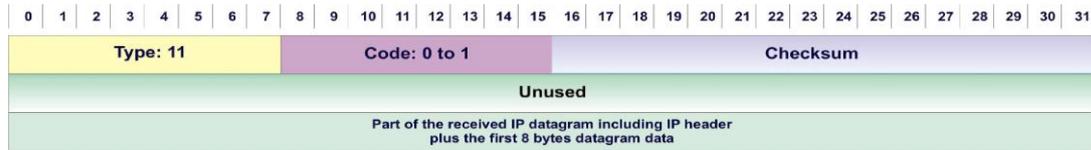
أن كل رسالة من رسائل ICMP لها بنية خاصة تختلف عن الرسائل الأخرى، وفي بعض الحالات تتولد رسائل من ICMP تحتوي على حقول غير مستخدمة يستفاد منها في تصميم القنوات المخفية، ومن أشهر هذه الرسائل المستخدمة في القنوات المخفية: [10] [16]

1. الوجهة لا يمكن الوصول إليها Destination Unreachable

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type: 3						Code: 0 to 15						Checksum																			
Unused																															
Part of the received IP datagram including IP header plus the first 8 bytes datagram data																															

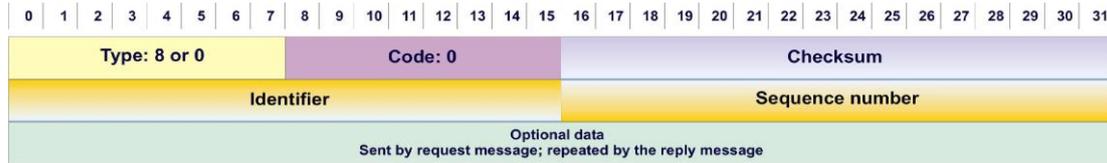
الشكل (5). بنية رسالة الوجهة لا يمكن الوصول إليها

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

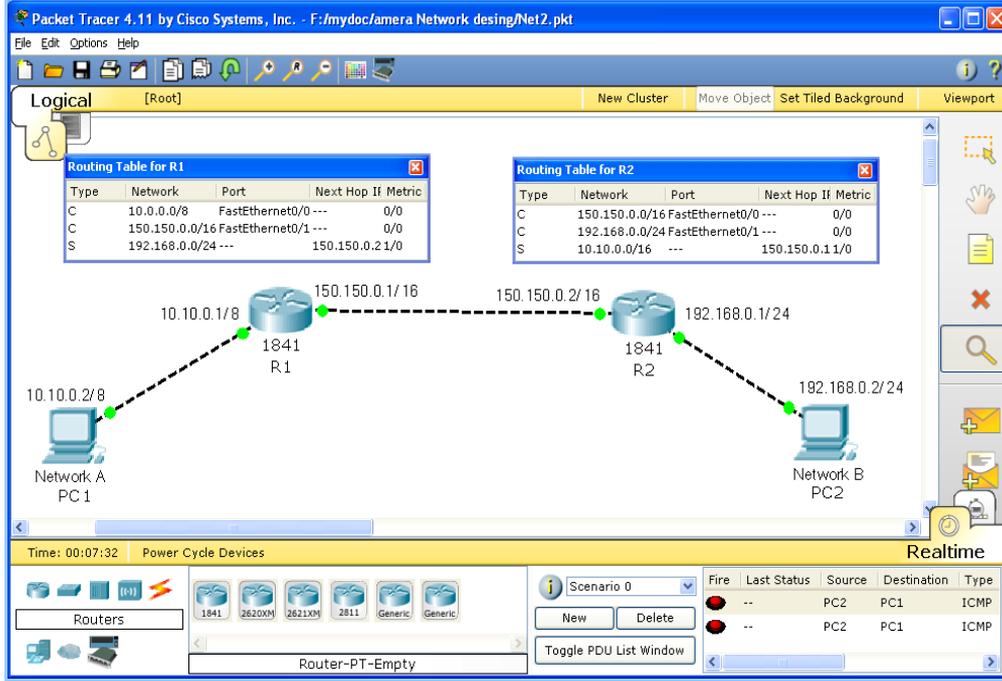
تم اقتراح نظام لإخفاء معلومات سرية (مشفرة) وإرسالها بصورة مخفية عبر شبكة الاتصال، حيث استخدم بروتوكول الانترنت IP في تصميم قناة مخفية باستخدام حقل التعريف Identification، وكذلك استخدام بروتوكول TCP في تصميم قناة مخفية باستخدام حقل مؤشر الحالة الطارئة Urgent Pointer، وبروتوكول UDP باستخدام حقل رقم منفذ المصدر Source Port، وأخيراً البروتوكول 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 المرسله عبر القنوات المخفية سواء أكانت تلك البيانات نصاً مشفراً أم صورة مخفية فيها نص مشفر.

1-5 تصميم القنوات المخفية

أ- تصميم شبكة الاتصال المحلية

تتكون الشبكة المحلية من ثلاث شبكات هي 10.10.0.0 و 150.150.0.0 و 192.168.0.0، 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 فيزيائياً.



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

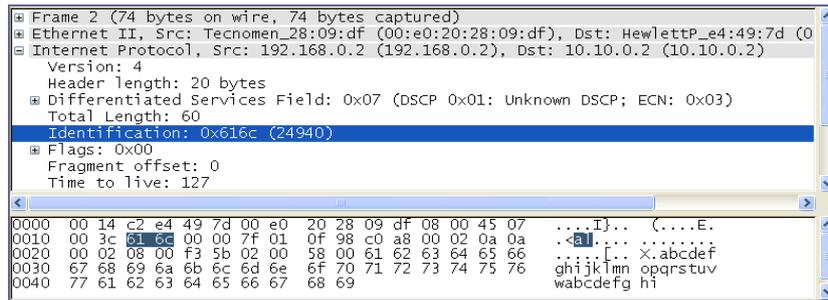
ب- خوارزمية الإخفاء باستخدام القنوات المخفية في بروتوكولات الشبكة

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

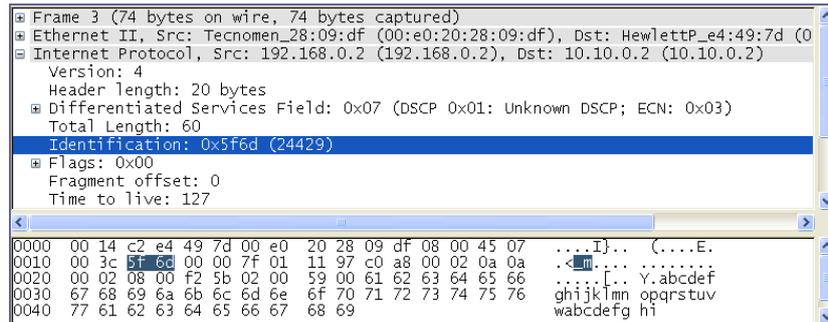
المخرجات: حزم الشبكة المُخفى فيها بيانات سرية.

خطوات الخوارزمية:

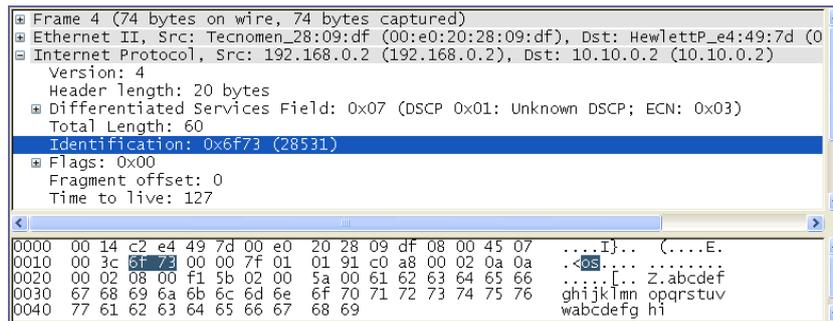
- 1- إدخال اسم ملف الإدخال المراد إرساله عبر القنوات المخفية.
- 2- حساب حجم الملف.
- 3- توليد حزم الشبكة.
- 4- قراءة حزمة شبكة تكون في حالة إرسال.
- 5- حشر حجم الملف في حقل ID في ترويسة IP.
- 6- تغيير قيمة الحقل TOS في ترويسة IP .
- 7- حساب قيمة المجموع التديقي IPCHECKSUM لترويسة IP.
- 8- إرسال حزمة 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 و 32 كتلة ثمانية في حالة الإخفاء في بروتوكول ICMP.
- 11- حساب قيمة المجموع التديقي 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 .



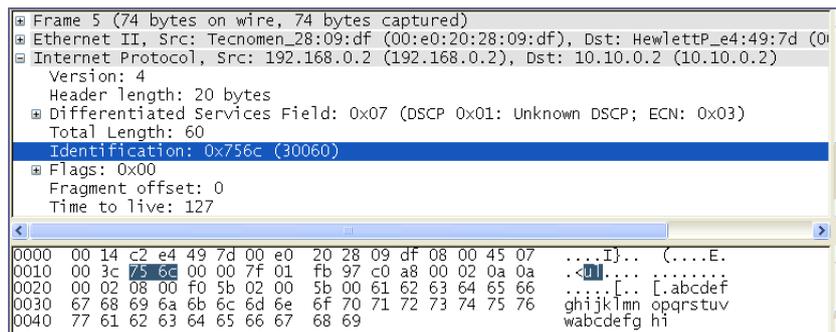
الشكل (11). ترويسة بروتوكول IP مخفي فيها الحرفان al



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



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



الشكل (14). ترويسة بروتوكول IP مخفي 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:

```

Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: 1107 (1107), Seq:
Source port: 1503 (1503)
Destination port: 1107 (1107)
Sequence number: 0 (relative sequence number)
[Next sequence number: 30 (relative sequence number)]
Acknowledgement number: 0 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
 0... .... = Congestion Window Reduced (CWR): Not set
 .0... .... = ECN-Echo: Not set
 ..0... .... = Urgent: Not set
0000 00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 07 .....IJ... (....E.
0010 00 46 6f 5e 00 00 7f 06 01 97 c0 a8 00 02 0a 0a ...FoA.....P.....
0020 00 02 05 df 04 53 42 7f 61 56 46 43 be 02 50 18 ...SB. avFC..P.
0030 5a d3 41 5a 61 6c 03 00 00 1e 02 f0 80 64 9a f3 ...Z.AZal.....d...
0040 9e d8 f0 10 08 00 00 00 00 00 00 00 73 00 63 00 .....s.c.
0050 63 00 00 00
    
```

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

```

Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: 1107 (1107), Seq:
Source port: 1503 (1503)
Destination port: 1107 (1107)
Sequence number: 0 (relative sequence number)
[Next sequence number: 86 (relative sequence number)]
Acknowledgement number: 0 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
 0... .... = Congestion Window Reduced (CWR): Not set
 .0... .... = ECN-Echo: Not set
 ..0... .... = Urgent: Not set
0000 00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 07 .....IJ... (....E.
0010 00 7e 6f 6d 00 00 7f 06 01 50 c0 a8 00 02 0a 0a ...nom.....P.....
0020 00 02 05 df 04 53 42 7f 61 56 46 43 be 02 50 18 ...SB. avFC..P.
0030 d3 a2 ca 89 5f 6d 03 00 00 1e 02 f0 80 64 9a f3 ...m.....d...
0040 9e d8 f0 10 08 00 00 00 00 00 00 00 73 00 63 00 .....s.c.
0050 63 00 00 00 03 00 00 1c 02 f0 80 64 9a f3 9e d8 c.....d....
0060 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    
```

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

```

Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: 1107 (1107), Seq:
Source port: 1503 (1503)
Destination port: 1107 (1107)
Sequence number: 0 (relative sequence number)
[Next sequence number: 226 (relative sequence number)]
Acknowledgement number: 0 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
 0... .... = Congestion Window Reduced (CWR): Not set
 .0... .... = ECN-Echo: Not set
 ..0... .... = Urgent: Not set
0000 00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 07 .....IJ... (....E.
0010 01 0a 6f 81 00 00 7f 06 00 b0 c0 a8 00 02 0a 0a ...o.....P.....
0020 00 02 05 df 04 53 42 7f 61 56 46 43 be 02 50 18 ...SB. avFC..P.
0030 cc a5 a1 80 6f 73 03 00 00 1e 02 f0 80 64 9a f3 ...os.....d...
0040 9e d8 f0 10 08 00 00 00 00 00 00 00 73 00 63 00 .....s.c.
0050 63 00 00 00 03 00 00 1c 02 f0 80 64 9a f3 9e d8 c.....d....
0060 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    
```

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

```

Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: 1107 (1107), Seq:
Source port: 1503 (1503)
Destination port: 1107 (1107)
Sequence number: 0 (relative sequence number)
[Next sequence number: 450 (relative sequence number)]
Acknowledgement number: 0 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
 0... .... = Congestion Window Reduced (CWR): Not set
 .0... .... = ECN-Echo: Not set
 ..0... .... = Urgent: Not set
0010 01 ea 6f ad 00 00 7f 06 ff a3 c0 a8 00 02 0a 0a ...o.....P.....
0020 00 02 05 df 04 53 42 7f 61 56 46 43 be 02 50 18 ...SB. avFC..P.
0030 c1 ee c6 3e 75 6c 03 00 00 1e 02 f0 80 64 9a f3 ...>ul.....d...
0040 9e d8 f0 10 08 00 00 00 00 00 00 00 73 00 63 00 .....s.c.
0050 63 00 00 00 03 00 00 1c 02 f0 80 64 9a f3 9e d8 c.....d....
0060 f0 0e 08 00 00 00 00 00 00 00 00 00 00 00 00
    
```

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:

```

# Frame 2 (102 bytes on wire, 102 bytes captured)
# Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:
# Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
# User Datagram Protocol, Src Port: 24940 (24940), Dst Port: 49609 (49609)
Source port: 24940 (24940)
Destination port: 49609 (49609)
Length: 56521
Checksum: 0xb8fd
Data (60 bytes)
0020 00 02 61 6c c1 c9 dc c9 b8 fd a1 c9 00 07 d2 ba ..a1.....
0030 21 f9 d3 d8 e1 22 00 00 01 b8 00 00 ca 9c 00 00 !.....
0040 01 96 12 ec eb c0 00 04 7d c0 81 ca 00 06 d2 ba !.....
0050 21 f9 01 0f 48 4f 4d 45 2d 36 45 42 43 32 33 38 !...HOME -6EBC238
0060 34 37 38 00 00 00 478...

```

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

```

# Frame 4 (78 bytes on wire, 78 bytes captured)
# Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:
# Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
# User Datagram Protocol, Src Port: 24429 (24429), Dst Port: 49609 (49609)
Source port: 24429 (24429)
Destination port: 49609 (49609)
Length: 11644
Checksum: 0xb98b
Data (36 bytes)
0010 00 40 cb ce 00 00 7f 11 a5 21 c0 a8 00 02 0a 0a .@.....
0020 00 02 5f 6d c1 c9 2d 7c b9 8b a0 c9 00 01 d2 ba !.m.-|.....
0030 21 f9 81 ca 00 06 d2 ba 21 f9 01 0f 48 4f 4d 45 !.....HOME
0040 2d 36 45 42 43 32 33 38 34 37 38 00 00 00 -6EBC238 478...

```

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

```

# Frame 6 (82 bytes on wire, 82 bytes captured)
# Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:
# Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
# User Datagram Protocol, Src Port: 28531 (28531), Dst Port: 49609 (49609)
Source port: 28531 (28531)
Destination port: 49609 (49609)
Length: 7550
Checksum: 0xd8af
Data (40 bytes)
0010 00 44 cb 11 00 00 7f 11 a4 e1 c0 a8 00 02 0a 0a .@.L.....
0020 00 02 6f 73 c1 c9 1d 7e d8 af a0 c9 00 01 d2 ba !.os...~.....
0030 21 f9 81 ca 00 07 d2 ba 21 f9 01 0f 48 4f 4d 45 !.....HOME
0040 2d 36 45 42 43 32 33 38 34 37 38 02 04 61 6d 6f -6EBC238 478..amo
0050 6f 00 o.

```

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

```

# Frame 8 (78 bytes on wire, 78 bytes captured)
# Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:
# Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
# User Datagram Protocol, Src Port: 30060 (30060), Dst Port: 49609 (49609)
Source port: 30060 (30060)
Destination port: 49609 (49609)
Length: 63470
Checksum: 0xb98b
Data (36 bytes)
0010 00 40 cc 4c 00 00 7f 11 a4 a7 c0 a8 00 02 0a 0a .@.L.....
0020 00 02 75 6c c1 c9 f7 ee b9 8b a0 c9 00 01 d2 ba !.u.....
0030 21 f9 81 ca 00 06 d2 ba 21 f9 01 0f 48 4f 4d 45 !.....HOME
0040 2d 36 45 42 43 32 33 38 34 37 38 00 00 00 -6EBC238 478...

```

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:

```

Frame 2 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:0c:29:14:c2:e4)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000  00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010  00 3c 13 f9 00 00 7f 01 5d 0d c0 a8 00 02 0a 0a  .<.....].....
0020  00 02 08 00 08 5c 02 00 a0 03 48 69 64 69 6e 67  .....\..Hiding
0030  20 6d 65 73 73 61 67 65 73 20 69 6e 20 69 6d 61  message s in ima
0040  67 65 20 64 61 74 61 2c 20 63                    ge data, c
    
```

الشكل(23). ترويسة الحزمة الأولى لبروتوكول ICMP

```

Frame 3 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:0c:29:14:c2:e4)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000  00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010  00 3c 13 fa 00 00 7f 01 5d 0c c0 a8 00 02 0a 0a  .<.....].....
0020  00 02 08 00 89 d8 02 00 a1 03 61 6c 6c 65 64 20  ..X... ..alled
0030  73 74 65 67 61 6e 6f 67 72 61 70 68 79 2c 20 69  steganog raphy, i
0040  73 20 75 73 65 64 20 62 79 20                    s used B y
    
```

الشكل(24). ترويسة الحزمة الثانية لبروتوكول ICMP

```

Frame 4 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:0c:29:14:c2:e4)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000  00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010  00 3c 13 fc 00 00 7f 01 5d 0a c0 a8 00 02 0a 0a  .<.....].....
0020  00 02 08 00 58 a1 02 00 a2 03 63 72 69 6d 69 6e  ..X... ..crimin
0030  61 6c 73 0a 61 6e 64 20 6e 6f 6e 63 72 69 6d 69  als.and noncrimi
0040  6e 61 6c 73 20 61 6c 69 6b 65                    nals ali ke
    
```

الشكل(25). ترويسة الحزمة الثالثة لبروتوكول ICMP

```

Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:0c:29:14:c2:e4)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000  00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010  00 3c 13 ff 00 00 7f 01 5d 07 c0 a8 00 02 0a 0a  .<.....].....
0020  00 02 08 00 fb 4d 02 00 a3 03 20 74 6f 20 73 65  ..M.. .. to se
0030  6e 64 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 6f  nd inform ation o
0040  76 65 72 20 74 68 65 20 69 6e                    ver the in
    
```

الشكل(26). ترويسة الحزمة الرابعة لبروتوكول ICMP

```

Frame 6 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (00:0c:29:14:c2:e4)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000  00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010  00 3c 14 00 00 00 7f 01 5d 06 c0 a8 00 02 0a 0a  .<.....].....
0020  00 02 08 00 75 6d 02 00 a4 03 74 65 72 6e 65 74  ..um.. ..ternet
0030  2e 0a 0a 54 68 65 20 64 65 74 65 63 74 69 6f 6e  ..The d etection
0040  20 6f 66 20 68 69 64 64 65 6e                    of hidd en
    
```

الشكل(27). ترويسة الحزمة الخامسة لبروتوكول ICMP

```

Frame 7 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (08:00:0c:2e:49:7d)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0010 00 3c 14 04 00 00 7f 01 5d 02 c0 a8 00 02 0a 0a  .<.....\.....
0020 00 02 08 00 3b 9d 02 00 a5 03 20 6d 65 73 73 61  .:.....\.. messa
0030 67 65 73 20 69 6e 20 69 6d 61 67 65 20 64 61 74  .:..6...n webs
0040 61 20 73 74 6f 72 65 64 20 6f 61 67 65 20 64 61 74  .:..6...tes and compute
        a stored o
    
```

الشكل (28). ترويسة الحزمة السادسة لبروتوكول ICMP

```

Frame 8 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (08:00:0c:2e:49:7d)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000 00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010 00 3c 14 07 00 00 7f 01 5c ff c0 a8 00 02 0a 0a  .<.....\.....
0020 00 02 08 00 c3 36 02 00 a6 03 6e 20 77 65 62 73  .:..6...n webs
0030 69 74 65 73 20 61 6e 64 20 63 6f 6d 70 75 74 65  .:..6...tes and compute
0040 72 73 2c 0a 63 61 6c 6c 65 64 61 67 65 20 64 61 74  .:..6...rs..call ed
    
```

الشكل (29). ترويسة الحزمة السابعة لبروتوكول ICMP

```

Frame 9 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Tecnomen_28:09:df (00:e0:20:28:09:df), Dst: HewlettP_e4:49:7d (08:00:0c:2e:49:7d)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 10.10.0.2 (10.10.0.2)
Internet Control Message Protocol

0000 00 14 c2 e4 49 7d 00 e0 20 28 09 df 08 00 45 05  ....I}.. (....E.
0010 00 3c 14 0e 00 00 7f 01 5c f8 c0 a8 00 02 0a 0a  .<.....\.....
0020 00 02 08 00 07 63 02 00 a7 03 20 73 74 65 67 61  .:..c... stega
0030 6e 61 6c 79 73 69 73 2e 20 61 6d 65 72 61 20 62  .:..c...nalysis. amera b
0040 69 62 6f 2e 0a 61 6c 6c 65 64 61 67 65 20 64 61 74  .:..c...tibo..all ed
    
```

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 التديقي 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 اتصالاً موثوقاً.
 - ج- يوفر بروتوكول UDP المستخدم في القناة المخفية اتصالاً مخفياً، 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 أكبر من مساحات البروتوكولات السابقة ولكنه يبعث على الشك لكثرة استخدامه في التشخيص أخطاء الشبكة. بالتالي فإن 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)، "احتراف 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 Snigdha, 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 Channels in TCP/IP & Protocol Steganography".
- [16] Smeets, Marc and Koot, Matthijs, (2006), "Covert Channels", Unpublished 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.