إنشاء جدار ناري لحماية الانترنيت من الاختراق

زينة هلال طعان
مهندس حاسبات

م.د.فالح حمزة عيدان
وزارة التعليم العالي والبحث العلمي
دائرة البحث والتطوير

١. الخلاصة

صمم برنامج (software) في نظام تشغيل لنكس باستخدام أوامر الـ (Iptables) والاستعانه بالبرمجة بلغة C++ لأنه النظام الأكثر أمناً وحماية والأقل تعرضاً للفايروسات ، وذلك بسبب الاختراقات الكثيرة لأنظمة التشغيل المتعددة ، والتي تشكل حاليا معضلة تعاني منها الشبكات الحاسباتية.

إن برنامج الجدار الناري الذي صمم في البحث يعمل في نظام التشغيل لنكس لكونه سهل الاستخدام ومفتوح المصدر ويمكن تطويره باستمرار ، وتستخدم الدول المتطورة هذا النظام في مؤسساتها .

يمتاز البرنامج المصمم في البحث عن غيره ، بإمكانية فتح المنافذ التي تحتاجها أو غلق المنافذ التي لا تحتاجها في العمل وذلك للتخفيف من كثرة الاختراقات.

Abstract

Preparation of Firewall System to Protect Internet from Penetration

The firewall software is designed in LNUIX operating system by using iptables orders and C++ tanguage program. The use of LNUIX Operating system in the internet network is usually more safe , more protected , and also highly virus

open source information , and also continuously developed , It's more preferred in the developed countries .

The major property of the present research compared the other researches to be distinguished by the possibility of opening the outlets that we needs , or , close the outlets that we don't need.

resisted compared to others operating systems . Because of so many penetrations that might accrued in to the internet network which is a major problem system , in the computers network operation .

The firewall program designed in the present research , which is working in the LNUIX operating system is consided to be easy ,

٣. المقدمة

أصبح الاتصال بالانترنيت من المتطلبات المهمة لعمل الشبكات في هذا العصر ، ويستوجب ذلك الحفاظ على الأمن الحاسباتي بقدر المستطاع ، فالأخطار محتملة الحدوث دائماً وان تقدم التقنية الحديثة في عمل الشبكات والأنظمة الحاسباتية .. حقق مستوىً جيد من الأمن للشبكات وفي متناول يد الجميع .وعليه تنقسم برامج حماية الشبكات على قسمين ؛ أحدهما يكون جدار ناري بين الشبكة والعالم الخارجي ، والآخر يخص حالة المنافذ والثغرات في مكونات الشبكة، و كلا القسمين من الضروريات عند اتصال الشبكة مع الانترنيت .

يفضل أن يكون برنامج الجدار الناري في حاسبة إلكترونية مستقلة ويعمل كنقطة دخول وحيدة إلى الشبكة ويحدد البرنامج المواقع المفيدة ويرفض المواقع الضارة او المواقع الملوثة بالفايروسات ، وكذلك يمنع برنامج الجدار الناري أرقام معينة من [(IP) (Internet Protocol)] عن الدخول ويمكن له ان يصرح بعدد محدود من مواقع الانترنيت ويمكن للجدار الناري ان يمنع عدد من التطبيقات والخدمات التي تتحكم بمستوى الأمن من التعامل مع الشبكة مثل خدمة نقل الملفات وفتح المواقع في الانترنيت

(File Transfer Protocol FTP)
و(Hyper Text Protocol (HTIP) Transfer او الاتصال بكمبيوتر بعيد (Telnet) (ملحق رقم ٣).

ومن الجدير بالذكر ان قدرة برامج الجدار الناري تختلف في اكتشاف الثغرات حسب نوع نظام التشغيل ، إذ أن نظام التشغيل لينكس ذو فعالية عالية وأمان اكثر من نظام التشغيل ويندوز الشائع الاستعمال لكون نظام لينكس ذو قدرة كبيرة على التحكم بالنظام وتغيير سلوك النظام، فالتحسينات الدائمة والتطويرات تجعل النظام اكثر ثباتاً وآمنا .[١]

هدف البحث

يهدف المشروع الى تصميم برنامج جدار ناري (Software) يستعمل لحماية شبكات الانترنيت من الاختراق وباستخدام اوامر برنامج الـ (iptables) والاستعانة بالبرمجة بلغة C++ في نظام التشغيل لينكس (LNUIX) .

٣. الكلمات الدالة

- الجدار الناري Fire Wall
- لغة البرمجة C++
- نظام تشغيل LNUIX
- خط إنترنيت Internet Protocol (IP)
- أوامر برنامج (iptables)

٤. المواد وطرائق التنفيذ

٣-١: الجدار الناري (الجانب النظري)

يعتبر الجدار الناري خط الدفاع في حل أمني شامل لتقنية المعلومات ، لذا يستعمل الجدار الناري في الشبكات التابعة للشركات والمنشآت ، ويسمح الجدار الناري للمستخدم بإرسال طلباته إلى الانترنيت ، ولكنه لا يسمح للبيانات بالمرور إلى المستخدم من الانترنيت (شكل رقم (١)) .

إنّ الجدار الناري في الشبكات هو مجموعة من البرامج المتصلة ببعضها وموجودة على مرور المدخلGot way server على شبكة ما من اجل حماية معلومات الشبكة الخاصة بالمستخدمين من شبكات أخرى ، فالشركة التي لديها شبكة داخلية و تسمح لموظفيها الاتصال بالانترنيت فان هذه الشركة تقوم بتثبيت جدار ناري لمنع الدخلاء من الحصول على بيانات الشركة

ان الجدار الناري هو مجموعة من الأنظمة تتحكم بالوصول بين شبكتين وله نوعان من الآلية هما :

النوع الأول يمنع مرور الحزم والنوع الثاني يسمح لها بالمرور بمعنى آخر فأن الجدار الناري ينفذ السياسة الأمنية للوصول الى الشبكة.[٢]

ومن ناحية أخرى فهناك مهام متعددة للجدار الناري التي تتمثل في كونه يسجل فعاليات الانترنيت بكفاءة لان جميع الحزم تمر عبره ، كما يؤمن الجدار الناري مكان ملائم لجمع المعلومات حول المنظومة خلال استعمال الشبكة .

يعد الجدار الناري بمثابة بؤرة القرارات الأمنية باعتباره منطقة فحص تمر خلالها الحزم للخدمات المسموح لها بالمرور فقط ، كما يحد الجدار الناري من المخاطر التي تتعرض لها الشبكة حيث يحافظ على مقطع من موقع الشبكة منفصلاً عن المواقع الأخرى. [٢]

تشبه السياسة الأمنية للجدار الناري ، الأمم التي لا تستطيع أن تضمن السلامة والأمن لمواطنيها بدون حدود مسيطر عليها ولا تمنع القرصنة و السرقة بحدودها المتناهية ، من ذلك لا تستطيع الشبكات ان تضمن الأمن والخصوصية للمعلومات بدون وجود مسيطر عليها لكي تبقى مصادر الشبكة أمينة دون أن تخترق ، حيث أن كفاءة الاتصالات المجهزة منه قبل الانترنيت جعل من السهل على المخترقين أن يستثمروا موارد الشبكة الخاصة .

٣-٢ مرتكزات بناء الجدار الناري

أن الجدار الناري هو تركيبه من الأجهزة والبرامج التي توفر نظام أمن والتي تستخدم عادة لمنع الوصول غير المصرح به من الخارج إلى شبكة اتصال داخلية ، إذ يراقب الجدار الناري كافة اوجه الاتصالات التي تعبر مساره و يختبر عنوان الوجهة والمصدر لكل رسالة يعالجها لمنع حركة المرور غير المطلوب من الطرف العام للاتصال إلى الطرف الخاص. [٢]

يؤدي الجدار الناري عمله باستعمال طريقتين أساسيتين :

١.ترشيح الحزم : يرفض الحزم من المستضيف غير المرخص ويرفض محاولات الاتصال بالخدمات غير المرخصة.

٢.ترجمة عناوين الشبكة : ترجمة عناوين بروتكول الانترنيت للحاسبة الداخلية لإخفائها عن المراقبة الخارجية ، وكذلك تؤدي معظم برامج الجدار الناري خدمات أمنية أخرى منها:

١. التخويل المشفر : يسمح للمستخدمين على الشبكة العامة بان يثبتوا هويتهم إلى الجدار الناري لكي يصل إلى الشبكة الخاصة من مواقع خارجية .

٢. **الاتفاق المشفر** : يؤسس اتصال آمن بين شبكتين خاصتين عبر وسط عام مثل الانترنيت

يعرف الجدار الناري كنظام او مجموعة نظم تطبق سياسة السيطرة على الدخول بين

شبكتين في نفس السياق بأخذ برنامج الحماية أحد الشكلين الاتيين:

١- جدران نارية مخصصة تعمل على الحواسيب الفردية.

٢-جدران نارية للشبكات كآلية صممت لحماية حاسوب او اكثر.

كما ان كلا النوعين السابقين للجدران النارية يسمحان للمستخدم بالتعرف على الارتباطات المتجهة للداخل . والكثير منها أيضا يستطيع التحكم في المنافذ القادرة على أن تصل إلى الانترنيت من الأجهزة المحمية.[٣]

يوضح الشكل رقم (٢) الجدار الناري كبرنامج في حاسبة تسيطر على مجموعة من الحاسبات ، ويمثله الشكل رقم (٣) الجدار الناري عندما يمكن ان يكون كجهاز مادي.

٣-٣التطبيقات الأمنية للجدار الناري

أن الجدار الناري لا يستطيع الحماية من :

١. المخربين من الداخل (Malicious Insider)
٢. التوصيلات التي لا تمر من خلاله.
٣. التهديد غير المعروف او الجديد.
٤. ضد الفايروسات.

لا يكفي الجدار الناري لوحده لتأمين الشبكة بل هو جزء مكمل لأي برنامج أمني لكنه ليس برنامج أمني بحد ذاته ، لان الحل الأمني الكامل يتألف غالباً من مجموعة من الطبقات التي تتضمن الطبقة الأولى فيه برامج مكافحة الفايروسات او أحد أشكالها (الديدان وأحصنة طروادة) وتضم الطبقة الثانية برامج تقنية المواقع ورسائل البريد الإلكتروني ، والثالثة الجدار الناري ، والرابعة البرامج التنبؤية المانعة للاختراقات والهجمات المجهولة الهوية ، والخامسة برامج كشف الثغرات الأمنية بصفة دائمة ، والسادسة برامج التشفير.[٢]

ينبغي أيضا أن يتوفر نظام تحكم لجميع البرامج والأدوات والطبقات الموجودة في الطبقات الستة المذكورة ، وتكون مهمة هذا النظام هو فرز تقارير الإخفاء الزائفة من الحقيقة توفيراً للوقت والجهد .[٤]

يتعين ان يكون فريق العمل مدرب و يتمتع بدرجة عالية من الكفاءة لادارة الشبكات وبذلك تكون المنظومة الأمنية متكاملة وإذا قامت شركة متخصصة بتنفيذ كل هذه الإجراءات فإنها تكون قد حققت أقصى درجات الحماية الشاملة ضد كافة أنواع الإخطار، وقد لا تحتاج بعض المؤسسات والشركات إلى هذه الأنظمة من الحماية من ناحية أخرى ، فلكي تكون قادر على تحديد حجم الاستثمارات اللازمة في مجال أمن وحماية البيانات والشبكات ، ينبغي أن تقوم بتحديد قيمة الأصول المعلوماتية التي تملكها

الشركة وحجم الخسائر التي يمكن أن تنجم من جراء فقدان البيانات او سرقتها وعلى ضوء النتائج يتم تحديد حجم الاستثمارات الأمنية المطلوبة بنسبة مئوية معينة. (٤)

٣-٤التجارب السابقة لبناء الجدار الناري

وضعت معظم برامج الحماية للاستعمال الفردي ، وجاءت هذه البرامج بخيارات امنية قد ي**ختار منها المستعمل ما يريد ، ومن هذا الجانب اقتصرت الدراسة الحالية على تحليل مجموعتين من البرامج المعدة سابقاً والواسعة للاستخدام مثل : (Norton Security Internet, Zone Alarm)**

١.برنامج (Zone Alarm)

هذا البرنامج من فئة الجدران النارية المنيعة يتميز بسهولة التعامل معه و تطويعه لكي يلائم متطلبات الأمن ويواجه التحديات الموجودة سلفاً وما يستجد منها .

المميزات :

١. **سهولة استعمال البرنامج بشكل عام .**
٢. **إمكانية التحكم في درجة أمن الشبكة الداخلية.**
٣. **القدرة العالية على غلق جميع المنافذ من خلال واجهة البرنامج.**
٤. **إمكانية عرض معلومات تفصيلية عن المخترق.**

العيوب :

أن ما يعيب برنامج (Zone Alarm) بشكل أساسي هو قصر الأداء عند التعامل مع المحتوى الداخلي لصفحات الشبكة.

٢.برنامج (Norter Internet Security) :

أن هذا البرنامج من فئة برامج الأمن المستعملة في الشبكات ، وما يميز البرنامج أن له قدرات خيالية وذو قدرة عالية من الأمن والحماية .

المميزات :

يتميز البرنامج بمنع تشغيل المتحكمات ألا بإيعاز من المشغل إذ يتعامل البرنامج مع الأمن وكأنه جدار ناري مميز يمنع إعلانات صفحات الانترنيت والتي تسبب الإرباك في العمل ، كذلك يتميز البرنامج بكشف عدد الصفحات التي تم طلبها والتي تم رفضها من الشبكة ، فيقوم البرنامج بحفظها جميعاً وتصفحها عند الحاجة .

العيوب :

صعوبة استخدام هذا البرنامج للمبتدئين في عمل الشبكات لانه يتطلب توفير مهارات عالية في تحديد متطلبات الأمن في الشبكة ، وهناك مجموعة أخرى من الجدران النارية المتداولة مثل (Clean و Black leas) وغيرها تؤدي حماية مفردة أي تكون في

مجملها جدار ناري خاص ، أي إنها لا تحمي الشبكات . [٥]

٣-٥ معنى الاختراق وأنواعه

الاختراق بشكل عام هو القدرة لبلوغ هدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف ، يعتمد الاختراق على السيطرة عن بعد Remote وهي لا تتم الا بوجود عاملين مهمين :

الأول : البرنامج المسيطر ويعرف بالعميل Client.

الثاني : الخادم Server الذي يقوم بتسهيل عملية الاختراق ذاتها ، لابد من توفر برنامج على كل من جهازي المخترق والضحية، ففي جهاز الضحية يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل .

تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق ، ولكنها جميعاً تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (Server) الخاص بالمخترق ، وجهاز المخترق على الطرف الآخر حيث يوجد برنامج المستفيد او العميل Client. [٦]

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة الى ثلاثة أقسام:

١. اختراق المزودات والأجهزة الرئيسية للشركات والمؤسسات او الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالباً ما يتم ذلك باستعمال المحاكاة (Spofing) وهو مصطلح يطلق على عملية انتحال شخصية للدخول إلى النظام ، اذ أن حزم الـ (IP) تحتوي على عناوين المرسل والمرسل إليه ، وهذه العناوين ينظر أليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة ومن خلال طريقة تعرف بمسارات المصدر (Source Routiy) ، فأن حزم الـ (IP) قد تم إعطائها شكلاً يبدو معه وكأنها قادمة من كومبيوتر معين بينما هي في حقيقة الأمر ليست قادمة منه وعلى ذلك فأن النظام اذا وثق بهوية عنوان مصدر الخدمة فانه يكون بذلك قد خدع .

٢. اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات ، وهي طريقة للأسف شائعة لسذاجة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب آخر.

٣.التعرض للبيانات أثناء انتقالها والتعرف على شفرتها أن كانت مشفرة وهذه الطريقه تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات المصرفيه. [٦]

ان تحديد الأخطار المحدقة بتقنية المعلومات بالمنشأة وأختيار أنسب الخطوات لحماية عملية معقدة لأدارة الأخطار والسيطرة عليها

.. تجعل المنشأة في وضع أفضل يمكنها من التحكم في إدارة الأخطار والسيطرة عليها إضافة إلي إدارة عملياتها بصورة أمنه ومن ثم تطوير سبل ثابتة لحماية المعلومات. (٧)
وعند استعمال شبكة الانترنيت فأن الحماية في هذه الحالة تعتمد على الجدار الناري ، وهذا الجدار يعتمد على عدة عوامل يجب فحصها بالكامل .وعليه فان الفحوصات التي تقوم بها لذلك الجدار وإمكانية اختراقه تحدد المخاطر المتعلقة بالتصميم والإدارة الحالية لذلك الجدار . فأننا تقوم بأختيارات اختراق جزء من عملية تحليل المخاطر ، وتقوم أيضا بأجراء وأختبار مفتوح لكل أساليب الاختراق المعروفة باستعمال كافة المعلومات المتاحة على تصميم الجدار وإمكاناته. (٧)

٣-٦ اعتماد نظام التشغيل لنكس في تصميم الجدار الناري (التطبيق العملي)

نظام التشغيل Linux :

إن Linux هو لب (Core) أو نواة نظام تشغيل للحاسبات شبيه بـ UNIX ، وقد قام Linus Torvalds بكتابته و أطلقه أول مرة عن طريق الانترنيت عام ١٩٩١ وازداد أحكاما مع كل نسخة جديدة او تنقيح جديد ، وعند القيام بتثبيت Linux ذلك يعني تتثبيت واستخدام توزيع مجموعة من البرامج المترابطة التي تتعامل مع نواة Linux . وهناك عدد من توزيعات Linux ذات الشعبية مثل Red Hat Linux و Stack ware و Caldera و Debian و Mandrake و Turbolinux , S.U.S.E ، ولكل من هذه التوزيعات طريقة مختلفة للتنصيب ويجري معالجتها بأدوات صيانة برمجية مختلفة.

باختيار Linux نكون قد اخترنا أحدث نظم تشغيل الحواسيب المعاصرة وأكثرها مرونة وقدرة ، ففي الوقت الذي تتوفر فيه الخلافات بين الحكومات والشركات حول قضايا تجارية متعلقة بنظام تشغيل او أخر، يكسب Linux القبول كنظام تشغيل بديل ويلاقي الانتشار ، وقد تجاوز لينكس القيود التي تكبل البرامجيات التجارية في السوق بطرق عديدة منها :

- يجري توزيع Linux كبرمجة حره ذات ترخيص عام (GPL) General public license وهذا النوع من الترخيص خاص بمؤسسة البرامجيات الحرة Free software و تحفظ هذه الرخصة حقوق البرمجة، لكنها تضمن توزيع البرامج مرفقة بملفات الرموز الأصلية (Source code).
- يجري توزيع Linux عن طريق الانترنيت وهو سهل التنصيب و التطوير .
- يقوم مبرمجون كثيرون على نطاق العالم بأكمله بالتطوير.. للتوزيع وتنقيح برامج مكتوبة كي تعمل تحت Linux و معظم هذه

البرمجيات توزع تحت ترخيص من نوع GPL.ينتمي Linux إلى زمرة البرامجيات المسماة البرامجيات الحرة أو مفتوحة الأصل (Oopen Source Software) ، والمقصود بهذا وجوب إرفاق البرمجيات بملفات الرموز الأصلية التي تم توليد البرمجة منها مع حيث ان كلمة (Free) من الحرية (Freedom) وليس مجاني. [٨]

يعتبر لينكس ظاهرة لم تسبق من قبل في أنظمة الحواسيب ، فهو الحل ضد الاحتكار والحل الاقتصادي والحل للأغراض التعليمية، وهو نظام تشغيل يعمل كوسيط بين المستخدم ومكونات الحاسب الآلي المادية . وهناك غرضان اساسيان من وجود الأنظمة التشغيلية الأولى منهما وهو توفير منصة تعمل عليها جميع البرامج الأخرى بتجرد تام ، أما الثاني فهو استغلال مكونات الحاسب المادية بالطريقة المثلى .ان لينكس يعمل على عدة أنواع مختلفة من الحاسبات من ضمنها الحاسب الشخصي ، كما ان نظام لينكس يوفر واجهة المستخدمة الرسومية وذلك تحت إحدى النوعين لسطح المكتب هما KDE,GNOME والتي تشابه WINDOWS فهي تساند سحب و إلقاء الملفات والتركيب الأوتوماتيكي للقرص المدمج والكثير من المهام الحديثة التي تشعر المستخدم بالراحة والسهولة .يشعر المستخدمون ومتصفحي الإنترنت باختلاف قليل مقارنة بالنوافذ ، ويمكن ان يعمل على سطح المكتب من لنكس بأمن اكثر ففي هذه المرحلة من التعليم هو القصد في اكتساب الخبرة الأساسية والخلفية العلمية البسيطة . ان نظام لينكس الذي بني على فكرة نظام التشغيل متعدد المستخدمين متعدد المهام فلا يوجد اي شيء مخفي عن المستخدم يمنعه من مواصلة التعلم والإسهام بإنجاح هذا النظام وانتشاره. [٩]يعد نظام Linux من اكثر أنظمة التشغيل شيوعاً لما يشمل عليه من قاعدة دعم كبير . وقد خرج هذا النظام أولا في منتصف السبعينات كنظام تشغيل متعدد التشغيل للبرامج Multitasking في الحاسبات المتوسطة والكبيرة Mini-computers & Mainframe .وقد تم أعداد هذا النظام بلغة C++ وهي أسهل بكثير من لغة التجميع مما ساعد المبرمجين في شتى أنحاء العالم على تطويره والخروج بإصدارات عديدة تستخدم مع جميع أنواع الحاسبات ، بدءاً من الحاسبات الشخصية وانتهاءاً بالحاسبات العملاقة مثل Cray Y-MP ، ويعزى إلى معظم الإصدارات التي ظهرت للحاسبات الشخصية أنها مرتفعة التكاليف مقارنة بأنظمة التشغيل الأخرى .

٥- النتائج ومناقشتها

١- تم إعداد برنامج Firewall باعتماد لغة C++ وأوامر نظام التشغيل Linux تجسدت فيه سهولة الاستخدام ، وبمفردات تشخيصيه شكلت كخط أولى للدفاع عندما يستخدم بصورة صحيحه وكما في البرنامج المرفق [ملحق رقم (١)]. وملحق رقم (٢) يوضح شرح مبسط لتصميم الجدار الناري .

٢ . تم تطبيق برنامج Firewall المقترح و المصمم لحل مشكلة البحث في الحد من كثرة الاختراقات لشبكة الانترنيت وبشكل محدود ، إذ ظهر عمليا بعد تطبيق البرنامج انه يحد من الاختراقات و بفترات زمنية واضحة .

٣. يغلق برنامج Firewall عدة منافذ ، ويتوقف ذلك على نوع المنفذ في المنظومة الحاسباتية التي تتناسب مع مديات الفترة الزمنية المحددة .. مع إجراءات الفحوصات واختبار الاختراقات كجزء من تحليل المخاطر على الشبكة .

٤. ان المؤشر التحليلي لتصميم برامج الجدار الناري يتطلب تحديد وتعريف الحدود بين مناطق الأمن في الشبكة ، وهذه الحدود ترتبط بمتغيرات لتقليل خطر إساءة استخدام المعلومات الحاسباتية وخلل الأمن المعلوماتي فيها ، وهذا التحليل يدعو إلى تصميم الحدود والمتغيرات المطلوبة في الشبكة الحاسباتية قبل اعداد برنامج جدار ناري معين .

٥. ظهر من تحليل النتائج ان برامج الجدار الناري إذا لم يصمم بهيكلية برمجية واضحة فأنة يحد من سرعة تناقل المعلومات واستجابتها في الشبكة الحاسباتية ، وهذا ما ظهر جليا في المراحل الأولية لتطبيق برنامج الجدار الناري المقترح .

٥-١ الاستنتاجات

١. أن الاتصال بشبكة الانترنيت والتعقيد المتزايد لأنظمة المعلومات يوفر ارض خصبة لأنواع عديدة من الهجمات،لذا يتطلب تصميم الجدار الناري تحديد وتعريف الحدود بين مناطق الأمن في الشبكة .

٢. يجب أن ينظر إلى الجدار الناري كخط أولي للدفاع وليس هو الحل الشامل وإذا لم يستخدم بصورة صحيحة فقد يصبح نقطة الفشل الوحيدة في المنظومة الحاسباتيه.

٣. إن خدمة تعديل وإعداد الجدار الناري وفق السياسة الأمنية الحالية او بعد تحليل المتطلبات الأمنية ، باستطاعة الجدار الناري الخاضع للإدارة الصحيحة أن يرفع من مستوى الأمن والأداء عبر الشبكة .

٤. أن الهدف من إجراءات الحماية هو تقليل الضرر الممكن حدوثه إلى اقل ما يمكن،اذ

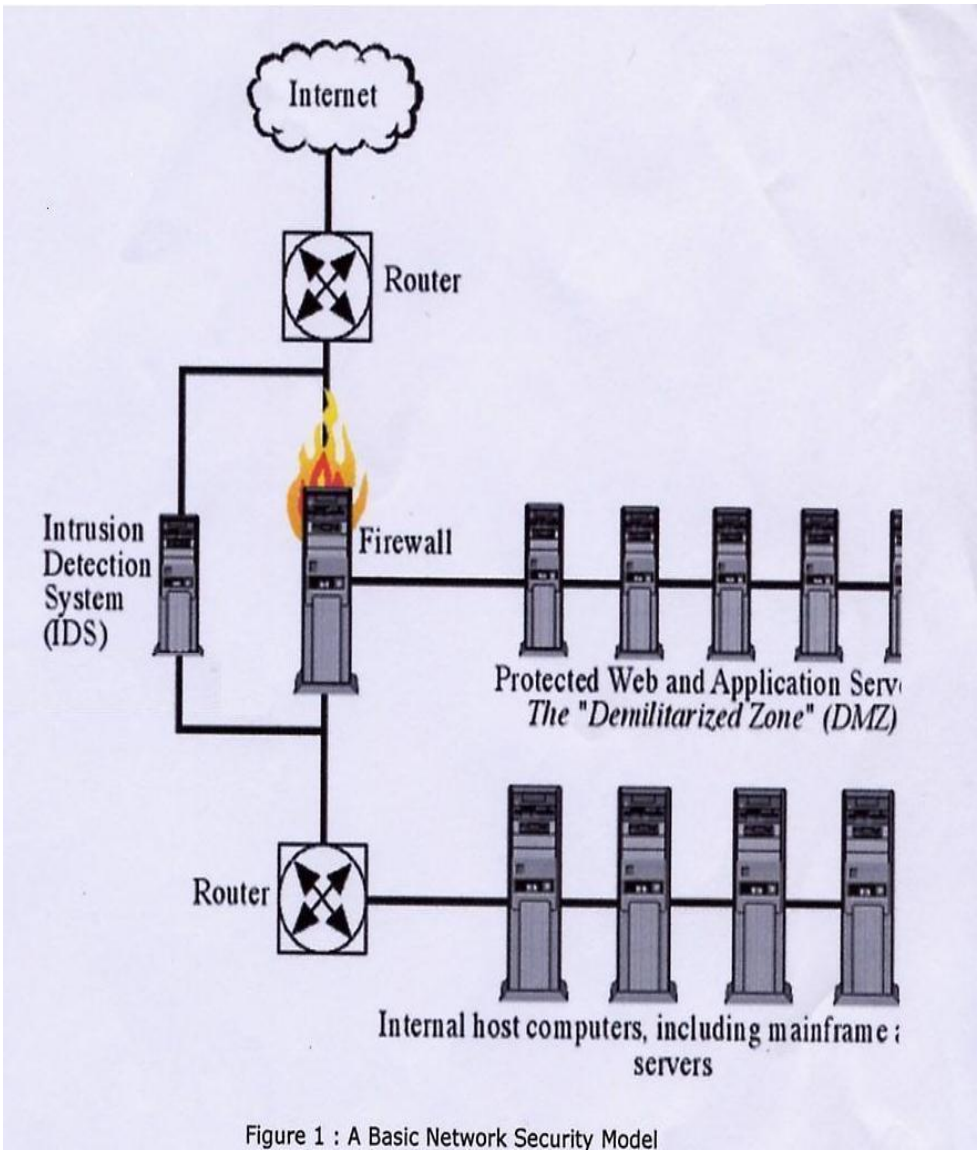
انه من غير الممكن تحقيق أمنية كاملة للمعلومات التي تعالج بواسطة برنامج معين ولكن من الممكن بواسطة إجراءات السيطرة والأمن الفعالة تقليل خطر إساءة استخدام او كشف المعلومات بصورة فعالة ومؤثرة .

٦-٢ التوصيات

١. أن كثرة ثغرات نظام التشغيل Windows وسهولة اختراقه وتعدد مشاكله مقارنه مع نظام يونيكس ولنكس الأكثر أمن وحماية فقد نوصي بتصميم برنامج في نظام التشغيل لنكس المفتوح المصدر والمتعدد المهام لحماية الشبكة من الاختراق بحدود اكبر.

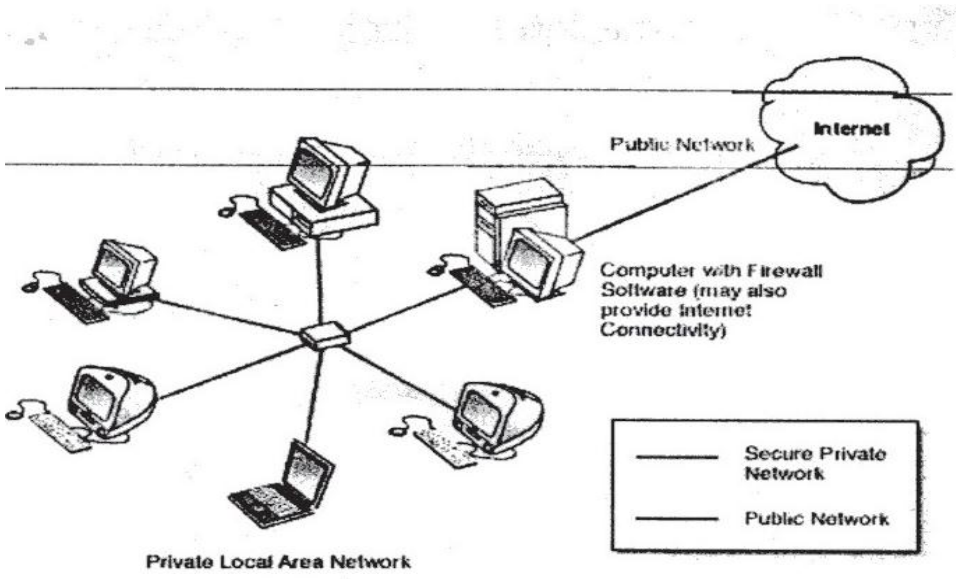
٢. عند استخدام شبكة الانترنيت فان الحماية تعتمد على الجدار الناري ، و هذا الجدار يعتمد على عدة عوامل يجب ان يتم فحصها بالكامل ، لذا فإننا نقوم باختبارات اختراق كجزء من عملية تحليل المخاطر ، و نقوم أيضا بتقييم التوافق بين لوائح أمن المعلومات وتصميم الجدار الناري .

٣. نوصي بأجراء اختبار مفتوح لكل أساليب الاختراق المعروفة باستعمال كافة المعلومات المتاحة عن تصميم الجدار و إمكانياته في حالات التطبيق العملي ،أن تطبيق هذه الإجراءات معقدة بعض الشيء..إلا أنها تجني ثمارها المتمثلة في الحد من المخاطر و تفاديها من المخاطر التي تنتج عبر الاتصال الشبكي فينبغي مراعاتها عند تصميم برنامج الجدار الناري.



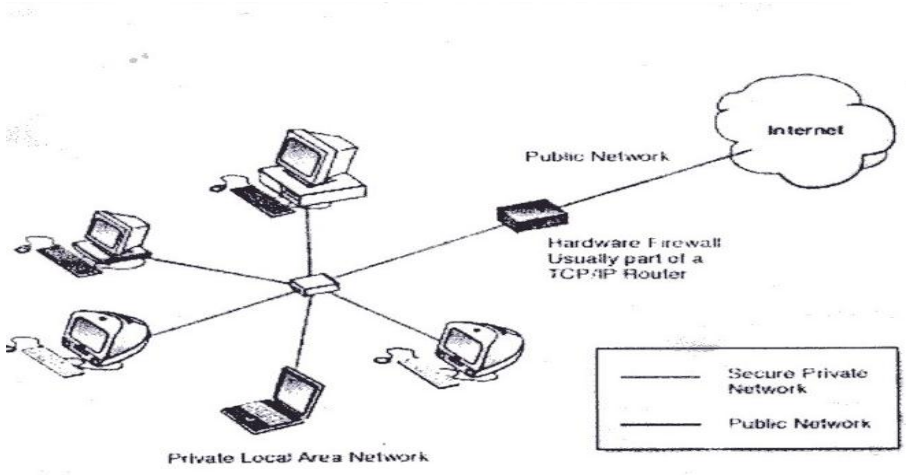
شكل رقم (١)

التصميم العام للجدار الناري



شكل رقم (٢)

الجدار الناري كبرنامج في حاسبة(SOFTWARE)



شكل رقم (٣)

الجدار الناري عندما يكون جهاز مادي (Hardware)

المصادر

١. مركز نور لخدمات الحاسب الآلي : النور للكومبيوتر والاتصالات ، منشورات من الانترنيت . عنوان الموقع www.nor2000.com ، ٢٠٠٠

٢. فرحان ، جابر كاظم : أمن الشبكات و الانترنيت ، منشورات دورة في مدرسة القدس ، بغداد ، ٢٠٠٤ ، (15,20,78,79).

٣. الموسوعة العربية للكومبيوتر والانترنيت منشورات من الانترنيت ، عنوان الموقع www.c4arab.com ، ٢٠٠١,

٤. سرهنك ، مصطفى: الحماية هي الغاية منشورات من الانترنيت ، عنوان الموقع www.internet security.com ، ٢٠٠٣ .

٥.الاختراق والحماية ، منشورات من الانترنيت ، عنوان الموقع www.hakeres.com ,٢٠٠٢

٦.العلم لامن المعلومات، منشورات من الانترنيت ،عنوان الموق www. information security.com٢٠٠١

٧.شياح ،محمود : الدليل العملي لتعلم و استخدام Linux، الشعاع للعلوم و المعارف ، سورية ، حلب ، ص١٠ ، ٢٠٠١ .

٨.عبد الرحمن الغادن ،احمد : معوقات انتشار نظام التشغيل لنكس المفتوح المصدر دار المشرق للطباعة و النشر ، عمان ، الاردن ، ٢٠٠١، ص١٥.

٩. المهدي ، جلال : دليل خدمة الحاسب بكلية علوم الحاسب و المعلومات دار الحرية للطباعة و النشر، المملكة العربية السعودية ٢٠٠٢، ص ١٢,

١٠. بروتوكولات الانترنيت ، منشورات من الانترنيت، عنوان الموقع Security 4 Arab www.٢٠٠٠ ، Forms.com

الملحق رقم (١)

The Firewall Program :

```
[root@localhost]# emacs firewall.c
        # include "stdio.h"
  int main( )
  printf ("program firewall") ;
   return 0 ;
  [root@localhost]# cc firewall.c
  [root@localhost]# ./a.out
  [root@localhost]# iptables –L
  [root@localhost]# cat > inactive.sh
  [root@localhost]# deleat firewall content
  [root@localhost]# iptables –A INPUT ALL
  [root@localhost]# iptables –A OUTPUT ALL
        [root@localhost]# iptables –F ALL
        [root@localhost]# echo"firewall is inactive now!"
            [root@localhost]# chmod +x inactive.sh
            [root@localhost]# iptables –L
[root@localhost]# ./inactive.sh
firewall is inactive now
  [root@localhost]# iptables –L
  [root@localhost]# cat > firewall.sh
    [root@localhost]# iptables –A INPUT –i eth0 –p ICMP –jDROP
    [root@localhost]# iptables –A INPUT –i eth0 –p TCP –
destination–port telnet –j DROP
    [root@localhost]# iptables –t filter –p FORWARD DROP
```

[root@localhost]# iptables –t filter –A FORWARD –m tcp –p tcp –s 172.16.1.0/24

--sport 80 –d 0/0 –j ACCEPT

[root@localhost]# iptables–t filter –A FORWARD –m tcp –p tcp –d 172.16.1.0/24

--dport 80 –s 0/0 –j ACCEPT

[root@localhost]# iptables –A INPUT –p tcp

[root@localhost]# iptables –A INPUT –s 172.16.1.0

[root@localhost]# iptables –A INPUT – i eth0

[root@localhost]# iptables –A INPUT –p tcp –sport 22

[root@localhost]# iptables –A INPUT –p tcp –dport 22

[root@localhost]# iptables –p tcp –tcp–flags SYN,FIN,ACK SYN

[root@localhost]# iptables –A INPUT –p udp –sport 53

[root@localhost]# iptables –A INPUT –p udp –dport 53

[root@localhost]# iptables –A INPUT –p icmp –icmp–type 8

[root@localhost]# iptables –A INPUT –m limit --limit 3/hour

[root@localhost]# iptables –A INPUT –p tcp –m multiport –source–port 22,53,80,110

[root@localhost]# iptables –A INPUT –p tcp –m multiport –destination–port 2 2,53,80,110

[root@localhost]# iptables –A INPUT –m state –state RELATED,ESTABLISHED

[root@localhost]# iptables –t filter –A INPUT –p udp –dport 53 –j DROP

[root@localhost]# iptables –N tcp_packets

[root@localhost]# iptables –A tcp_paket –m state –state NEW –i! ppp0 –j ACCEPT

```
[root@localhost]# iptables –A INPUT –p tcp –j tcp_packets
[root@localhost]# iptables –t nat –A POSTROUTING –p tcp –o eth0 –j SNAT
–to-source 194.236.50.155-194.236.50.160:1024-32000
[root@localhost]# iptables –t nat –A POSTROUTING –p tcp –d 15.45.23.67
–dport 80 –j DNAT –to-destination 192.168.1.1-192.168.1.10
[root@localhost]# iptables –t nat –A POSTROUTING –p TCP –j MASQUERADE
–to-ports 1024-31000
[root@localhost]# iptables -A INPUT –j DROP –p tcp –dport 23
[root@localhost]# iptables –A INPUT –j DROP –s 192.168.0.252
root@localhost]# chmod +x firewall.sh
[root@localhost]# ./firewall.sh
[root@localhost]#  emacs PID
# include "stdio.h"
#include "sys/types.h"
# include "unistd.h"
int main( )
pid_t pid ;
pid = getpid( ) ;
printf ("This process has the pid numper: %dnn ",  pid) ;
return 0;
[root@localhost]# cc pid
[root@localhost]# ./a.out
```

ملحق رقم (٢)

شرح مبسط لتصميم برنامج الجدار الناري

تم تصميم برنامج الجدار الناري في نظام التشغيل لنكس بواسطة لغة++ C و اوامر نظام التشغيل لنكس ، يمتاز البرنامج بسهولة استخدامه و امكانية تغير الشروط و فتح او غلق المنافذ حيث ان نظام التشغيل لنكس يحتوي على ٦٦٥٠ منفذ يجب غلق المنافذ التي لا نحتاج اليها لحماية الشبكة من الاختراق .

احدى وظائف (iptables) هو فلترة المغلفات العابرة الى الجهاز . حيث يتم وضع شروط خاصة اذ يقوم بتنفيذ الأمر الموضح في البرنامج . ان تحقيق هذا الامر يحتاج الى جملة من المعايير الأساسية والتي يمكن تلخيصها كالتالي:

اولا:

t– تحدد مهمة الامر و لها خيارين:

filter : تستخدم في فلترة المغلفات..

nat : تستخدم في gateway الشبكات و هي مختصر Network Address Translation

ثانيا:

تحدد النشاط الذي الذي نقوم بآخذه و خياراتها

A: إضافة شرط.

D: حذف شرط.

L: عرض الشروط.

F: حذف جميع الشروط.

ثالثا:

اختيار وجهة المغلف المفلتر و هي احدى ثلاثة :

INPUT: المغلفات القادمة .

OUTPUT: المغلفات المغادرة.

FORWARD: المغلفات المرسلة لاي جهاز اخر حتى من اجهزة اخرى مثل الموزعات.

رابعا :

IP مصدر ووجهة المغلف أي IP الجهاز الذي قدم منه المغلف او الجهاز الذي سيستقبل المغلف.

s– : بعده يوضع IP الجهاز المصدر للمغلف

t– : بعده IP يوضع الجهاز المستقبل للمغلف

خامسا :

p– :هو البروتوكول و أمثلتها (ICMP,UDP,TCP)

سادسا :

dport–– رقم المأخذ

سابعا:

j– هو الاجراء المتخذ و هو احدى ثلاثة

DROP : يتم الغاء المغلف و تجاهله بعدم إرسال شئ للكومبيوتر المرسل .

REJECT : مثل DROP لكن يتم إرسال رسالة خطا للجهاز المرسل .

ACCEPT : المغلفات مسموح لها بالمرور.

بالنسبة الى Network Address Translation فيكون عملها عادة في الشبكات لو كان هناك مجموعة حاسبات في شبكة و اتصال انترنيت ممكن نخلي حاسبة واحدة للجدار الناري للشبكة وأخرى إلى gateway لبقية الأجهزة و ذلك عن طريق اخذ المغلفات المرسلة من الحاسبات الأخرى و تغير المأخذ الرئيسي لها و جعل المصدر هو للجدار الناري لانه هو الي عنده الIP و الاتصال بالانترنيت.

أولا :

t nat– : يخبر البرنامج اننا نتعامل مع nat .

ثانيا :

A POSTROUTING–: لعمل مشاركة على الشبكة .

ثالثا :

s– : تحدد IP الأجهزة في الشبكة .

رابعا :

o– : تحدد الجهاز المتصل بالشبكة الاخرى (الانترنيت)

خامسا :

j MASQUERADE– : يقوم هذا الأمر بجعل أي حاسبة على الشبكة تشارك بالانترنيت .

ملحق رقم (٣)

بروتوكولات الانترنيت Internet Protocols

(IP) : Internet Protocol

يعتبر(IP) مسئولا عن نشاط الشبكة الرئيسي و يعتبر(IP) من اهم البروتوكولات التي يتم استخدامها على الشبكة . عندما تتعامل مع الشبكة ، نحتاج الى مكان نقوم بتخزين البيانات و هذا المكان هو عنوان الشبكة .

ويعمل الجزء الاساسي من (IP) مع عناوين شبكة الانترنيت ، و لا بد ان يمتلك كل جهاز حاسبة في شبكة (TCP/IP)عنوان رقمي . و سوف يفهم (IP) على جهاز الحاسبة كيفية و مكان الرسائل الى تلك العناوين .

في حين يتعامل (IP) مع العناوين ، لا يمكن لهذا البروتوكول ان يتاكد بشكل قاطع من وصول المعلومات الى المكان المطلوب و لا يهتم ال (IP) بالتعرف على ما قد يؤدي الى ضياع البيانات و عدم وصولها الى وجهتها .

: Transmission Control Protocol (TCP)

هو أحد أدوات تنظيم الشبكة و ايا كان نوع البيانات التي يمتلكها ، يتاكد الـ (TCP) من وجود كل البيانات و عدم فقدان اي منها .و يقوم ال (TCP) باستخدام (IP) لتسليم حزم البيانات للتطبيقات المتواجدة في الطبقات العليا كما يوفر انتقال بيانات يمكن الوثوق به بين اجهزة الكومبيوتر المتواجدة على الشبكة و تعتبر وظيفة (error checking) و التي تعمل على التاكد من وصول كل حزم البيانات بدون اتخطاء من اهم وظائف (TCP) و يبدا ال (TCP) في العمل بعد وصول ملفات حزم البيانات الى عنوان (IP) الصحيح ، و يقوم ال (TCP) بانشاء حوار على كل من جهاز الكومبيوتر المرسل و المستقبل للتعامل مع البيانات التي يتم نقلها .

: User Datagram Protocol (UDP)

يقوم الـ (UDP) بنقل البيانات عبر الشبكة .و يقوم(UDP) باستخدام (IP) في تسلم حزم البيانات إلى تطبيقات الطبقات العليا كما يعمل على تدفق البيانات عبر الشبكة .و لا يوفر (UDP) وظيفة Error (checking) على الرغم من أن هذه الوظائف يمكن لتطبيقات التي تستخدم (UDP) أن تضيفها .أن هذا البروتوكول يعمل مع عدم وجود شبكة حيث انه يسمح بإعادة إرسال البيانات في حالة حدوث أية أخطاء.

Internet Control Message Protocol : (ICMP)

يبلغ (ICMP) عن وجود أي مشاكل و يوفر بعض معلومات الشبكة المهمة مثل وضع الأخطاء في أحد أجهزة الشبكة . و يقوم (IP) بتقصي الاخطاء و يرسلها الـ(ICMP) . و هناك استخدام اخر شائع لـ (ICMP) و هو الحصول على نسخة من الطلب الذي يتم صنعه عن طريق امر Ping.

(FTP) : File Transfer Protocol

يساعد (FTP) في نسخ الملفات بين اجهزة الكومبيوتر .و يستخدم الـ (FTP) لتنزيل الملفات من جهاز بعيد او لتحميلها عليه .

Telnet:-

يسمح بروتوكول (Telnet) بالاتصال بجهاز كومبيوتر بعيد و العمل كما لو كنت جالسا أمام هذا الجهاز ، و أيا كان بعدك عن هذا الجهاز . بالإضافة لكونه بروتوكول ، يعتبر (Telnet) خدمة و تطبيق أيضا .و يساعد بروتوكول (Telnet) في الوصول إلى ما نرغب في الحصول عليه من بيانات . و يستخدم المتعاملون مع نظام التشغيل Linux و Unix بروتوكول (Telnet) لتسجيل الدخول على كومبيوتر بعيد و تشغيل البرامج التي قد لا تكون موجودة على جهاز الكومبيوتر الخاص بك عن بعد . يعمل مدير النظام إلى استخدام (Telnet) حيث انه يمكنه من الاعتناء بأجهزة الكومبيوتر على الشبكة بدون الحاجة إلى الانتقال لمكان كل منهم .

: Hyper Text Transfer Protocol (HTTP)

يقوم الـ (HTTP) بنقل (Hyper Text Markup Language HTML) ومكونات أخرى من وحدات الخدمة على شبكة الويب أي وحدات التصفح . (١١)