Study Guide for

GNU/Linux System Administration 2
Lab work for LPI 102

الدورة التدريبية

إدارة نظام التشغيل غنو/لينكس 2

مع تدريبات عملية لامتحان LPI 102

Arabic Translation by Arabeyes
تم إعداد الترجمة العربية من قبل مجموعة عربآيز Arabeyes

Powered by RichStyle.org
التنسيق والإخراج الفني والطباعي RichStyle.org

January 2003
النسخة العربية: 0.5 بيتا مارس/آذار 2007

شكر وعرفان Acknowledgments:

The original material was made available by LinuxIT's technical training centre www.linuxit.com. Many thanks to Andrew Meredith for suggesting the idea in the first place. A special thanks to all the students who have helped dilute the technical aspects of Linux administration through their many questions, this has led to the inclusion of more illustrations attempting to introduce concepts in a userfriendly way. Finally, many thanks to Paul McEnery for the technical advice and for starting off some of the most difficult chapters such as the ones covering the X server (101), modems (102) and the Linux kernel (102).

The manual is available online at http://savannah.nongnu.org/projects/lpi_manuals/. Thank you to the Savannah Volunteers for assessing the project and providing us with the Web space.

جزيل الشكر لأعضاء مجموعة عربآيز الذين ساهموا في إنجاز هذا العمل:

- أنس الحسيني
- عمر بقلة
- محمد أنس رمضان
- يوسف الشهيبي

تاريخ المستند History:

First release (version 0.0) October 2003. Reviewed by Adrian Thomasset
Second release (revision1) January 2003. Reviewed by Andrew Meredith.

الدورة التدريبية: إدارة نظام التشغيل غنو/لينكس 2 ـ الإصدار العربي 0.5 بيتا. مجموعة عربآيز www.arabeyes.org.

تبرئة المسؤولية No Guarantee:

The manual comes with no guarantee at all.

هـذا المسـتند غيـر مـرفق بأية ضمانات على الإطلاق، ولا تتحمل مجموعة عربآيز أي مسؤولية عن أية أضرار ناتجة عن استخدام هذا المستند أو المعلومات الواردة فيه.

GNU Free Documentation License

Version 1.2, November 2002

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not

Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

GNU Free Documentation License _ Version 1.2

This is an unofficial translation of GNU Free Documentation License into Arabic language. It was not published by the Free Software Foundation, and does not legally state the distribution terms of software that uses the GNU FDL _ only the original English text of the GNU FDL does that. However, we hope that this translation will help Arabic language speakers understand the GNU FDL better

فيما يلي الترجمة غير الرسمية لإتفاقية ترخيص المستندات الحرة GNU إلى اللغة العربية. هذه الترجمة غير منشورة من قبل مؤسسة البرمجيات الحرة، ولا تعبر عن الشروط القانونية لتوزيع البرمجيات التي تخضع لاتفاقية GNU FDL_ وتعتبر النص الأصلي باللغة الإنكليزية المصدر الوحيد لهذه الشروط. لكننا نأمل أن تساعد هذه الترجمة الناطقين باللغة العربية على استيعاب إتفاقية GNU FDL بشكل أفضل.

0_ تمهيد:

غاية هذا الترخيص هي جعل دليل ما أو كتاب أو أي مستند عملي وذو فائدة "حر" بمعنى الحرية: ليضمن للجميع الحرية الفعلية في نسخه وإعادة توزيعه (مع تعديل أو دون تعديل) سواء لغايات تجارية أو غير تجارية. كما يضمن هذا الترخيص لكل من المؤلف والناشر وسيلةً للحصول على العرفان بالجميل لقاء عملهم، دون أن يكونوا مسؤولين عن التعديلات التي يضيفها الآخرون.

ينضوي هذا الترخيص تحت مظلة "الحقوق المعاكسة Copyleft" ما يعني أن الأعمال المشتقة من المستند ينبغي أن تكون مستندات حرةً بنفس الأسلوب، ويتكامل مع إتفاقية الترخيص العمومية GNU Public License والتي تعنى بالبرمجيات الحرة.

لقد قمنا بتصميم هذا الترخيص لاستخدامه مع أدلة استخدام البرمجيات الحرة، لأن البرمجيات الحرة تحتاج إلى مستندات حرة: ينبغي أن يرفق البرنامج الحر بمستندات توفر نفس الحريات التي يوفرها البرنامج ذاته. إلا أن هذا الترخيص غير محدود بمستندات البرمجيات، فمن الممكن أن يستثمر لأية أعمال نصية، بغض النظر عن طبيعة موضوعها. أو إذا ما كانت منشورة بصيغة كتاب مطبوع. ننصح باستخدام هذا الترخيص بشكل أساسي للأعمال الهادفة لأن تكون أعمالاً مرجعية أو تعليمية.

1_ تطبيق الترخيص والمصطلحات:

ينطبق هذا الترخيص على أي دليل استخدام أو أي عمل أدبي آخر ضمن أية صيغة في حال احتوائه على تنويه أضافه مالك الحقوق الفكرية لهذا العمل ينص على إمكانية توزيع هذا العمل وفق شروط هذا الترخيص. يتيح هذا التنويه ترخيصاً عالمياً ودون أية قيود ولفترة زمنية غير محدودة لاستخدام هذا العمل ضمن الشروط الواردة في هذا الترخيص. تشير كلمة (المستند) في ما يلي إلى أي من هذه الأدلة أو الأعمال. أي شخص من العموم هو المرخص له، ويشار إليه بكلمة (أنت). وتعتبر أنت موافقاً على شروط هذا الترخيص في حال قمت بنسخ، تعديل أو توزيع هذا العمل بأسلوب يتطلب إذناً ضمن قوانين حماية الملكية الفكرية.

تعني عبارة (إصدار معدل) من المستند أي عمل يحتوي المستند أو جزءاً منه، سواء تم نسخه حرفياً أم مع بعض التعديلات أو تمت ترجمته إلى لغة أخرى.

تعني عبارة (قسم ثانوي) أية ملحقات أو مقدمات للمستند تعنى تحديداً بالعلاقة بين الناشرين أو المؤلفين لهذا المستند والموضوع العام للمستند (أو ما يتعلق به) ولا تحتوي على أي معلومات تنطوي تحت هذا الموضوع العام (أي أنه في حال كان المستند كتاباً في الرياضيات على سبيل المثال فإن أقسامه الثانوية لا ينبغي أن تحتوي أية معلومات عن الرياضيات). قد ترتبط هذه العلاقة بالحيثيات التاريخية للموضوع أو بحيثيات أخرى قد تكون قانونية أو فلسفية أو أدبية أو سياسية.

(الأقسام الثابتة) هي أقسام ثانوية تشير عناوينها بأنها (أقسام ثابتة) مع الأخذ بعين الاعتبار أن المستند خاضع لشروط هذه الإتفاقية. في حال لم يتطابق أحد الأقسام مع تعريف (الأقسام الثانوية) المذكور أعلاه فإنه لا يمكن اعتباره (قسماً ثابتاً). قد لا يحتوي المستند على أية أقسام ثابتة، وإذا لم يشر المستند بالتحديد إلى احتوائه على أقسام ثابتة فإن هذا المستند لا يحتوي على أية أقسام ثابتة.

(نصوص الغلاف) هي أية أجزاء نصية مختصرة محددة ومضمنة ضمن الغلاف الأمامي أو الخلفي للمستند، مع الأخذ بعين الاعتبار أن المستند خاضع لشروط هذه الإتفاقية. يجب ألا يتجاوز نص الغلاف الأمامي خمس كلمات وألا يتجاوز نص الغلاف الخلفي خمس وعشرون كلمة.

تعني عبارة (نسخة شفافة) من المستند أية نسخة قابلة للقراءة بالوسائل الآلية، والمرمزة بتنسيق ذو مواصفات متاحة للعموم، والملائمة لتعديل المستند بسهولة باستخدام برمجيات تحرير النصوص الشائعة أو (بالنسبة للصور المؤلفة من نقاط الكترونية) برمجيات تحرير الصور الشائعة أو (بالنسبة للرسوميات) أحد برمجيات تحرير الرسوميات المتاحة بشكل واسع، والملائمة أيضاً للإدخال إلى برمجيات تنسيق النصوص أو الترجمة الآلية إلى عدة تنسيقات أخرى ملائمة للإدخال إلى برمجيات تنسيق النصوص. وتعتبر أية نسخ مرمزة بصيغ ملفات (شفافة) أخرى صممت مواصفاتها (في حال وجود هذه المواصفات) لإعاقة أو إحباط التعديلات اللاحقة من قبل القراء غير شفافة. تعتبر أية صيغة رسومية غير شفافة فيما إذا تم استخدامها لتمثيل أية أجزاء كبيرة من النص. تدعى أية نسخة غير شفافة (مصمتة).

من بعض أمثلة صيغ الملفات الملائمة للنسخ الشفافة صيغة ASCII البسيطة دون أية تعليمات تنسيق، صيغة إدخال Texinfo، صيغة إدخال LaTeX، صيغ SGML و XML شريطة استخدام محددات DTD متاحة للعموم، صيغة HTML البسيطة والمطابقة للمعايير، إضافة إلى صيغ PostScript و

PDF المصممة للتعديل من قبل المستخدم. من بعض أمثلة صيغ الرسوميات الملائمة للنسخ الشفافة صيغ PNG، XCF و JPG. تتضمن الصيغ المصمتة صيغ الملفات الخاصة والتي لا يمكن قراءتها أو تعديلها إلا باستخدام برمجيات تحرير النصوص الخاصة بمنتجٍ ما، صيغ SGML و XML والتي لا تتاح محدداتها DTD أو أدوات معالجتها للعموم، ملفات HTML المولدة آلياً، وملفات PostScript و PDF المولدة من برمجيات تحرير النصوص لأغراض القراءة فقط.

تعني عبارة (صفحة العنوان) لكتاب مطبوع صفحة العنوان ذاتها لهذا الكتاب، إضافة إلى الصفحات اللاحقة اللازمة لاحتواء المواد التي تفرض هذه الإتفاقية تبيانها على صفحة العنوان. بالنسبة للأعمال المنشورة بصيغ لا تحتوي على صفحة للعنوان فإن صفحة العنوان تعني النص الوارد بالقرب من أكثر مواقع ظهور عنوان العمل وضوحاً وقبل بداية النص الرئيسي للعمل.

تعني عبارة القسم (المعنون بـ س ع ص) وحدة فرعية ذات تسمية من المستند إما أن يكون عنوانها (س ع ص) بالتحديد أو أن تحتوي (س ع ص) ضمن أقواس بعد النص الذي يمثل (س ع ص) مترجمةً إلى أية لغةٍ أخرى. (تمثل س ع ص هنا تسمية قسم محدد كما هو وارد أدناه، مثل "شكر وعرفان"، "إهداء" أو "تاريخ المستند"). للـ (محافظة على عنوان) أحد هذه الأقسام عندما تقوم بتعديل المستند يتوجب عليك أن تبقي هذا القسم (معنوناً بـ س ع ص) وفقاً لهذا التعريف.

قد يحتوي المستند على تصريحات لتبرئة المسؤولية بعد العبارة التي تنص على أن المستند خاضع لهذه الإتفاقية. تعتبر هذه التصريحات مضمنة بالمرجعية في هذه الإتفاقية، ولكن فقط ضمن سياق تبرئة المسؤولية؛ وأية تبعاتٍ أخرى قد تسببها هذه التصريحات لاغية حتماً ولا تملك أية تأثيرات على معنى هذه الإتفاقية.

2ـ النسخ الحرفي:

بإمكانك نسخ وتوزيع المستند بأي وسيلة، لغايات تجارية أو غير تجارية، شريطة الحفاظ على هذه الإتفاقية وتنويهات حفظ الحقوق وتنويه الترخيص الذي يشير إلى أن المستند خاضع لشروط هذه الإتفاقية في جميع النسخ، وعلى ألا تقوم بزيادة أية شروط إضافية مهما كانت إلى شروط هذه الإتفاقية. يحظر عليك استخدام أية وسائل فنية بهدف إعاقة أو التحكم في قراءة أو إعادة نسخ النسخ التي تقوم بإعدادها أو توزيعها. يمكنك على أية حال الحصول على مقابل لقاء هذه النسخ، ويتوجب عليك فيما إذا قمت بتوزيع عدد كبير بما فيه الكفاية من النسخ أن تلتزم بشروط الفقرة 3 أيضاً.

بإمكانك أيضاً إعارة النسخ ضمن نفس الشروط المذكورة أعلاه، كما يمكنك عرض النسخ للعموم.

3ـ النسخ بكميات كبيرة:

إذا ما قمت بنشر نسخ مطبوعة (أو بوسيلة تستخدم عادة أغلفة مطبوعة) من المستند يتجاوز عددها المئة نسخة، وكان تنويه ترخيص المستند يتطلب (نص غلاف) يتوجب عليك تضمين النسخ في أغلفة تحمل بوضوح وبشكل مقروء جميع (نصوص الغلاف) المطلوبة: نص الغلاف الأمامي على الغلاف الأمامي ونص الغلاف الخلفي على الغلاف الخلفي. كما يجب أن يتم تحديدك أنت ضمن هذين الغلافين بوضوح وبشكل مقروء بصفتك ناشر هذه النسخ. يجب أن يظهر الغلاف الأمامي العنوان الكامل بحيث تظهر جميع كلمات العنوان دون تمييز بشكل واضح وبيّن. بإمكانك إضافة مواد أخرى على الأغلفة. في حال كانت التعديلات في النسخ المنتجة مقتصرة على الأغلفة، شريطة الحفاظ على عنوان المستند والالتزام بهذه الشروط، فإن هذه النسخ تعامل معاملة النسخ الحرفي.

إذا كانت النصوص المطلوبة كبيرةً إلى درجة يصعب معها إظهارها بشكل مقروء بإمكانك إدراج النصوص الأولى (بما يتلاءم مع إظهارها بشكل واضح ومقروء) على الغلاف ذاته، وإدراج ما تبقى على الصفحات اللاحقة.

إذا ما قمت بنشر أو توزيع نسخ مصمتة من المستند يتجاوز عددها المئة نسخة يتوجب عليك أن تقوم بإرفاق نسخة شفافة قابلة للمعالجة الآلية مع كل نسخة مصمتة أو أن تقوم بالتنويه ضمن كل نسخة مصمتة أو أن ترفق بها عنواناً لموقع على شبكة حاسوبية يتاح الوصول إليه من قبل عموم مستخدمي الشبكة الحاسوبية للحصول على نسخةٍ شفافةٍ كاملةٍ من المستند بدون المواد المضافة إليه باستخدام بروتوكول تشبيك معياري. ينبغي عليك فيما إذا ما استخدمت الخيار الأخير توخي الحذر قدر المستطاع عند البدء بتوزيع كميات كبيرة من النسخ المصمتة لكي تبقى هذه النسخة الشفافة متاحةً ضمن الموقع المحدد ولمدةٍ لا تقل عن سنةٍ واحدةٍ بدءاً من تاريخ توزيع آخر نسخة مصمتة من هذا الإصدار للعموم (إما بشكل مباشر أو عبر وكلائك وموزعيك).

يطلب منك (دون إجبار) أن تقوم بالاتصال بمؤلفي المستند قبل فترة معقولة من إعادة توزيع أية كميات كبيرة من النسخ لمنحهم فرصة تزويدك بأية نسخةٍ معدلةٍ من هذا المستند.

4ـ التعديلات:

بإمكانك نسخ وتوزيع إصدار معدل من المستند ضمن الشروط الواردة في الفقرتين 2 و 3 أعلاه، شريطة التزامك بنشر الإصدار المعدل ضمن نفس هذه الإتفاقية، مع اعتبار الإصدار المعدل مكان المستند، وبالتالي ترخيص نسخ وتوزيع الإصدار المعدل لأي شخص يحصل على نسخة منه. يتوجب عليك إضافةً إلى ذلك أن تقوم بما يلي فيما يتعلق بالإصدار المعدل:

A. أن تستخدم عنواناً مختلفاً عن عنوان المستند الأصلي ضمن صفحة العنوان (والأغلفة في حال وجودها) ومختلفاً أيضاً عن عناوين

الإصدارات الأخرى من هذا المستند (والتي يجب أن تدرج في حال وجودها ضمن قسم (تاريخ المستند)). بإمكانك استخدام نفس العنوان لإصدارٍ سابقٍ في حال حصولك على موافقة الناشر الأصلي لهذا الإصدار.

B. أن تدرج ضمن صفحة الغلاف بصفة محررين الشخص (أو الأشخاص) أو الجهة (أو الجهات) الاعتبارية المسؤولين عن تحرير الإصدار المعدل، إضافة إلى خمسة محررين أساسيين للمستند على الأقل (أو جميع المحررين الأساسيين في حال كان عددهم أقل من خمسة) إلا إذا ما حرروك من هذا الشرط.

C. أن تقوم بالتنويه ضمن صفحة الغلاف إلى اسم ناشر الإصدار المعدل بصفة (الناشر).

D. أن تحافظ على جميع تنويهات حقوق الملكية الفكرية ضمن المستند.

E. أن تضيف تنويهاً ملائماً لحقوق الملكية الفكرية للتعديلات التي قمت بها إلى جوار تنويهات حقوق الملكية الفكرية الأخرى.

F. أن تضيف بعد تنويهات حقوق الملكية الفكرية مباشرةً تنويهاً للترخيص يمنح العموم حق استخدام الإصدار المعدل ضمن شروط هذه الإتفاقية بنفس الصيغة المذكورة في الملحق أدناه.

G. أن تحافظ ضمن هذا التنويه على القوائم الكاملة للأقسام الثابتة ونصوص الغلاف المطلوبة في تنويه ترخيص المستند الأساسي.

H. أن تضمّن نسخةً غير معدلةٍ من هذه الإتفاقية.

I. أن تحافظ على القسم المعنون بـ (تاريخ المستند) وأن تحافظ على عنوانه وأن تضيف إليه نصاً يشير على الأقل إلى عنوان، سنة إصدار، المؤلفين الجدد وناشر الإصدار المعدل كما تظهر في صفحة العنوان. إذا لم يحتوي المستند على قسم بعنوان (تاريخ المستند) يتوجب عليك إضافة قسم جديد يحتوي على عنوان، سنة إصدار، المؤلفين وناشر المستند كما تظهر في صفحة العنوان للمستند الأساسي وإضافة نصٍ يشير إلى الإصدار المعدل كما ورد في الجملة السابقة.

J. أن تحافظ على الموقع (في حال وجوده) على الشبكة والمشار إليه في المستند ليتيح للعموم الحصول على نسخةٍ شفافةٍ من المستند إضافةً إلى المواقع المشار إليها ضمن المستند للحصول على الإصدارات السابقة والتي اشتق منها هذا المستند. من الممكن أن تضاف هذه المعلومات في قسم (تاريخ المستند). بإمكانك حذف الموقع من على الشبكة لأي عملٍ نشر قبل ما يزيد عن أربع سنواتٍ من نشر المستند ذاته أو في حال خولك الناشر الأساسي للإصدار الذي يشير إليه هذا العنوان بحذفه.

K. أن تحافظ على عنوان أي قسم معنون بـ (شكر وعرفان) أو (إهداء) وأن تحافظ ضمن هذا القسم على جميع الأجزاء الأساسية واللهجة المستخدمة لجميع عبارات الشكر والعرفان و/أو الإهداءات الواردة ضمنه.

L. أن تحافظ على جميع الأقسام الثابتة في المستند دون أي تعديلٍ في نصوصها أو عناوينها. لا تعتبر أرقام الأقسام أو ما يعادلها جزءاً من عناوين هذه الأقسام.

M. أن تقوم بحذف أي قسمٍ معنونٍ بـ (ضمانات)، لا ينبغي أن تحتوي النسخة المعدلة أياً من هذه الأقسام.

N. أن لا تقوم بإعادة عنونة أي قسمٍ من المستند الأساسي بعنوان (ضمانات) أو بعنوان يتعارض مع عنوان أي قسمٍ ثابتٍ من المستند.

O. أن تحافظ على أية عباراتٍ لتبرئة المسؤولية.

إذا احتوى الإصدار المعدل على مقدماتٍ أو أقسامٍ ملحقةٍ يمكن اعتبارها أقساماً ثانويةً ولا تحتوي على أية مواد منسوخة من المستند الأساسي فإنك تملك الخيار في اعتبار بعض أو جميع هذه الأقسام أقساماً ثابتة. للقيام بذلك ينبغي عليك إضافة عناوين هذه الأقسام إلى قائمة الأقسام الثابتة ضمن تنويه ترخيص الإصدار المعدل. يتوجب أن تكون هذه العناوين مختلفة عن أية عناوين لأقسام أخرى من المستند.

بإمكانك إضافة قسم بعنوان (ضمانات) شريطة عدم احتوائه على أية معلومات باستثناء ضمان بعض الجهات لإصدارك المعدل، كعبارات المراجعة من قبل النظراء أو أن نص المستند قد تمت الموافقة عليه من قبل جهةٍ ما كإجماعٍ على اعتباره تعريفاً محدداً لمعيار ما.

بإمكانك إضافة عبارةٍ لا تزيد عن خمسة كلمات ضمن الغلاف الأمامي، وعبارةٍ لا تزيد عن خمسة وعشرين كلمةً ضمن الغلاف الخلفي في نهاية قائمة نصوص الغلاف في الإصدار المعدل.لا يجوز إضافة ما يزيد عن عبارةٍ واحدةٍ إلى نص الغلاف الأمامي وعبارةٍ واحدةٍ إلى نص الغلاف الخلفي من قبل (أو عبر تنسيق تم من قبل) أية جهةٍ بعينها. إذا احتوى المستند بالأساس على نص غلافٍ ضمن نفس الغلاف تمت إضافته سابقاً من قبلك أو عبر تنسيقاتٍ أجريت من قبل نفس الجهة التي تعمل أنت نيابةً عنها فإنه لا يسمح لك بإضافة غيره، ولكن يمكنك أن تستبدل النص القديم شريطة حصولك على موافقةٍ صريحةٍ من الناشر السابق الذي أضاف هذا النص القديم.

لا يمنح مؤلف (أو المؤلفون) أو ناشر (أو الناشرون) المستند ضمن هذه الإتفاقية الحق باستخدام أسمائهم لأغراضٍ دعائيةٍ أو لضمان أو دعم أي إصدارٍ معدل.

5ـ دمج المستندات:

بإمكانك دمج المستند مع مستنداتٍ أخرى تخضع لنفس هذا الترخيص ضمن الشروط المحددة في الفقرة 4 أعلاه فيما يتعلق بالإصدارات المعدلة شريطة تضمينك لجميع الأقسام الثابتة لجميع المستندات الأصلية دون تعديل في المستند المدمج، وأن تقوم بإدراجها جميعاً كأقسام ثابتة لعملك المدمج ضمن تنويه الترخيص الخاص به، وأن تحتفظ بجميع تصريحات تبرئة المسؤولية الواردة ضمنها.

يتوجب أن يحتوي العمل المدمج على نسخةٍ واحدةٍ فقط من هذه الإتفاقية، كما يمكن أيضاً الاستعاضة عن الأقسام الثابتة المكررة بنسخةٍ واحدةٍ منها فقط. إذا ما احتوى المستند على عدة أقسامٍ ثابتةٍ تملك نفس العناوين ولكن محتوياتها مختلفة يتوجب تمييز عنوان كل قسمٍ بأن يضاف إلى نهايته ضمن أقواس اسم المؤلف أو الناشر الأصلي فيما إذا كان معروفاً أو رقماً مميزاً في حال لم يكن اسم المؤلف أو الناشر الأصلي معروفاً. يتوجب عليك أيضاً أن تقوم بنفس هذه التعديلات في عناوين الأقسام الواردة ضمن قائمة الأقسام الثابتة في تنويه إتفاقية الترخيص للعمل

المدمج.

يتوجب عليك أن تقوم بتجميع أية أقسام معنونةٍ بـ (تاريخ المستند) ضمن المستندات الأصلية لتشكل قسماً واحداً عنوانه (تاريخ المستند)، كذلك ينبغي تجميع أية أقسامٍ معنونةٍ بـ (شكر وعرفان) وأية أقسامٍ معنونةٍ بـ (إهداء). يتوجب عليك حذف أية أقسامٍ معنونةٍ بـ (ضمانات).

6ـ تجميع المستندات:

بإمكانك تشكيل مجموعةٍ مؤلفةٍ من المستند بالإضافة إلى مستنداتٍ أخرى تخضع لنفس هذا الترخيص واستبدال جميع نسخ هذه الإتفاقية في المستندات المختلفة بنسخةٍ واحدةٍ تضمّن في المجموعة شريطة التزامك بشروط هذه الإتفاقية فيما يتعلق بالنسخ الحرفي لكلٍ من هذه المستندات وعلى جميع الأصعدة.

يمكنك عزل مستندٍ واحدٍ من إحدى هذه المجموعات وتوزيعه بشكلٍ مستقلٍ ضمن شروط هذه الإتفاقية شريطة تضمين نسخةٍ من هذه الإتفاقية في المستند المعزول، والإلتزام المطلق بجميع الشروط الواردة في هذه الإتفاقية فيما يتعلق بالنسخ الحرفي لهذا المستند.

7ـ التجميع مع الأعمال المستقلة :

تعتبر أية توليفةٍ مؤلفةٍ من المستند أو مشتقاته مع مستنداتٍ أو أعمالٍ أخرى مستقلة في أو على مصنفٍ للتخزين أو وسيطٍ للتوزيع (مجموعة) إذا ما لم تستخدم إتفاقية حقوق الملكية الفكرية الناتجة عن هذه التوليفة لتحديد الحقوق القانونية لمستخدمي التوليفة بما يتجاوز ما تسمح به هذه الأعمال منفردةً. عندما يتم تضمين المستند في مجموعةٍ فإن هذه الإتفاقية لا تنطبق على الأعمال الأخرى ضمن هذه المجموعة شريطة ألا تكون هذه الأعمال مشتقةً من المستند.

إذا ما كان شرط نص الغلاف الوارد في الفقرة 3 منطبقاً على هذه النسخ من المستند فإنه في حال كان حجم المستند يقل عن نصف حجم المجموعة بأكملها يمكن إضافة نصوص الغلاف ضمن الأغلفة التي تحيط بالمستند ضمن المجموعة، أو ما يكافئ هذه الأغلفة إلكترونياً إذا كان المستند في صيغة إلكترونية. وباستثناء ذلك فإن نصوص الغلاف ينبغي أن تظهر على الأغلفة المطبوعة المحيطة بالمجموعة بأكملها.

8ـ الترجمة:

تعتبر الترجمة إحدى أ شكال التعديل، ولذلك بإمكانك توزيع نسخ مترجمة من المستند ضمن الشروط الواردة في الفقرة 4. يتوجب عليك الحصول على موافقة خاصة من قبل مالك الحقوق الفكرية لأية أقسامٍ ثابتةٍ قبل أن تقوم باستبدالها بترجمتها، إلا أنه بمقدورك إضافة نصوصٍ مترجمةٍ للأقسام الثابتة أو لأجزاءٍ منها إلى جانب الإصدارات الأصلية من هذه الأقسام. بإمكانك إضافة ترجمة هذه الإتفاقية وجميع تنويهات التراخيص في المستند، وأية تصريحاتٍ لتبرئة المسؤولية شريطة تضمين النسخة الأصلية باللغة الإنكليزية لهذه الإتفاقية إضافةً إلى النصوص الأصلية لجميع تنويهات التراخيص وتصريحات تبرئة المسؤولية. في حال ظهور أي تعارض بين ترجمة هذه الإتفاقية والنسخة الأصلية لهذه الإتفاقية أو تنويه الترخيص أو تصريح تبرئة المسؤولية فإن النسخة الأصلية هي المعتبرة.

إذا ما كان أ حد أقسام المستند معنوناً بـ (شكر وعرفان) أو (إهداء) أو (تاريخ المستند) فإن الشرط الوارد في الفقرة 4 بالحفاظ على عنوانه (الشرط)يتطلب عادةً تغيير العنوان الأساسي.

9ـ إنهاء الإتفاقية:

لا يحق لك القيام بنسخ، تعديل، إعادة ترخيص أو توزيع المستند باستثناء الشروط الواردة صراحةً في هذه الإتفاقية. وتحظر أية محاولةٍ عدا ذلك لنسخ، تعديل، إعادة ترخيص أو توزيع المستند، وفي حال وقوعها فإنها ستلغي تلقائياً الحقوق الممنوحة إليك ضمن هذه الإتفاقية. على أيةٍ حالٍ فإن إتفاقية الترخيص للأطراف التي حصلت منك على نسخٍ أو حقوقٍ ضمن هذه الإتفاقية لا تلغى مازالت هذه الأطراف ملتزمةً بالكامل بشروط هذه الإتفاقية.

10ـ الإصدارات المستقبلية من هذه الاتفاقية:

قد تقوم مؤسسة البرمجيات الحرة بنشر إ صدارات جديدة ومعدلة من اتفاقية ترخيص المستندات الحرة بين الحين والآخر. هذه الإصدارات الجديدة ستكون مماثلةً للإصدار الحالي من حيث المعنى، إلا أنها قد تختلف في التفاصيل لمعالجة المشاكل أو الاعتبارات المستجدة. راجع www.gnu.org/copyleft/.

يتم منح كل إصدار من هذه الاتفاقية رقم إصدارٍ مميزاً. إ ذا ما أشار المستند بأن رقم إصدارٍ محددٍ من هذه الاتفاقية (أو أي إصدارٍ لاحقٍ) ينطبق عليه فإنك تملك حرية الخيار في اتباع شروط هذا الإصدار المحدد أو أي إصدارٍ لاحقٍ تم نشره (شريطة ألا يكون قد نشر بصيغة مسودة-) من قبل مؤسسة البرمجيات الحرة. إذا لم يحدد المستند رقم إصدارٍ محددٍ من هذه الاتفاقية بإمكانك اختيار أي إصدارٍ تم نشره (شريطة ألا يكون قد نشر بصيغة مسودة-) من قبل مؤسسة البرمجيات الحرة.

قام بترجمة وإعداد هذه الاتفاقية أنس طويلة anas@tawileh.net

This translation has been done by Anas TAWILEH at December 2004. Please send your comments to anas@tawileh.net

الفصل الأول
نواة لينكس

1. مفاهيم النواة

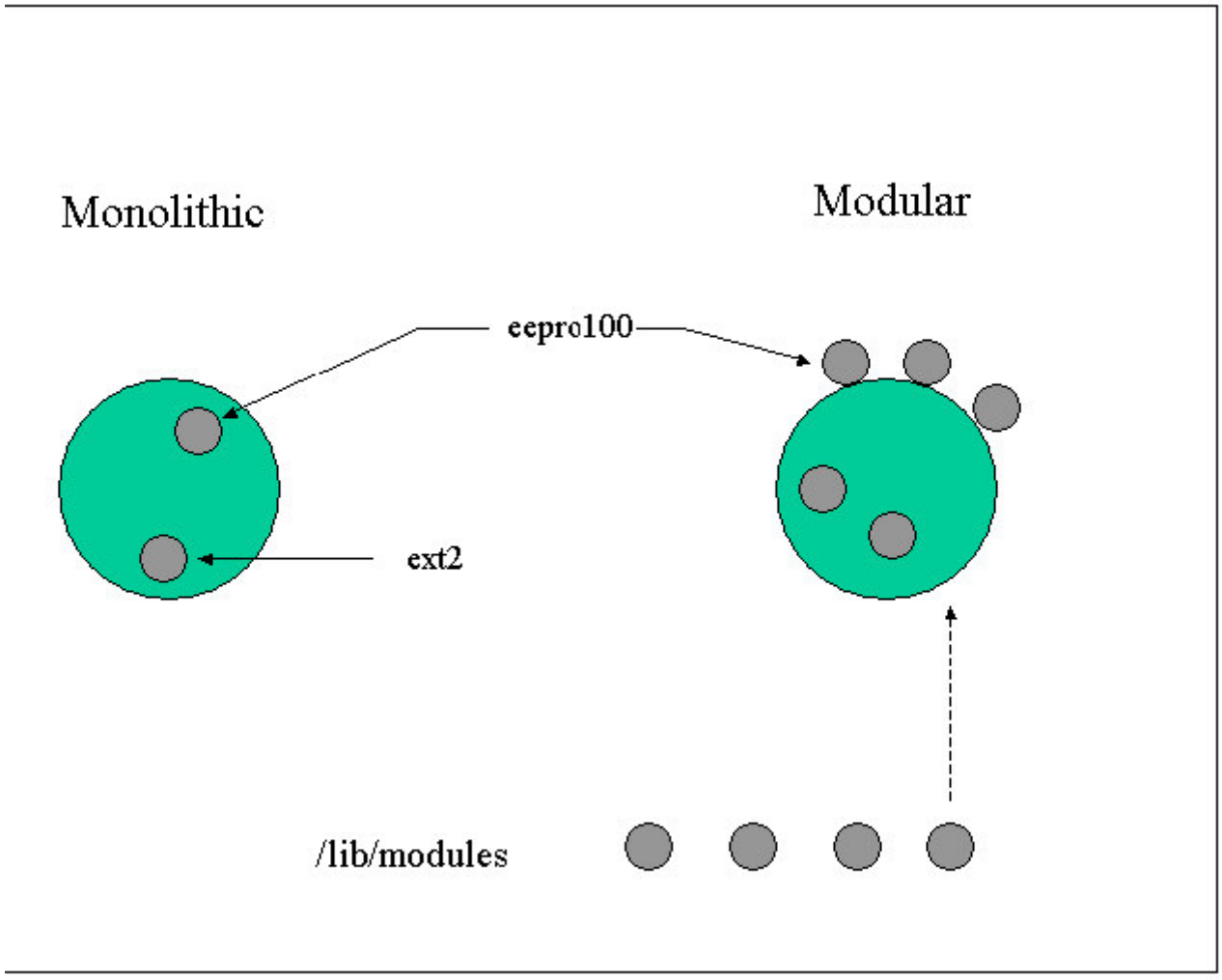
يوجد نوعان مختلفان لنواة لينكس:

أ: نواة موحّدة
Monolithic

النواة الموحّدة نواة تدعم الأجهزة والشبكة ونظام الملفات وتكون مترجمة في ملف صورة واحد.

ب: نواة أحادية
Modular

النواة الأحادية نواة بها سوّاقات مترجمة على شكل كائنات ملفات، يمكن للنواة تحميلها وإزالتها حسب الطلب. توجد الوحدات النمطية القابلة للتحميل في **/lib/modules** .



مـن إيجابيـات النـواة الأحاديـة كونها لا تحتاج لإعادة الترجمة عند إضافة جهاز أو استبداله. أما النواة الموحّدة، فتمتاز بانطلاق أسرع بقليل من الأنوية الأحادية، لكنها لا تتفوّق على النواة الأحادية من حيث الأداء.

2. النواة الأحادية

يمكن ترجمة عدة مكونات لنواة لينكس على شكل وحدات نمطية يمكن للنواة تحميلها أو إزالتها حسب الحاجة.

- تُسجّل الوحدات النمطية الخاصة بنواة معينة في الدليل /lib/modules/<kernel-version>
- من الأفضل تحويل المكونات غير اللازمة عند الانطلاق إلى وحدات نمطية، مثل الأجهزة الطرفية وأنظمة الملفات الإضافية.
- تتحكم في الوحداة النمطية للنواة عدة أدوات موجودة في حزمة modutils.
  - lsmod
  - rmmod
  - insmod
  - modprobe
  - modinfo

تعتمد الوحدات النمطية غالبا على وحدات نمطية أخرى. ولذلك يولّد أمر depmod ملف قاعدة بيانات مسطّحة لاعتمادات الوحدات النمطية /lib/modules/<kernel-version>/modules.dep. يقوم المخطوط rc.sysinit بتشغيل هذا الأمر عند بدء النظام.

- يحمّل modprobe الوحدات النمطية المذكورة في modules.dep مع الوحدات النمطية التي تعتمد عليها.
- تتم استشارة /etc/modules.conf من أجل الوحدات النمطية (طلب القطع IRQ والإدخال والإخراج IO) لكنه عادة ما يضم قائمة ألقاب. تسمح هذه الألقاب للتطبيقات بالإشارة إلى جهاز ما باستخدام اسم اعتيادي. مثلا، يُشار دائما إلى جهاز الأثيرنت الأول بإسم eth0 عوضاً عن اسم برنامج القيادة الخاص به.

شكل1: نموذج ملف /etc/modules.conf:

```
alias eth0 e100
alias usb-core usb-uhc
alias sound-slot-0 i810_audio
alias char-major-108 ppp_generic
alias ppp-compress-18 ppp_mppe
# 100Mbps full duplex
options eth0 e100_speed_duplex=4
```

3. وتيرة إعادة ترجمة النواة

3.1 استخلاص النواة

يُحْفَظُ مصدر النواة في شجرة الدليل /usr/src/linux ، الذي هو صلة وصلة إلى الدليل "/usr/src/"kernel-version . عند استخلاص مصدر نواة جديد ينصح بـ:

- إزالة الوصلة الرمزية الدالة على شجرة دليل مصدر النواة القديم

```
rm linux
```

غالبا ما تُنشِئ مصادر النواة على شكل حزمة RPM وصلةً بإسم linux_2_4

- استخلاص محفوظة المصدر الجديد (مثلا linux-2.4.20.tar.bz2)

```
tar xjf linux-2.4.29.tar.bz2
```

أنوية سلسلة 2.2 المحفوظة تنشِئ دليلا بإسم linux بدلاً من linux-version. هذا يجعل الخطوة الأولى مهمة جداً، ذ يُخشَى الكتابة فوق شجرة مصدر قديم بآخر جديد، ومنذ النواة 2.4 سمّي هذا الدليل kernel-version .

- إنشاء وصلة رمزية إسمها linux للدليل الذي تم إنشاؤه.

```
ln -s linux-2.4.20 linux
```

- حتى الآن، انتهى تشكيل النواة، لكن يجب قبل كل شيء التأكد من إزالة الملفات الثنائية القديمة من شجرة المصدر، باستخدام الأمر make mrproper.

"السيد نقي" mrproper منظف سكاندنافي يجعل الأشياء "أنقى من النقاوة"، وهو خطوة تفوق make clean.

3.2 تشكيل النواة

أولا، حرر ملف Makefile وتأكد من أن المتغير "EXTRAVERSION" مختلف عن النسخة الموجودة:

```
VERSION = 2
PATCHLEVEL = 4
SUBLEVEL = 20
EXTRAVERSION = -test
```

الآن النواة جاهزة للترجمة، يعني هذا إنشاء ملف تشكيل يسمى config..
يتم هذا انطلاقا من شجرة الدليل /usr/src/linux/ بعد أحد الأوامر التالية:

```
make menuconfig
```

```
make xconfig
```

```
make config
```

تسجِّل كل هذه الطرق ملف التشكيل في /usr/src/linux/.config

في معظم الأحيان، يكون من الأفضل تشكيل نواة جديدة باستخدام ملف تشكيل config. قديم بواسطة الأمر make ldconfig. حينئذ لا يدعى المستخدم إلا بشأن المميزات الجديدة في شجرة دليل النواة (إذا كانت النواة حديثة أو مصححة).

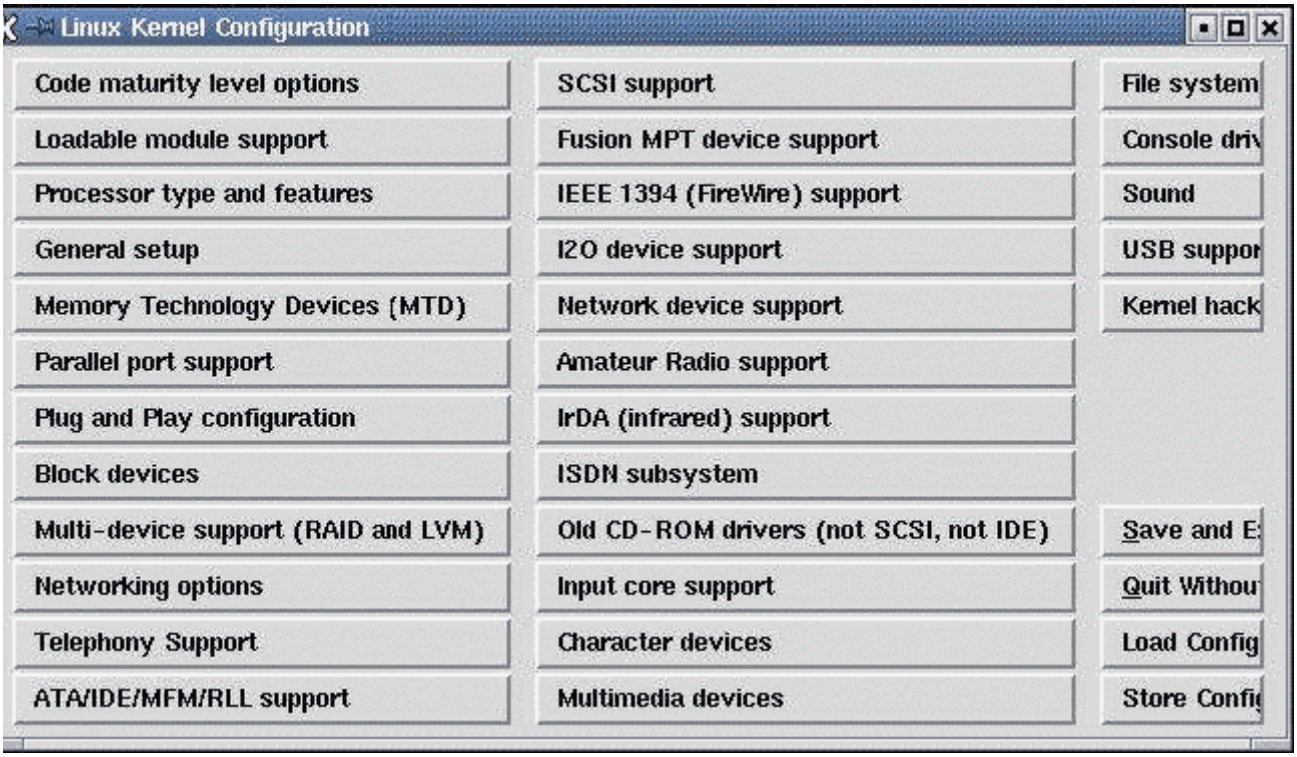
تحوي بعض التوزيعات مثل ردهات دليلا فرعيا إسمه configs يضم ملفات يمكن استعمالها كملفات config. مسبقة التشكيل.

قصد تفعيل مميزات النواة (باستخدام make menuconfig) أُدخل القسم الأعلى بالتحرك بواسطة أزرار الأسهم وضغط دخول لولوج القسم المطلوب. بعد الدخول إلى القسم الفرعي، يمكن تغيير دعم النواة لمميزة أو سوّاق معين بضغط زر الفراغ.

أنواع الدعم الممكنة هي:

- مدعوم (مترجم سكونيا) [*]
- أحادي (مترجم حركيا) [M]
- غير مدعوم [ ]

توجد نفس الخيارات في محررات قوائم الخيارات الأخرى config وxconfig .



شكل 2 ـ المستوى الأعلى لقائمة خيارات make xconfig:

3.3 ترجمة النواة

make dep

بعد إكمال مرحلة التشكيل، يجب عكس هذه الخيارات على جميع الدلائل الفرعية لشجرة مصدر النواة، ويتم ذلك بواسطة الأمر make dep. تُوَلِّد الملفات المسماة depend. ـ التي تضم طرقا إلى ملفات صديرية موجودة في شجرة مصدر لينكس (/usr/src/linux/include) ـ بواسطة الهدف dep.

make clean

يحصل الأمر make على الإر شادات من ملف Makefile ثم يبني ما هو مطلوب. إذا كانت بعض الملفات موجودة من قبل، فسيستعملها make كما هي. وخاصة الملفات ذات التمديد o.*. قصد التأكد من أن جميع خيارات التشكيل الموجودة في .config مستعمَلة من أجل إعادة بناء الملفات المطلوبة، يجب تنفيذ أمر make clean (هذا يمحي الملفات o.*).

ليس من الضروري تنفيذ أمر "make clean" في هذه المرحلة إذا سبق لك أن حضّرت دليل المصدر بواسطة الأمر "make mrproper".

تتم ترجمة النواة نفسِها بواسطة إحدى هذه الأوامر:

```
make zImage
```

```
make bzImage
```

عندما ينتهي الأمر دون أي خطأ، يكون في الدليل /usr/src/linux ملف إسمه vmlinux. إنه نواة غير مضغوطة.

ويكتب الأمران الآخران ملفا إضافيا في /usr/src/linux/arch/i386/boot/ يسمّى zImage وbzImage على التوالي. هذه أنوية مضغوطة بواسطة gzip وbzip2. انظر القسم التالي تثبيت نواة جديدة لمعرفة كيفية استعمال هذه الملفات.

make modules

تترجَم الوحدات النمطية بواسطة make modules.

make modules_install

بعـد ترجمتهـا، يجب نسخ الوحدات النمطية في الدليل الفرعي الموافق في /lib/modules . يتكلّف الأمر make modules_install بهذه المهمة.

يمثل الشكل 3 متوالية الأوامر المستعملة

```
make dep
make clean
make bzImage
make modules
make modules_install
```

3.4 تثبيت نواة جديدة

يمكن العثور على النواة الجديدة في /usr/src/linux/arch/i386/boot/bzImage، حسب بنية نظامك. يجب نسخ هذا الملف في دليل /boot، وتسميته vmlinuz-<full-kernel-version>.

```
/usr/src/linux/arch/i386/boot/bzImage /boot/vmlinuz-<full-kernel-version>
```

بعـد ذلـك، يجب تحرير الملفان /etc/lili.conf و/boot/grub/grub.conf لإضافة النواة الجديدة إلى قائمة خيارات الانطلاق. انسخ قسم "image" من نواتك الحالية ثم أضف قسما آخر "image" في نهاية الملف، كما يظهر أسفله:

تحرير الملف /etc/lilo.conf:

```
prompt
timeout=50
message=/boot/message
image=/boot/vmlinuz
label=linux
```

```
القسم الحالي a6
linuz-<full-kernel-version>
```

```
label=linux-new القسم المضاف
ev/hda6
------------------
```

ال

```
م
```

```
ل
```

ن كذلك عرض نسخة النواة من طرفية

رفية وهمية إذا أضيف الخيار k\ في /etc/issue

يمكن كذلك عرض نسخة النواة من طرفية وهمية إذا أضيف الخيار k\ في /etc/issue

3.5 أقراص ذاكرة التوصل العشوائي البدئية

إذا كانت وحدة نمطية للنواة مترجمة حركيا لازمة عند الانطلاق (مثلا سوّاق SCSI، أو وحدة نظام ملفات لقسم الجذر) يتم تحميلها بواسطة قرص ذاكرة النوصل العشوائي البدئي.

ينشأ هذا القرص البدئي بواسطة أمر mkinitrd الذي لا يأخذ بعين الاعتبار إلا معلمتين: اسم الملف ورقم نسخة النواة
إذا كنت تستعمل قرص ذاكرة بدئي عليكم إضافة initrd= في /etc/lilo.conf

مثال

```
mkinitrd /boot/initrd-$(uname -r).img $(uname -r)
```

3.6 خياري

يستحسن نسخ ملف /usr/src/linux/.config في /boot/config-<full-kernel-version> ، وذلك لمتابعة إمكانيات الأنوية المختلفة المترجمة.

3.7 إعادة تشغيل LILO LILO

و أخيرا، يبقى عليك تعديل LILO حتى يحدّث محمّل الانطلاق. افي أول الأمر، يمكن تشغيل ليلو في نمط الاختبار للتأكد من غياب الأخطاء في ملف التشكيل:

يجب تحديث محمّل الانطلاق LILO باستخدام الأمر lilo إثر أي تغيير في الملف /etc/lilo.conf

تمارين

قبل البداية في التمارين تأكد من أن /usr/src/ خال من أية شجرة نواة. إذا كان الأمر كذلك، احذر الوصلة الرمزية /usr/src/linux .

1. أعد ترجمة النواة يدويا باتباع خطوات الترجمة
   - خذ الحزمة kernel-version.src.rpm من موقع rpmfind أو من قرص. يعتمد تثبيت هذه الحزمة على حزم أخرى، مثل المترجم gcc وحزمة binutils، في حال ما إذا لم تكن مثبتة من قبل.
   - ثبّت الحزمة بـ i- (هذا يضع الشفرة بكاملها في /usr/src/)
   - اذهب إلى /usr/src/linux_version واعرض محتوى الدليل configs
   - انسخ ملف تشكيل النواة الموافق للبنية المستعملة في الدليل الحالي وسمّه config.
   - نفّذ make oldconfig
     في سطر الأوامر حتى يأخذ بعين الاعتبار ملف config. الجديد
   - حرّر ملف Makefile وتأكّد من أن نسخته تختلف عن نسخة النواة الموجودة. للحصول على معلومات حول النواة الحالية، نفّذ الأمر uname -a أو اعرض محتوى الدليل /lib/modules
   - نفّذ

```
make menu config
```

أو

```
menu
```

أو

```
xconfig
```

وأزل دعم ISDN من النواة

- عند مغادرة البرنامج أعلاه، يتغيّر الملف config. لكن التغييرات لا تؤخذ بعين الاعتبار في باقي شجرة المصدر. عليك إذن تنفيذ

```
make dep
```

- و أخيرا، لدفع الملفات الموضوعية الجديدة (o.) إلى الترجمة مع هذه التغييرات، عليك أن تزيل الشفرة المترجمة مسبقا واسطة

```
make clean
```

- يمكنك الآن بناء وحدات النواة النمطية وتثبيتها بواسطة:

```
make bzImage modules modules_install
```

- توجد الوحدات النمطية الآن في دليل /lib/modules/ version. تسمّى النواة الجديدة bzImage كما في الدليل التالي:

```
/usr/src/linux/arch/i386/boot
```

علينا تثبيت النواة يدويا في خطوتين:

أولا

```
cp /usr/src/linux/arch/i386/boot/bzImage /boot/vmlinuz-<full-kernel-version>
```

ثانيا
كان ذلك في غاية البساطة! الآن حرّر /etc/lilo.conf وأضف فقرة 'image' التي ترشد LILO إلى موقع النواة ونظام ملفات الجذر

- نفّذ /sbin/lilo وأعد التشغيل

2. بما أننا قد أنزلنا حزمة kernel-version.src.rpm يمكننا استعمال هذه الحزمة لإعادة ترجمة نوة 'ردهات مسبقة الترجمة'. لاحظ أنه رغم عدم الحاجة إلى أي تدخّل لن يمكنك تغيير قائمة خيارات config..
   - أولا، إعد بناء الحزمة الثنائية بـ:

```
rpm --rebuild kernel-version.src.rpm
```

(انتظر ...!)

- في النهاية، سيولّد kernel-*version*.i386.rpm في /usr/src/redhat/RPMS/i386/.
- ثم حدّث النواة مستخدماً مدير حزم RPM مع الخيار U-

الفصل الثاني
إقلاع لينكس

نظرة عامة

إن إلقاء نظرة أقرب إلى عملية الإقلاع يساعد في حل المشكلات عند التعامل مع من الأجهزة ومهام الإدارة.

نسلط الضوء بدايةً على دور برنامج init وملف تكوينه الملحق /etc/inittab.

يلعب LILO في فترة الإقلاع دوراً أعمق من ذلك. ونلخص في النهاية عملية الإقلاع.

يعد مستندي (From Power to Bash Prompt) بقلم Gerg O'Keefe وكتيب التعليمات boot(7) مرجعين جيدين لهذه الوحدة.

فهم مستويات التشغيل

خلافاً لمعظم أنظمة التشغيل التي لا تخضع لمعايير Unix والتي لديها نمطين وظيفيين (on و off) يوجد في أنظمة يونكس -بما فيها لينكس- مستويات تشغيل مختلفة، كمستوى (الصيانة) ومستوى (تعدد المستخدمين).. الخ. ترقم مستويات التشغيل من 0 إلى 6.

مستويات التشغيل المختلفة

مستوى التشغيل 0	يغلق الجهاز بأمان. مستوى التشغيل 6 يعيد تشغيل الجهاز بأمان
مستوى التشغيل 1	نمط المستخدم الوحيد
مستوى التشغيل 2	نمط تعدد المستخدمين لكنه لا يشغل NFS.
مستوى التشغيل 3	نمط تعدد مستخدمين كامل
مستوى التشغيل 4	غير معرف. وغير مستخدم عموماً
مستوى التشغيل 5	مماثل لـ 3 لكنه يشغل (مدير العرض) أيضاً

يستخدم كل من init و telnet للتبديل من مستوى تشغيل لآخر. تذكر أن init هو أول برنامج يشغل بعد الاستهلال بالنواة عند الإقلاع. معرف العملية PID لـ init هو 1 دائماً.

```
[root@nasaspc /proc]# ps uax |grep init
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.2 0.0 1368 52 ?S
20:17 0:04 init [3]
```

عند كل مستوى تشغيل، سيوقف النظام أو يشغل مجموعة معينة من الخدمات. هذه البرامج مخزنة في /etc/rc.d/init.d يحتوى هذا الدليل على كل الخدمات التي يمكن للنظام تشغيلها. حالما يتم تحميل هذه البرامج ستبقى فعالة/نشطة حتى يتم (الاتصال بـ/تسمية) مستوى تشغيل جديد. هذه الخدمات أيضاً تدعى daemons.

```
ls /etc/rc.d/init.d/
anacron cups identd kadmin krb5kdc mcserv nscd random smb xfs
apmd dhcpd innd kdcrotate kudzu named ntpd rawdevices snmpd xinetd
arpwatch functions ipchains keytable ldap netfs pcmcia rhnsd squid
atd gpm iptables killall linuxconf network portmp rwhod sshd
autofs halt irda kprop lpd nfs pgsql sendmail syslog
crond httpd isdn krb524 marsrv nfslock pppoe single tux
```

ملاحظة: من الممكن إيقاف أو تشغيل برنامج مراقبة daemon معطى يدوياً في /etc/rc.d/init.d بتمرير الوسيط المناسب. على سبيل المثال إذا كنت تريد إعادة تشغيل مزود أباتشي يمكنك كتابة:

```
/etc/rc.d/init.d/httpd restart
```

عنـد العمل مع مستويات التشغيل سوف تأمر/توجه مجموعة محددة وغير معرفة بعد من البرامج بالعمل، ومجموعة أخرى غير معرفة بعد أيضاً ـ بالتوقف.

```
/sbin/init 2
```

هذا بدوره يجبر init على قراءة ملف تكوينه etc/inittab/ لمعرفة ما الذي ينبغي أن يحصل عند مستوى التشغيل هذا.

تحديداً، (وبافتراض أننا نبدل إلى المستوى 2) فإن السطر التالي في inittab منفّذ.

```
l2:wait:/etc/rc.d/rc 2
```

إذا نظـرت إلـى ملـف etc/inittab/ فـإن أمـر etc/rc.d/rc N/ يبـدأ بتشغيل كافة الخدمات في etc/rc.d/rcN.d/ التي تبدأ بـ I بدءاً من S، ويوقف الخدمات التي تبدأ بـ K. هذه الخدمات هي عبارة عن روابط رمزية تشير إلى نصوص rc_scripts في etc/rc.d/init.d/.

إذا كنت لا تريد لعملية ما أن تعمل في مستوى تشغيل معطى N، يمكنك حذف الرابط الرمزي الموافق في etc/rc.d/rcN.d/ بدءاً من K.

روائع inittab

كما وعدنا، دعنا نلقي نظرة على etc/inittab/.

لهذا الملف البنية التالية:

```
id : runlevel : action : command
```

الشكل 3: ملف etc/inittab/:

```
id:3:initdefault:
# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
----------------------snip---------------------------------
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
----------------------snip---------------------------------
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

يمكن أن يكون id أي شيء. إذا كان مستوى التشغيل محدداً، عندئذ (الأمر) و(الإجراء) المطلوب سوف يتم إنجازه فقط عند ذلك المستوى المحدد. إذا لم يكن هنالك رقم محدد فسينفذ السطر عند أي مستوى تشغيل.

مزايا يمكن التعرف عليها/ إدراكها في ملف etc/inittab/

مستوى التشغيل الافتراضي: معد مع بداية الملف **id** id والإجراء. لاحظ أنه لا يوجد ثمة أمر معطى. هذا السطر يخبر init ببساطة بماهية مستوى التشغيل الافتراضي.

البرنـامج الأول المطلوب من قبل init: هذا النص البرمجي يعين الإعدادات الافتراضية، كمتغير PATH يعرف ما إذا كان التشبيك مسموحاً، اسم المضيف.. الخ.

الخد مات الافتراضـية لمـ ستوى التشغيل: إذا كان مستوى التشغيل الافتراضي هو 3، فإن السطر l3 فقط سيتم تنفيذه. الإجراء هو "wait". لن يتم تشغيل أي برنامج آخر حتى تكون كافة الخدمات في المستوى 3 قيد العمل.

طرفيات getty: الأسطر ذات التعريفات من 1 إلى 6 تشغل الطرفيات الافتراضية. من هنا يمكنك تبديل رقم الطرفيات الافتراضية.

مستوى التشغيل 5: السطر الأخير من inittab يقوم بتحميل Xwindwow Manager إذا تم تحميل مستوى التشغيل الخامس.

ملاحظة:

1. يمكنك اعداد مودم للاستماع إلى الاتصالات في inittab. إذا كان جهاز المودم لديك مربوطاً على dev/ttyS1/ فسيسمح السطر التالي باتصالات البيانات (وليس الفاكس) بعد طنينين:

```
S1:12345:respawn:/sbin/mgetty -D -x 2 /dev/ttyS1
```

2. عند عمل التغييرات في etc/inittab/ فسيتعين عليك إجبار init على إعادة قراءة ملف الإعدادات هذا. يمكنك إنهاء ذلك بسهولة بالغة باستخدام:

```
/sbin/init q
```

LILO: محرض إقلاع لينكس

المعلومـات المطلوبـة مـن قبـل المحمـل محدثـة بواسطة sbin/lilo/ (برنامج تثبيت برنامج الإقلاع) والذي يقوم بدوره بقراءة ملفات إعداداته / etc/lilo.conf.

خلال عملية الإقلاع يحتاج Lilo لمعرفة معلومات أساسية، كمعرفة مكان تخزين النواة (عادة في boot/) وما هو نظام الملفات الجذر.

لا يفهم LILO بنية نظام الملفات وأين توجد الأشياء. فقط يتعامل مع الأقراص الفيزيائية.

إذا كنت تقوم بتثبيت توزيعة لينكس ثانية (إضافية) B، والتي لن تكون قيد العمل عند إعداد lilo.conf سوف تحتاج لربط أقسام كقسم boot/ إلى B. يتعين عليك أيضاً الاحتفاظ بمسار إلى نظام الملفات الجذر الخاص بـ B.

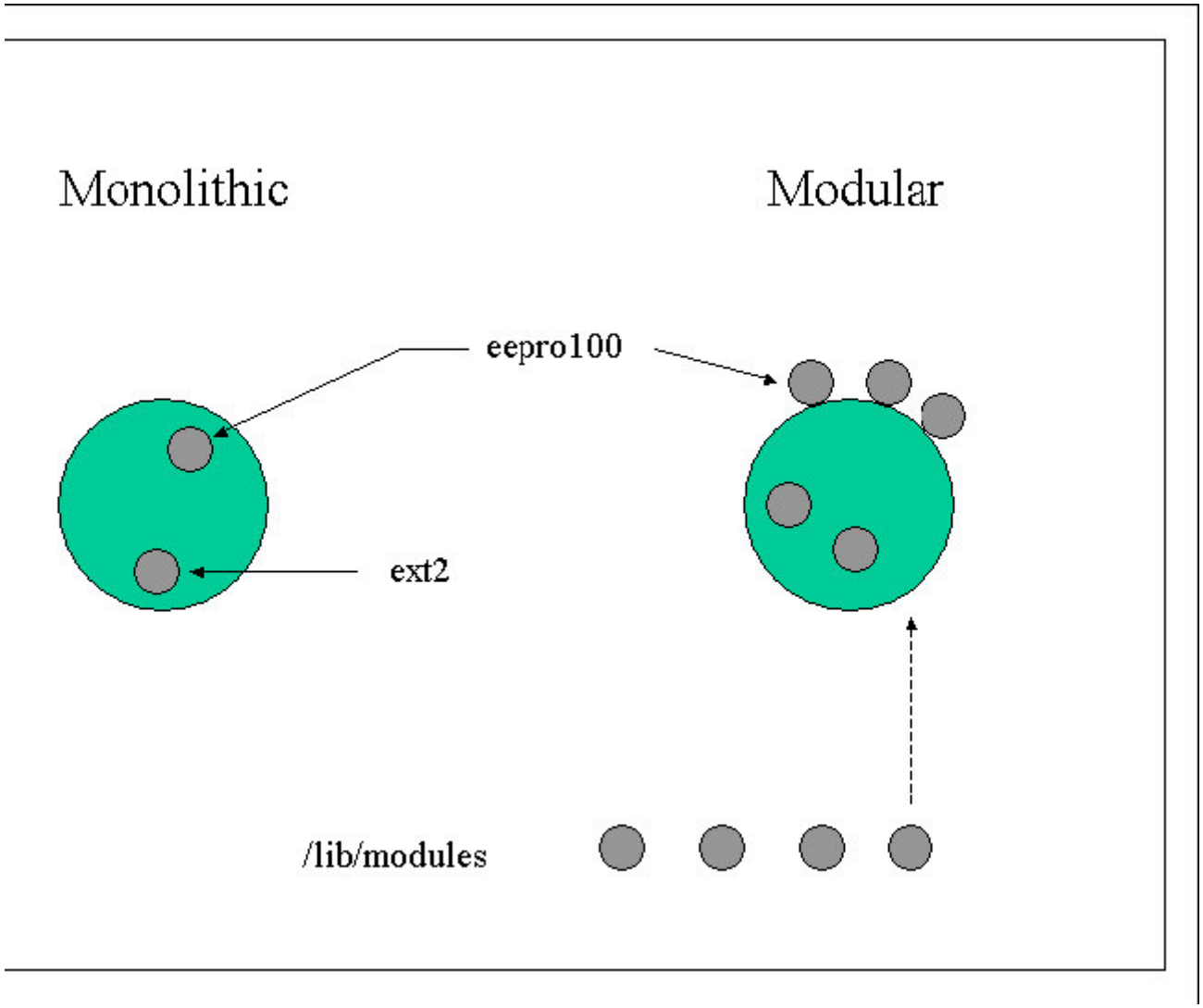
وسائط init:

عـلاوة علـى ذلـك يمـكن لـ LILO تمريـر وسائط مستويات التشغيل إلى init. حالما يتم تحميل النواة يتولى init عملية الإقلاع، وعندما لا يتم تمرير أي وسائط ستقوم init بتحميل مستوى التشغيل الافتراضي المحدد في etc/inittab/.

تمرير تعليمات مستوى تشغيل إلى init في موجه أوامر lilo:

```
Boot: linux s
```

إعراب/تمرير وسائط النواة:



يمكن تمرير وسائط للنواة عند مؤشر lilo أو تعيينها في /etc/lilo.conf بواسطة خيار append.

أمثلة

```
append= "pci=bisoirq"
append="ram=16M"
append="/dev/hdc=ide-scsi" (for CD writers)
```

تعد الوسائط الممررة إلى النواة عند الإقلاع مطلوبة/ضرورية للوحدات التي دمجت مسبقاً في النواة وتساعد غالباً في التعرف على العتاد.

عند الإقلاع، كافة رسائل النواة تدون في /var/log/dmesg بصورة افتراضية. يمكن لهذا الملف إما أن يقرأ أو يمرّر إلى الخرج النظامي بواسطة الأداة /bin/dmesg

4- من الإقلاع إلى الصدفة باش:

يمكننا الآن محاولة الخوض في الخطوات التي يتخذها نظام لينكس خلال عملية الإقلاع.

إذا كان ثمة قرص ذاكرة استهلالي محدد فسيكون محملاً هنا. يتم إدراج الوحدات النمطية من قرص الذاكرة الاستهلالي.

تحمل النواة من الوسط المحدد في تكوين lilo، وعندما يتم تحميلها يفك ضغطها، تقوم النواة عندئذ بربط نظام الملفات الجذر بما يتناسب مع التكوين المستلم من lilo (ro عادة).

تصبح برامج Hence المساعدة في /bin و /sbin متوفرة.

ثم تقوم النواة بتحميل init ـ أول عملية (متاحة للمستخدم).

تقوم init بقراءة الملف /etc/inittab وتتبع تعليماته. عملياً يتم تسجيل rc.sysinit. ينهي (تفحص سلامة نظام الملفات fcsk) مهمته بما يتناسب مع مدخلات /etc/fstab.

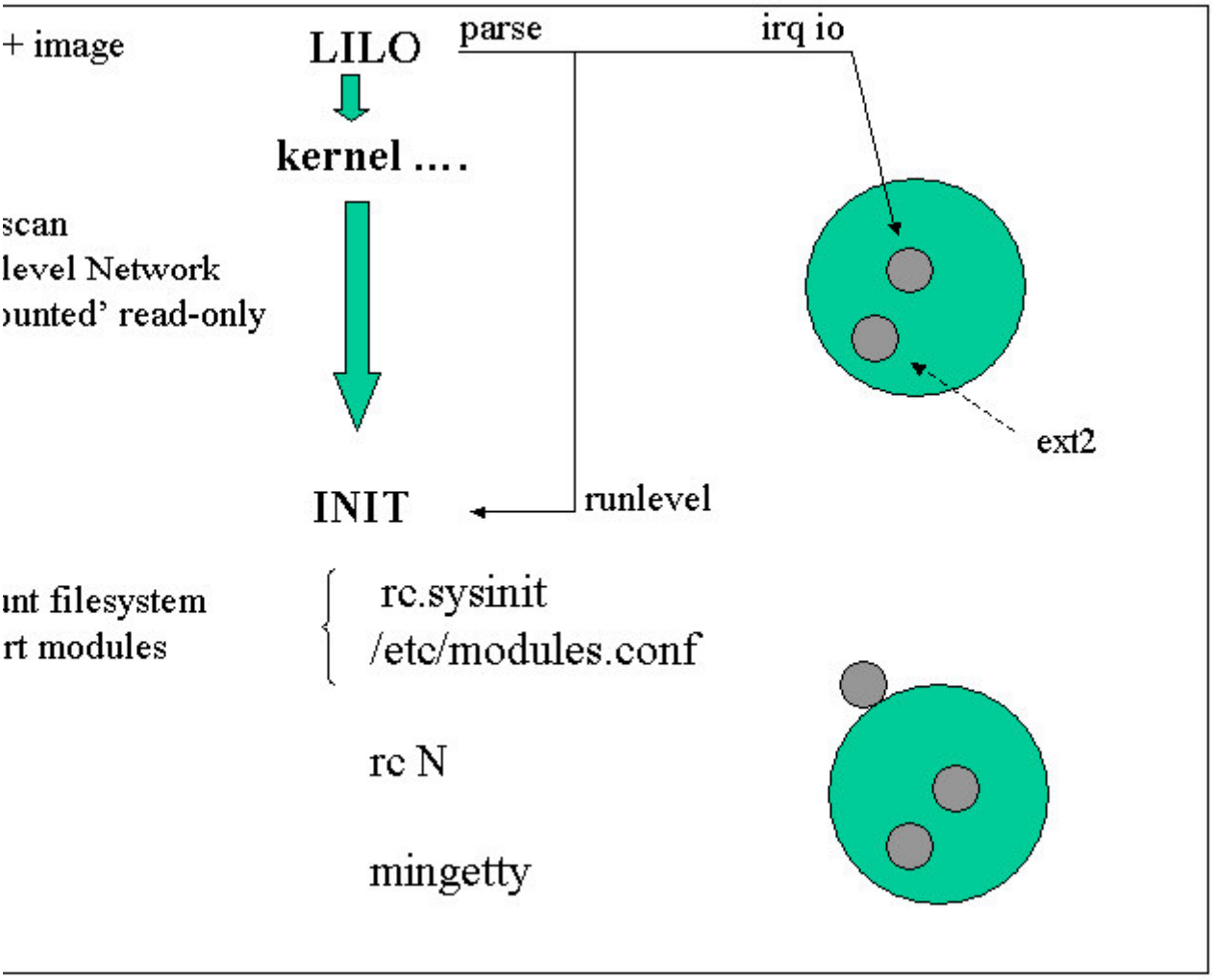
بعد ذلك تذهب init إلى مستوى التشغيل الافتراضي. يبدأ gettys وتنتهي عملية الإقلاع.

مؤشر تسجيل الدخول يدار الآن من قبل getty على ttys.

بعد أن يكون المرسل قد أدخل/طبع اسم وكلمة المرور الخاصة به وضغط مفتاح Enter يبدأ /bin/login

يتم إخطار المستخدم بواسطة /bin/login بإمكانية إدخال كلمة المرور. يدخل المستخدم كلمة المرور ويضغط Enter

تتم مقارنة كلمة المرور التي أدخلها المستخدم بكلمة المرور في /etc/passwd أو /etc/shadow.



تمارين:

الق نظرة على كتيب التعليمات boot(7)، فهو يغطي معظم ما تطرقنا له في هذا الفصل.

1. غير مستوى التشغيل الافتراضي إلى 3 ثم 5. كيف تعرف مستوى التشغيل الحالي لديك؟
2. اضغط/مكن Ctrl+Alt+Del في مستوى التشغيل 3 فقط.
3. أضف مؤشر تسجيل دخول جديد في tty7.
4. استخدم dmesg لقراءة طقم الرقاقات الخاص بالشبكة لديك
5. استكشف الفوارق بين shutdown, halt, restart ـ أي خيار في shutdown سوف يجبر إجراء fsck عند الإقلاع التالي؟
6. استخدم أدوات chkconfig أو ntsysv لتعطيل برنامج المراقبة sshd في مستوى التشغيل 2، 3، 4، و 5.
   تحقق أن الروابط الرمزية في الأدلة ---- قد تغيرت.
7. أعد إقلاع النظام. عند مؤشر الإقلاع مرر الوسيط init= لتجاوز /sbin/init وبدء جلسة باش بسيطة.

الفصل الثالث

إدارة المستخدمين والمجموعات Managing Groups and Users

1ـ إنشاء مستخدمين جدد Creating new users

الخطوة الأولى: إنشاء حساب جديد

الأمر /usr/sbin/useradd هو المسؤول عن إضافة مستخدمين جدد إلى النظام، والرابط useradd يؤشر إليه.

تركيبة الأمر:

```
useradd [options] login-name
```

مثال: إضافة مستخدم باسم rufus:

```
useradd rufus
```

سيتم استخدام القيم الافتراضية عند عدم تحديد الخيارات. يمكن سرد هذه القيم عن طريق الأمر useradd ـD .

الخيارات الافتراضية المسرودة عبر الأمر useradd ـD :

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
```

ملاحظة: هذه المعلومات متوفرة أيضاً في الملف /etc/default/useradd

الخطوة الثانية: تفعيل الحساب مع كلمة سر جديدة

للسماح لمستخدم بالدخول بواسطة حسابه، يجب على مدير النظام ربط حساب المستخدم بكلمة سر باستخدام الأداة passwd .

تركيبة الأمر:

```
passwd login-name
```

هاتان الخطوتان تنشئان مستخدماً جديداً، كما أنهما تبنيان محيط المستخدم الخاص (المؤلف من مجلد المنزل والقشرة الافتراضية). وأيضاً، يتم إضافة المستخدم إلى مجموعة، تحديداً إلى المجموعة الأولية.

2ـ العمل مع المجموعات Working with groups

كل مستخدم جديد يتم ضمه إلى مجموعة ابتدائية (أو أولية). هناك قاعدتان يتم تنفيذهما:

في العادة، تكون المجموعة الأولية هي نفسها لجميع المستخدمين الجدد وتُدعى **users** وذات رقم (GID) يساوي 100. كثير من توزيعات لينكوس يخضع لهذه القاعدة مثل دبيان و سوزي.

طريقة مجموعة المستخدم الخاصة (UPG) - التي تأتي مع ريد هات - تحتال على هذه القاعدة دون أن تخالف أسلوب عمل المجموعات في يونيكس. مع الـ UPG، كل مستخدم ينضم إلى مجموعته الأولية الخاصة. هذه المجموعة تحمل نفس اسم المستخدم (كقيمة افتراضية)، ورقمها سيكون بين 500 و 60000 (كما هو الحال بالنسبة لأرقام المستخدمين).

كنتيجة لذلك، عند استخدام الطريقة التقليدية في المجموعات، قيمة الـ umask ستكون 022 (راجع LPI 101)، بينما في طريقة الـ UPG ستكون قيمة الـ umask هي 002.

الانتساب إلى المجموعات

المستخدم الواحد يستطيع الانضمام إلى عدد غير محدود من المجموعات. ولكن في وقت واحد، ستكون هناك مجموعة فعالة واحدة فقط (عند إنشاء ملف كمثال).

يمكن سرد لائحة المجموعات التي ينتسب إليها المستخدم عن طريق أحد الأمرين id أو groups.

مثال عن المستخدم الجذر:

```
> id
uid=0(root) gid=0(root) groups=0(root), 1(bin), 2(daemon), 3(sys), 4(adm),
6(disk), 10(wheel), 600(sales)
```

```
> groups
root bin daemon sys adm disk wheel sales
```

الانضمام إلى مجموعة

الانضمام إلى مجموعة يغير **مجموعة المستخدم الفعالة** ويبتدئ جلسة جديدة يمكن للمستخدم تسجيل خروجه منها. يتم هذا عن طريق الأمر newgrp.

مثال: الانضمام إلى المجموعة *sales*

```
newgrp sales
```

إنشاء مجموعة جديدة

الأداة groupadd تُستخدم لإدارة المجموعات. ستضيف إدخالاً جديداً في الملف */etc/group*.

مثال: إنشاء المجموعة devel

```
groupadd devel
```

إضافة مستخدم إلى مجموعة

أعمال إدارة النظام تـُلقى على كاهل الأداة gpasswd الخيار a- يقوم بإضافة المستخدم، والخيار d- يقوم بحذفه من المجموعة، بينما الخيار A- يحدد مدير هذه المجموعة. هذه الأداة صُممت في الأساس لوضع كلمة سر للمجموعة، مما يخول جميع مستخدمي هذه المجموعة الدخول بكلمة سر موحدة. لأسباب أمنية، لم تعد هذه الخاصية تعمل.

مثال: إضافة المستخدم rufus إلى المجموعة devel

```
gpasswd -a rufus devel
```

3- ملفات إعدادات النظام Configuration files

ملفا /etc/passwd و /etc/shadow

أسماء جميع المستخدمين محفوظة في الملف /etc/passwd . بنية الملف كالتالي:

1. اسم المستخدم
2. كلمة السر (أو x بدلاً عنها إن تم استخدام ملف الظل)
3. رقم المستخدم
4. رقم المجموعة
5. وصف نصي للمستخدم
6. دليل مجلد المنزل
7. القشرة الافتراضية للمستخدم

تكون هذه البيانات مفصولة بنقطتين كما في المثال التالي (مثال مع كلمة سر مشفرة):

```
george:$1$K05gMbOv$b7ryoKGTd2hDrW2sT.h:Dr G Micheal:/home/georges:/bin/bash
```

لحجب كلمات السر المشفرة عن أعين المستخدمين العاديين، يجب استخدام ملف ظل. الملف /etc/shadow يحتوي على أسماء المستخدمين وكلمات مرورهم المشفرة، ولا يمكن قراءته إلا من قبل المستخدم الجذر.

إن كنت لاتملك ملف الظل في المجلد /etc ، يمكنك إنشاؤه عن طريق الأمر:

```
/usr/sbin/pwconv (passwd -> shadow)
```

هذا سيترك الحرف x مكان الخانة الثانية في كل سطر من الملف /etc/passwd وينشئ ملف الظل. يمكن عكس هذه العملية عن طريق الأمر:

```
/usr/sbin/pwunconv (shadow -> passwd)
```

تحذير : عند استخدام ملف الظل، الملف /etc/passwd يمكن أن يكون قابلاً للقراءة من قبل العموم (صلاحياته تساوي 644)، أما الملف /etc/shadow فيجب أن تكون صلاحياته تساوي 600 أو حتى 400. تأكد عند استخدام الأمر pwunconv من وضع الصلاحيات 600 أو 400 على الملف /etc/passwd .

ملفا /etc/group و /etc/gshadow

بطريقة مماثلة، يتم حفظ بيانات المجموعات في الملف /etc/group حيث يتألف كل سطر من أربعة حقول مفصولة بنقطتين فيما بينها:

1. اسم المجموعة

2. كلمة سر المجموعة (أو x بدلاً عنها إن كان ملف الظل مستخدماً)
3. رقم المجموعة
4. لائحة بأسماء المستخدمين المنتسبين (تفصل بين الأسماء فاصلة)

مثال عن الملف /etc/group :

```
java:x:550:jade, eric, rufus
```

كما الحال لدى المستخدمين، هناك ملف ظل خاص بالمجموعات يُدعى gshadow لتفعيل أو تعطيل استخدام ملف ظل المجموعات، يُستخدم الأمران التاليان:

لإنشاء ملف الظل: /usr/sbin/grpconv
لحذف ملف الظل: /usr/sbin/grpunconv

ملفات /etc/login.defs و /etc/skel/

يحتوي الملف /etc/login.defs على المعلومات التالية:

مجلد البريد: MAIL_DIR
ضوابط كلمات المرور: PASS_MAX_DAYS, PASS_MIN_DAYS, PASS_MAX_LEN, PASS_WARN_AGE
القيمة الدنيا والقصوى لأرقام المستخدمين: UID_MIN, UID_MAX
القيمة الدنيا والقصوى لأرقام المجموعات: GID_MIN, GID_MAX
الإنشاء الآلي لمجلد المستخدم: CREATE_HOME

المجلد /etc/skel يحتوي على الملفات الافتراضية التي يتم نسخها إلى مجلد المنزل الخاص بالمستخدمين الجدد، مثل: .bashrc, .bash_profiles, ...

4ـ خيارات الأوامر Command options

الأمر useradd

تعليق نصي (الاسم الكامل مثلاً)	**c_**
دليل مجلد المنزل	**d_**
رقم المجموعة الأولية (يجب أن تكون المجموعة موجودة مسبقاً)	**g_**
لائحة بأسماء المجموعات المراد الانضمام إليها (الأسماء مفصولة بفاصلة)	**G_**
رقم المستخدم	**u_**
قشرة المستخدم الافتراضية	**s_**
كلمة السر (مشفرة بواسطة md5، استخدم علامتي التنصيص!)	**p_**
تاريخ انتهاء صلاحية الحساب	**e_**
دليل مجلد الـ skel	**k_**
لتعطيل أسلوب الـ UPG	**n_**

الأمر groupadd

لتحديد رقم المجموعة (GID)	**g_**

5_ تعديل الحسابات والإعدادات الافتراضية Modifying accounts and default settings

كل الخيارات المتاحة أثناء إنشاء مستخدم أو مجموعة يمكن تعديلها فيما بعد. والأمر المسؤول عن تعديل إعدادات المستخدم هو الأمر usermod .

خيارات الأمر usermod

تغيير مجلد المستخدمين	d_
تغيير رقم مجموعة المستخدمين الأولية	g_
تغيير اسم المستخدم (login_name)	l_
تغيير رقم المستخدم (UID)	u_
تغيير القشرة الافتراضية	s_

كما نلاحظ، فخيارات هذا الأمر مشابهة لخيارات الأمر useradd .

وبشكل مماثل، نستخدم الأمر groupmod لتغيير إعدادات المجموعات.

خيارات الأمر groupmod

تغيير رقم المجموعة (GID)	g_
تغيير اسم المجموعة	n_

إقفال حساب

* يمكن إقفال حساب مستخدم عن طريق إضافة نقطة تعجب إلى بداية كلمة السر الخاصة به. ويمكن تنفيذ ذلك عن طريق الأوامر التالية:

إقفال	فتح
passwd _l	passwd _u
usermod _L	usermod _U

* عند استخدام ملف الظل، استبدل الـ x بالـ *
* هناك خيار أقل منفعة وهو حذف كلمة السر كلياً عن طريق الأمر passwd _d .
* وأخيراً يمكن تحديد الملف /bin/false كقشرة افتراضية للمستخدم المراد إقفال حسابه.

تغيير تاريخ انتهاء صلاحية كلمة المرور

افتراضياً، كلمة سر المستخدم تنتهي صلاحيتها بعد مرور 99999 يوماً أي ما يوازي 2739 سنة (القيمة الافتراضية لـ PASS_MAX_DAYS). يتم إنذار المستخدم قبل سبعة أيام من انتهاء الصلاحية (القيمة الافتراضية لـ PASS_WARN_AGE)، من خلال رسالة تظهر له عند تسجيل الدخول:

```
Warning: your password will expire in 6 days
```

هناك ضابط آخر لكلمات السر وهو PASS_MIN_DAYS. وهو عدد الأيام الأدنى التي يمكن للمستخدم بعدها تغيير كلمة مروره (قيمته الافتراضية موضوعة على الصفر).

الأداة chage تتيح لمدير النظام تعديل كل هذه الخيارات:

```
chage [ -l ] [ -m min_days ] [ -M max_days ] [ -W warn ] [ -I inactive ]
[ -E expire ] [ -d last_day ] user
```

الخيار الأول l- يسرد الضوابط الحالية لدى المستخدم. لن نناقش سوى الخيار E- المسؤول عن إقفال الحساب عند تاريخ معين. يمكن تحديد هذا التاريخ عن طريق أيام يونيكس أو تاريخ YYYY/MM/DD.

تجدر الإشارة إلى أن هذه البيانات محفوظة في الملف /etc/shadow ويمكن تعديلها من هناك يدوياً.

حذف حساب

يمكن حذف حساب مستخدم عن طريق الأمر userdel. لحذف مجلد المنزل الخاص بالمستخدم، أضف الخيار r-

مثال:

```
userdel -r jade
```

6ـ تمارين

1. إنشاء مستخدمين

استخدم الأمر useradd لإنشاء مستخدم اسمه tux، رقمه 600 ورقم مجموعته 550.

استخدم الأمر usermod لتغيير مجلد المنزل الخاص بالمستخدم
هل يحتاج المجلد الجديد لأن يكون موجوداً مسبقاً؟
هل يتم نسخ محتويات المجلد /etc/skel إلى المجلد الجديد؟
هل يمكن للمستخدم tux الوصول إلى محتويات المجلد القديم؟

استخدم الأمر usermod لإضافة المستخدم tux إلى المجموعة wheel.

2. العمل مع المجموعات

أنشئ مجموعة تـُدعى sales باستخدام الأمر groupadd.

أضف المستخدم tux إلى هذه المجموعة باستخدام الأمر gpasswd.

سجل دخولك باسم tux وانضم إلى المجموعة sales باستخدام الأمر newgrp.

3. ملفات إعدادات النظام

أضف مستخدماً إلى النظام عن طريق تعديل الملفين /etc/passwd و /etc/group .
أنشئ مجموعة تـُدعى share وأضف المستخدم tux إليها عن طريق التعديل اليدوي للملف /etc/group .

4. تعديل حساب

قم بتغيير تاريخ انتهاء صلاحية حساب المستخدم tux باستخدام الأمر usermod.
أقفل حساب المستخدم (استخدم الأوامر أو عدل الملف /etc/shadow).
امنع المستخدم من تسجيل الدخول عن طريق جعل الملف /bin/false قشرة افتراضية للمستخدم.
غير القيمة PASS_MAX_DAYS إلى 1 للمستخدم tux في الملف /etc/shadow .

5. تغيير الإعدادات الافتراضية

استخدم الأمر useradd لتغيير إعدادات المستخدمين الافتراضية، حيث يتم تعيين القشرة /bin/sh كقشرة افتراضية للمستخدمين الجدد (لاحظ أن هذا سيغير الملف في /etc/default).

عدل الملف /etc/login.defs وغير القيمة PASS_MAX_DAYS ليتم إجبار المستخدمين على تغيير كلمات مرورهم كل خمسة أيام.

الفصل الرابع
Network Configuration إعدادات الشبكة

1ـ واجهة الشبكة The Network Interface

بطاقة واجهة الشبكة (NIC) يجب أن تكون مدعومة من قبل النواة. لتحديد نوع بطاقة الشبكة التي تستخدمها، يمكنك الحصول على المعلومات من dmesg، أو /proc/interrupts، أو /sbin/lsmod، أو /etc/modules.conf.

مثال:

```
> dmesg

Linux Tulip driver version 0.9.14 (February 20, 2001)
PCI: Enabling device 00:0f.0 (0004 -> 0007)
PCI: Found IRQ 10 for device 00:0f.0
eth0: Lite-On 82c168 PNIC rev 32 at 0xf800, 00:A0:CC:D3:6E:0F, IRQ 10.
eth0:  MII transceiver #1 config 3000 status 7829 advertising 01e1.
```

```
> cat /proc/interrupts

0:    8729602        XT-PIC  timer
1:          4        XT-PIC  keyboard
2:          0        XT-PIC  cascade
7:          0        XT-PIC  parport0
8:          1        XT-PIC  rtc
10:     622417         XT-PIC  eth0
11:          0         XT-PIC  usb-uhci
14:     143040         XT-PIC  ide0
15:        180         XT-PIC  ide1
```

```
> /sbin/lsmod

Module       Size Used by
tulip       37360  1 (autoclean)
```

في المثال أعلاه، نرى أن نوع الـ chipset لبطاقة الإيثرنت هو Tulip، وعنوان الـ i/o هو 0xf800، ورقم الـ IRQ هو 10. يمكن الاستفادة من هذه المعلومات في حال حال تم استخدام الوحدة (module) الخطأ، أو في حال كانت الموارد (i/o أو IRQ) غير متاحة.

يمكن الاستفادة من هذه المعلومات أيضاً لإضافة وحدة (module) مع عنوان i/o مختلف (باستخدام modprob أو insmod)، كما يمكن حفظها في الملف /etc/modules.conf (سيتم قراءة هذه البيانات المحفوظة في عملية الإقلاع التالية).

2ـ معلومات المضيف Host Information

الملفات التالية تُستخدم لحفظ معلومات الشبكة:

ـ /etc/resolv.conf يحتوي على لائحة بأسماء ملقمات DNS

```
nameserver 192.168.1.108
nameserver 192.168.1.1
search linuxit.org
```

/etc/HOSTNAME يُستخدم لإعطاء جهاز الكمبيوتر اسماً.

- يمكن إعطاء اسم لواجهة الشبكة، تختلف طريقة فعل ذلك باختلاف التوزيعات.

- /etc/hosts يحتوي رقم الـ IP للجهاز مع أسماء المضيفات المعروفة.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1      localhost  localhost.localdomain
# other hosts
192.168.1.108  mesa  mesa.domain.org
192.168.1.119  pico
```

- /etc/sysconfig/network يحدد إن كان عمل الشبكة سيبدأ، يمكنه أن يحتوي أيضاً على المتغير HOSTNAME

```
NETWORKING=yes
HOSTNAME=mesa.domain.org
GATEWAY=192.168.1.1
GATEWAYDEV=
```

/etc/sysconfig/network_scripts/ifcfg_eth0 يحتوي بيانات الإعدادات لـ eth0

```
DEVICE=eth0
BOOTPROTO=none
BROADCAST=192.168.1.255
IPADDR=192.168.1.108
NETWORK=192.168.1.0
ONBOOT=yes
USERCTL=no
```

3- إيقاف وبدء عمل الشبكة Stop and Start Networking

من خلال سطر الأوامر

الأداة الرئيسية لاستدعاء واجهة الشبكة هي /sbin/ifconfig . عندما يتم تشغيلها يتم تحميل وحدة الـ eth0 (eth0 module) ذات الاسم المستعار (alias) من الملف /etc/modules.conf، وربطها برقم IP وبقيمة قناع الشبكة (netmask value).

كنتيجة لذلك، يمكن تشغيل أو إيقاف واجهة الشبكة دون فقدان هذه المعلومات طالما كانت الوحدة (module) محملة في النواة.

مثال عن استخدام ifconfig :

```
/sbin/ifconfig eth0 192.168.10.1 netmask 255.255.128.0
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
```

أداة أخرى هي /sbin/ifup، تقوم بقراءة ملفات إعدادات النظام في المجلد /etc/sysconfig/ وتقدم القيم المحفوظة إلى واجهة معينة. النص التنفيذي لـ eth0 يُدعى ifcfg_eth0 ويحتاج للإعداد. إن تم تحديد بروتوكول إقلاع كـ DHCP، فسيشغل الأمر ifup الواجهة مع هذا البروتوكول.

مثال عن استخدام ifup :

```
/sbin/ifup eth0
/sbin/ifup ppp0
/sbin/ifdown eth0
```

استخدام نص الشبكة التنفيذي

عند عملية الإقلاع، تقرأ بطاقة الإيثرنت إعداداتها من الملف /etc/rc.d/init.d/network . كل الملفات المتعلقة بالشبكة تكون موجودة كمصدر في المجلد /etc/sysconfig/ .

بالإضافة إلى ذلك، يقوم النص التنفيذي بقراءة خيارات الـ sysctl في الملف /etc/sysctl.conf، إنه المكان الذي تستطيع فيه إعداد الجهاز كموجه (router) (اسمح بتمرير ال IP في النواة). كمثال، السطر التالي:

net.ipv4.ip_forward = 1

سيسمح بتمرير ال ip والملف /proc/sys/net/ipv4/ip_forward/ سيحتوي على الرقم 1.

يتم بدء نص الشبكة التنفيذي عن طريق الأمر التالي:

```
/etc/rc.d/init.d/network restart
```

إعادة تجديد عقد الـ DHCP

الأدوات التالية ستستعلم الـ DHCP عن رقم IP جديد:

pump

dhcpclient

هناك عفريت (daemon) للعميل يُدعى dhcpcd (يجب عدم الخلط بينه وبين عفريت الخادم dhcpd).

4ـ التوجيه Routing

هناك اختلاف ملحوظ سيطرأ عند استخدام الأمر ifup ، وهو جدول التوجيه (routing table) الخاص بالنظام. سبب ذلك هو إما قراءة الملف /etc/sysconfig/network حيث يتم حفظ عنوان "البوابة الرئيسية" (default gateway)، أو أن ملقم الـ DHCP أرسل معلوماته مع رقم الـ IP سوية. يتم إعداد جداول التوجيه والتحقق منها وتعديلها بواسطة الأداة /sbin/route .

أمثلة عن التوجيه

إضافة مسار إلى الشبكة 10.0.0.0 عبر الجهاز eth1 واستخدام 192.168.1.108 كبوابة لهذه الشبكة:

```
/sbin/route add -net 10.0.0.0 gw 192.168.1.108 dev eth1
```

إضافة بوابة افتراضية:

```
/sbin/route add default gw 192.168.1.1 eth0
```

سرد جدول التوجيه الخاص بالنواة:

```
> /sbin/route -n

Kernel IP routing table
Destination     Gateway         Genmask         Iface
192.168.1.0     0.0.0.0         255.255.255.0   eth0
10.1.8.0        192.168.1.108   255.0.0.0       eth1
127.0.0.0       0.0.0.0         255.0.0.0       lo
0.0.0.0         192.168.1.1     0.0.0.0         eth0
```

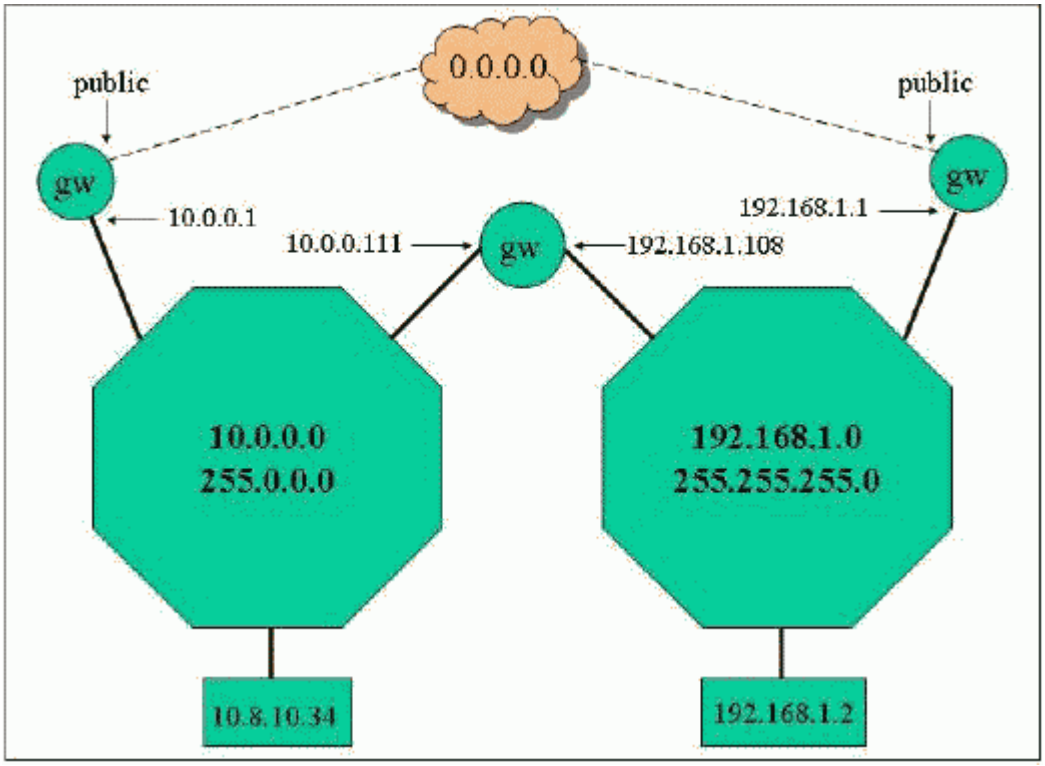
البوابة الافتراضية:
في اللائحة الأخيرة، عمود الهدف (Destination) هو عبارة عن لائحة من الشبكات. رقم 0.0.0.0 يعني "إلى أي مكان". بعد أن عرفنا هذا، سيبقى رقما IP في عمود البوابة (Gateway). أيهما البوابة الافتراضية؟

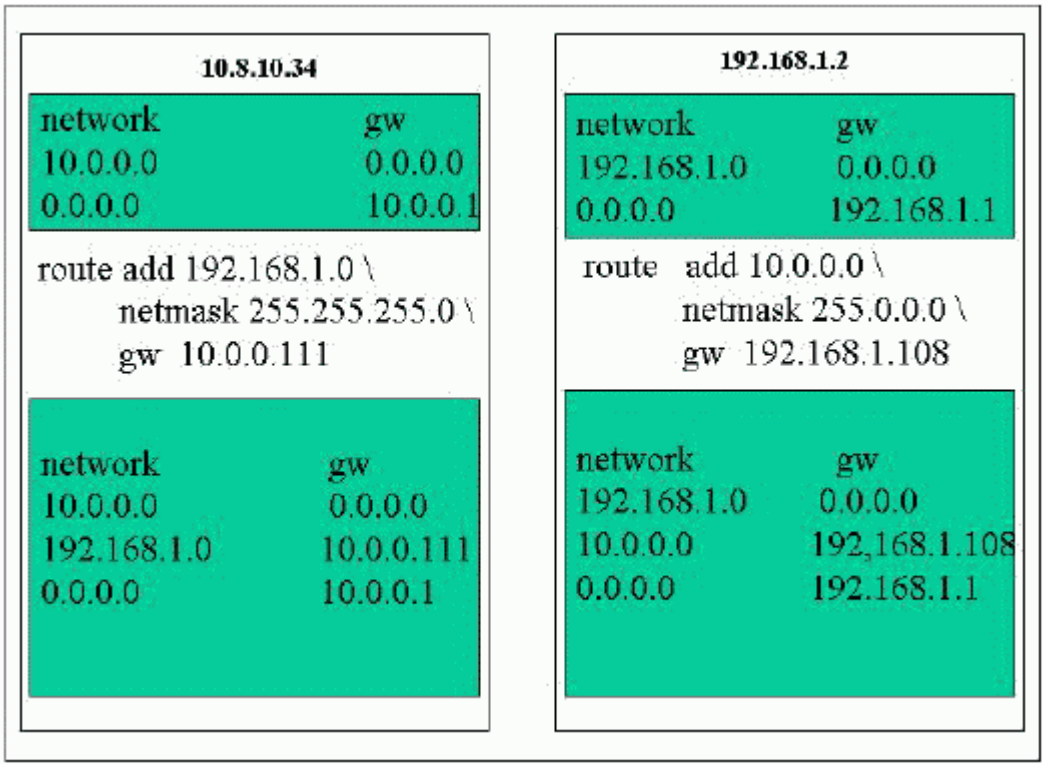
>> لتجنب دخول مسارات ساكنة عبر عفاريت (daemons) خاصة، استخدم gated أو routed للتحديث الديناميكي لجداول التوجيه عبر الشبكة.

>> إن كنت تتبع للشبكة 192.168.10.0، وأضفت مساراً إلى الشبكة 192.168.1.0، فقد تجد أن الأجهزة في تلك الشبكة لا تستجيب. سبب ذلك هو عدم وجود مسار عكسي من شبكة 192.168.1.0 إلى مضيفك!! حل هذه المشكلة يكمن في استخدام التوجيه الديناميكي.

المسارات الساكنة الدائمة:
إن كنت تملك عدة شبكات مع أكثر من بوابة افتراضية واحدة، يمكنك استخدام الأمر /etc/sysconfig/static_routes (بدلاً من عفاريت التوجيه).
سيتم إضافة هذه المسارات عند إقلاع الجهاز عن طريق النص التنفيذي network.

سيناريو توجيه:





5ـ أدوات الشبكة الشائعة Common Network Tools

هذه لائحة قصيرة بأدوات مفيدة في حال حصول مشكلات في اتصالات الشبكة.

• **ping *host*** :

هذه الأداة ترسل حزمة ICMP تـُدعى ECHO_REQUEST إلى المضيف المحددوتنتظر حزمة ECHO_REPONSE.

خيارات الأمر ping
b_ : عمل ping لعنوان إذاعي broadcast address
c N_ : إرسال عدد N من الحزمات.
q_ : النمط الصامت: يُظهر فقط رسائل البداية والنهاية.

• **netstat** :

يعطي معلومات عن اتصالات الشبكة الحالية، أو جدول التوجيه، أو إحصائيات الواجهة، وذلك تبعاً للخيارات المستخدمة فيه.

خيارات الأمر netstat
r_ : يعطي نتيجة مماثلة للأمر /sbin/route إن تم تنفيذه.
l_ : يظهر قائمة الواجهات.
n_ : عدم تحويل عناوين الـ IP.
p_ : يظهر الـ PID وأسماء البرامج (خاص بالمستخدم الجذر).
v_ : إظهار المزيد من التفاصيل.
c_ : تحديث متواصل.

مثال: ناتج الأمر netstat _inet _n

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address       Foreign Address    State
tcp        0      0 192.168.1.10:139   192.168.1.153:1992 ESTABLISHED
tcp        0      0 192.168.1.10:22    192.168.1.138:1114 ESTABLISHED
tcp        0      0 192.168.1.10:80    192.168.1.71:18858 TIME_WAIT
```

يمكننا، في السرد أعلاه، رؤية المضيف وقد أنشأ اتصالات على المنافذ 139، 22، 80.

- **arp**

يُظهر الـ ARP Cache الخاص بالنواة.

مثال:

```
> arp

Address      HWtype HWaddress         Iface
192.168.1.71 ether  00:04:C1:D7:CA:2D eth0
```

- **traceroute**

يُظهر المسار الموصل بين المضيف المحلي والمضيف الهدف. هذا الأمر يجبر الموجهات الوسيطة على إرجاع رسائل خطأ (ICMP TIME_EXCEEDED) بتخفيض قيمة الـ TTL (Time To Live) بشكل كبير. مع كل رسالة TIME_EXCEEDED تقوم traceroute بزيادة الـ TTL مجبرة الحزمة التالية على الوصول أبعد، حتى بلوغ هدفها النهائي.

مثال:

```
> /usr/sbin/traceroute -n www.redhat.com

traceroute: Warning: www.redhat.com has multiple addresses; using
216.148.218.197
traceroute to www.redhat.com (216.148.218.197), 30 hops max, 38 byte
packets
1 192.168.1.1 0.440 ms 0.347 ms 0.341 ms
     ---- snip ---
14 12.122.2.145 112.116 ms 110.908 ms 112.002 ms
15 12.122.2.74 156.629 ms 157.028 ms 156.857 ms
16 12.122.255.222 156.867 ms 156.641 ms 156.623 ms
17 216.148.209.66 159.982 ms 157.462 ms 158.537 ms
18 216.148.218.197 157.395 ms 156.789 ms 156.080 ms
```

خيارات الأمر traceroute
-f ttl : يغير قيمة الـ TTL الأساسية من 1 إلى الرقم المحدد.
-n : عدم تحويل أرقام الـ IP.
-v : إظهار المزيد من التفاصيل.
-w sec : تحديد مدة الانتظار للحزمة بالثواني.

6ـ تمارين

1. في سيناريو التوجيه المذكور في هذا الفصل، حدد جدول التوجيه للبوابة الافتراضية للشبكة المحلية.

2. ابدأ واجهة الشبكة لديك يدوياً

```
ifconfig eth0 192.168.0.x
```

قم بسرد وحدات النواة (kernel modules). تأكد أن وحدة الـ eth0 قد تم تحميلها: تحقق من الملف /etc/modules.conf

.3

أ- أوقف واجهة الشبكة باستخدام الأمر:

```
ifconfig eth0 down
```

```
ب- أثبت أنك تستطيع إعادة واجهة الشبكة إلى العمل من دون استخدام الأمر:


 ifconfig eth0 up
```

4
. أوقف الواجهة وأزل وحدة النواة (rmmod module). ماذا سيحدث لو أعدت الخطوة (3. أ-) ؟
5
. قسم الفئة إلى شبكتين (A: (192.168.1.0 و (B: (10.10.10.0.
*

جرب الوصول إلى الأجهزة عبر الشبكة
اختر جهازاً موجوداً ليكون البوابة الافتراضية (لكلا الشبكتين)
على جهاز البوابة الافتراضية فقط، قم بالتالي:

```
-- اسمح بتمرير الـ IP


echo 1 > /proc/sys/net/ipv4/ip_forward
```

- استحضر واجهة ذات اسم مستعار (aliased interface)، ستعمل كواجهة ثانية.
إن كنت في الشبكة 192.168.1.0، قم بالتالي:
ifup eth0:1 10.0.0.x (حيث x هو رقم IP متاح).
ووجه المسار إلى الشبكة الجديدة مجبراً إياه على استخدام جهاز eth0:1.

-- أضف مساراً إلى الشبكة الأخرى مستخدماً جهاز البوابة الافتراضية (عليك أن تعرف إن كانت إعدادات البوابة الافتراضية على الـ eth0 أو على الـ eth0:1 وفقاً للشبكة التي تتواجد عليها).

الفصل الخامس
شبكات TCP/IP

الأرقام الثنائية و Dotted Quad

الأرقام الثنائية

$10 = 2^1$	$100 = 2^2$	$101 = 2^2+1$	111 = 100 + 010 + 001

هذا يعني أنه يمكن تحويل أي رقم ثنائي إلى عشري كما يلي:

```
10000000 = 27 = 128
01000000 = 26 = 64
00100000 = 25 = 32
00010000 = 24 = 16
00001000 = 23 = 8
00000100 = 22 = 4
00000010 = 21 = 2
00000001 = 20 = 1
```

الخانات المنقوطة:

عنـوان الـــ IP الاعتيـادي المخصـص لواجهـة ما يدعى (Dotted Quad). وهي في حالة الإصدار الرابع IPv4 مكونة من 4 بايتات (8 بتات * أربع مرات) مفصولة بنقاط.

Binary	Decimal
11000000.10101000.00000001.00000001	192.168.1.1

عنوان البث، عنوان الشبكة، وقناع الشبكة

يتضمن عنوان الـ IP معلومات حول كل من عنوان المضيف (أو الواجهة) وقناع الشبكة.

قناع الشبكة

يستخدم قناع الشبكة لتعريف الجزء من عنوان IP المستخدم للشبكة. ويدعى أيضاً (قناع الشبكة الفرعية) Subnet Mask.

قناع شبكة عيار 16 بت و 17 بت

255.255.0.0	16_bit	11111111.11111111.00000000.00000000
255.255.128.0	17_bit	11111111.11111111.10000000.00000000

يعطى البث عادة بصورة عشرية.

مثال:

بقناع شبكة عيار 16 بت ستنتمي عناوين IP التالية إلى نفس الشبكات

```
00100000 . 10000000 . 00000001 . 00000001
00100000 . 10000000 . 00000000 . 00000011
```

هـذا يـعني أن أي تغير يطرأ على البتات داخل الصندوق (8 + 8 = 16 بت) سيتغير عنوان الشبكة وستحتاج الواجهات إلى بوابة Gateway للاتصال فيما بينها.

وبنفس الطيرقة فإن أي تغير يطرأ على البتات خارج الصندوق سيغير عنوان الواجهة دون تغير الشبكات.

على سبيل المثال، بقناع شبكة عيار 24 بت سيكون عنوانا الـ IP أعلاه على شبكتين مختلفتين:

```
00100000 . 10000000 . 00000001 . 00000001
00100000 . 10000000 . 00000000 . 00000011
```

عنوان الشبكة

لكل شبكة رقم يتم اللجوء إليه عند إعداد عمليات التوجيه. رقم الشبكة هو جزء من الـ Dotted Quad. يستبدل الجزء المخصص كعنوان للمضيف بالأصفار.

عنوان شبكة نموذجي: 192.168.1.0 .

عنوان البث

عنوان البث لجهاز هو نطاق الأجهزة المضيفة/الواجهات التي يمكن الوصول إليها على نفس الشبكة.

على سبيل المثال سوف يتمكن أي مضيف بعنوان بث 10.1.255.255 من الوصولى إلى أي جهاز يحمل عنوان IP : 10.1.x.x.

عنوان البث النموذجي: 192.168.1.255 .

إعادة زيارة الـ dotted quad

يمكن تطبيق عملية منطقية بسيطة على أرقام البث والقناع والشبكة.

لاسترداد عنوان الشبكة من رقم IP معين، قم ببساطة بجمع رقم الـ IP مع القناع

```
Network Address = IP AND Netmask
```

وبالمثل، يتم إيجاد عنوان البث من خلال العملية المنطقية (عنوان الشبكة أو ما عدا قناع الشبكة).

```
Broadcast Address = Network OR not[Netmask]
```

تمثل كل من AND و OR هنا معاملات منطقية مطبقة على الصيغ الثنائية لهذه العناوين

مثال:

لنأخذ عنوان IP : 192.168.3.5 مع قناع شبكة: 255.255.255.0. يمكننا القيام بالعمليات التالية:

```
Network address = IP AND MASK

11000000. 10101000.00000011.00000101 (192.168.3.5)
1.11111111.11111111.00000000 (255.255.255.000)
11111.11111111.00000000 (255.255.255.000)
_____________________
68.3.0)
```

```
0101000.00000011.00000101 (192.168.3.5)
```

```
11000000. 10101000.00000011.00000101 (192.168.3.5)
OR
00000000.00000000.00000000.11111111 (000.000.000.255)
_____________________________________________
11000000.10101000.00000011.11111111 (192.168.3.255)
```

من الواضح من المثال أعلاه أن أي رقم IP مع قناع شبكة كاف لإعطاء كافة المعلومات المتعلقة بالشبكة والمضيف.

فئات الشبكة

عناوين IP المحجوزة

يوجد في الشبكات الخاصة مجموعة محددة من عناوين IP مخصصة لأغراض معينة، لا تستخدم على الإنترنت. هذه الأرقام المحجوزة تستخدم بصورة نموذجية في الشبكات المحلية.

يبين الجدول التالي مختلف الفئات الخاصة/المحجوزة:

العناوين المحجوزة		
1	Class A	10.x.x.x
16	Class B	172.16.x.x _ 172.31.x.x
255	Class C	192.168.0.x

فئات الـ IP:

الفئة Class A
عنوان شبكة عيار 8 بت، وعنوان مضيف عيار 24 بت.
يتم إعطاء البايت الأول (الثمانية الأولى) كعنوان شبكة. وبالتالي سيكون القناع الافتراضي 255.0.0.0. أما الثمانيات الثلاث الباقية فهي متاحة لتعيين واجهات المضيف.
وحيث أن 255.255.255 و 0.0.0 هي أرقام مضيف غير صالحة، سيكون لدينا 2^{24} 2 = 16 777 214 مضيف محتمل.
البايت الأول (الثمانية الأولى) لرقم IP محصورة من 1 إلى 127. وهذا يكافئ النطاق الثنائي من 00000001 إلى 01111111. يمكن إعطاء البتين الأولين من عناوين الفئة Class A القيمة 00 أو 01.

الفئة Class B
عنوان شبكة عيار 16 بت، وعنوان مضيف عيار 16 بت.
يتم إعطاء البايتين الأولين (الثمانيتين الأولى والثانية) كعنوان شبكة. وبالتالي سيكون القناع الافتراضي 255.255.0.0.
سيكون لدينا 2^{16} 2 = 65 534 مضيف محتمل.
البايت الأول (الثمانية الأولى) لرقم IP محصورة من 128 إلى 191. لاحظ أن النطاق الثنائي للبايت الأول هو من 10000000 إلى 10111111. ذلك أن الزوج الأول من البتات لعنوان من الفئة B يتخذ القيمة 10.

الفئة Class C
عنوان شبكة عيار 24 بت، وعنوان مضيف عيار 8 بت.
يتم إعطاء البايتات الثلاث الأولى (الثمانيات الثلاث الأولى) كعنوان شبكة. وبالتالي سيكون القناع الافتراضي 255.255.255.0.
سيكون لدينا 2^{8} 2 = 254 مضيف محتمل.
البايت الأول (الثمانية الأولى) لرقم IP محصورة من 192 إلى 223. وهذا يكافئ النطاق الثنائي من 11000000 إلى 11011111. نخلص من ذلك إلى أن الزوج الأول من البتات لعنوان من الفئة C يتخذ القيمة 11.

الشبكات الفرعية

يحدث التشبيك الفرعي عندما تستخدم البتات المحجوزة في الشبكة. يتم تحديد ذلك من خلال قناع الشبكة والناتج في شبكات كونها منفصلة.

على سبيل المثال يمكن تغيير قناع شبكة من الفئة A الاعتيادية 255.0.0.0 للسماح للبت الأول من الثمانية الثانية ليكون جزءاً من الشبكة ليكون جزءاً من الشبكة. ينتج ذلك في عنوان شبكة 9 بت وعنوان IP عيار 32 بت.

سيبدو القناع ثنائياً كما يلي:

11111111.10000000.00000000.00000000 or 255.128.0.0

ثمة طريقة أخرى لبيان أن عنوان شبكة عيار 9 بت قيد الاستخدام هو إعطاء رقم IP 10.1.8.1 كـ 10.1.8.1/9

سوف نأخذ المثال الخاص بعنواون من فئة C: 192.168.1.0. سوف بنبحث في شبكات 25 ثم 26 بت.

شبكة عيار 25 بت

قناع الشبكة:

11111111.11111111.11111111.10000000 or 255.255.255.128

حيث أن عنوان الشبكة = رقم IP و قناع الشبكة، نرى من القناع أن عنواني شبكة يمكن أن يتكون اعتماداً على نطاق الأجهزة المضيفة:

1. عناوين المضيف في نطاق 192.168.1.**0**xxxxxxx ينتج في شبكة 192.168.1.**0**. نقول عندئذ: رقم الشبكة هو **0**.
2. عناوين المضيف في نطاق 192.168.1.**1**xxxxxxx ينتج في شبكة 192.168.1.**128**. نقول عندئذ: رقم الشبكة هو **128**.

في كلا الحالتين يعطي استبدال الخانات x بالأصفار أو الواحدات معنىً خاصاً

عنوان الشبكة	الاستبدال بالـ 1	الاستبدال بالـ 0
0	البث: 127	الشبكة: 0
128	البث: 255	الشبكة: 128

تبقى لدينا مهمة إكمال أرقام الأجهزة المضيفة لكل شبكة. حيث أن عنوان المضيف يبلغ 7 بتات ونستثني قيمتين (كافة الواحدات والأصفار) سيكون لدينا $2^7-2=126$ جهازٌ مضيفاً في كل شبكة، أو ما مجموعه 252.

لاحظ أنه إذا كان قناع الشبكة الافتراضية 255.255.255.0 مستخدماً فسيكون لدينا 254 عنوان مضيف متاح.

في المثال أعلاه، يوجد لكل من 192.168.1.127 و 192.168.1.128 معنى خاص، وهذا عدم تجاوز عدد عناوين الأجهزة المضيفة لـ 252 مضيفاً.

شبكة عيار 26 بت

قناع الشبكة:

11111111.11111111.11111111.11000000 or 255.255.255.192

هنا، وأيضاً بناء على عناوين المضيف يمكن تحديد 4 عناوين شبكة مختلفة فقط باستخدام القاعدة (و) (AND).

حيث أن عنوان الشبكة = رقم IP و قناع الشبكة، نرى من القناع أن عنواني شبكة يمكن أن يتكون اعتماداً على نطاق الأجهزة المضيفة:

1. عنوان المضيف في النطاق 192.168.1.**00**xxxxxx ينتج في شبكة 192.168.1.**0**.
2. عنوان المضيف في النطاق 192.168.1.**01**xxxxxx ينتج في شبكة 192.168.1.**64**.
3. عنوان المضيف في النطاق 192.168.1.**10**xxxxxx ينتج في شبكة 192.168.1.**128**.
4. عنوان المضيف في النطاق 192.168.1.**11**xxxxxx ينتج في شبكة 192.168.1.**192**.

باستبدال x في الأرقام أعلاه بـ 1 نحصل على عناوين البث الموافقة:

192.168.1.63
192.168.1.127
192.168.1.191
192.168.1.255

كل شبكة فرعية لها $2^6-2=62$ جهاز مضيف محتمل أو ما مجموعه 248 مضيف.

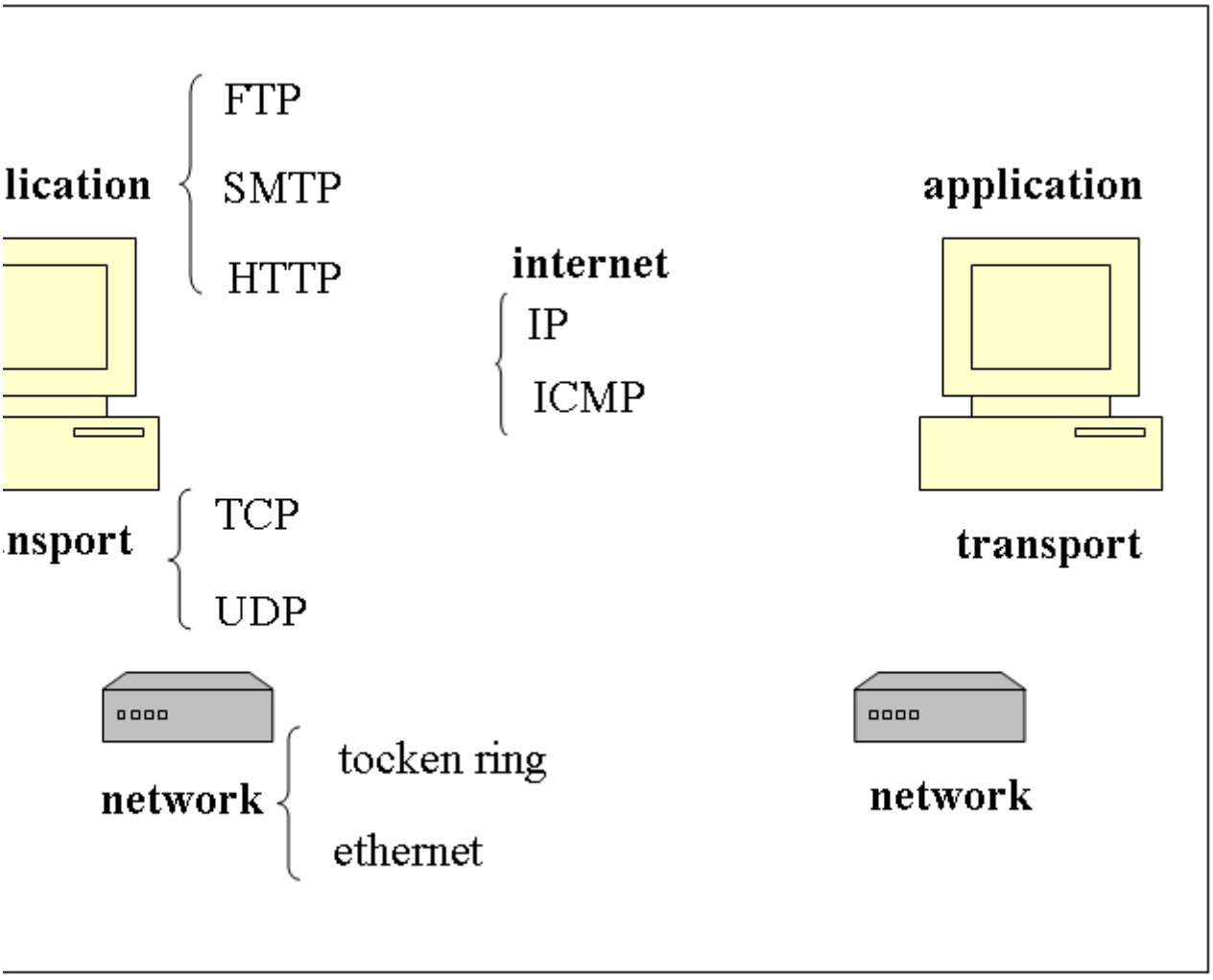
مجموعة بروتوكولات TCP/IP

TCP/IP هي مجوعة البروتوكولات المستخدمة على الإنترنت. يقصد بهذا الاسم أن حمل البيانات والبرامج عبر الإنترنت يتطلب العديد من البروتوكولات. البروتوكولين الرئيسين هما TCP () و IP ().

للتبسيط، يتحكم IP بالرزم أو مخططات البيانات فقط (عنوان الوجهة، الحجم...) في حين أن TCP يتحكم بالاتصال بين مضيفين. الفكرة في أن البروتكولات تعتمد على بعضها، كل منها يقوم بالمهمة المتخصص بها. هذا الحديث يذكرنا بمكدس TCP/IP.

وبالتالي تمر البروتوكولات عبر العديد من الطبقات من عملية التشبيك.

التطبيق	مستوى التطبيق (FTP, SMTP, SNMP)
النقل	تتحكم بالأجهزة المضيفة (TCP, UDP)
الإنترنت	التوجيه (IP, ICMP, IGMP, ARP)
عنوان الشبكة	بطاقات الشبكة، كإيثرنت و Token Ring.



عرض موجز للبروتوكولات

IP	بروتوكول إنترنت IP هو الناقل/نقل لبيانات TCP, UDP و ICMP. يقدم IP خدمة عديمة الاتصال غير موثوقة. تاركة قضايا سلامة البيانات لواحدة من بروتوكولات الطبقة الأعلى كـ TCP أو بعض التجهيزات الخاصة بتطبيقات معينة. ولا شي يضمن وصول مخطط البيانات إلى المضيف عند استخدام IP بمفرده. يتحكم روتوكول IP بالعنونة والتوجيه بين الشبكات، إذ إن IP هو في الحقيقية خدمة لتسليم مخططات البيانات.
TCP	يقدم TCP خدمة اتصالية المنحى موثوقة إلى التطبيقات التي يستخدمها. وهو ذو منحى اتصالي. ويتفقد في كل مضيف الترتيب الذي يتم إرسال/استقبال الرزم من خلاله. ويتحقق من أن كافة الرزم قد تم نقلها. تستخدم التطبيقات أمثال telnet أو FTP بروتوكول TCP، وليست بحاجة لمعالجة قضايا تتعلق بفقدان البيانات..الخ.
UDP	يقدم بروتوكول مخطط بيانات المستخدم UDP وصولاً مباشراً لـ IP إلى البرمجيات التطبيقية، ولكن خلافاً لـ TCP فهي غير اتصالية ولا يمكن الاعتماد عليها. وهي تقدم حداً أدنى من التركيز على التطبيقات فيما يتعلق بالسرعة. إذا كان ثمة حاجة لشكل من حساب الرزم فينبغي الحصول عليها من التطبيق.
ICMP	يستخدم من قبل أجهزة التوجيه والأجهزة المضيفة لإعطائها تقريراً حول حالة الشبكة، وتستخدم مخططات بيانات IP، وهي عديمة الاتصال بذاتها.
PPP	يؤسس بروتوكول نقطة إلى نقطة اتصال TCP/IP عبر خطوط الهاتف. ويمكن استخدامه أيضاً ضمن الاتصالات المشفرة كـ PPTP.

خدمات TCP/IP والمنافذ

يمكن الحصول على لائحة بالخدمات المعروفة ومنافذها الخاصة بها عموماً من /etc/services. يتم إدارة اللائحة الرسمية الخاصة بالخدمات والمنافذ الخاصة بها من قبل منظمة IANA (سلطة تخصيص أرقام الإنترنت).

وبما أن حقل المنفذ هو رقم بعيار 16 بت، فثمة 65535 رقماً متاحاً. الأرقام من 1 إلى 1023 هي منافذ ذات امتياز ومحجوزة للخدمات المشغلة من قبل المستخدم الجذر root. معظم التطبيقات المعروفة سوف تستمع إلى واحد من هذه المنافذ

سوف نلقي نظرة على نتاج أمر فحص المنافذ portscans. احذر من أن مسح المنافذ غير المرخص عمل غير شرعي على الرغم من أن الكثيرين يستخدمونه.

فيما يلي نتاج لفحص المنافذ:

```
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
70/tcp open gopher
79/tcp open finger
```

يبين ذلك المنافذ المفتوحة، هذه المنافذ قيد الاستخدام من قبل تطبيق ما.

منافذ /etc/services الرئيسية:

```
ftp-data 20/tcp
ftp 21/tcp
telnet 23/tcp
smtp 25/tcp mail
domain 53/tcp
domain 53/udp
http 80/tcp # www is used by some broken
www 80/tcp # progs, http is more correct
kerberos 88/udp kdc # Kerberos authentication--udp
kerberos 88/tcp kdc # Kerberos authentication--tcp
```

```
pop-2 109/tcp # PostOffice V.2
pop-3 110/tcp # PostOffice V.3
sunrpc 111/tcp
sftp 115/tcp
uucp-path 117/tcp
nntp 119/tcp usenet # Network News Transfer
ntp 123/tcp # Network Time Protocol
netbios-ns 137/tcp nbns
netbios-ns 137/udp nbns
netbios-dgm 138/tcp nbdgm
```

تمارين

تسجيل خدمة باستخدام xinetd

1. اكتب نصاً دفعياً يعطي "Welcome" إلى الخرج النظامي واحفظه في /sr/sbin/hi.
2. في etc/xinetd.d/ أنشئ ملفاً جديداً يدعى fudge يتضمن ما يلي:

```
service fudge
{
socket_type = stream
erver =/usr/sbin/hi
er = root
t = no
ble = no
```

ض

3. خدمة تدعى fudge في etc/services/ والتي سوف تستخدم المنفذ 60000.
4. تشغيل xinetd و telnet على إلى المنفذ 60000.
5. قمت بربط نطاق من عناوين IP على الشبكة 27/10.83.10.11 .

د الشبكات التي لديها نفس الثمانيات الأربع الأولى كما هي الحال بالنسبة لك؟

د المضيفات على شبكتك؟

عنوان البث لهذه الشبكة الأولى؟

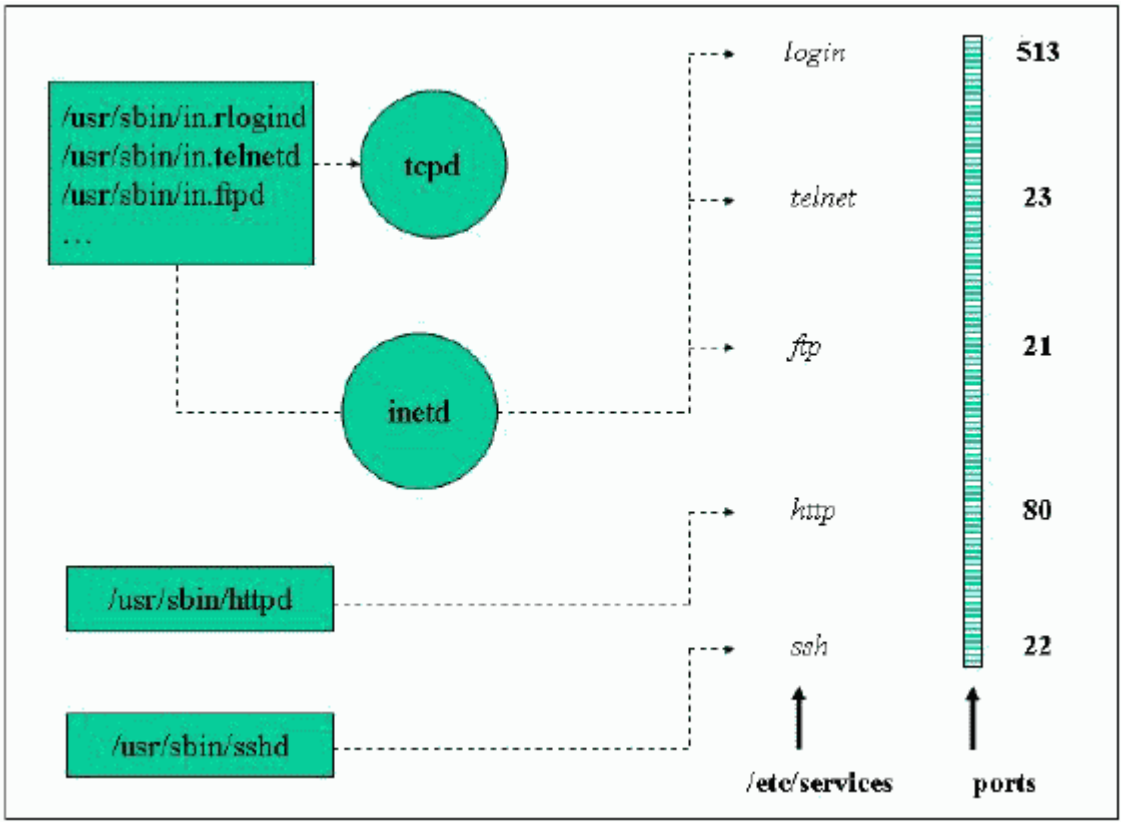
الفصل السادس
خدمات الشبكة Network Services

خدمات الشبكة يمكن تشغيلها كتطبيقات مستقلة بشكل مستمر، حيث تنصت إلى الاتصالات الواردة وتجيب طلبات العملاء مباشرة، أو يمكن استدعاؤها بواسطة عفريت الشبكة (network daemon)، سواء القديم inetd أو الحديث xinetd.

1ـ العفريت القديم inetd ـ The inetd daemon (old)

يتم تشغيل هذا العفريت مع إقلاع الجهاز، ويقوم بالإنصات للاتصالات على منافذ معينة. هذا يتيح للسيرفر تشغيل عفريت شبكة مخصص وقت الحاجة إليه فقط.

كمثال، خدمة **telnet** تملك عفريتاً في /usr/sbin/in.telnetd وهو المسؤول عن جلسات telnet. عوضاً عن تشغيل هذا العفريت طول الوقت، يقوم **inetd** بالإنصات إلى المنفذ 23. هذه التعليمات موضوعة في الملف /etc/inetd.conf .



الحقول في الملف /etc/inetd.conf تحتوي التالي:

service_name	اسم مقبول مأخوذ من /etc/services
socket type	stream إن كان من نوع TCP، و dgram إن كان من نوع UDP
protocol	بروتوكول مقبول مأخوذ من /etc/protocols
flag	nowait إن كان متعدد المهام أو wait إن كان ذا مهمة واحدة
user/group	تشغيل التطبيق لمستخدم أو مجموعة

program	tcpd عادة
argument	اسم البرنامج الذي سيتم تشغيله لهذه الخدمة

مثال:

```
pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
```

ملاحظة: الملف /etc/services يُستخدم للربط بين أسماء الخدمات وأرقام المنافذ الخاصة بها. الحقول في هذا الملف هي التالية:

service_name	port/protocol	[aliases]

2ـ عفريت xinetd ـ The xinetd Daemon

إنه النسخة الأحدث من **inetd**. عفريت **tcpd** لم يعد مستخدماً، بالمقابل **xinetd** يقوم بكل شيء بنفسه. الإعدادات عن طريق الملف الوحيد /etc/xinetd.conf أو عن طريق تعديل الملفات الشخصية في /etc/xinetd.d/ والمتعلقة بالخدمات المراقبة من قبل **xinetd**. من الممكن الانتقال من ملف إعداد **inetd** القديم إلى ملفات إعداد **xinetd** الحديث. لا حاجة لفعل أي شيء آخر.

تركيبة ملف الخدمات في xinetd.d

[Service_name	**اسم الخدمة]**
socket_type	stream ـ TCP و dgram ـ UDP
protocol	بروتوكول مقبول من /etc/protocols
wait	< نعم أو لا >
user	المستخدم الذي يُشغل البرنامج باسمه
group	المجموعة التي يُشغل البرنامج باسمها
server	اسم البرنامج الذي يتم تشغيله لهذه الخدمة
]	**[**

3ـ تغليفات TCP ـ TCP wrappings

إن كانت البرامج مصرفة باستخدام libwrap ، فقد يتم سردهم في الملفين /etc/hosts.allow و /etc/hosts.deny . المكتبة **libwrap** ستتفحص هذين الملفين لإيجاد المضيفات المتطابقة.

الهيئة الافتراضية للملف /etc/hosts.[allow,deny] هي:

```
DAEMON : hosts [ EXCEPT hosts ] [: spawn command ]
```

يمكن استخدام هذه الملفات أيضاً لتسجيل الخدمات غير المشروعة. هذا سيساعد كنظام إنذار مسبق. هاكم بضع أمثلة:

تحصيل معلومات عن مضيف

- **/etc/hosts.allow**

```
in.telnetd: LOCAL, .my.domain
```

/etc/hosts.deny

```
in.telnetd: ALL : spawn (/usr/sbin/safe_finger -l @%h | mail root) &
```

إعادة التوجيه إلى خدمة زائفة أو وعاء عسل (honey pot)

* **/etc/hosts.allow**

```
in.telnetd: ALL : twist /dtk/Telnetd.pl
```

المثال الأخير مأخوذ من ال dtk (طقم أدوات الخداع = Deception Tool Kit). يمكن تحميلها من الرابط التالي:
http://all.net/dtk/download.html

4ـ تنصيب Setting Up NFS _ NFS

أـ إعدادات العميل

على العميل الذي يستخدم لينوكس، ربط (mount) أنظمة الملفات البعيدة (remote file systems).

1. نظام الملفات **NFS** يجب أن يكون مدعوماً من النواة.

2. عفريت **portmapper** يجب أن يكون يعمل.

يتم تشغيل portmapper عن طريق السكريبت /etc/rc.d/init.d/portmap . الأمر **mount** سوف يربط نظام الملفات. الإدخال النموذجي في الملف **/etc/fstab** ينبغي أن يكون:

```
nfs-server:/shared/dir /mnt/nfs nfs defaults 0 0
```

بـ إعدادات الخادم (السيرفر)

خادم **NFS** يحتاج إلى تشغيل **portmapper** قبل أن يبدأ بالعمل. يمكن أن يتم بدء أو إيقاف خادم NFS بواسطة السكريبت /etc/rc.d/init.d/nfs .
ملف الإعدادات الرئيسي هو: /etc/exports .

مثال عن الملف /etc/exports :

```
/usr/local/docs *.local.org(rw, no_root_squash) *(ro)
```

هنا: المجلد /usr/local/docs يُصدر من قبل جميع المضيفات بصيغة القراءة فقط، وبصيغة القراءة والكتابة بالنسبة للمضيفات الواقعة ضمن *.local.org

الخيار الافتراضي root_squash ، والذي يجنب المستخدم الجذر (uid=0) على جهاز العميل من الوصول إلى التشاركات على الخادم، يمكن تغييره إلى الخيار no_root_squash.

> الملف /etc/exports يطابق المضيفات كـ *.machine.com ، بينما الملف /etc/hosts.allow/deny يطابقها كـ machine.com.

في حال التعديل على الملف /etc/exports ، يجب تشغيل الأمر **exportfs** . إن تم تعديل مجلدات موجودة في /etc/exportfs، فمن الضروري إلغاء

ربط (unmount) جميع تشاركات nfs قبل إعادة ربطهم. المجلدات الشخصية يمكن ربطها أو إلغاء ربطها بواسطة **exportfs**.

- **تصدير وإلغاء تصدير جميع المجلدات في /etc/exports**

```
exportfs -a ; exportfs -ua
```

5_ SMB و NMB

أجهزة لينوكس يمكنها الوصول إلى ومعالجة موارد ويندوز المتشاركة (المجلدات والطابعات). البروتوكول المستخدم لهذا يُدعى MS Windows Server Message Block SMB (قالب رسائل الخادم لمايكروسوفت ويندوز). سامبا (Samba) هو أكثر أدوات لينوكس شيوعاً لمعالجة برامج الخادم والعميل.

من خلال سطر الأوامر

يُستخدم الأمر **smbclient** لسرد موارد التشاركات. المجلدات البعيدة يمكن ربطها عن طريق الأمر **smbmount** أو باستخدام الأمر mount _t smbfs .

أمثلة:

- إرسال رسالة (في صندوق منبثق) إلى جهاز يُدعى win98desk

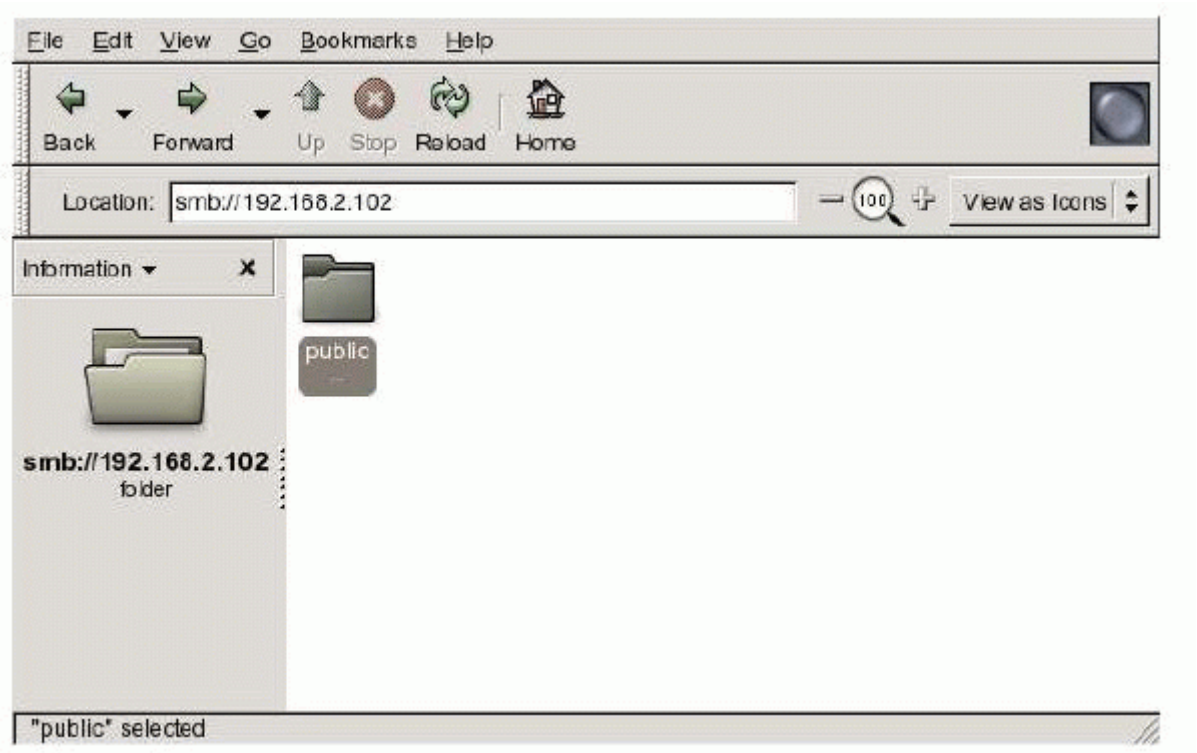
```
smbclient -M win98desk
```

- ربط مجلد تشاركات موجود في الجهاز winserv

```
smbmount //winserver/shared /mnt/winserver/shared
```

يمكن إعداد خادم السامبا من خلال الملف /etc/smb.conf . يمكن تشغيل وإيقاف الخادم (السيرفر) من خلال السكريبت **/etc/rc.d/init.d/smb** .
لاحظ أنه يتم تشغيل خدمات **NMB** عند تشغيل **smb**. إنه قالب رسائل NetBios والذي يسمح بتحديد الأسماء في محيط ويندوز.

صورة: استعراض تشاركات SMB في مدير مكتب Nautilus



الإدخالات الرئيسية في /etc/smb.conf :

```
[global]
        workgroup = LINUXIT
        os level = 2
        kernel oplocks = No
        security = user
        encrypt passwords = Yes
        guest account = nobody
        map to guest = Bad User
[homes]
        comment = Home Directories
        read only = No
        create mask = 0640
        directory mask = 0750
        browseable = No
[printers]
        comment = All Printers
        path = /var/tmp
        create mask = 0600
        printable = Yes
        browseable = No
```

إعدادات الواجهة الرسومية لـ SWAT و Webmin

إن قمت بتنصيب حزمة ال **SWAT**، فيمكنك إدارة خادم السامبا من خلال واجهة رسومية مرتكزة على الويب عبر المنفذ 901. أداة إدارة شعبية أخرة هي **webmin**. يمكنك تحميلها من www.webmin.com .

ملاحظة

ملف الإعدادات /etc/samba/sm.conf هو مصدر جيد لوثائق المساعدة. كل الخيارات مشروحة فيه ويمكن تفعيلها مباشرة عن طريق حذف الفاصلة المنقوطة ';' من أول السطر. راجع أيضاً صفحة ال man الخاصة بـ **smb.conf(5)**

6_ خدمات DNS _ DNS Services

* المحللات (The Resolvers)

عندما يريد برنامج ما تحليل اسم مضيف (hostname)، يحتاج إلى عملية تسمى التحليل (resolving). يقوم المحلل (resolver) أولاً بمراجعة الملف /etc/nsswitch (سابقاً /etc/host.conf)، ومن ثم يحدد الطريقة التي سيتم بها تحليل أسماء المضيفات (ملفات محلية، أو خادم أسماء، أو NIS، أو خادم ldap).

ملف /etc/host.conf (أو /etc/nsswitch)

هذه الملفات تُقرأ من قبل المحلل (resolver). مهمتها تحديد إن كانت الملفات، أو خادمات DNS، أو قواعد بيانات ldap أو خادمات NIS هي التي يجب أن تُراجع.

مثال (/etc/nsswitch):

```
hosts: files dns nis
networks: files
```

السطر الأول يشير إلى أن الملفات هي التي يجب أن تُستعلم أولاً (هنا /etc/hosts)، أو خادم DNS إن فشل هذا الاستعلام. السطر الثاني يأمر باستخدام الملف /etc/network لمعلومات الشبكة.

ملف /etc/hosts

مع عدد قليل من الأجهزة في الشبكة، يمكن تحويل أرقام الآي بي العشرية إلى أسماء باستخدام الملف /etc/hosts . حقول الملف كالآتي:

```
IP machine machine.domain alias
```

مثال عن ملف /etc/hosts :

```
192.168.1.233 io       io.my.domain
61.20.187.42  callisto callisto.physics.edu
```

ملف /etc/resolv.conf

إن احتاج المحلل إلى خادم أسماء ميادين (Domain Name Server = DNS)، سيستعلم الملف /etc/resolv.conf للحصول على لائحة بأسماء الخوادم المتاحة للاستعلام.

* البنية الطبقية (Hierarchical structure)

خادمات الأسماء تملك بنية طبقية. وفقاً لموقعه في اسم الميدان الموصوف بشكل كامل (FQDN)، يسمى الميدان بالطبقة العليا، أو الطبقة الثانية، أو الطبقة الثالثة.

أمثلة عن ميادين الطبقة العليا:

com	الشركات التجارية
edu	المؤسسات التعليمية
gov	المؤسسات الحكومية

mil	المؤسسات العسكرية
net	البوابات ومزودات الشبكة
gov	المواقع اللا ربحية
uk	المواقع البريطانية

* أنواع خوادم DNS

الميادين يمكن تقسيمها إلى ميادين فرعية. هذا يقلل حجم المعلومات اللازمة لإدارة ميدان. المناطق (Zones) تملك خادم أسماء الميادين **سيداً** (**master** domain name server)، كان يُدعى سابقاً DNS الأولي؛ بالإضافة إلى واحد أو أكثر من خوادم أسماء الميادين **العبيد** (كان يُدعى سابقاً DNS الثانوي).
إدارة خادم الأسماء تتطلب تحديثاًدائماً للمعلومات حول منطقة معينة. الخوادم الأسياد تُعتبر ذوات سلطة.

* ملفات إعداد DNS

في نسخ BIND القديمة (ما قبل النسخة 8)، ملف الإعداد كان /etc/named.boot . ابتداء من النسخة 8، أصبح ملف الإعداد هو /etc/named.conf . يمكن استخدام البرنامج named_bootconf.pl لتحويل ملفات الإعدادات القديمة.

الملف /etc/named.boot :

```
directory                /var/named
cache     .              named.ca
primary   myco.org               named.myco
primary   0.0.127.in-addr.arp    named.local
primary   1.168.192.in-addr.arp named.rev
```

السطر الأول يعرف المجلد الأساس الذي سيُستخدم. الملف named.ca يحتوي على لائحة أرقام آي بي DNS للاستعلامات عن العناوين الخارجية.
السطر الثالث اخياري ويحتوي سجلات للشبكة LAN المحلية. السطران التاليان خاصان بالبحث العكسي (reverse lookup).

في الملف /etc/named.conf : أ

cache	تُستبدل بـ *hint*
primary	تُستبدل بـ *master*
secondary	تُستبدال بـ *slave*

بتطبيق هذه التغييرات على ملفات إعدادات BIND4 سيتم توليد ملفات إعدادات BIND8 و BIND9 كالتالي:

الملف /etc/named.conf :

```
options       {
              directory "/var/named";
};
zone    "."     {
              type hint;
              file "named.ca";
};
zone "myco.org"         {
              type master;
              file "named.myco";
};
zone "1.168.192.in-addr.arp" {
              type master;
              file "named.rev";
};
zone "0.0.127.in-addr.arpa" {
              type master;
              file "named.local";
```

```
};
```

*** ملفات مناطق DNS**

في هذا المثال، تم إعداد السيرفر كسيرفر تخزين فقط (caching_only server). جميع ملفات المناطق تحتوي سجلات الموارد.

نموذج عن ملف المناطق named.local :

```
@  IN  SOA    localhost. root.localhost. (
                  2001022700 ; Serial
                  28800      ; Refresh
                  14400      ; Retry
                  3600000 ; Expire
                  86400 ) ; Minimum
  IN  NS   localhost.
1 IN  PTR   localhost.
```

إنه ملف مناطق بسيط جداً ولكنه يعطينا المعلومات الكافية لفهم أساسيات عمل خادم الأسماء (name server).

الرمز @ سيتم تحويله إلى المنطقة المتعلقة والمعرفة في /etc/named.conf . هذا سيسمح لأي ملف مناطق بأن يُستخدم كأنموذج للمناطق الأبعد (انظر التمارين).

جدول 1: أنواع السجلات الشائعة

لتحديد خادم الأسماء الأولي للمناطق	NS
التحويل العكسي لأرقام الآي بي إلى أسماء مضيفات	PTR
سجل التبادل البريدي	MX
ربط رقم آي بي باسم مضيف	A
ربط اسم مستعار باسم المضيف الرئيسي	CNAME

جدول 2: معطيات المناطق

بدء التصريح (SOA). تتعرف على المنطقة متبوعة بالخيارات المحصورة بين معقوفتين	@ IN SOA
تزداد قيمته يدوياً عند حدوث تغيير في البيانات. الخادمات الثانوية تستعلم الرقم التسلسلي للخادم السيد. إن كان قد تغير، يتم تحميل ملف المنطقة بأكمله.	serial
الوقت (بالثواني) قبل استعلام سجل الخادم الثانوي لبدء التصريح (SOA) الخاص بالميدان الأولي. يجب أن يكون هذا الوقت يوماً على الأقل.	refresh
المدة الزمنية بالثواني قبل تبني عملية نقل منطقة جديدة في حال فشل التحميل السابق.	retry
الوقت الذي يهمل بعده الخادم الثانوي كل بيانات المنطقة إذا اتصل بالخادم الأولي. يجب أن يكون هذا الوقت أسبوعاً على الأقل.	expire
إنه وقت الحياة (ttl) للبيانات المحفوظة. القيمة الافتراضية هي يوم واحد (86400 ثانية)، ولكن ينبغي أن يكون أطول على شبكات LAN الثابتة.	minimum

7ـ الإعدادات الرئيسية لـ sendmail ـ Sendmail main Configuration

sendmail هو أكثر عملاء إرسال البريد شهرة على الإنترنت. إنه يستخدم بروتوكول نقل البريد البسيط (SMTP)، ويعمل كعفريت (daemon) منصت للاتصالات القادمة على المنفذ 25.

سكريبت sendmail الذي يبدأ أو يوقف عفريت sendmail موجود عادة في المجلد */etc/rc.d/init.d* .

ملف الإعدادات الرئيسي هو */etc/mail/sendmail.cf* (أو */etc/sendmail.cf*). يمكنك تحديد اسم الخادم وأسماء المضيفات التي يكون توجيه تخزين البريد منها وإليها مسموحاً.

الملف */etc/aliases* يحتوي على حقلين كالتالي:

```
alias: user
```

عندما يتم التعديل على هذا الملف، يجب تنفيذ الأمر *newaliases* لإعادة بناء قاعدة البيانات */etc/aliases.db* .
عندما
ندما يقبل الخادم البريد، يقوم بربطه مع ملف مفرد يحتوي اسم المستخدم. هذه الملفات تُخزن في */var/spool/mail/* . اعتماداً على عميل البريد لمستخدم، يمكن للمستخدم تخزين الرسائل في مجلد المنزل الخاص به أو تحميلهم على جهاز آخر.
إن
ن كان الخادم في حالة استرخاء، أو كانت الشبكة بطيئة وكان هناك عدد من الرسائل قد تم إرسالها. سيتم تخزين البريد في **صف البريد** لموجود في */var/spool/mqueue/* . يمكنك استعلام هذا الصف عن طريق الأمر *mailq* أو *sendmail -bq*. بالنسبة لمدير النظام، يمكنه إنعاش لصف عن طريق الأمر *sendmail -q*.
وأخيراً
أخيراً، بالنسبة لتسجيل اسم ميدان كعنوان بريدي مقبول، يجب إضافة حقل MX إلى قاعدة بيانات DNS.
كمثال،
مثال، إن كان mail.company.com هو خادم البريد، إذاً لقبول بريد مثل joe@company.com ينبغي وجود الإعداد التالي:
1
. إضافة company.com إلى الملف */etc/mail/local-host-names*
. إضافة company.com MX 10 mail.company.com إلى ملف مناطق DNS.

8- سيرفر الأباتشي The Apache Server

* ملفات الإعدادات

لملف */etc/httpd/conf/httpd.conf* يحتوي على جميع تفاصيل الإعدادات.
لإصدارات الأقدم من أباتشي كانت تملك ملفين إضافيين، أحدهما يُدعى access.conf حيث تُحدد المجلدات الممنوعة الوصول، والآخر يُدعى rm.conf وهو يحدد مجلد الجذر للخادم.
أهم بنـ
هم بنود الإعدادات:

```
ServerType    standalone/inetd
ServerRoot    "/etc/httpd"
DocumentRoot        "/var/www/html"
Directory "/var/www/cgi-bin">
     AllowOverride None
     Options ExecCGI
     Order allow,deny
     Allow from all
/Directory>
VirtualHost    122.234.32.12>
     DocumentRoot        "/www/docs/server1"
     ServerName virtual.mydomain.org
/VirtualHost>
```

* تشغيل الأباتشي

لبدء وإيقاف الخادم، يمكن استخدام السكريبت */etc/rc.d/init.d/httpd* . يُفضل على خادم مشغول استخدام *apachectl* خصوصاً مع الخيار graceful والذي سيعيد تشغيل الخادم فقط عند انتهاء التعامل مع الاتصالات الحالية.

ملفات السجلات الرئيسية (log) موجودة في */var/log/httpd* . سيكون مفيداً لأسباب أمنية تفقد الملفين error_log و access_log بشكل دوري.

9ـ تمارين

إعداد خادم DNS سيد

كتمرين، سنقوم بتنصيب حزمة ال rpm الخاصة بـ **BIND9** (bind9_9.1.3_252.i386.rpm) وإعداد ميدان يُدعى gogo.com .

1. أجر التغييرات التالية في الملف **/etc/named.conf** :

```
zone "localhost" in {
    type master;
    file "localhost.zone";
}
```

ستصبح

```
zone "gogo.com" in {
    type master;
    file "gogo.zone";
}
```

و

```
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};
```

ستصبح

```
zone "2.168.192.in-addr.arpa" in {
    type master;
    file "192.168.2.zone";
};
```

2. في الملف **/var/named** :

```
cp 127.0.0.zone 192.168.2.zone
cp local.zone gogo.zone
```

3. غير الحقول الملائمة في ملفات المنطقة الجديدة. أضف مضيفاً (host) يُدعى *harissa*.

4. أضف السطر "nameserver 127.0.0.1" إلى الملف **/etc/resolv.conf** .

5. استخدم الأمر **host** لتحليل *harissa.gogo.com* .

إدارة أباتشي (Apache)

الإعدادات الأساسية في الملف /etc/httpd/conf/httpd.conf
أ
1. غير المنفذ الموجه (directive port) من 80 إلى 8080.

2. تأكد أن الأباتشي يجيب على الأمر **telnet localhost 8080**. يجب أن تحصل على الناتج التالي:

```
Trying 127.0.0.1...
Connected to localhost.linuxit.org.
Escape character is '^]'.
```

ثم اكتب الأمر 'GET /' لتحميل الصفحة الرئيسية (index).
أ
3. اجعل قيمة **StartServer** هي 15. أعد تشغيل **httpd** وتأكد أن 15 تطبيقاً قد بدأ (بدلاً من العدد الافتراضي 8).

الخادم الفرضي المرتكز على الآي بي (IP based virtual server)

بطاقتك الإيثرنت يجب أن تكون مسماة إلى رقم آي بي جديد (فلنسمه *new_ip*).

```
ifconfig eth0:0 new-IP
```

أضف المقطع التالي إلى الملف **/etc/httpd/conf/httpd.conf** :

```
<VirtualHost new-IP>
ocumentRoot /var/www/html/virtual
erverName www1
/VirtualHost>
```

تنصيب مجلد SMB متشارك

في معظ

ي معظم الحالات لست مضطراً إلى إضافة مستخدمي SMB إلى النظام لفعل هذا. بكل بساطة، عدل الملف **smb.conf** وأضف التالي:

```
[public]
        comment = Example Shared Directory
        path = /home/samba
        guest ok = yes
        writeable = yes
```

تنصيب

نصيب طابعة متشاركة:

```
[global]
-- snip ---
printcap name = /etc/printcap
  load printers = yes
printers]
  comment = All Printers
  path = /var/spool/samba
  browseable = no
Set public = yes to allow user 'guest account' to print
  guest ok = yes
```

```
writable = no
printable = yes
```

الفصل السابع
البرمجة بلغة bash _ Bash Scripting

1_ محيط لغة bash _ The bash environment

المتغيرات

عندما تطبع أمراً على سطر الأوامر الخاص، يقوم ال bash باستخدام المتغير PATH لإيجاد البرنامج الذي تريد من النظام تطبيقه. يمكنك التحقق من قيمة هذا المتغير باستخدام الأمر:

```
> echo $PATH


/usr/bin:/bin:/usr/sbin:/usr/X11R6/bin:/usr/local/bin:/sbin/:/usr/local/sbin/
```

في الواقع، تحتاج القشرة (Shell) عدداً من المتغيرات للتكيف مع محيط كل مستخدم. PWD، HOME، DISPLAY و TERM هي بعض هذه المتغيرات.

لإنشاء وتعريف متغير، نستخدم التركيبة التالية:

```
VARIABLE=VALUE
```

من المهم جداً عدم وضع مسافات حول إشارة المساواة '='. بعد إنشاء المتغير وتعريفه، يمكننا استدعاؤه متى شئنا عن طريق إضافة إشارة الدولار '$' إلى أوله. كما في هذا المثال:

```
echo $VARIABLE
```

عندما تبدأ جلسة القشرة (Shell Session)، يتم قراءة عدد من ملفات الإعدادات ويتم تحديد قيم معظم المتغيرات.

لتحرير متغير من قيمته الحالية، استخدم الأمر unset.

ملفات الإعدادات

ينبغي أولاً التفريق بين ملفات الإعدادات التي يتم قراءتها عند تسجيل الدخول، ولبن تلك التي يتم قراءتها مع كل بدء لجلسة قشرة جديدة.

ملفات إعدادات تسجيل الدخول

الملفات التي تُقرأ عند تسجيل الدخول هي /etc/profile و ~/.bash_profile (سيبحث ال bash أيضاً عن ملفات بديلة، ~/.profile مثلاً).
أما قشرة ال bash، فهي تقرأ مع كل جلسة جديدة الملف ~/.bashrc والملف /etc/bashrc (إن وُجد).

ملفات الـ bashrc

تتم قراءة هذه الملفات في كل مرة يتم فيها تشغيل جلسة قشرة (كـ xterm مثلاً). هذه الملفات هي ~/.bashrc و /etc/bashrc .

الأسماء المستعارة (Aliases) والدوال يمكن أن تكون محفوظة في الملف ~/.bashrc

تركيبة الدالة:

```
function-name ()
{
 command1;
 command2;
}
```

يمكنك معرفة ما هي الملفات التي تتم قراءتها عن طريق إضافة السطر echo Profile إلى الملف /etc/profile . النوع:
bash لن تتم قراءة ملف ال profile، ولن يمكنك رؤية شيء.
bash _login سيجبر ذلك ال bash على البدء كقشرة تسجيل دخول، سوف ترى الكلمة Profile تظهر على الشاشة.

وهناك خيارات أخرى لبدء ال bash بطريقة معينة:
bash _norc لبدء ال bash من دون الملف bashrc
bash _noprofile لبدء ال bash من دون الملف profile

تجدر الإشارة إلى أن أي جلسة قشرة جديدة سترث المتغيرات العمومية من منشئها، والموجودة في الملفات /~/.bash_profile و /etc/profile .

2_ أساسيات البرمجة Scripting Essentials

ملف النص البرمجي (السكريبت)

سكريبت القشرة هو قائمة من الأوامر محفوظة في ملف نصي. هناك أمران ضروريان يجب تنفيذهما:

1. أول سطر في ملف السكريبت ينبغي أن يكون: #!/bin/bash (في حال كان bash هو نوع السكريبت).
2. يجب أن تكون صلاحيات القراءة والتنفيذ معطاة للملف (755 كمثال للصلاحيات).

إن لم يكن هذان الشرطان منفذين، يمكن تشغيل السكريبت عن طريق الأمر:

```
bash program-name
```

تمرير المتغيرات إلى السكريبت

المتغيرات المدخلة عن طريق سطر الأوامر، يتم استدعاؤها من الداخل باسم $1 للمتغير الأول و $2 للثاني وهكذا.

مثال عن سكريبت يُدعى mycat:

```
#!/bin/bash
cat $1
```

هذا السكريبت ينتظر مدخلاً واحداً، والذي سيكون ملفاً، سيتم حينها عرض الملف باستخدام الأمر cat. لتنفيذ هذا السكريبت على الملف /etc/lilo.conf (كمثال)، نكتب الأمر التالي:

```
./mycat /etc/lilo.conf
```

هناك طريقة أخرى لتمرير المتغيرات إلى السكريبت، وهي بجعل السكريبت يطلبها من المستخدم بشكل تفاعلي. يُطبق هذا باستخدام الدالة read. الاسم الافتراضي لمتغير هذه الدالة هو REPLY. إليكم السكريبت بعد تعديله:

```
#!/bin/bash
echo "Wich file shall I display ?"
```

```
read
cat $REPLY
```

أو

```
read -p "File to display: " FILENAME
cat $FILENAME
```

متغيرات خاصة

المتغيرات الخاصة معينة آلياً من ال bash، ولا يمكن استدعاؤها إلا منه. إليكم أكثر المتغيرات الخاصة شيوعاً التي قد تواجهونها.

سرد جميع المتغيرات المدخلة عن طريق سطر الأوامر	$*
عدد المعطيات (arguments) المدخلة في سطر الأوامر	$#
اسم السكريبت	$0
رقم ال PID لأحدث أمر نُفذ في الخلفية	$!
رقم ال PID للقشرة الحالية	$$
قيمة مخرج آخر أمر	$?

بالنسبة للمعطيات الموضعية (positional parameters)، مثل $1، $2، ... ، هناك معامل إزاحة shift يعيد تسمية كل معطى باسم المعطى الذي يسبقه.
$2 يصبح $1، $3 يصبح $2، هكذا.
يمكن تلخيص ذلك بـ: س$ --> (س-1)$

3- المعادلات المنطقية Logical Evaluations

الجمل المنطقية يتم تقييمها باستخدام الأمر test أو المعقوفات []. في كلا الحالتين، سيُخزن الناتج في المتغير $? بحيث:
إن كانت الجملة صحيحة منطقياً: $؟ يساوي 0
وإن لم تكن صحيحة: $؟ لا يساوي 0

وهذه بعض الأمثلة للتوضيح:

باستخدام test	باستخدام []	المعنى
test -f /bin/bash	[-f /bin/bash]	فحص إن كان /bin/bash ملفاً
test -x /etc/passwd	[-x /etc/passwd]	فحص إن كان /etc/passwd تنفيذياً

يمكن تقييم أكثر من جملة منطقية في آن واحد باستخدام المعاملات المنطقية: و (&&)، أو (||) في سطر الأوامر. كمثال: سنفحص إن كان الملف /bin/bash تنفيذياً وإن كان الملف /etc/inittab موجوداً في نفس الوقت:

```
test -x /bin/bash && test -e /etc/inittab
[ -e /bin/kbash ] || [ -f /etc/passwd]
```

يمكن الاستعاضة عن المعاملين المنطقيين "و" و "أو"، بالخيارين "a-" و "o-". كمثال مرادف للمثال الأخير:

```
test -x /bin/bash -a -e /etc/inittab
[ -e /bin/kbash -o -f /etc/passwd ]
```

4_ الحلقات Loops

- *if then loop*

التركيب:

```
if     CONDITION ;
then
```

```
   command1
```

```
   command2
```

```
fi
```

مثال:

```
#!/bin/bash
if [ -x /bin/bash ] ; then
echo "The file /bin/bash is executable"
fi
```

- *if then else*

التركيب:

```
if     CONDITION ;
then
```

```
   command1
```

```
   command2
```

```
else
```

```
   command3
```

```
fi
```

- *while loop*

التركيب:

```
while CONDITION is true;
do
```

```
command
```

```
done
```

مثال: جعل السكريبت يكتب 10 رموز # على سطر واحد.

```
#!/bin/bash
COUNTER=0
while [ COUNTER -lt 10 ]; do
echo -n "#"
leep 1
t COUNTER=COUNTER+1
e
```

- ***until loop***

ركيب:

```
til CONDITION is false;
```

```

```

```
mand
```

```
ne
```

ثال

ل: كما في المثال السابق، لاحظوا طريقة زيادة أو إنقاص العداد المأخوذة من لغة C

```
/bin/bash
NTER=20
il [ COUNTER -lt 10 ]; do
o -n "#"
p 1
OUNTER-=1
```

- ***f***
or loop

ب:

```
for VARIABLE in SET; do
```

```
command
```

```
done
```

كمثال، SET يمكنها أن تكون أسطر ملف محدد:

```
#!/bin/bash
for line in `cat /etc/lilo.conf`; do
IMAGE=$(echo $line | grep image)
if [ "$IMAGE" != "" ]; then
echo Kernel configured to boot: $line
fi
done
```

5ـ توقع إدخال المستخدم Expecting user input

سنفترض أن السكريبت ينتظر إدخالات المستخدم. اعتماداً على الإجابة، ستُنفذ أوامر البرنامج على وجه محدد. هناك طريقتان لفعل ذلك، وهما select و case.

- ***استخدام case***

التركيب:

```
case $VARIABLE in
CHOICE command ;;
HOICE command ;;
ac
```

- ***استخدام select***

تركيب:

```
elect VARIABLE in SET; do
      if [ $VARIABLE = CHOICE ]; then
              command
      fi
      if [ $VARIABLE = CHOICE ]; then
              command
      fi
ne
```

6ـ العمل مع الأرقام Working with numbers

بينما تتعامل سكريبتات القشرة مع المحرفات النصية بسلاسة، يتطلب التعامل مع المعادلات الحسابية الأساسية جهداً أقل.

* المعادلات الثنائية Binary operations

المعادلات الحسابية يمكن إجراؤها عن طريق الأمر expr أو عن طريق وضعها في $(( )) .

مثال:

```
expr 7 + 3; expr 2 \* 10; expr 40 / 4; expr 30 - 11
$((7+3)); $((2*10)); $((40/4)); $((30-11))
```

* مقارنة القيم Comparing values

الأرقام	النصوص
ـlt	<
ـgt	>
ـle	<=
ـge	>=
ـeq	=
ـne	!=

7ـ تمارين

1. على سطر الأوامر، عرف المتغير TEST

```
export TEST=old
```

2. اكتب السكريبت التالي:

```
#!/bin/bash
echo old variable: $TEST
export $TEST=new
echo exported variable: $TEST
```

3. ما هي قيمة المتغير $TEST لحظة تشغيل السكريبت ؟

4. السكريبت التالي المدعو test_shell سيطبع رقم ال PID للقشرة التي تنفذه.

```
#!/bin/bash
if [ -n $(echo $0 |grep test) ]; then
echo The PID of the interpreter is: $$
else
echo The PID of the interpreter is: $$
fi
```

5. غير تصريحات الملف test_shell إلى 755 ثم جرب الأوامر التالية:

```
test_shell
./test_shell
bash test_shell
. test_shell
source test_shell
exec ./test_shell
```

الفصل الثامن
أساسيات الأمن

1ـ الأمن المحلي

نظام الدخل/الخرج الأساسي BIOS

إذا تمكن شخص ما من الدخول إلى أقراص الإنقاذ Rescue Disks أو أي نظام لينكس قابل للإقلاع من قرص مرن أو مدمج، فسيتمكن بسهولة بالغة من قراءة ملفات النظام. للحيلولة دون ذلك ينبغي أن يكون نظام الدخل/الخرج الأساسي BIOS معداً للإقلاع من القرص الصلب فقط. مع تعيين كلمة مرور لنظام الدخل/الخرج الأساسي BIOS.

برنامج LILO

يمكن تزويد برنامج LILO بخيارات معينة عند الإقلاع. يجدر بالذكر أن بعض توزيعات لينكس لن تطالبك بكلمة مرور عندما تشغل النظام بنمط (مستخدم وحيد) أو runlevel1.

ثمة خيارين يجب إضافتهما إلى /etc/lilo.conf :

- خيار restricted (مقيد) لمطالبة المستخدم بكلمة مرور.
- خيار password="" لتعيين نص كلمة المرور.

خيار restricted (مقيد) يعني أنه لا يمكن تزويد LILO بأي وسائط ما لم يتم تعيين كلمة مرور في lilo.conf.

```
boot=/dev/hda
install=/boot/boot.b
prompt
timeout=50
password="password"
restricted
```

سماحيات الملفات

لمنع المهاجمين من التسبب بأضرار جسيمة، يستحسن اتباع الخطوات التالية:

1. قم بتثبيت/تجميد/تعطيل أدوات النظام الخطرة أو ؟؟؟

```
chattr +i /bin/login
chattr +i /bin/ps
chattr +a /var/log/messages
```

2. عين سمة nosuid و noexec للدليلين home/ و tmp/:

```
Lines to be changed in /etc/fstab
/tmp /tmp ext2 nosuid 1 2
/home /home ext2 noexec 1 2
```

3. ابحث عن جميع ملفات النظام التي لا تعود لأي مستخدم أو مجموعة:

```
find / -nouser -o -nogroup
```

```
find / -perm +4000
```

ملفات الأحداث Log

ملفات الأحداث الرئيسية هي:

/var/log/messages	: يحتوي معلومات مدونة بواسطة البرنامج الخدمي syslogd.
/var/log/secure	: يحتوي معلومات حول محاولات الدخول الفاشلة، المستخدمين المضافين/الجدد... الخ.

تولد أداة last لائحة بكافة عمليات الدخول الناجحة وعمليات الإقلاع. تتم قراءة المعلومات من الملف /var/log/wtmp.

تولد أداتي who و w لائحة بكافة المستخدمين الداخلين حالياً في النظام باستخدام ملف /var/run/utmp.

قيود المستخدم

عندما يعطي ملف /etc/nologin رسالة (can be empty)، فهذا سيمنع كافة المستخدمين من الدخول إلى النظام (باستثناء المستخدم الجذر root). إذا تضمن nologins رسالة، فستظهر بعد عملية مصادقة authentication ناجحة.

توجد في الدليل /etc/security/ مجموعة من الملفات تسمح للمدراء بتقييد زمن معالج المستخدم limit user CPU time، الحد الأقصى لحجم الملف، العدد الأقصى للاتصالات... الخ.

/etc/security/access.conf : يمنع دخول المستخدمين والمجموعات لمسارات محددة.

/etc/security/limits.conf

تنسيق هذا الملف هو على النحو التالي:

```
<domain> <type> <item> <value>
```

حيث:

domain		اسم مستخدم، اسم مجموعة (مع @group)
type		hard أو soft
item	core	تحديد حجم الملف (بالكيلوبايت)
	data	الحد الأقصى لحجم البيانات (بالكيلوبايت)
	fsize	الحد الأقصى لحجم الملف (بالكيلوبايت)
	memlock	الحد الأقصى لمساحة العنوان المحجوزة في الذاكرة (بالكيلوبايت)
	nofile	الحد الأقصى لعدد الملفات المفتوحة
	cpu	الحد الأقصى لزمن المعالج (بالدقائق)
	proc	الحد الأقصى لعدد العمليات
	as	حد مساحة العنوان
	maxlogins	العدد الأقصى لعمليات الدخول المتزامنة لهذا المستخدم
	priority	الأولوية التي سيتم تشغيل المستخدم بها.
	locks	max number of file locks the user can hold

2ـ أمن الشبكات

يمكن تقسيم أمن الشبكات إلى فئتين:

أمن المضيف Host Based Security

يمكن منح حق الوصول إلى الموارد اعتماداً على المضيف الذي يطلب الخدمة. يتم التحكم بذلك باستخدام tcp_warppers. تعرّف مكتبة libwarp أيضاً كـ tcp_warppers تقدم لوائح تحكم بالدخول للخدمات المختلفة للشبكة.

الكثير من الخدمات كـ xinetd، sshd، و portmap، مترجمة مقابل مكتبة libwrap من خلال تمكين دعم tcp_warpper لتلك الخدمات.

عندما يتصل زبون بخدمة ما من خلابل دعم tcp_warpper، يتم إعراب ملفي /etc/hosts.deny و /etc/hosts.allow لتحدي/لاعتراض المضيف الذي يطلب الخدمة. وبالمحصلة سيتم إما منح أو حجب الخدمة.

تمتلك ملفات hosts_access ثلاثة حقول (أعمدة) منفصلة، ثالثها اختياري. الحقل الأول هو اسم العملية، والحقل الثاني هو اسم المضيف أو النطاق كامل الصلاحية مع "نقطة في البداية"، عنوان IP أو الشبكة الفرعية مع "نقطة في النهاية". نائبات المحارف WildCards كـ All و EXPECT مسموحة أيضاً.

الصيغة البرمجية لملف /etc/hosts.{allow | deny} هو على النحو التالي:

```
service : hosts [EXCEPT] hosts
```

مثال:

```
/etc/hosts.deny
ALL: ALL EXCEPT .example.com

/etc/hosts.allow
ALL: LOCAL 192.168.0.
in.ftpd: ALL
sshd: .example.com
```

يمكن أن يقوم Tcp_wrappers بتشغيل أمر محلياً upon a host match في ملفات host_access.

يتم ذلك باستخدام أمر spawn. باستخدام الحرف % يمكن إنشاء نائب/بديل لاسم المضيف والخدمة.

مثال:

```
/etc/hosts.deny

ALL: ALL : spawn (/bin/echo `date` from %c for %d >> /var/log/tcpwrap.log)
```

للمزيد من المعلومات حول استخدام نائبات/بدائل % انظر كتيب التعليمات man page لـ (5) host_access.

أمن المنافذ Port Based Security

يمكن باستخدام تصفية الحزم المبيتة وظيفياً تقييد الوصول إلى الموارد بإنشاء مجموعة قواعد بواسطة أداة مثل ipchains و iptables، القادرة على تقييم رزمة واردة إلى اي بطاقة شبكة خاصة بها، ومعرفة ما الذي حل بتلك الحزمة.

توجد ثلاثة Chains مبيتة في ipchains و iptables، وهي:

input, forward و output لـ ipchains.
INPUT, FORWARD، و OUTPUT لـ iptables.

على سبيل المثال، عند استخدام ipchains، فإن كافة الرزم الواردة إلى واجهة الشبكة سوف تجتاز output chain.

كافة الرزم غير الموجهة من أجل هذا المضيف سوف تتخطى السلسة الأمامية

كافة الرزم المولدة من داخل المضيف و packets being forwarded سوف تتخطى سلسة الخرج.

كافة قواعد ipchains و iptables يمكنها تحديد المصدر s والوجهة d والبروتوكول p والمنفذ.

مثال:

كافة الحزم القادمة من العنوان 192.168.0.254 سيتم رفضها:

```
ipchains -A input -s 192.168.0.254 -j DENY
```

يمكن معالجة قواعد Ipchains و iptables بالخيارات التالية:

-A	تضمين
-D	حذف
-P	تغيير السياسة الافتراضية لـ chain
-L	إدراج
-F	تدفق القاعدة/القواعد في chain
-N	إنشاء chain معرف من قبل المستخدم
-X	حذف chain معرف من قبل المستخدم
-L	لائحة

مثال:

يمكن تغيير السياسة الافتراضية لـ iptable من القبول إلى الرفض كما يلي:

```
iptables -P INPUT REJECT
iptables -P FORWARD REJECT
iptables -P OUTPUT REJECT
```

مع تطور نواة لينكس 2.4 جاء مشروع تطوير Netfilter، والذي يستخدم أداة iptables لإدارة قواعد جدار حماية Firewall. الفرق الرئيسي بين iptables و ipchains هو أن iptables يدعم تقييم الحزم اعتماداً على حالتها في عبارات الحزم الأخرى التي مُررت إلى النواة. هذا هو تقييم stateful packet الذي يجعل من iptables الأفضل إلى حد بعيد.

المثال أدناه يبين كيفية استخدام جدار حماية stateful، وهو شكلياً، عبارة عن نص برمجي لمجموعة أوامر Shell Script تكتب لتحقيق الهدف النهائي.

مثال

نص برمجي أساسي يعمل بـ صورة جيدة للمستخدم المنزلي، أو أي شخص لا يحتاج للاتصال بالإنترنت. إلا أنه يعمل كبوابة للشبكة المحلية ويسمح باتصالات من الشبكة المحلية إلى كافة الخدمات.

ملاحظة:

الأسطر الإضافية الملونة تسمح حالياً باتصالات إلى المنفذ 80 فقط.

```
#!/bin/sh
# Variables
```

```
IPTABLES="/sbin/iptables"
LAN_IFACE="eth0"
INET_IFACE="eth1"
INET_IP="1.2.3.4"
LOCALHOST_IP="127.0.0.1/32"
LAN_IP="192.168.0.1/32"
LAN_BCAST="192.168.0.0/24"

# Setup IP Masquerading

echo "1" > /proc/sys/net/ipv4/ip_forward
$IPTABLES -t nat -A POSTROUTING -o $INET_IFACE -j MASQUERADE

# Specify the default policy for the built in chains
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD DROP
$IPTABLES -P OUTPUT DROP

# Specify INPUT Rules
$IPTABLES -A INPUT -i !$INET_IFACE -j ACCEPT
$IPTABLES -A INPUT -p TCP -i $INET_IFACE -m state --state NEW --dport http -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Specify FORWARD Rules
$IPTABLES -A FORWARD -i $LAN_IFACE -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Specify OUTPUT RULES
$IPTABLES -A OUTPUT -p ALL -s $LOCALHOST_IP -j ACCEPT
$IPTABLES -A OUTPUT -p ALL -s $LAN_IP -j ACCEPT
```

3ـ الغلاف الأمني The Secure Shell

مصادقة المضيف

باستخدام ssh يكون كل من المضيف والمستخدم موثوقَين. تتم المصادقة على المضيف بواسطة مفاتيح المبادلة. تحفظ مفاتيح المضيف العامة والخاصة عادة في /etc/ssh. إذا كنت تستخدم OpenSSH اعتماداً على البروتوكول المستخدم سوف يدعى م لف مفتاح المضيف ssh_host_key للبروتوكول 1 و ssh_host_rsa_key أو ssh_host_dsa_key للبروتوكول 2. كل من هذه المفاتيح لها مفتاح عمومي مطابق، على سبيل المثال ssh_host_key.pub.

عندما يتصل زبون ssh بمزود سوف يعطي الأجهزة المضيفة مفتاحاً عموماً.

في هذه المرحلة سوف يتم إخطار المستخدم بشيء ما له الشكل التالي:

```
The authenticity of host 'neptune (10.0.0.8)' can't be established.
RSA key fingerprint is 8f:29:c2:b8:b5:b2:e3:e7:ec:89:80:b3:db:42:07:f4.
Are you sure you want to continue connecting (yes/no)?
```

إذا قبلت بمتابعة الاتصال، ستتم إضافة المفتاح العمومي للمزود إلى الملف المحلي $HOME/.ssh/known_hosts.

مصادقة المستخدم (باستخدام كلمات المرور)

ثم يتم إخطار المستخدم بكلمة المرور المخصصة لحسابه على المزود ليتمكن من الدخول.

مصادقة المستخدم (باستخدام المفاتيح)

يمكن أن تتضمن مصادقة المستخدم مفاتيح مبادلة. سوف يحتاج المستخدم في هذه الحالة إلى توليد زوج مفاتيح خاص/عمومي. مثلاً:

```
ssh-keygen -t dsa -b 1024
```

سوف يولد مفتاح DSA عيار 1024 بت. في الحالة الافتراضية سوف يتم حفظ المفاتيح في $HOME/.ss وتدعى في مثالنا id_dsa و id_dsa.pub.

إذا افترضنا أن لدينا id_dsa.pub فنستطيع (غرس) هذا المفتاح في حساب بعيد ومنع كتابة كلمات مرور من أجل اتصالات إضافية أخرى. للقيام بذلك نحتاج لنسخ محتويات الملف id_dsa.pub إلى ملف يدعى authentication_keys2 مخزن في دليل $HOME.ssh البعيد.

تحذير

كافة المفاتيح الخاصة في /etc/ssh و ~/.ssh يجب أن تتمتع بالسماحية 600.

ملف تكوين sshd

ملف /etc/ssh/sshd_config بسيط:

```
#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
```

ملف تكوين ssh

ملف /etc/ssh/sshd_config أو $HOME/.ssh/config بسيط:

```
# Host *
# ForwardX11 no
# RhostsAuthentication no
# RhostsRSAAuthentication no
# RSAAuthentication yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# CheckHostIP yes
# IdentityFile ~/.ssh/identity
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# Port 22
# Protocol 2,1
# Cipher 3des
```

4- ضبط الوقت

تاريخ النظام

يمكن تغيير تاريخ النظام باستخدام أمر date. الصيغة البرمجية هو:

```
date MMDDhhmmCCYY[.ss]
```

ساعة العتاد

يمكن تغيير ساعة العتاد مباشرة باستخدام الأداة hwclock. الخيارات الرئيسية هي:

r- أو show--	طباعة الوقت الحالي.
w- أو systohc--	ضبط ساعة العتاد وفقاً للتوقيت الحالي للنظام.
s- أو hctosys--	ضبط توقيت النظام وفقاً لساعة العتاد الحالية.

استخدام NTP

التـوقيت الإحـداثي العالمي UTC هو معيار يستخدم للتسلسل الزمني المعتمد على دوران الأرض حول محورها. في حين أنه بسبب الشذوذات التي يمكن إهمالها للدوران تتطلب الثواني الإضافية (المتخطية) إدراجها في مقياس UTC باستخدام ساعات ذرية (دقيقة).

بما أن الحواسب غير مجهزة بساعات ذرية (دقيقة)، فالفكرة هي استخدام بروتوكول لمزامنة/ضبط المزامنة/ ضبط التزامن بين ساعات الحواسب عبر الإنترنت. NTP يعني Network Time Protocol، بروتوكول التوقيت الشبكي، وكأي بروتوكول آخر.

تدعى الحواسيب التي تم تحديثها مباشرة بواسطة ساعات دقيقة primary time servers (مزودات الوقت الرئيسية)، وتستخدم لتحديث عدد أكبر مـن مـزودات الـوقت الفرعيـة. يشكل ذلك بنية شجرية أشبه ببنية مزود أسماء النطاقات DNS. المزودات الجذرية في المستوى أو الطور الأول، والمزودات الثانوية في المستوى الثاني.. وهكذا.

إعداد زبون للاستعلام من مزود NTP

بسـتخدم برنـامج خدمي Daemon لـ NTP يدعى ntpd للاستعلام بصورة نظامية عن الوقت من مزود توقيت بعيد. كل ما تحتاجه هو إدخال في ملف /etc/ntp.conf يشير إلى مزود NTP تجاري أو عمومي. يمكن الحصول على عناوين مزودات NTP من الإنترنت.

يمكن لبروتوكول NTP تقدير أخطاء التردد لساعة عتادية من سلسة من الاستعلامات، حيث تخزن قيمها في ملف تحدده الواصفة driftfile.

ملف /etc/ntp.conf في حده الأدنى

```
server ntp2.somewhere.com
driftfile /var/lib/ntp/drift
```

ما إن يبدأ ntpd سيتحول نفسه إلى مزود NTP مقدماً خدماته عبر المنفذ 123 باستخدام UDP.

One off queries:The **ntp** package also provides the **ntpdate** tool which can be use to set the time on the command line:

```
<re>ntpdate ntp2.somewhere.com
```

5ـ أمن النواة

ثمة العديد من الخيارات الأمنية في نواة لينكس. تتضمن بصورة رئيسية آلية sync_cookie. يتم التحكم بـ Stack overflow بواسطة رقعة أمنية تدعى openwall أو OWL.

tcp_syncookies

لتمكين هذا الخيار، ببساطة قم بما يلي:

```
[root@nasaspc /proc]#echo "1" > /proc/sys/net/ipv4/tcp_syncookies
```

ذلك سيمنع النواة من إرسال cookie إلى الزبون عند استجابة SYN+ACK لديه. في هذا النمط سيقوم المزود عندئذ بإغلاق المقابس وانتظار ACK الزبون مع الكوكي الملائمة.

إذا لم يكن ملف tcp_syncookies موجوداً في الدليل /proc فيتعين عليك عندئذ إعادة ترجمة النواة بحيث تدعم syncookies.

ملاحظة:

في الحالة الافتراضية، حتى لو كانت syncookies مدعومة من قبل النواة، يتعين عليك تنشيط هذا الدعم بإضافة "1" إلى /proc/sys/net/ipv4/tcp_syncookies. يتم ذلك عادة في /etc/rc.d/rc.local. على كل حال مع ذلك ستضيف المزيد من الحلول الفعالة مدخلات إلى /etc/sysctl.conf ___ would be to add an entry to.

رقعة OWL الأمنية (لا علاقة لهذا المقطع بالامتحان):

تهتم هذه الرقعة بمعظم المواضيع المتعلقة بـ stack، وهي خارج نطاق هذه الدراسة. ومع ذلك، فمن السهل اختبار ما إذا كان النظام لديك vulnerable with binaries provided with the downloaded patch.

موارد حول رقعة OWL ونواة لينكس:
http://www.openwall.com
http://www.kernel.org/pub/linux/kernel/v2.2/

مدعوم فقط في النواة 2.2.19 حتى الآن.

بعد تنزيل linux-2.2.19.tar.gz و linux-2.2.19-ow1.tar.gz في دليل /usr/src/، تأكد من أنك حذفت رابطة linux الرمزية.

```
[root@nasaspc src]#pwd
/usr/src/
[root@nasaspc src]#rm -rf linux
```

ثم قم بفك الحزم:

```
[root@nasaspc src]#tar xvzf linux-2.2.19.tar.gz
[root@nasaspc src]#tar xvzf linux-2.2.19-owl.tar.gz
```

لاختبار النظام لديك، انتقل إلى الدليل linux-2.2-19-owl. يوجد دليل يدعى optional يحتوي ملفاً يدعى stacktest.c.

```
[root@nasaspc optional]#pwd
/usr/src/linux-2.2.19-ow1/optional
[root@nasaspc optional]#gcc stacktest.c -o stacktest
```

إذا كنت تشغل stacktest ستحصل على لائحة خيارات. شغل محاكي الدفق.

A successful buffer overflow attack:

```
[root@nasaspc optional]#stacktest
Usage: ./stacktest OPTION
Non-executable user stack area tests

-t call a GCC trampoline
-e simulate a buffer overflow exploit
-b simulate an exploit after a trampoline call
```

```
[root@nasaspc optional]#stacktest -e
Attempting to simulate a buffer overflow exploit...
Succeeded.
```

لتطبيق هذه الرقعة يتعين عليك الانتقال إلى دليل linux. إليك الأوامر:

تطبيق رقعة openwall

```
[root@nasaspc linux]#pwd
/usr/src/linux
[root@nasaspc linux]#patch -p1 < /usr/src/linux-2.2-19-owl/linux-2.2.19-ow1.diff
```

الآن إذا قمت بتنفيذ make menuconfig فيجب أن تشاهد مدخلاً جديداً يدعى Security options (خيارت الأمن). التحديدات الافتراضية جيدة من هنا يمكنك المباشرة بترجمة وتنصيب النواة كالعادة.

الفصل التاسع
إدارة نظام لينوكس Linux System Administration

نظرة شاملة

سوف نركز على مهمات إدارة النظام الرئيسية مثل مراقبة ملفات السجلات، وجدولة الأعمال بواسطة at و cron. هذا يشمل أيضاً نظرة شاملة على الوثائق المتاحة (صفحات man والموارد المتاحة على الخط)، بالإضافة إلى مفاهيم التخزين الاحتياطي.

1ـ ملفات السجلات وملفات الإعداد Log Files and Configuration Files

المجلد /var/log/

هذا هو المجلد الذي يحتفظ بمعظم ملفات السجلات. بعض التطبيقات تقوم بتوليد ملفات سجلها الخاصة (مثل squid و samba). معظم سجلات النظام يتم إدارتها بواسطة العفريت syslogd . ملفات النظام الشائعة هي:

cron	يحتفظ بآثار الرسائل المولدة أثناء تشغيل cron
mail	الرسائل المتعلقة بـ mail
messages	تسجيل جميع الرسائل، ما عدا ذات التصاريح الخاصة مثل authpriv، mail، cron، news
secure	تسجيل جميع عمليات التصريح (authentification) الفاشلة، إضافة وحذف مستخدمين، إلخ.

أهم ملف سجلات هو messages، حيث يتم تسجيل معظم الأنشطة.

الملف /etc/syslog.conf

عند بدء syslogd، يقوم افتراضياً بقراءة ملف الإعدادات /etc/syslog.conf . يمكن بدء syslogd مع الخيار f- لتحديد مكان وجود ملف الإعدادات البديل. هذا الملف يجب أن يحتوي على لائحة من المواد متبوعة بأولويتها، متبوعة بمكان وجود ملف السجل:

```
item1.priority1 ; item2.priority2 /path-to-log-file
```

المواد المقبولة هي:

auth و authpriv	التصريح العام والخاص للمستخدم
corn	رسائل عفريت cron
kern	
mail	
news	
user	أعمال المستخدم
uucp	

الأولويات المقبولة هي (من الأكبر إلى الأصغر):

emerg
alert
crit
err
warning
notice

info
debug
*
none

الأولويات هي أقلية! كل الأولويات العليا سيتم تسجيلها أيضاً. لإجبار أولولية أن تكون info تحتاج فقط إلى إضافة علامة المساواة '=' كما الآتي:

```
user.=info
/var/log/user_activity
```

سرد للملف /etc/syslog.conf

```
# Log all kernel messages to the console.
# Logging much else
clutters up the
screen.
#kern.*
/dev/console
# Log anything (except mail) of level info or higher.
#
Don't log private authentication
messages!
*.info;mail.none;news.none;authpriv.none
/var/log/messages
# The authpriv file has restricted
access.
authpriv.*
/var/log/secure
# Log all the mail messages in one
place.
mail.*
/var/log/maillog
# Log cron
stuff
cron.*
/var/log/cron
# Everybody gets emergency messages, plus log them on
another
#
machine.
*.emerg
*
*.emerg
@10.1.1.254
# Save boot messages also to
boot.log
local7.*
/var/log/boot.log
 #
news.=crit
/var/log/news/news.crit
news.=err
/var/log/news/news.err
news.notice
/var/log/news/news.notice
```

2ـ أدوات السجلات Log Utilities

الأمر logger

الأداة الأولى المفيدة logger تفوم بشكل تقليدي بتسجيل الرسائل في الملف /var/log/messages
إذا كتبت التالي:

```
logger program myscipt ERR
```

ستحتوي نهاية الملف /var/log/messages الآن على رسالة شبيهة بالتالي:

Jul 17 19:31:00 localhost penguin: program myscript ERR

الإعدادت المحلية

الأداة logger تسجل الرسائل في الملف /var/log/messages افتراضياً. هناك مواد محلية مصممة لكي تساعدك على إنشاء ملفات سجلاتك الخاصة بك. local0 إلى local7 هي المواد المتاحة لاستخدام المدراء. إتاحة هذه المواد راجعة إلى النظام (معلومات ملف سجلات local7 لـ"ريدهات" عند الإقلاع موجودة في /var/log/boot.log). أضف السطر التالي إلى الملف /etc/syslog.conf :

local4.* /dev/tty9

أعد تشغيل syslogd :

```
killall -HUP syslogd
```

الأمر التالي يجب أن يُسجل على /dev/tty9 :

```
logger -p local4.notice "This script is writing to /dev/tty9"
```

/dev/speech هو جهاز مهم، وهو موجود مع الأدوات المهرجانية (festival tools).

logrotate

يتم تحديث ملفات السجلات بواسطة logrotate. في العادة، يتم تشغيل logrotate يومياً كعمل من أعمال cron. ملف الإعدادات /etc/logrotate.conf يحتوي أوامر لإنشاء أو ضغط ملفات.

سرد الملف logrotate.conf

```
# rotate log files weekly
weekly
# keep 4 weeks worth of
backlogs
rotate 4
# send errors to root
errors root
# create new
(empty) log files after rotating old ones
create
# uncomment this if
```

```
you want your log files compressed
compress
# RPM packages drop log
rotation information into this directory
include /etc/logrotate.d
# no
packages own lastlog or wtmp -- we'll rotate them here
/var/log/wtmp
{
    monthly
    create 0664 root
utmp
    rotate 1
}
```

3ـ الأعمال الآلية Automatic Tasks

باستخدام cron

البرنامج المسؤول عن تشغيل ال crons يُدعى crond. يقوم crond كل دقيقة بقراءة ملفات محددة تحتوي الأوامر التي ينبغي تنفيذها. تلك الملفات تُدعى crontabs.

تتواجد ملفات crontabs للمستخدمين في /var/spool/cron/<username> . هذه الملفات لا ينبغي تحريرها مباشرة من قبل مستخدمين عاديين (غير الجذر)، بل يتم تحريرها عن طريق الأداة crontab (انظر الأسفل).

برنامج الـ crontab للنظام موجود في /etc/crontab . سيقوم البرنامج بشكل دوري بتنفيذ النصوص البرمجية الموجودة في /etc/cron.*، هذا يشمل أي روابط رمزية تشير إلى السكريبتات أو الملفات الثنائية في النظام.

لمعالجة إدخالات cron يمكن استخدام الأداة crontab. يمكن رؤية الأعمال المجدولة باستخدام الخيار l- كما الآتي:

```
crontab -l
   # DO
NOT EDIT THIS FILE - edit the master and reinstall
   #
(/tmp/crontab.1391 installed on Tue Jul 17 17:56:48 2001)
   #
(Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp
$)
   0 * * 07 2 /usr/bin/find /home/penguin -name core
-exec rm {} \;
```

هل يملك المستخد الجذر أي crontab ؟

بشكل مشابه، يقوم الخيار e- بفتح محررك الافتراضي والسماح لك بإدخال cron جديد.
المستخدم الجذر يمكنه استخدام الخيار u- لرؤية وتعديل إدخالات cron للمستخدمين.
لحذف ملف ال crontab، استخدم الأمر r- crontab .

هذه هي الصيغة للـ crontab :

```
Minutes(0-59) Hours(0-23) Day of Month(1-31) Month(1-12) Day of
Week(0-6) command
```

الأذونات:

بشكل افتراضي، يمكن لأي مستخدم استخدام crontab. يمكن على أي حال التحكم بالوصول إليها بواسطة الملفين /etc/cron.deny و /etc/cron.allow .

الجدولة باستخدام "at"

أعمال at تنفذ بواسطة عفريت atd. جميع الأعمال تكون مذكورة في /var/spool/at/ .

الأمر at يُستخدم لجدولة عمل في وقت محدد، من خلال التركيبة:

```
at [time]
```

حيث time يمكن أن يكون:
now
3am +2days
midnight
April 12 10:15
teatime

للحصول على لائحة كاملة بهيئة الأوقات الممكن ذكرها، راجع الملف /usr/share/doc/at_xxx/timespec .

يمكن سرد الأوامر التي تم جدولتها باستخدام الأمر atq أو at ـ l . أعمال at تكون محفوظة في المجلد /var/spool/at/ :

```
> ls /var/spool/at/

 a0000100fd244d   spool
```

عند استخدامك لـ atq، سترى أن كل عمل مجدول مرفق برقم. يمكنك استخدام هذا الرقم في عملية الحذف.

```
> atq
1
-07-17 18:21 a root
```

من هذا السرد أن رقم العمل المجدول هو 1، يمكننا حذفه كالتالي:

```
-d 1
```

لأذونات
ذونات:

افتراضي، at محصورة فقط بالمستخدم الجذر. للالتفاف حول ذلك، عليك إما أن تضع ملف /etc/at.deny فارغاً أو أن تملأ ملف etc/ at.allow/ بالأسماء المطلوبة.

4
-
النسخ الاحتياطي والضغط Backups and Compressions

قنيات ا
يات النسخ الاحتياطي

هناك ثلاث وسائل للحصول على نسخة احتياطية للنظام:

الوسيلة الشاملة: تنسخ جميع الملفات.
الوسيلة التراكمية: عند استخدامها لأول مرة، تنسخ الملفات الجديدة والمعدلة بعد آخر نسخ احتياطي شامل. وعند استخدامها ثانية، تنسخ الملفات الجديدة والمعدلة بعد آخر نسخ احتياطي تراكمي.
الوسيلة المفرقة: تقضي بنسخ الملفات الجديدة والمعدلة بعد آخر نسخ احتياطي شامل.

مثال: إن كنت قد قمت بنسخ احتياطي شامل و 3 عمليات نسخ مفرقة قبل حدوث انهيار في النظام. فكم قرصاً من هذه الأقراص الاحتياطية الأربعة ستحتاج لإعادة استرجاع النظام؟

الأرشفة باستخدام tar

الخيار الرئيسي لإنشاء أرشيف tar هو c- . يمكنك تحديد اسم الأرشيف في المدخلة الأولى بإضافة الخيار f- .

```
tar -cf home.tar /home/
```

إن لم تحدد اسم الأرشيف، يمكنك ببساطة توجيه مخرجات الأمر tar نحو الملف المطلوب:

```
tar -c /home/ >
home.tar
```

فك الأرشفة باستخدام tar

فك الأرشفة يتم بنفس الطريقة: استبدل الخيار x- مكان الخيار c- . هذا سيجعل البرنامج ينشئ المجلدات - إن لزم - ويفك الأرشفة في المجلد الحالي. لإعادة توجيه فك الأرشفة إلى مجلد /usr/share/doc كمثال، استخدم الأمر التالي:

```
tar -xf backeddocs.tar -C
/usr/share/doc
```

الضغط

كل الأرشيفات يمكن ضغطها بطرق ضغط مختلفة. هذه هي الخيارات التي يمكن استخدامها أثناء إنشاء أو فحص أو فك الأرشيفات:

خيار الأرشفة	نوع الضغط
Z	ضغط عادي
z	ضغط gzip
j	ضغط bzip2

الأداة cpio

الأداة cpio تُستخدم لنسخ الملفات من وإلى الأرشيفات. يتم تمرير لائحة الملفات المراد نسخها إلى cpio عبر الأنابيب (pipe) (كما الحال عند الحصول على الخرج من الأمر find)، أو من خلال ملف نصي كموجه إدخال.

- فك أرشفة ملفات مخزنة على قرص:

```
cpio -i < /dev/tape
```

- إنشاء أرشيف للمجلد /etc :

```
find /etc | cpio -o > etc.cpio
```

5- الوثائق Documentation

صفحات man وقاعدة بيانات whatis

صفحات man موزعة على أقسام	
NAME	اسم المادة متبوعة بسطر واحد من الوصف المختصر
SYNOPSYS	تركيبة الأمر
DESCRIPTION	وصف مطول
OPTIONS	لائحة بكل الخيارات ووظيفتها
FILES	الملفات المتعلقة بالمادة الحالية (ملفات الإعداد، إلخ)
SEE ALSO	صفحات man أخرى متعلقة بنفس الموضوع

هذه هي الأقسام الرئيسية التي يمكن توقعها في صفحات man.

قاعدة بيانات whatis تختزن القسم NAME لكل صفحات man في النظام. يمكن تحقيق ذلك عن طريق cron يومي. قاعدة البيانات هذه تملك المدخلين التاليين:

```
الاسم (المفتاح) - سطر واحد
وصفي
```

تركيبة whatis هي:

```
whatis <string>
```

الخرج سيكون القسم الكامل NAME الذي يتطابق عنوانه أو جزء منه مع الاسم (المفتاح).

يمكن استخدام الأمر man لاستعلام قاعدة بيانات whatis. التركيبة هي التالية:

```
man -k <string>
```

خلافاً لـ whatis، هذا الأمر سيستعلم عن الأسماء والسطر الوصفي المختصر لكل منها في قاعدة البيانات. إن تطابق الاسم مع أي كلمة في هذه الحقول سيتم إرجاع قسم ال NAME الكامل.

مثال:

```
whatis lilo
lilo
(8)  - install boot loader
lilo.conf [lilo]
```

```
(5)  - configuration file for lilo
```

```
man -k  lilo
grubby
(8)   - command line tool for configuring grub, lilo, and elilo
lilo
(8)   - install boot loader
lilo.conf [lilo]   (5)   - configuration
file for lilo
```

الـ FHS تنصح بإبقاء صفحات ال man محفوظة في /usr/share/man .

أقسام صفحات man	
القسم 1	معلومات الملفات التنفيذية
القسم 2	استدعاءات النظام. مثل: mkdir(2)
القسم 3	استدعاء المكتبات. مثل: stdio(3)
القسم 4	الأجهزة (الملفات في /dev)
القسم 5	ملفات الإعداد والتهيئة
القسم 6	الألعاب
القسم 7	حزمات الماكرو
القسم 8	الأوامر الخاصة بالإدارة
القسم 9	روتين النواة

للوصول إلى قسم محدد ذي الرقم N، اكتب: man N command

أمثلة:

```
man mkdir
man 2 mkdir
```

```
man crontab
man 5 crontab
```

صفحات Info

ال FHS تنصح بإبقاء صفحات info محفوظة في المجلد /usr/share/info . إنها مجموعة من الملفات المضغوطة التي يمكن قراءتها عن طريق الأمر info.

أدوات GNU (جنو) الأصلية تستخدم صفحات info بدلاً من صفحات man. ولذلك تمت إعادة كتابة معظم صفحات info كما الحال في صفحات man. على أي حال، المعلومات حول مشاريع GNU كـ gcc و glibc متوفرة أكثر في صفحات info مقارنة مع صفحات man.

الوثائق المتوفرة على الخط

مشاريع GNU تتضمن وثائق كـ README و FAQ و CHANGELOG وأحياناً مساعدات للمستخدم/المدير. صيغة هذه الملفات قد تكون ملفاً نصياً (ASCII) أو ملف HTML أو LateX أو postscript.

هذه المستندات محفوظة في المجلد /usr/share/doc/ .

وثائق HOWTO و LDP (مشروع وثائق لينوكس)

مشروع وثائق لينوكس (The Linux Documentation Project = TLDP) يوزد عدة مستندات مفصلة حول مواضيع متخصصة. هناك مساعدات مصممة لتشرح المفاهيم والتجهيزات. عنوان موقع المشروع هو: www.tldp.org . يمكن نشر وتوزيع وثائق LDP بشكل مجاني وحر تحت رخصة GPL.

مجموعات أخبار Usenet

مجموعات الأخبار الرئيسية للينوكس هي مجموعات comp.os.linux.* (مثل comp.ps.linux.networking أو comp.os.linux.security ...). بمجرد تثبيت قارئ أخبار والاتصال بخادم الأخبار (News server) والذي يكون عادة متوفراً لدى ال ISP أو حرم الجامعات، يمكن تحميل لائحة بكل مجموعات المناقشة الموجودة والاشتراك أو إلغاء الاشتراك في مجموعة معينة.

هناك عدد كبير من الخبراء ومن المستخدمين الجدد الذين يعتمدون على مجموعات الأخبار للحصول على معلومات حول أعمال ومشاريع محددة. يمكنك إمضاء بعض الوقت في الإجابة على الأسئلة إن كنت تشعر أنك تملك الخبرة الكافية في الموضوع.

ملاحظة: الخيار man -k يستعلم كلا الحقلين في قاعدة بيانات whatis. وهذا سيجد كل شيء عن المادة المطلوبة. هناك أداة تُدعى apropos (والتي تعني "حول") يمكنها أن تقوم بنفس عمل man -k.

5ـ تمارين

السجلات

1. عدل الملف /etc/syslog.conf لإخراج بعض السجلات إلى /dev/tty9 (تأكد من إعادة تشغيل syslogd ومن أن الإخراج موجه بشكل مباشر).

2. أضف عنصراً خاصاً يُدعى local5 مع أولوية critical إلى ملف /etc/syslog.conf ثم وجه الإخراج إلى /dev/tty10 . أعد تشغيل syslogd ثم استخدم مسجل الدخول لكتابة المعلومات عبر local5.

أ

3. اقرأ السكريبت /etc/rc.d/init.d/syslof وغير /etc/sysconfig/syslog للسماح للمضيفات البعيدة بإرسال خرج السجلات.

الجدولة

4. أنشئ إدخال cron يقوم بتشغيل xclock كل دقيقتين. تذكر أن cron لا يهتم بمتغيرات النظام مثل PATH و DISPLAY.

ا

5. استخدم at لتشغيل xclock بعد خمس دقائق من الآن.

الأرشفة

6. استخدم find لسرد جميع الملفات التي تم تعديلها في ال 24 ساعة الماضية.
(تلميح: قم بتمرير خرج find ـmtime 1 إلى ملف).

7. استخدم cpio لإنشاء أرشيف يُدعى Incrmental.cpio
(الإجابة: استخدم الملف المنشأ في التمرين السابق ونفذ الأمر: cat FILE | cpio ـov > Incremental.cpio).

ا

8. استخدم xargs و tar لإنشاء أرشيف لكل الملفات التي تم تعديلها أو استخدامها خلال الدقائق الخمس الأخيرة.

9. قم بنفس الشيء مستخدماً الخيار execـ في **find**. لاحظ أن الملفات المسرودة من قبل find يمكن الترميز إليها بالرمز {}.

10. قم بفك الأرشيف الذي أنشأته للتو.

الفصل العاشر
إعداد PPP

المودمات التسلسلية:

بشـكل عـام يفترض لينوكس أن المودم التسلسلي مربوط إلى منفذ تسلسلي (على أحد الأجهزة /dev/ttySN). وبذل يجب عليك أولاً تحديد على أي منفذ تسلسلي تم ربط المودم.

إن الأمر setserial -g سوف يسأل المنافذ التسلسلية وإذا كانت المصادر غير متوفرة فإن القيمة UART ستكون غير معروفة.

مثال لخرج الأمر setserial:

```
setserial -g /dev/ttyS[0-3]
/dev/ttyS0, UART: 16550A, Port: 0x03f8, IRQ: 4
/dev/ttyS1, UART: 16550A, Port: 0x02f8, IRQ: 3
/dev/ttyS2, UART: unknown, Port: 0x03e8, IRQ: 4
/dev/ttyS3, UART: unknown, Port: 0x02e8, IRQ: 3
```

ومـن اجـل المودمات الغير تسلسلية من الممكن أن تحصل على المعلومات عن المصادر المتوفرة في /proc/pci . وهنا فإن إعدادات I/O و IRQ يمكن أن تنقل إلى جهاز
/dev/ttyS? فارغ . وهذا ممكن من خلال السطرين التاليين:

```
setserial /dev/ttyS2 port 0x2000 irq 3
setserial /dev/ttyS2 autoconfig
```

السطر الأخير يتعامل بشكل بسيط مع الإعدادات الخاصة بإعدادات UART المحتملة.

```
setserial /dev/ttyS2 port 0x2000 irq 3
setserial /dev/ttyS2 autoconfig
```

إن هـذه الإعـدادات سـوف تفقـد عند الإقلاع الثاني للحاسب ويمكن أن تحفظ في الملف /etc/rc.serial . وإن هذا النص البرمجي هو أحد النصوص البرمجية التي تنفذ بواسطة rc.sysinit خلال الإقلاع.

النص البرمجي لـ rc.serial :

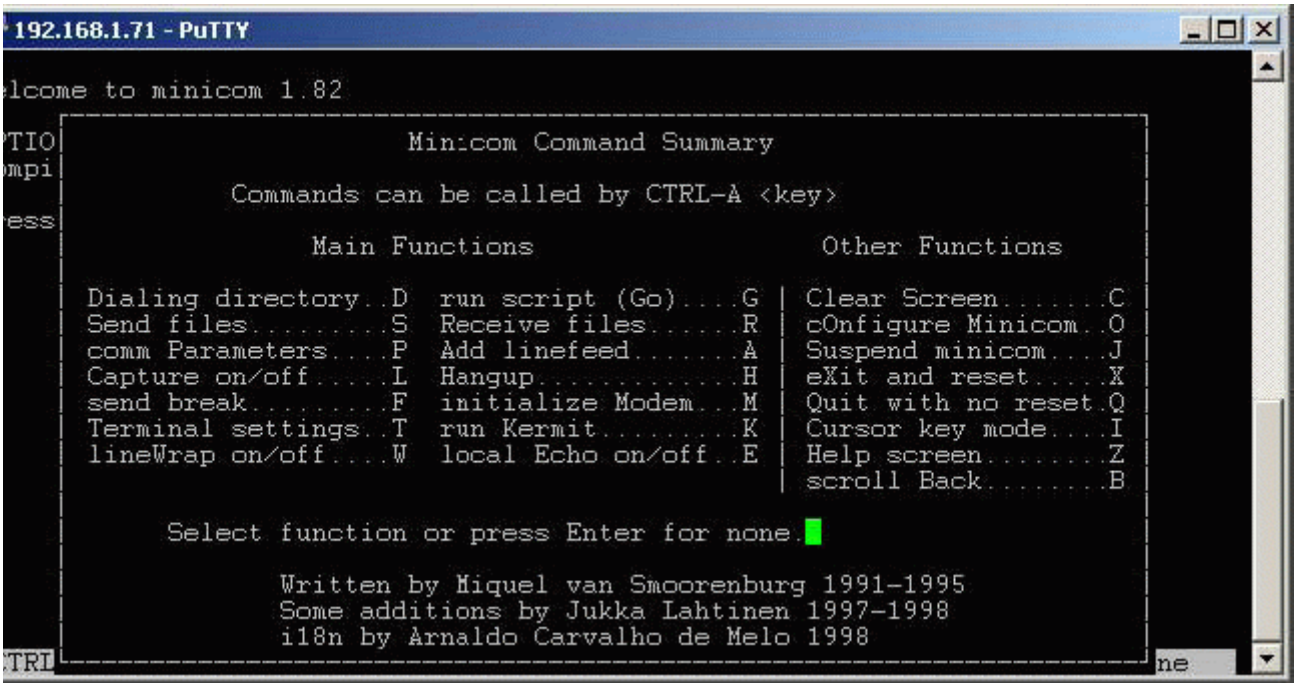
```
#!/bin/bash

TTY=/dev/ttyS2
PORT=0x2000
IRQ=3

echo "Setting up Serial Card ..."
/bin/setserial $TTY port $PORT irq $IRQ 2>/dev/null
/bin/setserial $TTY autoconfig 2>/dev/null
```

إعدادات الطلب الهاتفي:

بدايـةَ المـودم معـرف بـأن يكون موصولاً إلى جهاز تسلسلي يمكن إرسال تعليمات خاصة بالمودم مثل ATZ أو ATDT . والأداة الوحيدة كواجهة terminal هي minicom.



والأداة الأخـرى الشـائعة هـي wvdialconf . هذه الأداة ستقوم بشكل آلي بتفحص المودمات المتواجدة على ttyS's وتقوم بإنشاء ملف توصيف هذا الجهاز . وهذا الملف يستخدم للتعامل مع كلمة الدخول وإنشاء العميل pppd حالما يتم تأسيس اتصال .

pppd والمحادثة:

بدايـة فـإن كـل النصـوص البرمجيـة للمحادثـة تستخدم الاتصال مع مودم المضيف البعيد. وتكون عبارة عن سلسلة من استقبال/ إرسال. الصيغة بالشكل:

```
'expected query' 'answer'
```

قبول استعلام من المودم بالشكل:

```
' ' 'OK' 'CONNECT' 'login' 'password'
'TIMEOUT' '>'
```

يقـرأ النص البرمجي بشكل متتابع ويبدأ بالاستعلام الفارغ ' ' والذي يتطابق مع الأمر 'ATZ' بمجرد أن يبدأ المودم . يتم استقبال الاستعلام 'OK' . عندها يجيب النص البرمجي بالأمر 'ATDT' . هذه المحادثة تتكرر حتى يصل موجه الأمر '>' إلى المرحلة الأولى ليستطيع تشغيل pppd.

مثال عن chat script:

```
'ABORT' 'BUSY'
'ABORT' 'ERROR'
'ABORT' 'NO CARRIER'
'ABORT' 'NO DIALTONE'
'ABORT' 'Invalid Login'
'ABORT' 'Login incorrect'
'' 'ATZ'
'OK' 'ATDT01172341212'
'CONNECT' ''
'ogin:' 'adrian'
'ord:' 'adrianpasswd'
'TIMEOUT' '5'
'>' pppd
```

بالطبع هذه طريقة واحدة لأداء ما سبق. ويمكن أيضاً بدء pppd يدوياً وعندها ينتج عن النص البرمجي محادثة كالتالي:

```
pppd /dev/ttyS2 115200 \
nodetach \
lock \
debug \
crtscts \
asyncmap 0000000 \
connect "/usr/sbin/chat -f /etc/sysconfig/network-scripts/chat-ppp0"
```

السطور الموجودة أسفل الأمر pppd يمكن أن تخزن في *etc/ppp/option* وهذا الملف يحوي معظم الميزات التي تجعل pppd أكثر ثبات وقوة. كمثال يستخدم require_chap لـ /etc/ppp/chap-secrets في عملية الولوج الموثوق.

أنداد pppd:

هنـاك دليل اسمه peers في /etc/ppp/ . يمكن داخل هذا المجلد إنشاء ملف يحوي كل سطور الأوامر الضرورية لتحديد خصائص pppd. في هذه الطريقة الاتصال peer يمكن أن يبدأ مع كل المستخدمين.

في ما يلي يظهر مثال للملف PPP peer:

```
# This optionfile was generated by pppconfig 2.0.10.
hide-password
noauth
connect "/usr/sbin/chat -f /etc/sysconfig/network-scripts/chat-ppp0"
/dev/ttyS0
115200
defaultroute
noipdefault
user uk2
```

إن الملف peer السابق (يدعى uk2) سوف يستخدم كالتالي:

```
# pppd call uk2
```

وهـذا سـيطلب هاتفيـاً الرقم المحدد في " chat script" وسيتم الدخول كمستخدم uk2 . نرجو ملاحظة أن هذا يتطلب التوافق مع المدخلات في /etc/ppp/chap-secret والملف /etc/ppp/pap-secrets. وإن طريقة كتابة هذين الملفين هي كالتالي:

```
# Secrets for authentication using CHAP
# client server secret IP addresses
uk2 * "uk2"
*
```

طريقـة الكتابة هذه تسمح باستخدام عدة كلمات مرور عند الاتصال بعدة مخدمات، كما تسمح بتخصيص عنوان IP. على الأغلب هذا لن يعمل عند الاتصـال بـــ ISP، ولـكن عندمـا تأسـيس اتصال اتصالات مخصصة، ويمكنك تحديد عناوين IP إن كان هناك ضرورة، وكمثال عندما تحتاج إلى تدقيق نشاط شبكتك، وترغب بتخصيص IP محدد لمن يريد أن يحصل على IP محدد.

5. Wvdial:

هذه هي الطريقة الافتراضية والمستخدمة من قبل RedHat للاتصال بشبكة الطلب الهاتفي، لإعداد Wvdial من السهل استخدام أحد أدوات الإعداد الخاصة بكل من KDE أو Gnome ويتم إعدادها في الملف /etc/wvdial.conf. فيما يلي مثال لملف wvdial:

```
[Modem0]
Modem = /dev/ttyS0
```

```
Baud = 115200
Dial Command = ATDT
Init1 = ATZ
FlowControl = Hardware (CRTSCTS)
[Dialer UK2]
Username = uk2
Password = uk2
Phone = 08456091370
Inherits = Modem0
```

لاستخدام Wvdial من خلال سطر الأوامر يمكنك تنفيذ العبارة التالية:

```
# wvdial <dialer-name>
```

في ملف الإعداد كمثال يظهر الأمر التالي والذي سيطلب هاتفياً بالاسم uk2.

```
# wvdial uk2
```

الفصل الحادي عشر
الطباعة

الغـايتين الرئيسـييتين مـن هذا الفصل هما التعريف أولاً بأدوات GNU الخاصة بالطباعة والمتاحة في الأجهزة المزودة بنظام لينكس، وثانياً فهم ملفات الإعداد الخاصة بمزود الطباعة.

1ـ المرشحات و gs

تسـتخدم أنظمـة لينكـس ويونكـس المرشـحات مـع الأنسـاق غير النصية. تقوم هذه المرشحات بترجمة أنساق الملفات JPEG أو troof إلى نسق بوستسـكريبت. والتـي يمـكن إرسـالها مبا شرة إلـى طابعـة بوستسـكريبت. ولـكن بمـا أنـه ليس كل الطابعات المعهودة يمكنها معالجة نصوص بوستسكريبت يتم استخدام طابعة بوستسكريبت افتراضية وسيطة تدعى gs (غوستسكريبت) ليصار بالنهاية إلى ترجمة بوستسكريبت إلى PCL.

الإصدار التجاري من غوستسكريبت هو (غوستسكريبت علاء الدين)، في حين أن إصدار GNU أقدم.

تتضمن أداة gs قاعدة بيانات لبرامج قيادة الطابعات التي يمكنها معالجة وتحويل نصوص البوستسكريبت مباشرة إلى PCL لتلك الأنواع المعروفة. (هذه اللائحة تتحدث باستمرار. على سبيل المثال من طابعات USB مدعومة). تلعب أداة gs دوراً محورياً في الطباعة في لينكس.

الطابعات وأرتال الطباعة

كمـا يبـدو أعـلاه، لا تتـم معالجة طباعة نصوص آسكي بالطريقة ذاتها التي تتم فيها معالجة لاصور وملفات بوستسكريبت. إذا كان لديك فقط طابعـة واحـدة وتـود طباعـة بـريدك على سبيل المثال، فقد لا تكون بحاجة لاستخدام اي مرشح. قد تود تعريف رتل دون المرشحات، الأمر الذي سيؤدي إلى طباعة البريد بصورة أسرع. يمكنك أيضاً تعريف رتل في الطابعة ذاتها والتي سوف تعالج فقط ملفات بوستسكريبت.

تعرّف كافة الأرتال والطابعات ضمن الملف *etc/printcap*. فيما يلي الإعداد الكامل لطابعة بعيدة 192.168.1.20 باستخدام الرتل البعيد lp:

```
lp:\
:sd=/var/spool/lpd/lp:\
mx#0:\
h:\
=192.168.1.20:\
lp:
```

ارات الرئيسية هنا هي rm (المضيف البعيد) و sd (دليل الطباعة spool) و rp (الرتل البعيد).

أنه لا توجد أية فلاتر محددة (سوف نستخدم if لمرشح الإدخال). كافة عمليات الترشيح تتم على المضيف البعيد.

دوات الطباعة

تسـتخدم أد

دم أداة lpr لإرسـال مهمـات معينـة إلى الطابعة. وهي إصدار حديث من lp ـ (line print). من وجهة نظر المستخدمين من المفيد إدراك أنه يمكن للطابعة ان تقترن بأكثر من رتل واحد. إليك المثالين التاليين لطباعة ملف يدعى LETTER.

ل المهمة إلى الطابعة الافتراضية:

```
LETTER
```

ل المهمة إلى الرتل 'ljet'

```
-Pljet LETTER
```

الخيارات الرئيسية لـ lpr:

#num ـ	طباعة num نسخة
Pqd ـ	تحديد رتل الطباعة pq
s ـ	إنشاء ارتباط رمزي في دليل الطباعة spool بدلاً من نسخ الملف كاملاً إليه

يمكن لأي مستخدم مراقبة حالة أرتال الطباعة باستخدام أداة lpq. إليك بضعة أمثلة...

إظهار المهام في الرتل الافتراضي	lpq
إظهار كافة المهام لكافة الأرتال في النظام	lpq ـa
إظهار كافة المهام في الرتل remote	lpq ـPremote

lprm

استناداً إلى خيارات الملف /etc/lpd.perms يمكن السماح للمستخدمين بحذف مهام معينة من رتل معين باستخدام lprm.

إزالة آخر مهمة تم إرسالها	lprm
إزالة المهام التي تم إرسالها من قبل المستخدم hill	lprm dhill
إزالة كافة المهام المرسلة	lprm ـa (أو ببساطة lprm ـ)

من الممكن إزالة مهمة طباعية spooled معينة بالإشارة إلى رقم المهمة، والذي يمكن الحصول عليه باستخدام lpq.

lpc

تستخدم أداة Line Printer Control للتحكم بأرتال الطباعة وبالطابعات. يمكت تعطيل وتمكين أرتال الطباعة، لاحظ أنه يمكن من جهة أخرى إزالة المهام من الرتل ولكنها لا توقف الرتل.

يمكن للمرء إما أن يستخدم lpc بصورة تفاعلية (لها مؤشرها الخاص بها) أو من سطر الأوامر.

فيما يلي مخرجات lpc ـhelp:

```
CMD: /usr/sbin/lpc help
Commands may be abbreviated. Commands are:
abort e
bort enable disable help restart status topq ?
ean exit down quit start stop up
```

ارات up/topq/disable/enable متعلقة بالأرتال.

ارات down/stop/start متعلقة بالطابعات.

ملفات الإعدادات:

etc/printcap

ا رأينا في بداية هذا الفصل، يعرف هذا الملف كافة الطابعات والأرتال التي يمكن للنظام استخدامها (محلياً وعن بعد).

كن تحديد الطابعة الافتراضية من خلال المتغيراتLPDEST أو PRINTER: PRINTER=lp. إذا لم يكن قد تم تعيين متغييرات للبيئة فستكون ابعة الافتراضية هي الطابعة الأولى المحددة في الملف /etc/printcap.

التعريفات الرئيسية هي:

lp	اسم الجهاز ـ عادة /dev/lp0
mx	الحجم الأقصى للملف (Zero= لا محدود)
sd	دليل spool ـ (/var/spool/lpd/<queuename>)
if	فلتر الإدخال
rm	إزالة عنوان المضيف أو الـ IP
rp	اسم الرتل البعيد

إذا تم تعديل هذا الملف فسوف نحتاج لإعادة تشغيل دايمون lpd.

/etc/lpd.conf

وهـو ملف طويل جداً. وكافة الخيارات في الحالة الافتراضية ليس ثمة تعليقات عليها. يستخدم هذا الملف إذا أراد مشرف النظام مزيداً من التحكم (بمعنى: تخويل الوصول البعيد، صلاحيات المستخدم) **خلال** الطباعة.

/etc/lpd.perms

يتحكـم هـذا الملـف بصـلاحيات أدوات lpc و lpq و lprm. يمكنـك تحديداً منح المستخدمين الحق في **إعادة ترتيب** الأرتال للمهام الخاصة بهم (باستخدام أداة lprm) من خلال السطر التالي:

```
ACCEPT SERVICE=M SAMEHOST SAMEUSER
```

تستخدم LPRng نظاماً للمفاتيح لتقليص المدخلات في lpd وليس من **الصعب جداً** فهمه على كل حال.

على سبيل المثال الخدمة 'M' تقابل lprm في السطر المذكور أعلاه.

مثال لملف /etc/lpd.perms:

```
## Permissions are checked by the use of 'keys' and matches. For each of
## the following LPR activities, the following keys have a value. ## ## Key Match Connect
Job Job LPQ LPRM LPC
## Spool Print
## SERVICE S 'X' 'R' 'P' 'Q' 'M' 'C'
## USER S - JUSR JUSR JUSR JUSR JUSR
## HOST S RH JH JH JH JH JH
## GROUP S - JUSR JUSR JUSR JUSR JUSR
## IP IP RIP JIP JIP RIP JIP JIP
## PORT N PORT PORT - PORT PORT PORT
## REMOTEUSER S - JUSR JUSR JUSR CUSR CUSR
## REMOTEHOST S RH RH JH RH RH RH
## REMOTEGROUP S - JUSR JUSR JUSR CUSR CUSR
## REMOTEIP IP RIP RIP JIP RIP RIP RIP
## CONTROLLINE S - CL CL CL CL CL
## PRINTER S - PR PR PR PR PR
## FORWARD V - SA - - SA SA
## SAMEHOST V - SA - SA SA SA
## SAMEUSER V - - - SU SU SU
## SERVER V - SV - SV SV SV
## LPC S - - - - - LPC
## AUTH V - AU AU AU AU AU
## AUTHTYPE S - AU AU AU AU AU
## AUTHUSER S - AU AU AU AU AU
## AUTHFROM S - AU AU AU AU AU
```

```
## AUTHSAMEUSER S - AU AU AU AU AU
## ## KEY:
## JH = HOST host in control file
## RH = REMOTEHOST connecting host name
## JUSR = USER user in control file
## AUTH will match (true) if authenticated transfer
## AUTHTYPE will match authentication type
## AUTHUSER will match client authentication type
## AUTHFROM will match server authentication type and is NULL if not from server
## AUTHSAMEUSER will match client authentication to save authentication in job
## ## Example Permissions
## ## # All operations allowed except those specifically forbidden
## DEFAULT ACCEPT
## ## #Reject connections from hosts not on subnet 130.191.0.0
## # or Engineering pc's
## REJECT SERVICE=X NOT REMOTEIP=130.191.0.0/255.255.0.0
## REJECT SERVICE=X NOT REMOTEHOST=engpc*
## ## #Do not allow anybody but root or papowell on
## #astart1.astart.com or the server to use control
## #facilities.
## ACCEPT SERVICE=C SERVER REMOTEUSER=root
## ACCEPT SERVICE=C REMOTEHOST=astart1.astart.com REMOTEUSER=papowell
## ## #Allow root on talker.astart.com to control printer hpjet
## ACCEPT SERVICE=C HOST=talker.astart.com PRINTER=hpjet REMOTEUSER=root
## #Reject all others
## REJECT SERVICE=C
## ## #Do not allow forwarded jobs or requests
## REJECT SERVICE=R,C,M FORWARD
## #
# allow root on server to control jobs
ACCEPT SERVICE=C SERVER REMOTEUSER=root
# allow anybody to get server, status, and printcap
ACCEPT SERVICE=C LPC=lpd,status,printcap
# reject all others
REJECT SERVICE=C
#
# allow same user on originating host to remove a job
ACCEPT SERVICE=M SAMEHOST SAMEUSER
# allow root on server to remove a job
ACCEPT SERVICE=M SERVER REMOTEUSER=root
REJECT SERVICE=M
# all other operations allowed
DEFAULT ACCEPT
```

[etc/hosts.[lpd.equiv/

كانت تلك الملفات تستخدم من قبل مجموعة أدوات الطباعة LPR وتسبب مخاطر أمنية. عند تشغيل مزود الطباعة كان عليك تحديد أي المضيفات يمكنها الوصول إلى الطباعة في /etc/hosts.lpd. وكان عليك أيضاً إضافة أجهزة مضيفة إلى /etc/hosts.equiv.

وقد تم استبدال هذه الملفات الآن في LPRng بملف /etc/lpd.perms.

تمارين

1. شغل printtool وأنشئ رتلاً محلياً جديداً يدعى lp.
2. قم بتخصيص الجهاز /dev/tty10 كجهاز طابعة (لا تنس تنفيذ الأمر chmod 666 /dev/tty10 للسماح بالطباعة على هذا الجهاز). أصبح لديك الآن طابعة افتراضية على النظام لديك!
3. أرسل مهاماً إلى رتل الطباعة باستخدام lpr و pr (أداة ما قبل التنسيق).
4. باستخدام أداة الطابعة الخاصة بالنظام لديك، قم بتعريف عدة أرتال بعيدة:
   - رتل UNIX
   - رتل SMB

   إذا كنت أنت المزود، فتأكد من أن كافة القواعد الملائمة معرفة في /etc/lpd.perms.
   في كل حالة
   - تفقد الملف /etc/printcap. أي الفلاتر مستخدم؟ كيف هو المضيف البعيد معرف؟
   - تفقد الدليل /var/spool/lpd.
5. أوقف مختلف أرتال الطابعات والطابعات ذاتها باستخدام lpc.
6. تفقد محتويات كل رتل باستخدام lpq.
7. **أعد ترتيب** أرتال المهام المحددة باستخدام lprm.