بنام خدا

چک لیست ایمنی لیونکس

بهار ۱۳۹۰

۱-آیا فایل‌ها و پوشه‌های محرمانه و حساس پنهان شده اند؟

- در لینوکس فایل‌ها و پوشه‌ها با اضافه کردن یک نقطه "." به ابتدای نامشان پنهان (Hidden) می‌شوند.
- بنابراین برای مثال فایل "Test" در یک مرورگر فایل نمایش داده می‌شود اما ".Test" نه .
- اکثر کاربران نمی‌دانند که اجرای دستور "ls - a" فایل‌ها و پوشه‌های پنهان را نمایش خواهد داد.
- در حالت گرافیکی هم با زدن همزمان دکمه‌های "Ctrl + H" می‌توانید فایل‌ها و پوشه‌های پنهان را ببینید.
- از خط فرمان هم می‌توانید با اجرای این دستور یعنی mv test .test از آن استفاده کنید.
- تشخیص فایلهای محرمانه و حساس برعهده پشتیبان هر سیستم است.
- باید همواره فایل‌هاي مخفي را کنترل کند. براي مشاهده فایل‌هاي مخفي از یکي از دستورهاي زیرین استفاده کنید :

- **Ls –a**
- **Find / -name '.*' –ls > /file.txt**

۲-آیا یک پسورد قوی و مطمئن انتخاب نموده اید؟

- مي توان با ويرايش تنظيمات مربوط به كلمات عبور در فايل /etc/login.defs بر اساس نوع كار با سرور و درجه ي امنيتي كه براي خود در نظر مي گيريدكاربران را مجبور به داشتن كلمات عبور ايمن كنيد.توضيحات كامل در مورد هر يک ازپارامتر هاي فايلlogin.defsداخل خود فايل و در بالاي هر كدام ازپارامترهاموجودميباشد .

  معمولاً كلمات عبور بايد حداقل ۸ حرفي و شامل حرف - عدد وعلائم باشند. هيچ وقت از كلمات معني دار يا تاريخ هاي مهم استفاده نكنيد.
- گذرواژه راهبر: بايد حداقل ۱۲ حرفي و شامل حرف - عدد و علائم باشند. هيچ وقت از كلمات معني دار يا تاريخ هاي مهم استفاده نكنيد.طول عمر كلمه عبور ۶۰ روز شود.
- گذرواژه كاربر: بايد تركيبي از حروف ؛ اعداد و كاركترهاي ويژه با طول حداقل ۸ كاراكتر
  - in file /etc/login.defs (change value)
  - PASS_MAX_DAYS 60
  - PASS_MIN_DAYS 0
  - PASS_MIN_LEN 12
  - PASS_WARN_AGE 8

۳-آیا نرم‌افزارهای اشتراک فایل حذف شده اند؟

- به عنوان یک قانون ، نرم‌افزارهای اشتراک فایل را نصب نکنید.به عنوان مثال Samba يك بسته نرم افزاري است كه اجازه مي دهد تا فايلها بين Windows وLinux به اشتراك گذاشته شوند.
- همين طور برنامه SSH كه به منظور اتصال از سيستم عامل ويندوز به لينوكس استفاده مي شود به نحوي باعث دسترسي به Core لينوكس و نيز فايل ها برروي پارتيشن هاي مختلف آن مي گردد

- disable file sharing service
- #service smb stop
- Shutting down SMB services: [OK]
- Shutting down NMB services: [OK]

- uninstall smb service
- #rpm -e samba-client
- #rpm -e system-config-samba
- #rpm -e samba-swat
- #rpm -e samba

۴-آیا به روز رسانی سیستم به طور مرتب انجام می گیرد؟

در لینوکس یک به روز رسانی امنیتی ممکن است چند دقیقه یا چند ساعت بعد از شناسایی یک حفره امنیتی منتشر شود.

هم در KDE و هم در Gnome نرم‌افزارهای به روز رسانی در اینترنت وجود دارند. اگر همیشه آنها را در حال اجرا داشته باشید می‌توانید از انتشار به موقع یک به روز رسانی مطلع شوید.

۵-آیا سرویس‌ها و DAEMON های بلااستفاده را غیرفعال نموده اید؟

- سرویس‌هایی مانندftpd ,httpdوsshd ،در صورت عدم استفاده باید غیر فعال شوند. فایل/etc/inetd.conf را چک کنید و مطمئن شویدکه تمام سرویس‌های غیر لازم Comment شده‌اند (اگر اول یک خط # قرار بگیرد آن خط یک Comment یا توضیح به حساب می‌آید و اجرا نمی‌شود).
- همچنين مي توان ازطريق دستور Setup در Terminal سرويس ها را فعال يا غيرفعال نمود.
- هر سرويس كه روي سرور شما فعال باشد و به ديگران اجازه ي وصل شدن به آن و گرفتن اطلاعات به كاربران راميدهد داراي باگ امينتي هست و اگر از آن استفاده نمي كنيد بايد آن رابنديد . خود لينوكس هم يک سري سرويس هاي زائد (daemons)دارد كه براي يک سرويس دهنده ي وب نيازي به آنها نيست .
- سرويس ها را مي توانيد در /etc/xinetd.con ويرايش كنيد .براي مثال سيستم اشتراک فايل (nfs/statd) ياسيستم مديريت پرينت (cupsd).

۵-آیا سرویس‌ها و DAEMON های بلااستفاده را غیرفعال نموده اید؟

- # ps –a — این عبارت تمامي پردازش هاي درحال اجرارا ليست مي كند.
- # netstat –a — این عبارت تمامي پورت هاي باز را مشخص مي كند.
- # chkconfig –list — این عبارت وضعيت فعلي تمامي سرويس ها رانشان مي دهد.
- # service stop nfs — به منظور توقف اجراي سرويس اين دستوررا مي زنيم.
- # netstat –tulp — این عبارت تمامی پورت های شبکه درحال استفاده را ليست می كند.
- براي حذف اسكريپت هاي درحال اجرا اين دستوررا مي زنيم .
- # /bin/mv /etc/rc.d/rc5.d/S25netfs /etc/rc.d/rc5.d/K25netfs

- 5- rename S25netfs
- # mv /etc/rc.d/rc5.d/S25netfs /etc/rc.d/rc5.d/.S25netfs

۶-آیا پروتکل SSH شما امن شده است؟

بهتر است همیشه براي ورود به سرور از public key authentication استفاده شود و هیچ وقت دسترسي SSH را براي عموم باز نگذارید.

همیشه پورت SSH را عوض کنید. معمولا کاربران مزاحم ابتدا به دنبال پورت ۲۲ مي گردند و اگر اطلاعات کافي در مورد سرور شما نداشته باشند از دسترسي به SSH نا امید خواهند شد.

لذا هیچ وقت SSH را روي پورت ۲۲ باز نگذارید. مي توانید پورت SSH را از طریق ویرایش فایل etc/ssh/sshd_config به یک پورت باز دیگر مثلا 2333تغییر دهید.

در همین فایل etc/ssh/sshd_config مي توانید خط Protocol 2 را تایپ کنید.

- **/etc/ssh/ssh_config**

۷-آیا پارتیشن TMP را امن نموده اید؟

اولاً اینکه حتماً باید براي **tmp** پارتیشن ایجادنمائید.

ولي بازهم كافي نيست در قسمت**fstab**سیستم باید**tmp** را حتما با گزینه ي **nosuid**بسازید ویاآن را **mount** کنید. این گزینه باعث میشود که تک تک **proccess** ها با سطح دسترسي **executor** اجرا شوند .

۱- ابتدا مطمئن شوید که تمامی سرویس هایی را که ممکن است در **/tmp** اطلاعاتی بنویسند را متوقف نموده اید.مانند **web server**،**ftpd** و **mysql**

۲-ایجاد یک فایل خالی به منظور **mount** نمودن آن به عنوان **/tmp**

- # mkdir /usr/local/tmppartition
- # cd /usr/local/tmppartition
- ساخت ۱۰۰ مگابایت فضا جهت ذخیره سازی
- # dd if=/dev/zero of=tmpMntbs=1024 count=100000

۳-فرمت نمودن فایل بافایل سیستم

- # /sbin/mke2fs /usr/local/tmppartition/tmpMnt

۷-آیا پارتیشن TMP را امن نموده اید؟

۴- ایجاد یک پشتیبان:

- cp –R /tmp /tmp_backup

۵- Mount نمودن فایل به /tmp

- #mount -o loop,noexec,nosuid,rw /usr/local/tmppartition/tmpMnt /tmp

- rm -rf /temp_backup

۶- بادستور chmod مجوزهای کامل را به آن می دهیم:

- # chmod 0777 /tmp

۷- پشتیبان تهیه شده را کپی می کنیم:

- cp –R /tmp_backup/* /tmp/

۸- پشتیبان را حذف می کنیم:

- rm –rftmp_backup

۷-آیا پارتیشن TMP را امن نموده اید؟

- create temp partition
- # mkdir /temp
- # cd /temp/
- # dd if=/dev/zero of=tempmnt bs=1024 count=100000
- output :
- 100000+0 records in
- 100000+0 records out
- # /sbin/mke2fs /temp/tempmnt
- # mkdir /temp_backup
- # cp /tmp /tmp_backup
- # mount -o loop,noexec,nosuid,rw /temp/tempmnt   /tmp
- # chmod 0777 /tmp
- # cp -R /temp_backup/*   /tmp
- # rm -rf /temp_backup

۸- آیا COMPILERها برای کاربران دیگر غیر فعال شده اند؟

بسیاري از کاربران نمي دانند compiler ها بر روي Host به چه درد مي خورند و اصلا استفاده اي از آنها ندارند پس بهتراست براي همه ي کاربراني که استفاده ندارند آن را disable کنید.

این کار را مي توانید در whm در قسمت Compilers Tweak انجام بدهید. اکثر باگ هاي امینتي کشف شده نیاز دارند تا همان موقع روي سرور compileبشوند.

۹-آیا از MAILDIR به جای MAILBOX استفاده می کنید؟

براي ايميل دونوع ذخيره سازي روي لينوكس داريم.

اولي به صورت mail box و دومي maildir كه گزينه ي دوم از لحاظ امنيتي بسيار بهتراست وباعث افزايش سرعت Mail Server هم ميشود.

البته در نسخه ي جديد cpanel به صورت پيش فرض maildir نصب ميكند.

قبل از آن حتماً از اطلاعاتتان backup بگيريد.

به منظور جلوگیری از دریافت mail ازطریق شبکه فایل /etc/mail/sendmail.cf رااز مسیر مورد نظر به صورت زیر تغییر می دهیم:

SMTP daemon options

- DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA

in file /etc/mail/sendmail.cf edit line

#SMTP daemon options

O DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA

۱۰-آیا پورت ها یا نرم افزار های مشکوکی که روی سرورRUNهستند رابررسی نموده اید؟

دستور netstat -anp لیست کلیه connection های باز سرور را به شما می دهد تا به دنبال پورت ها یا نرم افزار های مشکوکی که روی سرور run هستند ولی شما اجازه اجرا شدن به انها نداده اید را مشاهده کنید و در صورت لزوم بوسیله firewall دسترسی به آنها را مسدود کنید.

به منظور دستیابی به پورتهای سیستم عامل لینوکس دستور زیر را می زنیم :

#netstat -anp --tcp --udp | grep LISTEN

#netstat –anp

#nmap -sT -p0-65535 <server IP>

۱۱-آیا فایل ها و پوشه هایی که دارای بیشترین مجوز هستند را بررسی نموده اید؟

دستور find / -type f -perm 777>> world_writable.txt لیست کلیه فایل هایی را که permission 777 دارند و توسط کلیه کاربران روی سرور قابلیت ویرایش دارند رابه شما نشان میدهد (داخل فایلtxt ذخیره می کند) اکثر مشکلات امنیتی داخل همین پوشه ها اتفاق می افتد

check permission files

#find / -type f -perm 777 > /u01/permission.txt

۱۲-آیا فایل های گزارش سرویس ها تحلیل و بررسی میشوند؟

بادستور **ls /var/log/** اکثر لاگ فایل ها قابل رؤیت هستند ،در صورت نیاز به گزارش از هر سرویس خاصی می توانید در این پوشه به آن مراجعه کنید.به عنوان مثال گزارش وضعیت **Startup** شدن سرویس ها در فایل **boot.log** و یا گزارش ورودبه سیستم در شبکه از طریق نرم افزار **SSH** در فایل **secure** و ...

البته لاگ های **apache** در فولدر **/usr/local/apache/logs** مي باشد

weeklly checking files :

/var/log/messages

/var/log/secure

۱۳-آیا آنتی ویروس مصوب برروی سیستم نصب و به روز رسانی می گردد؟

درست است که امکان ایجاد یک مشکل در لینوکس که دلیلش یک ویروس باشد بسیار کم و در حد صفر است ؛ اما به عنوان مثال ارسال ایمیل می‌تواند مشکل‌ساز باشد.

نسخه تك كاربره آنتي ويروس برروي سيستم عامل لينوكس استفاده مي شود و نسخه تحت شبكه آن در دست پيگيري مي باشد.

۱۴-آیا امنیت فایل های کلیدی بررسی شده است؟

درمورد فایل/etc/fstabمجوززیر بایدتنظیم گردد:

644 (rw-r----)

بررسي گردد كه مالك فايل هاي زير كاربر (root) باشد:

/etc/passwd, /etc/shadow & /etc/group

بررسي گردد كه مجوزفايل هاي /etc/passwd& /etc/group به صورت زير باشد:

rw-r--r-- (644)

بررسي گردد كه مجوزفايل هاي /etc/shadow به صورت زير باشد:

r-------- (400)

check opermission :

/etc/fstab 644 (rw-r--r--)

/etc/passwd 644

/etc/ashadow 400

/etc/group 644

۱۵-آیا دسترسی به برنامه زمانبندی CRON فقط به کاربر ROOT اعطاء شده است؟

براي افزايش امنيت استفاده از Cron فايل هاي Cron.deny و Cron.allow تغيير دهيد.

دستورات زير فقط كاربر root را مجاز به تعريف Job ها روي Cron مي نمايند.

```
# cd /etc/

# rm -f cron.deny at.deny

# echo root > cron.allow

# echo root> at.allow

# chown root:root cron.allow at.allow

# chmod 400 cron.allow at.allow
```

۱۶-آیا برای دسترسی از راه دور از ssh استفاده شده است؟

نسخ پیاده سازی شده SSH ، دارای مجموعه ای از گزینه های انتخابی بوده که مدیران سیستم با استفاده از آنان و با توجه به سیاست های موجود می توانند پیکربندی مناسبی در این خصوص انجام دهند به طور مثال امکان محدودیت در دستیابی به ماشین مورد نظر و اتصال به آن ، روش های تائید کاربران و ماهیت کاربران مجاز ، نمونه هائی از گزینه های انتخابی بوده که می توان از آنان بمنظور پیکربندی مطلوب استفاده گردد.

باید توجه شود که از نسخه هاي قديمي SSHاستفاده نشود و براي ارتقاء آن باید تنظیمات زیررا در فایل sshd_config درج کنیم.

Telnet براي دسترسي از راه دور توصيه نمي شود ،SSH دسترسي رمز شده Telnet را ايجاد مي نمايد.

باید توجه شود که از نسخه هاي قديمي SSHاستفاده نشود وبراي ارتقاء آن باید تنظیمات زیررا در فایل sshd_config درج کنیم.

Protocol 2
PermitRootLogin yes
PermitEmptyPasswords no
Banner /etc/issue

عدم استفاده از فایلهای rhosts و shosts در Authentication

IgnoreRhosts yes

عدم استفاده ازروش هویت شناسی برپایه rhosts توسط SSH

RhostsAuthentication no
RhostsRSAAuthentication no
HostbasedAuthentication no

۱۶-آیا برای دسترسی از راه دور از ssh استفاده شده است؟

مدت زمان انتظار سرور جهت ورود مجدد کاربر قبل ازقطع ارتباط آن

LoginGraceTime 1m (or less – default is 2 minutes)

SyslogFacility AUTH (provides logging under syslog AUTH)

AllowUsers admin,… لیست کاربراني که دسترسي آنها مجاز مي باشد.

DenyUsers لیست کاربراني که مجاز نمي باشند.

MaxStartups 1

edit file /etc/ssh/sshd.config

```
Protocol 2
LoginGraceTime 1m
PermitRootLogin yes
SyslogFacility AUTH
PermitEmptyPasswords no
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
RhostsAuthentication no
AllowUsers root oracle
MaxStartups 1
```

۱۷-آیا از قابلیت SYSTEMLOGGING استفاده می شود؟

قابلیت مذکور به منظور اشکال زدایي از سیستم و مشکلات شبکه استفاده مي شود.

تنظیمات Logging در فایل /etc/syslog.conf ذخیره مي گردد.این فایل سطح Logging و محل فایل هاي گزارشگیري راتعیین مي کند.

مالك این فایل ها کاربر root مي باشد.

براي ممیزي ، تلاش براي ورود ، اجرا کردن SU ، راه‌اندازي مجدد ، و سایر رویدادهاي امنیتي دستور زیرین را در فایل syslog.conf درج کنید :

Auth.info /var/log/auth.log

البته قبلاً فایل /var/log/auth.log را بسازید

check file /etc/syslog.conf (log file path)

۱۸-آیا از داده ها BACKUP تهیه می گردد؟

ابزارهايي نظير tar ،zip و bzip2 همچنان ابزارهاي مناسبي ميباشند.

به منظور تهيه Backup از ليستي از دايركتوريها به يك tar Archive ابتدا فرمان tar را براي ايجاد tarball اجراكنيد و به دنبال آن براي فشرده نمودن آن ، ازدستور gzip استفاده نمائيد.

tar -cvf archive_name.tar dir1 dir2 dir3....

gzip -9 archive-name.tar

backup sterategy : exp/imp Rman standby

۱۹-آیا دسترسی کاربران به SHELL سیستم عامل محدود شده است؟

در اکثر سیستم عامل هاي لینوکس مي توانیدمحدودیت هایي را روي دسترسي هاي shell اعمال کنید .

با استفاده از تنظیماتي که در/etc/security/limits.conf وجود دارد مي توانید محدودیت هاي بسیار جالب رابراي تک تک کاربران shellایجاد کنیدتا استفاده ي نابجاي آنها باعث وارد آوردن فشار بیش از حد به سرور شما و down شدن آن نشود.

برای مشاهده محدودیت های Shell دستور ulimit –a را می زنیم.

/etc/limits.conf (limit user access)

۲۰-آیا BIND DEAMON را غیر فعال نموده اید؟

(به آن named نیز اطلاق می گردد)

بمنظور پیشگیری ازاعمال برخی تغییرات خاص (نظیر فعال نمودن مجدد آن)روی سیستم هائی که بعنوان یک سرویس دهنده DNS در نظر گرفته شده اند می توان نرم افزار BIND را از روی اینگونه سیستم ها حذف نمود.

بدین منظور می توان دستور setup را در terminal اجرا کرده و در قسمت system services سرویس namedرا غیر فعال نمود

diable DNS service (named)

#service named stop

۲۱- آیا banner مربوط به version string را از bind حذف نموده اید؟

بدین منظور فایل named.conf واقع در /etc را باز نموده و در قسمت options

درصورتیکه نسخه Deamon BIND ذکرشده باشد ، تغییرات زیر را اعمال نمایید:

```
options {version " "};
```

۲۲-آیا امکان recursion و glue fetching را در deamon bind غیر فعال نموده اید؟

این عمل بمنظور حفاظت در مقابل عملکرد ناصحیح DNS Cache ، انجام میشود.بدین منظور فایل named.conf واقع در /etc را باز نموده و در قسمت options تغییرات زیر را اعمال نمایید:

```
options {
        recursion no;
        fetch-glue no;
  };
```

۲۳-آیا سرویس های Rpcکه ضرورتی به استفاده ازآن نمیباشد را غیر فعال نموده اید؟

غیر فعال نمودن و یا حذف هر یک از سرویس های RPC که ضرورتی به استفاده از آن بر روی شبکه نمی باشد .

بدین منظور در terminalدستور setup را اجرا کرده و در قسمت system serviceسرویس مورد نظر را غیر فعال کنید.سرویس های مذکور عبارتنداز:

Rpcgssd

Rpcidmapd

Rpcsvcgssd

۲۴-آیا گزینه ی SAFE MODE در فایل PHP.INI را فعال نموده اید؟

این گزینه هر لحظه چک می نماید که فردی که فایلی را اجرا میکند مالک آن است یا خیر و بسیاری دستورات را خود به خود مسدود میکند.

بدین منظور فایل php.ini واقع در /etc را ویرایش نمایید:

Safe_mode = on

in file /etc/php.ini

safe_mode = on

۲۵-آیا VERSION آپاچی و اطلاعات دیگر را مخفی نموده اید؟

در فایل httpd.conf تغییرات زیر را اعمال نمایید.

ServerSignature Off
ServerTokens prod

in file /etc/httpd/conf/httpd.conf
ServerSignature Off
ServerTokens prod

۲۶- آیا SNMP را غیرفعال نموده اید؟

غیر فعال نمودن SNMP در صورت عدم ضرورت استفاده از آن . بدین منظور دستور setupرا در terminal اجرا کرده و در قسمت system services سرویس مورد نظر را غیر فعال می کنیم.

۲۷-آیا پورتهای ۱۶۱ TCP/UDP و ۱۶۲ TCP/UDP را غیر فعال نموده اید؟

در سطح روتر و یا فایروال بلاک نمائید.

(در صورتی که ضرورتی به مدیریت دستگاه ها به صورت خارجی وجود نداشته باشد)

۲۸-آیا امکان استفاده از rsh را غیر فعال می کنید؟

در مواردی سرویس گیرنده ممکن است بدلیل عدم امکان برقراری ارتباط از طریق SSH به عقب برگشته و استفاده از rsh را در این رابطه مفید تشخیص دهد . بمنظور پیشگیری از مواردی اینچنین می بایست به کلید IgnoreRhosts در فایل پیکربندی SSH (sshd_config) ، مقدار yes را نسبت داد.

in file /etc/ssh/sshd.conf

IgnoreRhosts yes

۲۹-آیا پورتهای پورت ۱۱۱ (PORTMAP) و پورت ۲۰۴۹ (RPC.NFSD) راکنترل نموده اید؟

در سطح روتر و یا فایروال بلاک نمائید.

۳۰-آیا ورود به سیستم با سطح دسترسی راهبر محدود شده است؟

درصورتیکه کاربر جدید غیر از root تعریف و دسترسیهاي لازم مانند کاربر oracle جهت کاربران پشتیبان سیستم تخصیص داده شده باشد

۳۱-آیا راهبر (rootکاربر)فقط به کنسول دسترسی دارد؟

منظور اینکه کاربر root فقط از طریق کنسول tty1 وصل شود و با XWindow،SSHو VNC نتواند به سیستم متصل گردد.همچنین مي توان ازطريق Firewall دسترسي توسط VNC Server و SSH را کنترل نمود.

تجربه نشان داده‌است که محدود کردن ورود به سيستم لينوکس با سطح دسترسي راهبر ، از نظر امنيتي بهتر است. زيرا در اين صورت امکان مميزي فعاليت‌ها ميسر بوده و در صورت حمله موفق ، سطح دسترسي نفوذگر نيز محدود خواهد بود. راهبر نيز مي‌تواند بدواً با شناسه کاربر محدود وارد شده و سپس با دستور SU به سطح راهبري دست يابد.

با ويرايش فايل /etc/security مي‌توان پيکربندي مناسبي ايجاد کرد تا راهبر نيز فقط به کنسول دسترسي داشته باشد. اين فايل شامل فهرستي از TTY هاي مجاز است که مي‌تواند براي ورود با نام راهبر مورد استفاده قرار گيرد. محتويات اين فايل بايد /dev/tty1 باشد.

محتويات فايل /etc/security بايد /dev/tty1 باشد

۳۳-آیا فهرست کاربران مجاز بررسی و کاربران زائد حذف گردیده اند؟

روش تعیین کاربران مجاز:

awk –F:’{print “username:” $1}’ /etc/passwd

check users and groups

users: #awk -F: '{ print "username: " $2 }' /etc/passwd

groups: #awk -F: '{ print "groupname:" $1 " Gid:" $3 " member_list:" $4 }' /etc/group

۳۳-آیا کاربران در گروه‌های مجاز قرار داده اید؟

روش تعیین کاربران در لیست هاي مجاز:

awk –F:’{print “GroupName:” $1 “GID:” $3 “MemberList:” $4}’ /etc/group

۳۴-آیا فایل‌های SUID,GUID کنترل میشود؟

براي يافتن و كنترل آنها دستور زيرين را وارد كنيد:

۱.تعيين فايل هايي كه مجوز اجراي آنها در حد گروه مالك آن فايل مي باشد.

Find / -type f –perm -04000 –ls

۲.تعیین فایل هایی که مجوز اجرای آنها درحد کاربر مالک آن فایل می باشد.

Find / -type f –perm -02000 –ls

۳۵-آیا فایل‌هایی که برای نوشتن عموم آزاد است کنترل میشود؟

براي يافتن اين قبيل فايل ها دستور زير را صادر كنيد :

Find / -type f –perm -2 –ls

طريقه گرفتن مجوز در مورد فايل از كاربر ، گروه يا مالك:

chmod a-w install.log

chmod g-x install.log

۳۶-آیا سرویس ftp عقیم واز scp استفاده میشود؟

نحوه غیر فعال کردن سرویس ftp:

service xinetd stop

chkconfigxinetd off

نحوه استفاده از scp:

scp –r /u01 root@10.33.1.x :/u01

۳۷-آیا فایلهای با حجم بزرگ مشخص و کنترل شده است؟

بر عهده پشتیبان می باشد که با توجه به اطلاعات موجود بر روی هر سیستم فایل های بزرگ آن را بررسی نماید.

۳۸-آیا مقدار umask بدرستی تعیین شده است؟

مدیر سیستم باید مقدار صحیح را با علت انتخاب آن بداند ، حداقل مقدار آن باید

۰۰۲۲ باشد که حداقل دسترسي خواندن به group و other داده شود

۳۹-آیا فقط راهبر دارای UID صفر میباشد؟

هر کاربر در یونیکس داراي شماره شناسايي است که اين شماره شناسايي‌ها در فايل /etc/passwd ذخيره شده است. و بيانگر اين است که هر کاربر داراي چه کد شناسايي کاربري « UID » بوده وکد گروه «GID» وي چيست.

توجه داشته باشيد که کد شناسايي « ۰ » متعلق به مدير بوده و دارنده اين کد مي‌تواند تمام مجوزهاي لينوکس را دور بزند بنابراين UID=0 مهمترين کد اشتراك يا شناسايي است.

با صدور دستور زيرين مي‌توان تمام کاربراني را که داراي کد شناسايي صفر هستند مشخص نمود.

```
awk -F: ‘{if ($3==0)print $0} ‘ /etc/passwd
```

۴۰-آیا مد مختلط کنترل شده است؟

راهبر باید با این امر آشنا و به طور متناوب مراتب را کنترل نماید.دستور ifconfig –a را صادر کنید اگر پیام زیر مشاهده شد یك sniffer در حال اجرا است: PROMISC

پایان