به نام خدا

تکلیف عملی سیستم عامل

پیاده سازی network loadable kernel module

امروزه با گسترش دنیای لینوکس کرنل ماژول ها نیز از اهمیت بیشتری برخوردار شده اند و از آن ها در بسیاری از زمینه ها نظیر ساخت rootkit ها و انواع device driver ها استفاده می شود.

لینوکس نقش پررنگی را در دنیای شبکه و اینترنت ایفا می کند لذا وجود ماژول هایی که بتوانند سطح امنیت را در این زمینه بالا ببرند از اهمیت بالایی برخوردار است. در این تمرین با توجه به مطالب ارائه شده در کلاس حل تمرین و سایر منابع معرفی شده سعی داریم تا ماژولی را به منظور فیلتریگ packet ها در سطح شبکه پیاده سازی کنیم.

ماژول پیاده شده در تمرین به منظور اعمال فیلترینگ بر روی packet ها ابتدا یک فایل config را می خواند.خط ابتدایی فایل config نوع فیلترینگ را مشخص خواهد کرد که به دو دسته blacklist و whitelist تقسیم می گردد.

فیلترینگ بر اساس whitelist به این صورت است ماژول تمامی packet های دریافتی را drop می کند مگر آن که آن packet به صورت source_ip:source_port در whitelist نوشته شده باشد و در مقابل فیلترینگ بر اساس blacklist به این صورت است ماژول تمامی packet ها را دریافت می کند جز در مواردی که مشخصات packet به صورت source_ip:source_port در blacklist نوشته شده باشد.

تمامی packet های دریافتی را به همراه زمان در سیستم به صورت لاگ کرنل ماژول ذخیره کنید.

نکته ۱ : kernel module را بر روی لینوکس و حتما به صورت مجازی تست کنید. kernel خود را به کرنل stable تغییر دهید.

نکته ۲ : نحوه پیاده سازی را به صورت دقیق مستند کنید.

نکته ۳: در مورد نحوه ی خواندن فایل و ارسال اطلاعات آن به ماژول محدودیتی وجود ندارد و می توانید به هر نحوی این کار را انجام دهید اما توصیه می شود یک برنامه بنویسید که آدرس فایل را از کاربر بگیرد و اطلاعات آن را برای ماژول(کرنل ماژول کاراکتری) ارسال کند.

نکته ۴:مواردی که باید در سامانه آپلود کنید یک فایل zipبا فرمتname_stdno.zip شامل فایل مستندات در قالب Markdown، سورس کد ها ، makefile و فایل اجرایی ماژول باشد.