پوریا غفوری ۴۰۱۱۰۶۲۷۷

بخش‌های عملی:

توضیحات کامل بخش‌های عملی در فیلم‌های ضبط شده موجود می‌باشد همچنین پرچم‌های هر بخش نیز در فایل flags.txt موجود است.

پیش‌نیاز اجرای exploitها این است که برای exploit2 و exploit4، فایل‌های اجرایی برنامه‌ها دقیقا در کنار exploit باشد و برای exploit3، فایل اجرایی داخل پوشه app و پوشه app در کنار exploit باشد.

سوال اول:

مطابق با اصول دسترسی BLP، عامل‌ها می‌توانند از اشیای با سطوح امنیتی پایین‌تر یا مساوی خود بخوانند و عامل‌ها می‌توانند در اشیای با سطوح امنیتی بالاتر یا مساوی خود بنویسند. ما باید دسترسی‌ها را مطابق با این دو اصل به گروه‌های مختلف واگذار کنیم.

permission	owner	group	File name
rw-rw--w-	root	secret	secret_file
rw-rw-r--	root	unclassified	unclassified_file

مطابق با دسترسی‌های بالا، گروه کاربران به فایل‌های هم‌گروه خود هم دسترسی نوشتن دارند هم خواندن، گروه کاربران secret به فایل‌های unclassified_file که سطح دسرسی پایین‌تر است، دسترسی خواندن دارند و گروه کاربران unclassified به فایل‌های secret_file که سطح دسترسی بالاتری است، دسترسی نوشتن دارند و اصول BLP رعایت شده است.

سوال دوم:

با توجه به اینکه برای تغییر رمز عبور نیاز داریم تا فایل /etc/shadow را تغییر دهیم و این فایل فقط به root دسترسی نوشتن را می‌دهد، پس نیاز داریم تا هنگام اجرای /usr/bin/passwd دسترسی root داشته باشیم تا بتوانیم رمز عبور را تغییر دهیم و چون این برنامه دارای مجوز اجرای بیت setuid است و در کد خود uid را صفر می‌کند (دسترسی root، چون owner فایل کاربر root می‌باشد) در نتیجه هر کاربری با هر سطح دسترسی این برنامه را اجرا کند، این برنامه دسترسی root داشته و می‌تواند فایل shadow را تغییر داده و رمز عبور کاربر مورد نظر را تغییر دهد.

اگر passwd دارای آسیب‌پذیری باشد، باعث می‌شود که یک کاربر با سطح دسترسی پایین‌تر، بتواند از این آسیب‌پذیری بهره برده و به shell با دسترسی root ارتباط بگیرد و سطح دسترسی بالاتری را برای خود فراهم کند و کدهای دیگر و برنامه‌هایی که می‌خواهد را بتواند با این دسترسی اجرا کند.

سوال سوم:

در این ابزار همان‌طور که در صورت سوال اشاره شده از مدل کنترل دسترسی اجباری و نقش-مبنا استفاده می‌شود. این ابزار این قابلیت را می‌دهد که به هر برنامه یک context امنیتی خاص اختصاص داد. به طور مثال passwd در دامنه امنیتی خاصی به نام passwd_t اجرا می‌شود که در این سطح دسترسی صرفا می‌توانیم به /etc/shadow دسترسی داشته باشیم و نه هیچ فایل دیگری. که این باعث می‌شود که حتی اگر برنامه passwd دارای آسیب‌پذیری باشد، با Exploit کردن آن صرفا به همان فایل دسترسی داریم و کار دیگری نمی‌توانیم انجام دهیم (به طور مثال نمی‌توانیم به bin/sh دسترسی داشته باشیم چون passwd_t همچین دسترسی‌ای ندارد). به طور کلی با استفاده از این ابزار، دسترسی‌ها محدودتر شده و حتی اگر برنامه‌ای دسترسی سطح بالا هم داشته باشد، به دلیل برچسب‌هایی که بر روی آن قرار داده شده، باز هم دسترسی کامل آن سطح را نداشته و صرفا می‌تواند در محدوده‌ای که به او اجازه داده شده است فعالیت کند.