

به نام خدا



امنیت داده و شبکه

نیم سال دوم ۱۴۰۴-۱۴۰۳

دانشکده‌ی مهندسی کامپیوتر

دانشگاه صنعتی شریف

موضوع	بهره‌برداری از آسیب‌پذیری برنامه‌ها
موعده تحویل	ساعت ۲۳:۵۹ یک‌شنبه ۲۶ اسفند ۱۴۰۳
طراحی تمرین توسط	محمد حدادیان و رضا سعیدی
با سپاس از	امیرمهدی کوششی

مقدمه

هدف از این تمرین تجربه بیشتر در شناسایی و بهره‌برداری از آسیب‌پذیری‌های برنامه‌ها است. این تمرین از پنج بخش تشکیل شده است. برای چهار بخش اول شما باید ابتدا آسیب‌پذیری برنامه‌ی داده‌شده را پیدا کرده و سپس با نوشتن یک اسکریپت (به هر زبان دلخواه) از آن آسیب‌پذیری سوءاستفاده کرده، به shell دست یابید. در بخش‌های دوم و سوم و چهارم تمرین بعد از دستیابی به shell، به پرچم موجود روی ماشین هدف دسترسی پیدا کنید (هدف اصلی شما دسترسی به پرچم است، گاهی برای دسترسی نیاز است تا دسترسی کامل shell بگیرید و گاهی خواندن محتوای پرچم بدون دستیابی کامل به shell امکان‌پذیر است). پرچم هر بخش به صورت یک رشته به فرمت `CE441{xxxx}` می‌باشد.

۱ بخش اول

۱.۱ راه‌اندازی محیط

برای بخش اول این تمرین، یک ماشین مجازی^۱ در اختیار شما قرار گرفته است. در بهره‌برداری از آسیب‌پذیری‌ها، همه چیز از نسخه‌ی کامپایلر تا مکانیزم‌های امنیتی سیستم‌عامل دخیل خواهند بود. با داشتن این ماشین مجازی، در اجرای اکسپلویت‌های خود یکپارچه خواهید بود.

این ماشین مجازی نسخه‌ی Ubuntu Linux 16.04 LTS با ASLR خاموش است. این ماشین یک کاربر با نام user و رمز ce441 دارد. شما می‌توانید به صورت موقتی با دستور sudo به کاربر root تبدیل شوید اما اکسپلویت‌های شما با دسترسی کاربر user اجرا می‌شوند و باید در آن به shell `/bin/sh` با دسترسی‌های root دست پیدا کنید.

پس از اجرای این ماشین، یک سرویس OpenSSH روی آن اجرا می‌شود که می‌توانید از سیستم خود به این ماشین ssh بزنید یا فایل منتقل کنید: `ssh user@192.168.56.144`

۲.۱ اهداف

در پوشه‌ی `targets/` از ماشین مجازی، کد منبع چند هدف آسیب‌پذیر همراه با `Makefile` آن‌ها برای کامپایل و اجرا قرار داده شده است که شما در بخش اول این تمرین فقط اهداف ۱ و ۲ را باید هدف قرار دهید. برای کامپایل این اهداف دستورات زیر را اجرا کنید:

```
1 cd targets
2 make
3 sudo make install
```

با این دستورات، فایل‌های اجرایی اهداف در آدرس `/tmp` قرار می‌گیرند. دقت کنید که اکسپلویت شما باید این اهداف را دقیقاً در پوشه‌ی `/tmp/target1` اجرا و بهره‌برداری کند. برای حل این بخش تمرین شما باید دنبال buffer overflow در آرایه‌های برنامه‌های هدف باشید؛ هرچند این سرریز بافر ممکن است به صورت کامل در اختیار شما نباشد.

۳.۱ ساختار کد اکسپلویت

پوشه‌ی `sploits/` شامل ساختار موردنیاز برای نوشتن اکسپلویت شما است. همچنین هدر فایل `shellcode.h` شامل shell کد موردنیاز برای حل این بخش از تمرین است که شما باید اکسپلویت‌های خود برای این بخش تمرین را با استفاده از این ساختارها بنویسید.

^۱http://partov.ce.sharif.edu/assets/40441-991/CE441_vm.ova.xz

۲ بخش دوم

۱.۲ راه اندازی محیط

در بخش های دوم و سوم و چهارم این تمرین به منظور فراهم کردن یک محیط یکسان برای exploit کردن آسیب پذیری ها، داکر فایل های در اختیار شما قرار خواهد گرفت تا بتوانید محیط مسئله را روی رایانه ی شخصی خود داشته و تست کنید. این داکر فایل فقط برای تمرین شماسست و تنها در صورتی که روی سرورهای مقصد به پرچم دست یابید نمره ی بخش های مربوطه را کسب می کنید. همچنین برای اینکه داکر فایل به خوبی روی سیستم شما اجرا شود، مطمئن شوید که معماری سیستم شما x86 باشد.

برنامه ی آسیب پذیر در داکر ایمج هایی که در اختیار شما قرار داده شده با پورت مشخص شده اجرا می شوند و شما باید با بهره برداری از آن ها به این ماشین ها دسترسی پیدا کرده و پرچم را بدست آورید. به جهت راه اندازی محیط بر روی رایانه شخصی کافیسست پس از نصب ابزارهای docker به پوشه ی تمرین رفته و آن را build و نهایتاً run کنید. با این دستور محیط تمرین روی سیستم شما بالا آمده و با دستور `nc localhost [port]` می توانید به آن ها متصل شوید. همچنین در صورت نیاز می توانید با کمک دستور `docker exec` از محیط داکر برای بررسی سوالات و بهره برداری از آسیب پذیری ها استفاده کنید.

۲.۲ ابزارها

Pwntools یک کتابخانه ی پایتون است که exploit نویسی را بسیار ساده می کند. در این تمرین از این ابزار برای یافتن gadget ها به صورت خودکار، ساختن ROP chain و موارد مشابه می توانید استفاده کنید. همچنین برای پیدا کردن return address ها می توانید از ابزارهایی مانند gdb و objdump بهره ببرید. برای آشنایی بیشتر با pwntools می توانید به این [سایت](#) مراجعه کنید. همچنین برای خواندن داکيومنت های این کتابخانه می توانید به این [سایت](#) مراجعه کنید. شما نیز می توانید فیلم های متعددی در یوتوب در رابطه با حل سوال با pwntools پیدا کنید. برای آشنایی با gdb می توانید به این [سایت](#) مراجعه کنید. یک اکستنشن خوب و قوی نیز برای کار حرفه ای با gdb به نام gef موجود است که در صورت علاقه نیز می توانید با آن به حل سوالات بپردازید یا راجع به آن مطالعه کنید. شما راجع به این اکستنشن نیز می توانید در این [سایت](#) مطالعه کنید.

۳.۲ هدف

در اهداف هر سه بخش یک فایل باینری به شما داده شده است. به ویژگی های امنیتی این فایل ها توجه کنید. یک راه کار این موضوع استفاده از دستور `checksec` است. برای اتصال به ماشین میزبان این بخش تمرین، از دستور زیر استفاده کنید (چنانچه دسترسی به سرور از داخل ایران مسدود شود، این موضوع تاثیری بر زمان تحویل تمرین ندارد و ضمن اطلاع موضوع از روش های جایگزین برای اتصال استفاده کنید):

```
nc 65.109.201.174 5002
```

در این بخش پس از اتصال هیچ پیغامی چاپ نمی شود و برنامه هدف منتظر ورودی های شماست. اکسپلویت را با بررسی، دیگامپایل و دیباگ فایل های باینری شروع کنید. شما باید با بهره برداری از آسیب پذیری برنامه ی داده شده، به شل دسترسی پیدا کنید و پرچم موجود در ماشین را چاپ کنید. احتمالاً در رسیدن به پرچم پس از سرریز بافر، نیاز به استفاده از کدها و گجت های خود فایل باینری هم خواهید داشت.

۳ بخش سوم

۱.۳ هدف

در هدف این بخش یک فایل باینری به شما داده شده است. به ویژگی‌های امنیتی این فایل توجه کنید. یک راه کار این موضوع استفاده از دستور `checksec` است.

برای اتصال به ماشین میزبان این بخش تمرین، از دستور زیر استفاده کنید:

```
nc 65.109.201.174 5003
```

پس از اتصال به سرور پیامی برای شما چاپ می‌شود و شما امکان تعامل با برنامه را خواهید داشت. شما باید با بهره‌برداری از آسیب‌پذیری برنامه‌ی داده شده، به شل دسترسی پیدا کنید و پرچم موجود در ماشین را چاپ کنید. برای شروع اکسپلویت، چون کد برنامه در اختیار شما نیست بهتر است آن را در ابزارهای دیباگ یا دیکامپایل بررسی کنید. دقت کنید که در این بخش تمرین شل کد در اختیار شما نیست و باید با استفاده از توابع برنامه به هدف برسید.

۴ بخش چهارم

۱.۴ هدف

در هدف مربوط به این بخش هم مانند بخش قبل، یک فایل باینری به شما داده شده است. برخی ویژگی‌های امنیتی این فایل ممکن است متفاوت باشد. با بررسی فایل به حل تمرین بپردازید.

برای اتصال به ماشین میزبان این بخش تمرین، از دستور زیر استفاده کنید:

```
nc 65.109.201.174 5004
```

در این بخش تمرین شما نیاز به گرفتن شل ندارید و هدف اجرای تابع win در این فایل باینری است. مثل همیشه دیکامپایل و دیباگ باینری توصیه اکید می‌شود.

۵ بخش پنجم - سوالات تئوری

۱.۵ کنترل دسترسی

۱. می‌خواهیم یک سیستم کنترل دسترسی اجباری با دو سطح محرمانگی `secret` و `unclassified` را با استفاده از سیستم کنترل دسترسی اختیاری لینوکس شبیه‌سازی کنیم. برای این کار دو گروه با نام دو سطح محرمانگی ساخته و هر کاربر یا فایل را در یکی از این دو گروه قرار می‌دهیم. مجوزهای دو فایل زیر که با علامت سؤال مشخص شده را طوری تعیین کنید که اصول دسترسی BLP رعایت شوند. فرض کنید نیازی به کنترل دسترسی کاربر `root` وجود ندارد.

permission	owner	group	file name
rw-??-??-	root	secret	secret_file
rw-??-??-	root	unclassified	unclassified_file

۲. در سیستم عامل لینوکس، رمز عبور تمام کاربران به صورت رمز شده در فایل `/etc/shadow` نگهداری می‌شود. این فایل تنها توسط کاربر `root` قابل دسترسی و تغییر است. اگر کاربر بخواهد رمز عبور خود را تغییر دهد، باید از برنامه `/usr/bin/passwd` استفاده کنید. مجوز اجرای این برنامه دارای بیت `setuid` است. توضیح دهید این ویژگی چگونه امکان تغییر رمز کاربر را فراهم می‌کند و در صورتی که `passwd` دارای آسیب‌پذیری باشد، باعث چه خطر امنیتی می‌شود.

۳. ابزار SELinux برای تکمیل سیستم کنترل دسترسی لینوکس طراحی شده و امکان استفاده از مدل کنترل دسترسی اجباری و نقش-مبنا را فراهم می‌کند. توضیح دهید چگونه می‌توان از این ابزار از خطر مطرح شده در سؤال قبل پیشگیری کرد.

۶ تحویل دادنی‌ها

شما باید برای هر بخش، اسکریپت خود برای بهره‌برداری از آسیب‌پذیری سوال را به همراه یک ویدیو جامع برای هر بخش، که شامل توضیح اسکریپت و نحوه‌ی رسیدن به اطلاعات لازم برای حل و ساخت shell است ارسال کنید. ویدیوهای خود را در سایت‌های میزبانی فایل مانند گوگل درایو قرار داده و فقط لینک آن‌ها را همراه با hash ویدیو در cw ارسال کنید. ساختار فایل زیپ ارسالی شما با نام **ce441-hw1-SID** باید به شکل زیر باشد:

```
1 sploit1-1.c
2 sploit1-2.c
3 exploit2.py
4 exploit3.py
5 exploit4.py
6 urls.txt
7 theory.pdf (if any document is needed)
```

فراموش نکنید که دسترسی فایل در سرویس گوگل درایو برای عموم آزاد باشد. لازم است در گزارش به طور خلاصه‌ی مراحل‌ی که طی کرده‌اید را به همراه پرچم نهایی (پرچم روی سرور) گام به گام ذکر کنید. همچنین توضیحات مورد نیاز برای نحوه‌ی اجرای اسکریپت‌ها و پیش‌نیازهای آن را نیز به طور کامل در گزارش ذکر کنید. دقت کنید که اسکریپت‌های شما باید به صورت مستقل توسط ما اجرا شده و به پرچم برسد تا نمره‌ی آن بخش را کسب کنید. در صورت داشتن هرگونه سوال در مورد این تمرین می‌توانید با ایمیل **m.hadadian76@sharif.edu** یا تالارهای گفتگوی درس در cw در ارتباط باشید.