به نام خدا

درس امنیت داده و شبکه

نیم‌سال اول ۱۴۰۱-۱۴۰۰

دانشکدهٔ مهندسی کامپیوتر

دانشگاه صنعتی شریف

مدرس **مهدی خرازی**

موضوع **بهره‌برداری از آسیب‌پذیری برنامه‌ها**

موعد تحویل **ساعت ۲۳:۵۹ پنج‌شنبه ۲۹ مهر ۱۴۰۰**

طراحی چالش توسط **سارا عسگری**

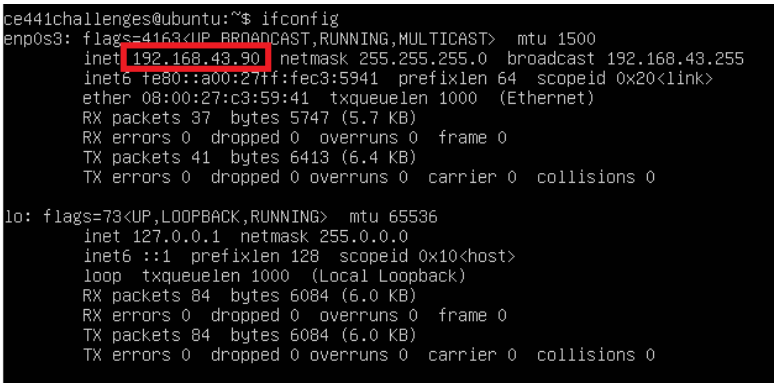
با سپاس از **محمد حدادیان**

۱ مقدمه

هدف از این چالش تجربه بیشتر در شناسایی و بهره‌برداری از آسیب‌پذیری‌های برنامه‌ها است. این چالش از دو بخش تشکیل شده‌است. برای هر بخش شما باید ابتدا آسیب‌پذیری برنامه‌ی داده‌شده را پیدا کرده و سپس با نوشتن یک اسکریپت (به هر زبان دلخواه) از آن آسیب‌پذیری سوءاستفاده کرده و به shell دست یابید. به منظور سهولت در شناسایی و بهره‌برداری از این آسیب‌پذیری‌ها علاوه بر فایل باینری، کدمنبع [1] نیز در اختیار شما قرار داده شده‌است. فایل‌های مربوط به بخش یک و بخش دو به ترتیب در پوشه‌های part۱ و part۲ در ماشین مجازی‌ای که در اختیار شما قرار داده شده‌است در دسترس هستند.

۱.۱ راه‌اندازی محیط

به منظور فراهم کردن یک محیط یکسان برای exploit کردن آسیب پذیری‌ها یک ماشین مجازی در اختیار شما قرار داده شده‌است. روی این ماشین مجازی Ubuntu server 20.04.3 نصب شده‌است. همچنین مجموعه‌ای از ابزارهای موردنیاز شما از جمله pwntools و gdb روی این ماشین مجازی نصب شده‌است. شما می‌توانید بسته به نیاز نرم افزارهای دیگری را نیز روی این ماشین مجازی نصب کنید. در این ماشین مجازی ASLR غیرفعال شده‌است. این ماشین مجازی را از این لینک دریافت کنید و در VirtualBox ، import کنید. برای این کار در منوی فایل روی import appliance کلیک کرده و سپس `ce441chal.ova` را انتخاب کنید. پس از روشن کردن این ماشین مجازی با نام کاربری `ce441chal` و کلمه عبور `ce441` وارد شوید و با دستور ifconfig همان‌گونه که در شکل ۱ مشاهده می‌کنید آدرس IP این ماشین را به دست بیاورید. دقت کنید که تنظیمات شبکه‌ی ماشین مجازی بر روی bridge بوده و adapter مناسب را انتخاب کنید.



شکل ۱: دستور ifconfig برای به دست آوردن ip ماشین مجازی.

روی این ماشین مجازی سرور OpenSSH در حال اجرا است. بنابراین شما با استفاده از آی‌پی‌ای که در مرحله‌ی قبل به دست آوردید و با دستور `ssh ce441chal@vm_ip` می‌توانید به این ماشین مجازی وصل شوید.
برای انتقال فایل از ماشین مجازی به ماشین خود یا بالعکس می‌توانید از scp استفاده کنید. لازم به ذکر است که کلمه عبور root نیز ce441 است.

۲.۱ ابزارها

Pwntools یک کتابخانه‌ی پایتون است که exploit نویسی را بسیار ساده می‌کند. در این چالش از این ابزار برای یافتن gadget ها به صورت خودکار، ساختن ROP chain و موارد مشابه می‌توانید استفاده کنید. استفاده از هیچ کتابخانه‌ای برای پیدا کردن return address ها مجاز نیست ولی می‌توانید از ابزارهایی مانند gdb و objdump بدین منظور بهره ببرید.

[1] Souce Code

۲ بخش اول

در این بخش یک فایل باینری ۶۴ بیتی به همراه کد منبع آن به شما داده شده‌است که ویژگی‌های امنیتی آن را می‌توانید در شکل ۲ مشاهده کنید:

```
Arch:     amd64-64-little
RELRO:    Partial RELRO
Stack:    Canary found
NX:       NX disabled
PIE:      No PIE (0×400000)
```

شکل ۲: ویژگی‌های امنیتی برنامه ۱.

در این باینری از قناری برای محافظت در برابر حمله سرریز بافر استفاده شده است. هدف از این بخش، تمرین دور زدن محافظت‌های امنیتی با بهره‌برداری از چند آسیب‌پذیری در یک برنامه است. این برنامه‌ی ساده دچار دو آسیب‌پذیری format string و سرریز بافر است. شما باید با سوءاستفاده از آسیب‌پذیری format string قناری را به دست آورده و سپس با بهره‌برداری از آسیب‌پذیری سرریز بافر به shell دست یابید.

۳ بخش دوم

در این بخش یک فایل باینری ۳۲ بیتی به همراه کدمنبع آن به شما داده شده‌است که ویژگی‌های امنیتی این برنامه در شکل ۳ نشان داده شده‌است:

```
Arch:     i386-32-little
RELRO:    Partial RELRO
Stack:    No canary found
NX:       NX enabled
PIE:      No PIE (0×8048000)
```

شکل ۳: ویژگی‌های‌امنیتی برنامه ۲.

همان گونه که مشاهده می‌کنید ویژگی NX [۲] برای این باینری فعال است. در این بخش شما با ساختن زنجیره ی ROP برای اجرای `execve("/bin/sh",0,0)` باید به shell برسید.

۴ تحویل‌دادنی‌ها

شما باید یک ویدئو با حجم حداکثر ۴۰ مگابایت و مدت زمان حداکثر ۱۵ دقیقه تهیه کنید و در این ویدئو مراحلی که برای حل هر یک از بخش‌ها طی نموده‌اید را نشان داده و توضیح دهید. در این ویدئو نکات مهم شامل آسیب‌پذیری آن برنامه، منطق exploit ی که نوشته‌اید و مراحلی که برای به دست آوردن آدرس‌ها یا سایر موارد طی کرده‌اید را گام به گام نشان داده و توضیح دهید. این ویدئو را در یکی از سرویس‌های میزبانی فایل مانند Google Drive آپلود کنید و سپس لینک آن را در یک فایل به نام links.txt در پوشه‌ی `chals/chal1` قرار داده و این فایل را در مخزن خود در طرشت push کنید. به علاوه اسکریپت‌های خود را به همراه یک گزارش که نحوه‌ی اجرای اسکریپت‌ها به صورت کامل در آن توضیح داده شده‌است را در همین پوشه از مخزن خود در طرشت push کنید.

[2] Non-eXecutable