پیک پرومتیم

پرومتیوم (Promethium) از عنصرهای شیمیایی جدول تناوبی با عدد اتمی آن ۶۱ است. در بین ۹۲ عنصر اول جدول تناوبی فقط دو عنصر تکنسیم (۴۳) و پرومتیم (۶۱) در طبیعت یافت نمی‌شوند. یکی از دلایل این موضوع این است که به‌طور کلی عناصر با عدد اتمی فرد تعداد ایزوتوپ‌های پایدار کم تری نسبت به عناصر با عدد اتمی زوج دارند.

فهرست مطالب

فصل ۱ نکات ۱

فصل ۲ مفاهیم مربوط به هک ۲

۱.۲ یک مقاله! ۲

۲.۲ پیاده‌سازی Mirai ۲

۳.۲ شما هم داستان خودتان را بگویید ۴

۴.۲ حمله Heap Overflow ۴

۵.۲ پیاده‌سازی یک بدافزار ۵

مراجع ۶

فهرست اختصارات ۷

واژه نامه انگلیسی به فارسی ۸

واژه نامه فارسی به انگلیسی ۹

۱ نکات

در تحویل این تمرین به نکات زیر دقت کنید:

- پاسخ تمرین‌ها می‌بایست به صورت یک گزارش به زبان فارسی و در قالب LaTeX باشد. کدهای پیاده‌سازی را نیز در کنار فایل گزارش قرار دهید و به صورت یک فایل با پسوند zip، در سامانه قرار دهید.
- تمامی پیاده‌سازی‌ها می‌بایست با زبان Python صورت پذیرد.
- تمرین‌ها به صورت گروهی و تنها توسط یک نفر از اعضای گروه تحویل داده می‌شود. نیازی نیست هر یک از اعضای گروه جداگانه تمرین را در سامانه قرار دهد.
- به هیچ‌وجه کپی نکنید. در صورت مشاهده هرگونه کپی، نمره کل تمرین دو یا چند گروه درگیر، برابر با صفر خواهد شد.
- تمرین به صورت کامل باید در موعد مقرر تحویل داده شود. در صورت تاخیر، سیاست کسر نمره بیان شده در کلاس اعمال خواهد شد.

۲ مفاهیم مربوط به هک

۱.۲ یک مقاله!

به سایت کنفرانس Blackhat مراجعه کنید، یک موضوع را هر گروه باید انتخاب کند، و یک گزارش از آن تهیه کند.

- موضوعات انتخاب شده، می‌بایست برای هر گروه متفاوت باشد،. این موضوع نباید مشابه موضوعاتی باشد که در فصل اول درس بیان شد. لطفا هر گروه موضوع انتخابی خودش را به نماینده کلاس اطلاع دهید. تا بازه انتخاب موضوع، هر گروه موضوع خودش را ارسال می کند. در صورتی‌که دو گروه موضوع یکسانی داشته باشند، قرعه‌کشی انجام خواهد شد، و از گروه بازنده خواهیم خواست که موضوع دیگری را انتخاب کند.
- موضوعات انتخاب شده، باید برای کنفرانس Blackhat از 2020 به بعد باشد.
- از شما دو خروجی دریافت می‌شود. یک خروجی یک گزارش است که این گزارش با زبان فارسی در قالب کنفرانس کامپیوتر با LaTeX، باید باشد. گزارش شما باید بین چهار تا شش صفحه باشد. همچنین یک ارایه ۱۵ دقیقه‌ای باید از این گزارش داشته باشید. این ارایه باید به صورت PowerPoint یا ارایه صداگذاری شده یا هر روش دیگر تولید محتوایی.
- مقاله انتخاب شده به همراه گزارش (فایل PDF کافی است) و همچنین فایل ارایه، باید در نهایت در سامانه سامیا قرار داده شود.
- برای مشاهده مقالات این پیوند شاید مفید باشد.

۲.۲ پیاده‌سازی Mirai

در این پروژه از شما خواسته شده است به نوعی بدافزار[1] Mirai را پیاده‌سازی کنید. از شما می‌خواهیم که دو برنامه با Bash لینوکس بنویسید. اجازه دهید برنامه Bash اول را Bash Attacker Side و برنامه Bash دوم را Bash Victim نامگذاری کنیم. در ادامه به نیازمندی‌ها و نکات زیر دقت کنید.

❶ در Bash Attacker Side، می‌بایست بتوانید کل واسط‌ها[2]ی شبکه را شناسایی کنید. در واقع باید به طور مثال برای خروجی هر واسط در دستوری به مانند ifconfig، تمام کلاس‌های IP[3] را بتوانید شناسایی کنید. سپس ببینید که کدام IPها در دسترس است و می‌توان به آن متصل شد.

[1] Malware
[2] Interface
[3] Internet Protocol

❷ یافتن شماره درگاه[۴]های باز و ذخیره‌سازی آن در یک فایل CSV. برای دست‌یابی به این مهم، سعی کنید با دستورات لینوکس در این حوزه آشنا شوید و از آن استفاده کنید. این مورد باید در Bash Attacker Side، پیاده‌سازی شود.

❸ اتصال به Deviceهای یافت شده و تست فهرستی از نام کاربری[۵] و رمز عبور[۶] معمول. این فهرست را از یک فایل CSV که در کنار برنامه قرار می‌گیرد، بخوانید. دقت کنید این مورد باید در Bash Attacker Side، پیاده‌سازی شود.

❹ وقتی به دستگاه قربانی متصل شدید، تلاش کنید که فایل دوم اجرایی یعنی Bash Victim را از یک خدمت‌گزار[۷] دانلود کنید. یک راه‌کار پیدا کنید که Bash Victim در هر بار شروع به کار سیستم‌عامل[۸]، به طور خودکار کار خود را آغاز کند.

❺ Bash Victim در دستگاه قربانی در بازه‌های مشخصی اطلاعات متعددی (نوع و نسخه لینوکس، مدل پردازنده، تاریخ و زمان دستگاه، میزان فضای اشغالی هارددیسک) را به یک خدمت‌گزار مشخص ارسال می‌کند. ببینید دیگر چه اطلاعاتی می‌توانید بگیرید و ارسال کنید. تلاش کنید اطلاعات بیشتری را کسب کنید. این‌هایی که بیان شد، صرفا حکم یکسری نمونه را دارد. در ضمن بهتر است این اطلاعات رمزشده و یا به طریقی ارسال شود که کسی در بین راه متوجه آن نشود. در ضمن برنامه شما یعنی همان bash دوم باید به صورت متناوب چک کند که ارتباط اینترنت و ارتباط به خدمت‌گزار موردنظر آیا برقرار هست یا نه؟ اگر برقرار هست داده‌ها را ارسال کند.

❻ Bash Victim، باید واسط مربوط به اینترنت را شناسایی کند، در صورتی که در یک شماره درگاه مشخص، بسته‌ای ارسال یا دریافت می‌شود را بگیرید و شنود کند، سپس آن را در یک فایل ذخیره کند. خود بسته لازم نیست در فایل ذخیره شود. فقط کافی است آدرس IP مبدا و مقصد بسته و همچنین شماره درگاه مبدا و مقصد و شناسه برنامه‌ای که دارد این بسته‌ها را ارسال می‌کند یا همان PID در لینوکس به همراه زمان این رخداد در یک فایل ذخیره کند.
پس به طور خلاصه، Bash Victim، دو سری اطلاعات به سمت خدمت‌گزار ارسال می‌کند. یک مورد همان اطلاعات عمومی به مانند نوع و نسخه لینوکس، مدل پردازنده، تاریخ و زمان دستگاه، میزان فضای اشغالی هارددیسک است، و دومین سری اطلاعات همین مورد اخیر که بیان شد. یعنی دریافت و استخراج اطلاعات بسته‌ها از یک شماره درگاه معین. هر دوی این اطلاعات به سمت خدمت‌گزار ارسال می‌شود، و احتمالا باید در یک پایگاه داده[۹] در دو جدول مجزا ذخیره شود.

❼ در سمت خدمت‌گزار، هم یک برنامه بنویسید که اطلاعات دریافت شده را در یک برنامه تحت وب نمایش دهد. پس برای این کار باید یک Backend و Frontend ساده بنویسد.

برای تست این سامانه می‌توانید ایده‌های جذاب خودتان را دنبال کنید. مثلا در یک حالت خیلی ساده می‌توانید سه VM بالا بیاورید. یکی برای محل قرارگیری و اجرای Bash Attacker Side، دیگری که در حقیقت نماد دستگاه[۱۰] قربانی است و محل اجرای Bash Victim. در نهایت نیز یک VM برای خدمت‌گزار دریافت اطلاعات از قربانی‌ها.

نکته

دقت کنید که نمره این پروژه به صورت مقایسه‌ای و نسبی داده می‌شود. تقلب کردن عملا میزان نمره شما و گروه مقابل را پایین می‌آورد. در ضمن این پروژه ارایه حضوری نیز خواهد داشت.

[4] Port Number
[5] Username
[6] Password
[7] Server
[8] Operating System
[9] Database
[10] Device

۳.۲ شما هم داستان خودتان را بگویید

در فصل اول، تعدادی داستان در حوزه امنیت تعریف کردیم. در این تمرین می‌خواهیم که شما هم داستان خود را بگویید. در این تمرین از هر گروه خواسته شده است که یک داستان زیبا و جذاب در حوزه امنیت را به صورت خلاصه در طی حداکثر دو صفحه (بدون احتساب تصاویر احتمالی) بنویسد. تمام داستان‌ها در اختیار همه قرار خواهد گرفت و هر گروه موظف است به گروه‌های دیگر نمره بدهد. نمره نهایی مجموع وزن‌داری از نمرات دستیاران آموزشی و نمره گروه‌ها به یکدیگر خواهد بود.

- داستان باید به زبان فارسی باشد و نباید Copy-Paste از جایی باشد. باید به زبان خودتان بیان شود.
- همه داستان‌ها باید واقعی و درست و همراه با مرجع باشد.
- داستان گروه‌ها نباید یکسان و یا مشابه باشد. لطفا هر گروه داستان انتخابی خودش را به نماینده کلاس اطلاع دهید. تا بازه انتخاب داستان ، هر گروه داستان خودش را ارسال می کند. در صورتی‌که دو گروه داستان یکسانی داشته باشند، قرعه‌کشی انجام خواهد شد، و از گروه بازنده خواهیم خواست که داستان دیگری را انتخاب کند.
- داستان نباید مشابه داستان‌هایی باشد که در فصل اول بیان شد.

۴.۲ حمله Heap Overflow

در مورد حمله[۱۱] Heap Overflow توضیح دهید؟ این حمله چگونه کار می‌کند؟ می‌توانید با یک مثال مطلب را به خوبی تشریح کنید.

[11] Attack

۵.۲ پیاده‌سازی یک بدافزار

در این سوال از شما خواسته شده است تا یک بدافزار بنویسید. البته در نوشتن آن به نکات زیر دقت کنید:

- بدافزار شما باید یک ویروس یا کرم[۱۲] باشد. پس باید ویژگی تکثیر پذیری داشته باشد.
- حتما باید به زبان C یا C++ باشد.
- علاوه بر کد خروجی، باید به طور کامل در گزارش توضیح دهید که بدافزار شما چگونه کار می‌کند و چه راه‌هایی برای انتشار آن وجود دارد؟
- بدافزار شما باید یک اثر تخریبی بر روی کامپیوتر قربانی داشته باشد! گروه‌های مختلف تلاش کنند تا در این زمینه هم نوآوری داشته باشند و هم بتوانند بدترین اثر تخریبی را داشته باشند.

[12] Worm

مراجع

فهرست اختصارات

I

IP . . . . . Internet Protocol

واژه‌نامه انگلیسی به فارسی

A

Attack ..... حمله

D

Database ..... پایگاه داده

Device ..... دستگاه

I

Interface ..... واسط

M

Malware ..... بدافزار

O

Operating System ..... سیستم‌عامل

P

Password ..... رمز عبور

Port Number ..... شماره درگاه

S

Server ..... خدمت‌گزار

U

Username ..... نام کاربری

W

Worm ..... کرم

واژه‌نامه فارسی به انگلیسی

ب

بدافزار ..... Malware

پ

پایگاه داده ..... Database

ح

حمله ..... Attack

خ

خدمت‌گزار ..... Server

د

دستگاه ..... Device

ر

رمز عبور ..... Password

س

سیستم‌عامل ..... Operating System

ش

شماره درگاه ..... Port Number

ک

کرم ..... Worm

ن

نام کاربری ..... Username

و

واسط ..... Interface