روز صفرم

ماهنامه علمی

سال سوم / شماره بیست‌وسوم / اسفندماه ۰۰

انجمن رمزایران
iranian Society of Cryptology

این ماهنامه با حمایت مادی و معنوی اداره کل امور فرهنگی دانشگاه اصفهان چاپ و منتشر شده است.

نشریه علمی روز صفرم
شماره ۲۳ - اسفند ۱۴۰۰

صاحب امتیاز:
شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان

سردبیر:
محمد آقائی

مدیر مسئول:
الهه رهبران

طراح جلد و صفحه‌آرا:
نوریه سادات مدنیان
محمد آقائی

هیئت تحریریه:
زهرا اشرفی
فراز زوراوند
حسین علی‌ترکان
امیر فیض

اخبار:
سروش ذوالفقاری

ویراستار:
الهه رهبران

t.me/SBISC

SBISC.UI.AC.IR

t.me/CTFPREP

twitter.com/SBISC1

instagram.com/SBISC_UI

درباره انجمن:

شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان از سال ۱۳۸۶ فعالیت خود را پیرامون مباحث مرتبط با امنیت اطلاعات آغاز کرد. این انجمن که هم‌اکنون یازده دوره از آغاز فعالیت آن می‌گذرد، تصمیم به انتشار نشریه‌ای با عنوان "**روز صفرم**" گرفته است تا از این طریق بتواند دانش امنیتی در فضای سایبر را به مخاطبان خود منتقل کند.این نشریه به صورت ماهانه و از اردیبهشت ۹۸ منتشر شده است.


نوروز مبارک باد
انجمن رمز ایران

Fuzz Testing

فازینگ (آزمون فاز)

Fuzzing (Fuzz Test)

زهرا اشرفی
ashrafi.zahra81@gmail.com

فازینگ چیست؟

فازینگ، یک تکنیک تست نرم‌افزار خودکار است که سعی می‌کند باگ‌های نرم‌افزاری قابل هک را با تغذیه تصادفی ورودی‌ها و داده‌های نامعتبر و غیرمنتظره به یک برنامه کامپیوتری و به‌منظور یافتن خطاهای کدگذاری و حفره‌های امنیتی پیدا کند. خطاهای پیدا شده، مناطقی را نشان می‌دهد که به طور بالقوه در معرض خطر بالای تهدیدات امنیتی هستند. نام "فاز" اشاره‌ای به ماهیت تصادفی این فرایند است. حامیان Fuzz Testing آن را به دلیل کاملا خودکار بودن و یافتن نقاط ضعف مبهم، تحسین می‌کنند؛ درحالی‌که مخالفان شکایت دارند که راه‌اندازی آن دشوار است و مستعد ارائه نتایج غیرقابل اعتماد است.

به طور خلاصه می‌توان گفت فازینگ، هنر پیدا کردن اشکالات و باگ‌های نرم‌افزاری به صورت خودکار و رفع این خطاها در صورت امکان می‌باشد.

فازینگ بر خلاف دیگر روش‌های تست، در دسته Negative Testing قرار می‌گیرد. تست Negative تستی است که Robustness یا دوام یک برنامه را تست می‌کند. در مقابل، Positive Testing به بررسی Featureها و Performance برنامه می‌پردازد. کاربرد اصلی فازینگ در پیدا کردن آسیب‌پذیری‌های مختلف در برنامه‌هاست. درحالی‌که دیگر روش‌های تست، موارد زیر را بررسی می‌کنند:

- تست Feature: بررسی این‌که آیا یک قابلیت بر روی نرم‌افزار به درستی مهیا شده است یا خیر (مثلا قابلیت ساخت حساب کاربری در یک سامانه).
- تست Performance: بررسی این‌که آیا نرم‌افزار کارایی لازم را دارد یا خیر (مثلا انجام عملیات ذخیره‌سازی در دیتابیس در یک زمان قابل قبولی انجام می‌شود یا خیر).

فازینگ، هم مورد استفاده هکرهایی که به دنبال آسیب‌پذیری برای سوءاستفاده هستند و هم مدافعانی که سعی در پیدا کردن و رفع آن‌ها دارند، قرار می‌گیرد.

تاریخچه‌ی فازینگ

در یک عصر طوفانی در سال ۱۹۸۸، بارتون میلر(Barton Miller)، استاد علوم کامپیوتر در دانشگاه ویسکانسین-مدیسون، در آپارتمان به‌وسیله Dial-Up یک ارتباط از راه دور با کامپیوتر یونیکسی خود برقرار کرده بود. او در حال دادن ورودی‌های مختلف به یک برنامه بود ولی مشاهده می‌کرد که ورودی‌های او باعث Crash کردن برنامه می‌شوند. با بررسی‌هایی که انجام داد، متوجه شد ورودی‌های او به واسطه نویزهای حاصل از طوفان، دچار تغییر می‌شوند. به این صورت که ورودی‌های آقای میلر به هنگام عبور از خطوط تلفن، مختل می‌شدند. از آن‌جایی که این ورودی‌ها دچار اختلال شده بودند، برنامه مذکور را دچار اختلال و Crash می‌کردند، چرا که برنامه انتظار چنین ورودی‌هایی را نداشت. لغت فاز (Fuzz) نیز به همین دلیل

انتخاب شد. فاز همان اختلالاتی است که در خطوط تلفن رخ می‌دهد.
این اتفاق از آن‌جایی برای دکتر میلر عجیب بود، که حتی برنامه‌هایی که مقاوم به نظر می‌رسیدند، با ورودی‌های مختل شده و غیرمنتظره، Crash می‌کردند. حداقل از برنامه‌های پخته و مقاوم انتظار می‌رفت تا در برابر چنین ورودی‌هایی، دچار خطا نشوند. بنابراین این ایده به ذهن آقای میلر رسید که به صورت عامدانه، اقدام به دادن ورودی‌های نامعتبر و غیرمنتظره به برنامه‌های تحت تست کند تا بتواند به این شکل، باگ‌های موجود در این برنامه‌ها را شناسایی کند.
درواقع نگرانی میلر در مورد آن‌چه که در طول تجربه طوفان دید، فراتر از خراب شدن برنامه‌ها به‌طور غیرمنتظره بود. برنامه‌هایی که قادر به مدیریت ورودی غیرمنتظره نیستند، مشکلات و نگرانی‌های امنیتی ایجاد می‌کنند. خطاهایی که توسط برنامه کنترل نمی‌شوند، آسیب‌پذیری‌هایی هستند که مهاجمان می‌توانند برای هک کردن سیستم‌ها از آن‌ها استفاده کنند.

فازینگ در دنیای امروز

از اوایل کشف تصادفی در دهه ۱۹۸۰، Fuzzing به یک تکنیک بسیار مورد توجه برای آزمایش نرم‌افزار برای قابلیت اطمینان در زمانی که با ورودی غیرمنتظره یا نامعتبر تحت فشار قرار می‌گیرد، تبدیل شده است. بزرگترین کاربرد Fuzzing، آزمایش مسائل مربوط به قابلیت اطمینان یا آسیب‌پذیری‌های امنیتی است. حالت غیرمنتظره‌ای که نرم‌افزار می‌تواند در هنگام برخورد با ورودی‌های غیرمنتظره در آن باقی بماند، اغلب شرایطی عالی برای یک مهاجم برای اصلاح داخلی یک برنامه و دستیابی به اهداف خود ایجاد می‌کند.

کاربرد فازینگ

ابزارهای SAST کد برنامه را در حالت ایستا (بدون اجرا کردن برنامه) بررسی می‌کنند و اشتباهات شناخته‌شده‌ای را که می‌توانند منجر به آسیب‌پذیری‌های امنیتی شوند، اسکن می‌کنند، درحالی‌که ابزارهای DAST با اجرای برنامه اشکالات را پیدا می‌کنند. فازینگ مشابه DAST است زیرا بررسی می کند که یک برنامه در حال اجرا چگونه با دریافت ورودی های مختلف رفتار می‌کند. اما انواع دیگری از خطاها وجود دارد که ابزارهای SAST و DAST قادر به تشخیص آن‌ها نیستند. دیوید دسانتو(David DeSanto)، مدیر امنیت محصولات در GitLab، مثالی از یک قطعه کد ارائه کرد که مقدار مشخصی از حافظه را برای یک آرایه اختصاص می‌داد، سپس به خواندن مقداری فراتر از فضای اختصاص داده شده به آرایه پرداخت. این نوع خطا یک برنامه را از کار می‌اندازد و آسیب‌پذیری‌های امنیتی را معرفی می‌کند، اما در نوع خطاهای کدی که ابزارهای SAST و DAST به دنبال آن هستند، گنجانده نشده است. با این حال، یافتن این نوع باگ برای Fuzzer آسان است.

مزایا و معایب فازینگ

به دلیل ماهیت تصادفی تست فاز، کارشناسان می‌گویند که این روشی است که به احتمال زیاد باگ‌هایی را پیدا می‌کند که توسط تست‌های دیگر از قلم افتاده‌اند. این تست، به عنوان روش آزمایشی بسیار کم تلاش، شناخته می‌شود و امروزه در مسائل مختلف امنیتی بسیار پرکاربرد می‌باشد. اما با این حال، این تست معایبی نیز دارد. برای مثال، تنها خطاها یا تهدیدات ساده را شناسایی می‌کند و برای اجرای موثر، به زمان نسبتا زیادی نیاز دارد. از مهم‌ترین سختی‌های کار با این تست می‌توان به این نکته اشاره کرد که تنظیم یک شرط مقدار مرزی با ورودی‌های تصادفی، کار سختی است، اما امروزه با استفاده از الگوریتم‌های قطعی مبتنی بر ورودی‌های کاربران، اکثر آزمایش‌کنندگان این مشکل را حل می‌کنند.

در مهندسی نرم‌افزار، تست Fuzz وجود باگ را در یک برنامه نشان می‌دهد. Fuzzing نمی‌تواند تشخیص کامل باگ‌ها را در یک برنامه تضمین کند؛ اما اطمینان می‌دهد که برنامه قوی و ایمن است، زیرا این تکنیک به افشای بیشتر آسیب پذیری‌های رایج کمک می‌کند.

منابع:
- History, fuzzinginfo.wordpress.com
- Fuzzing, security.tosinso.com
- Fuzzing, owasp.org
- What is fuzz testing, about.gitlab.com
- fuzz testing, guru99.com

کنترل دسترسی در سیستم‌های ابری

Security & Access Control in Cloud Computing Systems

فراز زوراوند

farazzvdd@gmail.com

رایانش ابری چیست؟

به‌طور کلی ارائه سرویس‌ها و منابع مختلف از طریق اینترنت را رایانش ابری می‌نامند. از جمله این منابع، می‌توان به ابزارها و کاربردهایی چون حافظه، سرورها، پایگاه‌داده‌ها، شبکه و نرم‌افزار اشاره کرد. برای مثال، به کمک ذخیره‌سازی مبتنی بر ابر، به‌جای نگه‌داری فایل‌ها روی فضاهای ذخیره‌سازی محلی یا هارد درایو، می‌توان آن‌ها را روی یک پایگاه‌داده راه دور[1] ذخیره کرد. برای دسترسی به این داده‌ها و نرم‌افزارهای لازم برای استفاده از آن‌ها از طریق یک دستگاه الکترونیکی، کافی است این دستگاه به اینترنت دسترسی داشته باشد. رایانش ابری بنا به دلایلی از جمله صرفه‌جویی در هزینه‌ها، افزایش بهره‌وری، سرعت و بازدهی، کارایی و امنیت، یک گزینه مناسب برای افراد و کسب‌وکارها است.

مزایای رایانش ابری

• اولین مزیت رایانش ابری که به ذهن می‌رسد، احتمالاً جابجایی‌پذیری[2] آن است. این به این منظور است که قابلیت استفاده از نرم‌افزار از طریق هر دستگاهی که اتصال مناسب به اینترنت داشته باشد، به کمک مرورگر و یا برنامه بومی[3] وجود خواهد داشت.

• رایانش ابری به صرفه‌جویی در هزینه‌ها منجر می‌شود. عدم نیاز به اقلام فیزیکی و سخت‌افزاری بخش بزرگی از هزینه‌ها را کاهش می‌دهد. همچنین پرسنل متخصص برای نگه‌داری و کار با این اقلام نیز از لیست هزینه‌ها حذف می‌شود.

• سرعت استقرار[3] سرویس‌ها روی فضای ابری بسیار بیش‌تر است. رایانش ابری این امکان را می‌دهد که سرویس مدنظر با سرعت بسیار بیش‌تری مستقر شود. این استقرار سریع‌تر باعث می‌شود منابع مورد نیاز سیستم در مدت کم‌تری در دسترس قرار گیرند.

• قابلیت اطمینان[4] یکی از بزرگ‌ترین مزایای میزبانی ابری[5] است. بروزرسانی‌های موجود در لحظه در دسترس قرار می‌گیرند.

• پشتیبان‌گیری و بازنشانی[6] هنگامی که داده روی ابر ذخیره شده باشد، راحت‌تر و سریع‌تر است.

معایب رایانش ابری

• وقتی در یک فضای ابری کار کنید، برنامه شما روی سروری اجرا می‌شود که به طور هم‌زمان منابع مورد نیاز دیگر کسب‌وکارها را نیز فراهم می‌کند. در نتیجه در صورت استفاده نامناسب از این سرویس ابری و همچنین با حملات DDoS به آن، عملکرد منبع مشترک شما تحت تاثیر قرار می‌گیرد.

• در رایانش ابری اتصال با کیفیت به اینترنت ضروری است. بدون اینترنت نمی‌توان به ابر دسترسی داشت و هیچ راه دیگری برای جمع‌آوری اطلاعات از ابر وجود ندارد.

• برای استفاده از ابر، باید زمان از کار افتادگی[7] نیز در نظر گرفته شود. ارائه‌دهنده‌ها ممکن است با مشکلات اینترنت، برق، نگه‌داری سیستم و غیره مواجه شده و در نتیجه به طور موقت از کار بیافتند.
• در برخی موارد شرکت‌های ارائه‌دهنده خدمات ابری در ارائه پشتیبانی مناسب برای مشتریان خود با مشکل مواجه می‌شوند. به‌علاوه، این شرکت‌ها تمایل دارند که کاربران برای رفع اشکالات خود به بخش سوالات رایج و پشتیبانی آنلاین تکیه کنند، که این کار می‌تواند برای افراد غیرفنی چالش‌برانگیز و خسته‌کننده باشد.
• تهدیدات و خطرات امنیتی یکی دیگر از چالش‌ها و گاه، معایب مهم کار با سیستم‌های ابری است.

کنترل دسترسی در سیستم‌های ابری

اکثر محصولات مدیریت هویت و دسترسی[7]، روش‌های مختلفی را برای پیاده‌سازی چارچوب‌های کنترل دسترسی به منابع سازمانی فراهم می‌کنند. با این وجود، همه اَشکال کنترل دسترسی را می‌توان در چهار دسته مرسوم دسته‌بندی کرد که عبارت اند از کنترل دسترسی اختیاری، اجباری، مبتنی بر نقش و مبتنی بر ویژگی. در ادامه به توصیف کلی هر یک از این دسته‌ها می‌پردازیم.

• کنترل دسترسی اختیاری
در این روش، کنترل دسترسی به منابع، با توجه به درخواست‌کننده و قواعد دسترسی انجام می‌شود. قواعد دسترسی تعیین می‌کنند که هرکدام از درخواست‌کننده‌ها اجازه انجام چه کارهایی را دارند و چه کارهایی برای آن‌ها غیرمجاز است. برای مثال مدیر می‌تواند به‌طور دل‌خواه به یک کاربر دیگر اجازه دسترسی به یک برنامه را بدهد.

• کنترل دسترسی اجباری
این روش دسترسی را با مقایسه برچسب‌های امنیتی با عناوین امنیتی (از جمله محرمانه، سری، فوق سری) کنترل می‌کند. از این روش معمولاً برای حفاظت از اطلاعات محرمانه در سیستم‌های نظامی استفاده می‌شود.

• کنترل دسترسی مبتنی بر نقش
دسترسی در این روش، بر اساس نقش‌هایی که درون سیستم به کاربران اختصاص داده شده است و قواعدی که تعیین می‌کنند چه دسترسی‌هایی برای هر نقش از نقش‌های کاربران مجاز است، کنترل می‌شود.

• کنترل دسترسی مبتنی بر ویژگی
منظور از ویژگی، مقادیر یا خصوصیات یک موجودیت درگیر در عمل دسترسی است. در فرایند کنترل دسترسی مبتنی بر ویژگی، این ویژگی‌ها با قوانین وضع شده مقایسه می‌شوند. این قوانین تعیین می‌کنند که چه ترکیباتی از ویژگی‌ها به منزله مجاز بودن یک عمل دسترسی به منابع هستند. در این روش، کنترل دسترسی می‌تواند بر پایه سه نوع ویژگی مختلف انجام شود: ویژگی‌های کاربر، ویژگی‌های مربوط به اپلیکیشن یا سیستمی که قرار است دسترسی به آن کنترل شود و همچنین شرایط محیطی فعلی. در مقایسه با سه روش قبلی، این روش انعطاف‌پذیرترین، قدرتمندترین و البته پیچیده‌ترین روش کنترل دسترسی به سیستم‌های ابری است. در واقع ABAC می‌تواند هر سه روش دیگر کنترل دسترسی را به‌طور ضمنی پوشش دهد. سیستم‌های توزیع شده، مناسب‌ترین سیستم‌ها برای استفاده از سیستم کنترل دسترسی مبتنی بر ویژگی هستند.

برای مثال فرض کنید قاعده زیر برای کنترل دسترسی وجود دارد:
«اگر درخواست‌کننده نقش شغلی از مجموعه ارتباطات دارد، باید دسترسی خواندن و ویرایش استراتژی‌های رسانه‌ای را در واحد خود داشته باشد.»
در این صورت، هنگامی که یک درخواست دسترسی ارسال می‌شود، سیستم ABAC مقادیر ویژگی‌ها را تحلیل می‌کند. اگر این مقادیر با مقادیر تعیین شده در قواعد دسترسی مطابقت داشته باشد، اجازه دسترسی صادر می‌شود و برعکس. این اتفاق تا زمانی که این تطابق پا بر جا باشد، باید رخ دهد.

مزایای کنترل دسترسی مبتنی بر ویژگی

• ایجاد قواعد دقیق و با جزئیات بالا، و در عین حال انعطاف‌پذیر
• سازگاری با کاربران جدید
• امنیت و حریم خصوصی سخت‌گیرانه

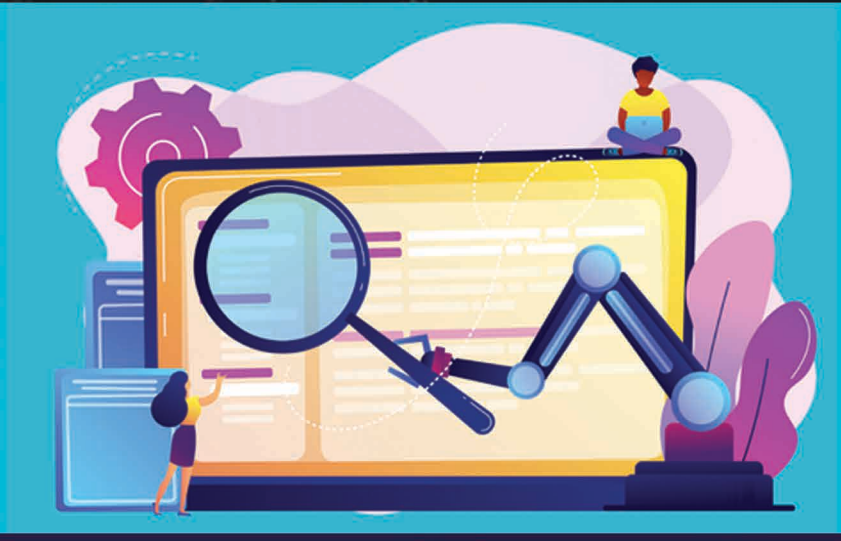
معایب کنترل دسترسی مبتنی بر ویژگی

مزایای کنترل دسترسی مبتنی بر ویژگی به قدری مهم هستند که معایب آن قابل چشم‌پوشی باشد. با این حال مهم‌ترین ایرادی که می‌توان به این روش کنترل دسترسی وارد دانست، پیچیدگی در پیاده‌سازی است.

بنابراین، کنترل دسترسی مبتنی بر ویژگی، به مدیران سیستم اجازه می‌دهد که کنترل با دقت و جزئیات بالا و بر پایه قاعده بر دسترسی به سیستم پیاده‌سازی کرده و از ترکیبات مختلف ویژگی‌ها برای ایجاد شرایط دسترسی مختص به یک وضعیت خاص استفاده کنند.

[1] Remote
[2] Mobility
[3] Native
[4] Deployment
[5] Reliability
[6] Cloud hosting
[7] Restore
[8] Downtime

منابع:
• Cloud computing, investopedia.com
• Survey on Access Control Mechanisms in Cloud Computing, riverpublishers.com
• RBAC vs ABAC Access Control Models, blog.identityautomation.com
• What Is Attribute-Based Access Control (ABAC)?, otka.com



هوش مصنوعی در امنیت

Artificial Intelligence in Security

حسین علی‌ترکان

h.alitorkan1380@gmail.com

امروزه هوش مصنوعی یکی از موضوعات پرمخاطب در دنیای تکنولوژی است و ترکیب آن با حوزه‌های مختلف باعث گسترده شدن کاربرد آن شده است. سیستم‌هایی که هوش مصنوعی در آن‌ها استفاده می‌شود با انجام موردها و اتخاذ تصمیمات هوشمند بدون دخالت انسان شناخته می‌شوند که این کار با استفاده از یادگیری از اطلاعات و تجربه‌های گذشته همانند انسان و الگوسازی ممکن است. در حوزه امنیت نیز می‌توان از این کاربرد هوش مصنوعی در بخش‌های مختلف استفاده کرد و باتوجه به گسترده و پیچیده شدن حملات، استفاده از هوش مصنوعی در امنیت در بعضی مواقع الزامی است. در ادامه به صورت کلی به این موضوع می‌پردازیم.

هوش مصنوعی در امنیت چگونه است؟

هوش مصنوعی در امنیت شامل مواردی می‌شود که در آن‌ها سیستم بدون دخالت انسان بتواند با استفاده از یادگیری از اطلاعات و تجربیات، تصمیمات هوشمندانه بگیرد. ابزار هوش مصنوعی اغلب برای شناسایی فعالیت خوب و بد با استفاده از مقایسه فعالیت‌های ورودی در محیط نسبت به محیط‌های مشابه هستند. این فرایند سیستم را قادر می‌سازد یادگیری کند. در سطح پیشرفته‌تر، کاربرد هوش مصنوعی می‌تواند فراتر از این باشد و به تجزیه و تحلیل حجم وسیعی از اطلاعات بپردازد و مجموعه‌ای از فعالیت‌های مخرب مرتبط را تشخیص داده و عمل مناسب را انجام دهد یا بهترین گزینه‌ها را پیشنهاد کند و در نهایت از نتیجه‌ها برای یادگیری بیشتر استفاده کند. بر اساس یک نظرسنجی، ۶۹ درصد شرکت‌ها معتقد بودند که استفاده از هوش مصنوعی برای امنیت بیشتر لازم است و از هر چهار مدیر مورد بررسی، سه نفر می‌گویند که هوش مصنوعی به سازمان‌شان اجازه می‌دهد سریع‌تر به نقص‌ها پاسخ دهد.

چرا هوش مصنوعی در امنیت مهم است؟

• یکی از دلایل استفاده از هوش مصنوعی در امنیت می‌تواند کاهش نیروی کار انسانی لازم باشد. همیشه یکی از چالش‌های شرکت‌ها استخدام نیروی خوب است و همیشه کمبود نیروی کار مناسب احساس می‌شود. این امکان وجود دارد که با استفاده از هوش مصنوعی بخشی از این کمبود را جبران کرد. می‌توان با استفاده از این ابزار بسیاری از کارها مانند کشف تهدیدها را سریع‌تر از قبل انجام داد. درحالی‌که نیروی انسانی ممکن است دچار خطا شود و زمان بیشتری نیاز دارد، شاید همه منابع خطر را نتواند بررسی کند و هزینه‌ها را افزایش دهد.

مهاجمان اغلب تاکتیک‌های خود را تغییر می‌دهند، اما بهترین شیوه‌های امنیتی اساسی معمولا زیاد تغییر نمی‌کنند. اگر شخصی را برای انجام این وظایف استخدام کنید، ممکن است در طول مسیر خسته شود. یا ممکن

است احساس نارضایتی کند و یک وظیفه امنیتی مهم را از دست بدهد و شبکه شما را افشا کنند. هوش مصنوعی ضمن تقلید از بهترین ویژگی‌های انسانی و کنار گذاشتن کاستی‌ها، از فرایندهای امنیت سایبری تکراری مراقبت می‌کند که می‌تواند بررسی تهدیدهای امنیتی اساسی و جلوگیری از آن‌ها را به طور منظم انجام دهد. همچنین شبکه شما را به صورت عمیق تجزیه و تحلیل می‌کند تا ببیند آیا حفره‌های امنیتی وجود دارد که می‌تواند به شبکه شما آسیب برساند یا خیر.

• علاوه‌بر این، تجزیه و تحلیل و بهبود وضعیت امنیت سایبری دیگر یک مشکل در مقیاس انسانی نیست.
در بحث جلگیری از نفوذ، علاوه‌بر یافتن فعالیت‌های خطرناک و شناسایی، پاسخگویی سریع به آن‌ها هم اهمیت زیادی دارد. هوش مصنوعی و یادگیری ماشین (ML) به فناوری‌های حیاتی در امنیت اطلاعات تبدیل شده‌اند، زیرا می‌توانند به سرعت میلیون‌ها رویداد را تجزیه و تحلیل کنند، انواع مختلفی از تهدیدات را شناسایی کنند، خطرهای آن‌ها را پیش‌بینی کنند، درصد خسارات را تخمین بزنند و بر این اساس بهترین روش‌ها را پیشنهاد دهند و علاوه‌بر این‌ها می‌توانند یادگیری داشته باشند و عملکرد خود را بهبود بخشند. از حمله یا کدهای مخرب در طول زمان یاد می‌گیرند و از گذشته برای شناسایی انواع جدید حملات در حال حاضر استفاده می‌کنند. با استفاده از تاریخچه رفتار، پیش‌فرض‌هایی را برای کاربران، دارایی‌ها و شبکه‌ها ایجاد می‌کنند و به مسئولان اجازه می‌دهند تا انحرافات از هنجارهای تعیین شده را شناسایی کرده و به آن‌ها پاسخ دهند.

• یکی دیگر از مزایای استفاده از AI در امنیت، شناسایی بهتر حملات ناشناخته و زیرو دی (zero day) است. هر ساله تعداد بسیار زیادی حمله با استفاده از روش‌های مختلف از جمله مهندسی اجتماعی پیچیده تا حملات بد افزار به شرکت‌ها صورت می‌گیرد که بسیاری از آن‌ها می‌توانند جدید باشند. بنابراین شناسایی و دفع آن‌ها توسط انسان ممکن است خیلی زمان‌بر، سخت، پرهزینه و گاها غیر ممکن باشد و استفاده از ابزار جدید می‌تواند به متخصصان کمک کند خطرات را با هزینه کمتری دفع کنند. هوش مصنوعی ثابت کرده است که یکی از بهترین فناوری‌ها در نقشه‌برداری و جلوگیری از تهدیدات ناشناخته برای ویران کردن یک شرکت است.

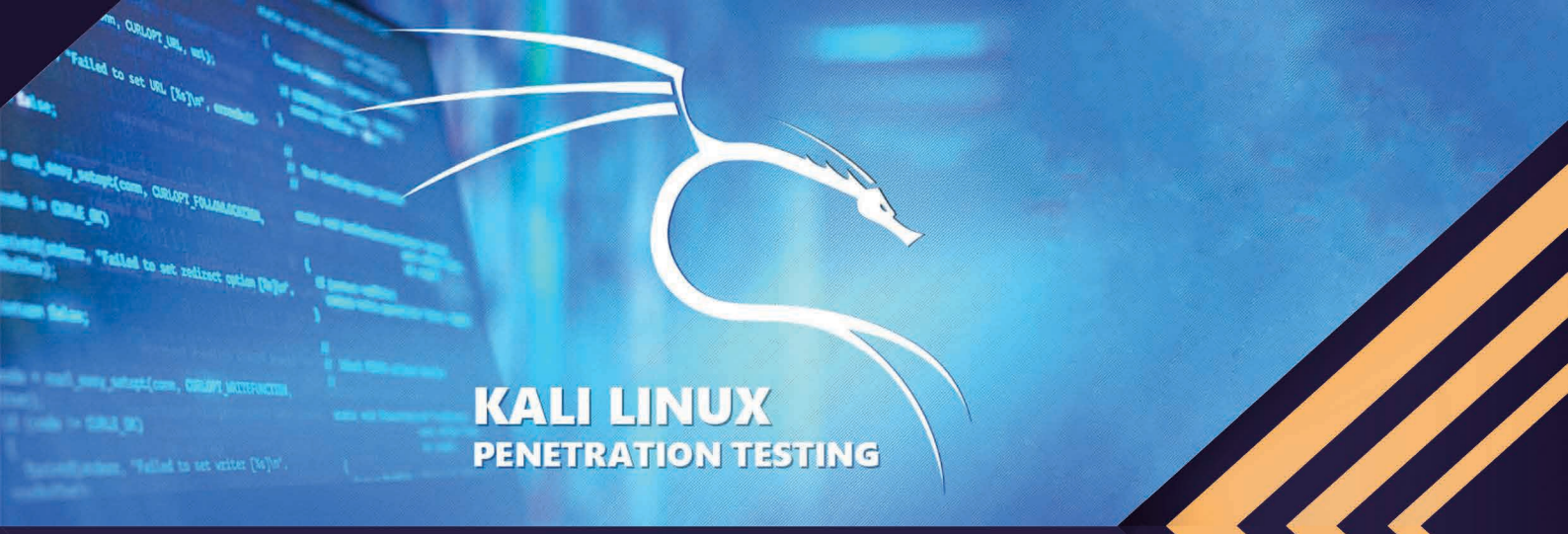
• یکی دیگر از مواردی که هوش مصنوعی می‌تواند در حوزه امنیت مفید باشد، احراز هویت است. قطعا یکی از مهم‌ترین بخش‌های هر سیستمی قسمت احراز هویت کاربران است و اگر امنیت این بخش به درستی فراهم نشود می‌تواند خطرات زیادی به دنبال داشته باشد. از این رو همواره تلاش بر این بوده است که راه‌های احراز هویت را از لحاظ امنیتی ارتقا ببخشند و در این راستا هوش مصنوعی در مواردی مانند تشخیص چهره و حسگرهای اثر انگشت و دیگر ابزار شناسایی می‌تواند بسیار مفید و کارآمد باشد و عمل تشخیص واقعی بودن یا نبودن را انجام دهد. همچنین هوش مصنوعی در تهیه کپچا و تایید آن نیز کاربرد دارد.
البته این ابزارها نمی‌توانند به‌طور کامل جایگزین نیروهای انسانی شوند و تکیه بیش از حد بر روی آن‌ها خطرناک است زیرا این ابزارها هنوز قادر به پیاده‌سازی همه متودولوژی‌های مورد نیاز برای دفاع نیستند.

استفاده از هوش مصنوعی توسط هکرها و خطرات آن

با این حال، مانند هر چیز دیگری، استفاده از هوش مصنوعی در زمینه امنیت نیز دارای معایبی است. به‌منظور ایجاد و حفظ یک سیستم هوش مصنوعی، سازمان‌ها به منابع و سرمایه‌گذاری‌های مالی بیشتری نیاز دارند. از آن‌جایی که سیستم‌های هوش مصنوعی با استفاده از مجموعه داده‌ها آموزش می‌بینند، باید مجموعه‌های متمایز زیادی از کدهای بدافزار، کدهای غیرمخرب و ناهنجاری‌ها را به دست آورد. بدون حجم عظیمی از داده‌ها و رویدادها، سیستم‌های هوش مصنوعی نتایج نادرست و مثبت کاذب ارائه می‌دهند که می‌تواند به پیش‌بینی‌های نادرست منجر شود که برای سیستم خطرناک است. دستیابی به همه این مجموعه داده‌ها زمان‌بر است و نیاز به سرمایه‌گذاری‌هایی دارد که اکثر سازمان‌ها قادر به پرداخت آن نیستند.
همان‌طور که برای افزایش امنیت و دفاع و تعقیب حمله‌ها می‌توان از هوش مصنوعی استفاده کرد، مهاجمان نیز می‌توانند از این ابزار برای حمله و شکستن دفاع‌ها و اجتناب از شناسایی و تولید و تجزیه و تحلیل بدافزارهای هوشمند استفاده کنند که می‌تواند بسیار خطرناک باشد.
با وجود رشد این تکنولوژی و بهبود آن، استفاده از آن‌ها همچنان خطراتی دارد. یادگیری ماشینی و هوش مصنوعی می‌توانند به محافظت در برابر حملات سایبری کمک کنند، اما هکرها می‌توانند با هدف قرار دادن داده‌هایی که روی آن‌ها آموزش می‌دهند و پرچم‌های هشداری که به دنبال آن هستند، الگوریتم‌های امنیتی را خنثی کنند. به گفته Accenture، هوش مصنوعی متخاصم باعث می‌شود مدل‌های یادگیری ماشین، ورودی‌های سیستم را اشتباه تفسیر کنند و به گونه‌ای رفتار کنند که برای مهاجم مطلوب باشد.
به عنوان مثال، ابزار تشخیص هویت «FaceID» آیفون از شبکه‌های عصبی برای شناسایی چهره‌ها استفاده می‌کند و مهاجم می‌تواند آن را در معرض حملات هوش مصنوعی قرار دهد. هکرها می‌توانند تصاویر متخاصم ایجاد کنند تا ویژگی‌های امنیتی Face ID را دور بزنند و به راحتی بدون جلب توجه به حمله خود ادامه دهند. همچنین با استفاده از سیستم‌های هوش مصنوعی می‌توان از سد کپچا نیز گذشت که خطرات سیستم‌ها را در برابر حملات افزایش می‌دهد.

در نهایت باید این ابزار نوین و قدرتمند را در کنار روش‌های قدیمی مورد توجه قرار دهیم و آن را از جنبه‌های مختلف هم برای رشد و توسعه سیستم و هم از نظر خطرات احتمالی مورد بررسی قرار دهیم تا بتوانیم سیستم را به‌روز نگه داریم، در برابر خطرات و حملات جدید حفظ کنیم و نیازهای مورد نظر را به نحو مناسب برطرف کنیم.

منابع:
• ai-security, awakesecurity.com
• artificial intelligence in cybersecurity, balbix.com



تست نفوذ با کالی

Penetration Test with Kali (PWK)

امیر فیض
amir.feiz.1381@gmail.com

اول از همه باید گفت تست نفوذ با کالی به چه سودی دارد و چگونه می‌توان با کالی به سیستم‌های مختلف نفوذ کرد؟

تست نفوذ برای مهندسان امنیت و شبکه کاربرد بیشتری دارد؛ یافتن اطلاعات و درجه‌بندی آن‌ها از مهم‌ترین قسمت‌های نفوذ است. تمام این قسمت‌ها از پشت میز مهندس امنیت یا هکر اتفاق نمی‌افتند؛ بعضی اوقات تماس مستقیم هم لازم است. در برخی از موارد نفوذکننده با هدف تماس گرفته و مقداری از اطلاعات را با چرب زبانی از وی می‌گیرد. در برخی موارد هم با فرستادن لینک‌های مخرب به هدف، به سیستم او نفوذ می‌کند. برای مثال در شرکت X مردی کار می‌کند که چند ماه به بازنشستگی‌اش مانده است، این مرد حدود ۲۰ سال است که منشی مدیر شرکت است. می‌توان حدس زد که مرد حدود ۶۰ سال سن دارد. بنابراین به احتمال زیاد از فضای مجازی اطلاعات زیادی ندارد. به تازگی یاد گرفته که چگونه ایمیل بفرستد و یا ایمیل‌هایش را بخواند. تیم نفوذگر مدتی او را زیر نظر می‌گیرند و تا حدودی متوجه اطلاعات گفته شده می‌شوند. کمی تحقیق بیشتر باعث می‌شود که متوجه علاقه شدید مرد به گربه‌ها شوند. کمی بعد متوجه می‌شوند مرد به خیریه‌ای که به گربه‌های خیابانی کمک می‌کنند پول می‌دهد. کار اصلی اینجا آغاز می‌شود.

تیم نفوذگر با جعل اسم و لوگوی خیریه و با ایمیلی که بسیار نامش شبیه به شرکت است به مرد ایمیل می‌دهند که ما کمی پول اضافه از شما دریافت کرده‌ایم و چون خیریه ورشکست شده پول اهدایی شما را برمی‌گردانیم، برای وارد کردن اطلاعاتتان لطفا بر روی لینک کلیک کنید. از این‌جا به بعد محتوای لینک بستگی به هدف گروه دارد، هدف اول این است که با استفاده از فیشینگ حساب مرد خالی شود؛ اما در این مقاله بحث ما نفوذ است، بنابراین گروه PDF پرداخت جعلی را برای مرد ارسال می‌کنند. اما فایل ارسالی قابلیت باز شدن ندارد؛ مرد در پاسخ ایمیلی ارسال می‌کند که فایل باز نمی‌شود. در این مرحله مهم‌ترین اطلاعات در دسترس گروه قرار می‌گیرد. چگونه؟ پس از باز نشدن فایل خراب گروه از مرد می‌خواهند که سیستم عامل دستگاهش، نسخه PDF Reader و از این قبیل اطلاعات را برای آن‌ها ارسال کند. سپس با اطلاعات کامل شروع به نوشتن بدافزار می‌کنند و سپس یک فایل PDF که حامل این بدافزارها است برای مرد ارسال می‌کنند و نفوذ به شرکت آغاز می‌شود. لطفا توجه کنید که سناریو بالا واقعی نیست و برای پیاده‌سازی آن مشکلات بسیار زیادی وجود خواهد داشت و وقت زیادی باید صرف شود.

برای این‌که به یک امنیت‌کار موفق با کالی تبدیل شوید چند قدم از این مسیر را برای شما آماده کرده‌ایم.

اول از همه باید بگویم همیشه نمی‌توان این‌طور فکر کرد که هک کردن از پشت میز و توسط یک نابغه کامپیوتر صورت می‌گیرد و نمی‌توان گفت آن فرد تمامی اسکریپت‌های کالی یا بقیه ابزارها را حفظ است. عموما هک کردن و نفوذ موفق حاصل تلاش شبانه‌روزی و امتحان راه‌های مختلف است. باید گفته شود که برخی از هک‌ها توسط تلفن و لو رفتن اتفاقی رمز توسط یک کارمند ساده اتفاق می‌افتد بنابراین فکر نکنید هر هکر یک نابغه تمام عیار است، ولی مطمئن باشید هر مهندس هک و امنیت موفق یک فرد بسیار تلاشگر است.

مرحله اول: آشنایی با کالی لینوکس

کالی یکی از توزیع‌های اصلی لینوکس بر پایه دبیان است که افراد مختلفی که در زمینه هک و امنیت فعالیت دارند از این توزیع استفاده می‌کنند. کالی دارای ابزارهای بسیار زیادی است (ظاهرا بیش از ۳۰۰ هزار ابزار!) و با دانش اندکی می‌توان از هر یک بهره برد.

بش (Bash) چیست؟ یکی از جدیدترین shellهای لینوکس که به‌صورت پیش‌فرض در اکثر توزیع‌ها وجود دارد بش نام دارد. حالا ممکن است بپرسید shell چیست؟ تقریبا می‌توان گفت shell در لینوکس همان خط فرمان ویندوز است که با تایپ اسکریپت‌ها و زدن دکمه Enter دستورات ارسال می‌شوند و یک امنیت‌کار موفق باید به صورت کامل کار با Bash را بلد باشد. برای آشنایی بیشتر یک مثال کار با Bash در ادامه آورده‌ایم.

بر فرض مثال شما می‌خواهید فایل html یک سایت را دانلود کنید مثل سایت آردوینو؛ برای این کار با استفاده از دستور wget این کار را همانند تصویر انجام می‌دهیم.

```
┌──(kali㉿kali)-[~]
└─$ wget www.arduino.cc
--2022-03-17 11:47:26--  http://www.arduino.cc/
Resolving www.arduino.cc (www.arduino.cc)... 104.18.28.45, 104.18.29.45, 2606:4700::6812:1c2d, ...
Connecting to www.arduino.cc (www.arduino.cc)|104.18.28.45|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.arduino.cc/ [following]
--2022-03-17 11:47:27--  https://www.arduino.cc/
Connecting to www.arduino.cc (www.arduino.cc)|104.18.28.45|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

index.html.1                                [ <=>

2022-03-17 11:47:28 (2.88 MB/s) - 'index.html.1' saved [4543]
```

همان‌طور که در تصویر مشاهده می‌کنید فایل دانلودی با عنوان index.html.1 ذخیره شده است.

با توجه به مثال بالا می‌توان گفت کار Bash تا حدودی آسان کردن کار برای امنیت‌کار است که توسط اسکریپت‌نویسی انجام می‌شود.

سرویس های مهم:

۱- SSH (Secure Shell): شل ایمنی یا SSH یکی از رایج‌ترین سرویس‌ها برای دسترسی ریموت به یک کامپیوتر به صورت رمزنگاری شده است.

۲- HTTP: در طی فرایند تست نفوذ بارها به کار می‌آید و به‌صورت پیش‌فرض به پورت ۸۰ گوش می‌دهد.

مرحله دوم: تمرین و تکرار

هیچ دو نفوذی همانند هم نیستند؛ سناریوهای مختلفی باید طی شوند تا یک نفوذ، موفق باشد. همان‌طور که قبل هم اشاره شده، یک نفوذگر انسان بسیار پرتلاشی است که راه‌های مختلف را تست کرده و از میان آن‌ها بهترین را انتخاب می‌کند. بسیاری از شرکت‌ها و سازمان‌ها برای این‌که به سایت یا دیتابیس آن‌ها نفوذ شود یا اصطلاحا حفره‌های امنیتی آن‌ها شناسایی شود هزینه‌های فراوانی به تیم‌های نفوذ پرداخت می‌کنند؛ بنابراین مهندسی امنیت موقعیت شغلی بسیار خوبی دارد. برای انجام تست‌های نفوذ بهترین دوره‌ها، دوره‌های PWK می‌باشند که هم به‌صورت خودآموز و هم به‌صورت آنلاین برگزار می‌شوند. ولی در هر دو حالت باید سناریوهای مختلف به‌صورت مداوم توسط امنیت‌کار تست شوند و کارهای یکسان را با ابزارهای مختلفی انجام دهد. بر فرض مثال فقط با ابزار nmap اسکن نکند و کار با بقیه ابزارهای اسکن شبکه را هم یاد بگیرد و همیشه به‌روز باشد. با توجه به تمام مطالب گفته شده پی‌میبریم که همه موارد به فراگیری و میزان تلاش او بستگی دارد.

منابع:

- Pwk penetration testing with kali linux, netamooz.net
- Kalilinux, kaliboys.com
- What is shell in linux, iranadmin.com
- what-is-bash, datisnetwork.com

خبرهای مهم

گزیده اخبار اسفندماه

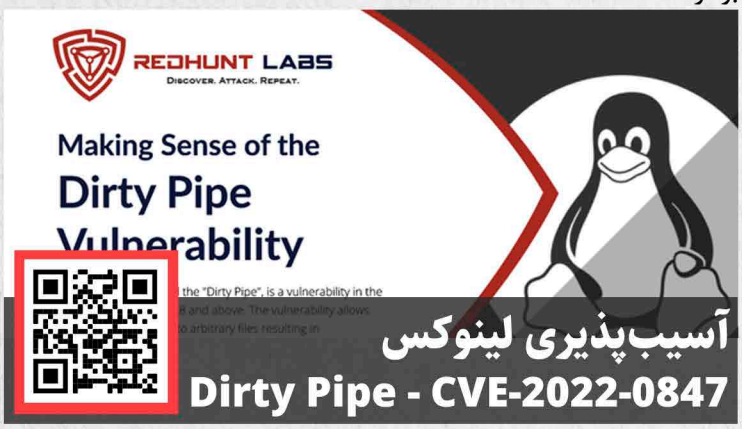
گردآورنده: سروش ذوالفقاری
zolfaghari.soroush@gmail.com

فیشینگ پیامکی به سبک همتا و عدل ایران

مدتیست که بازار فیشینگ‌های پیامکی دوباره رونق گرفته است. تا جایی که پلیس فتا به ارسال پیامک "کلیک روی لینک‌های نامطمئن = هک شدن" به مردم روی آورده است.
در حال حاضر مرسوم‌ترین این فیشینگ‌ها، ارسال پیام جعلی شکواییه (یا همان شکایت) به مردم است. محتوای پیام به این صورت است که علیه شما شکایت شده است و لینک یک برنامه را به آن‌ها می‌دهد و از این طریق آن‌ها را مورد فیشینگ قرار می‌دهد.
در لینک درج شده می‌توانید بررسی بدافزار فیشینگ رجیستری تلفن همراه را به شکل دقیق بررسی کنید.

درخواست مردم اوکراین برای بستن سرویس Cloudflare بر روسیه

اوکراین به شرکت Cloudflare درخواست داد تا سرویس‌های ابری خود را بر روی روسیه مسدود کند تا از حملات (DDOS) سایبری احتمالی روسیه جلوگیری شود. اما در نهایت این شرکت فناوری ۳۰ میلیارد دلاری تصمیم گرفته است تا به ارائه خدمات به روسیه ادامه دهد و در پاسخ درخواست‌های اوکراین جواب منفی داده است.



آسیب‌پذیری لینوکس Dirty Pipe - CVE-2022-0847

این داستان CVE-2022-0847 است، یک آسیب‌پذیری در هسته لینوکس از نسخه 5.8 که امکان بازنویسی داده‌ها در فایل‌های فقط خواندنی دل‌خواه را فراهم می‌کند. این روش منجر به افزایش سطح دسترسی می‌شود زیرا فرایندهای غیرمجاز می‌توانند کد به فرایندهای ریشه تزریق کنند.
این آسیب‌پذیری همانند آسیب‌پذیری CVE-2016-5195 معروف به Dirty Cow می‌باشد و در نسخه‌های Linux 5.16.11 , 5.15.25 , 5.10.102 برطرف شده است.

سامسونگ نشر اطلاعات را تایید کرد

هکرهای $Lapsus اطلاعات حساس به ارزش ۱۸۹ گیگابایت را فاش کرده‌اند، سامسونگ وقوع این حادثه را تایید کرده است اما ادعا کرد که این نشت شامل اطلاعات مشتریان یا کارمندان نمی‌شود.

طبق تایید سایت Hackread.com اطلاعات اکنون در تلگرام و چندین انجمن هک و جرایم سایبری، به ویژه انجمن‌های فعال روسی زبان، معامله می‌شوند. طبق اخبار یک گروه هکری جدید برزیلی که توسط شرکت آنلاین $Lapsus اداره می‌شود، مسئولیت این حمله را بر عهده گرفته است. $Lapsus اخیرا برای هدف قرار دادن انویدیا و سرقت ۱ ترابایت داده سرفصل خبرها شده است. در آخرین اخبار، این گروه می‌گوید سورس کد مخفی سامسونگ را به همراه الگوریتم باز کردن قفل بیومتریک و سایر داده‌های حساس به‌دست آورده است.

انتشار وحشیانه باج‌افزار Conti: تعداد قربانیان به ۱۰۰۰ افزایش یافت

در ماه مارس، پس از اینکه کونتی وفاداری خود را با ولادیمیر پوتین اعلام کرد، یک منبع داخلی طرفدار اوکراین یک حساب توییتری به نام Conti leaks ایجاد کرد تا باند باج‌افزار را افشا کند، که برای بسیاری از قربانیان آن، از جمله HSE ایرلند، گروه فولکس واگن، چندین شهر، شهرستان و منطقه آموزشی ایالات متحده کابوس بود.

با وجود گمانه‌زنی‌ها مبنی بر این‌که داده‌های داخلی گروه فاش شده؛ ممکن است این اتفاق به معنای پایان این باج‌افزار بدنام مرتبط با روسیه باشد. Conti همچنان آزاد است.

فازینگ (آزمون فاز)

کنترل دسترسی در سیستم‌های ابری

هوش مصنوعی در امنیت

تست نفوذ با کالی

Cyber news

روز صفرم ترجمه ی عبارت Zero Day می‌باشد که در تعبیر لغوی یعنی روزی که هنوز به آن نرسیده‌ایم و از وجود چنین چیزی هم خبر نداریم، وقتی صحبت از حمله Zero Day می‌شود یعنی در خصوص حمله ای صحبت می کنیم که هیچکس تا کنون آن را شناسایی نکرده است و هیچ دانشی هم در خصوص آن وجود ندارد که چگونه آن را تشخیص و بعضا از بروز آن جلوگیری کنیم.

در این نشریه سعی بر آن است تا زوایای پنهان و ناشناخته در دنیای امنیت اطلاعات مورد بررسی قرار گرفته و به جدیدترین اخبار و تکنولوژی‌های این حوزه پرداخته شود. مخاطبین این نشریه تمامی دانشجویان و افرادی خواهند بود که به حوزه امنیت اطلاعات علاقمند هستند.

برای ارسال مقالات جهت چاپ در نشریه به @elahe_rahbaran در تلگرام پیام دهید.