



به کارگیری ابزارهای هوش مصنوعی در امنیت سایبری

مصطفی حسینی

کارشناسی ارشد نرم افزار - مرکز آموزش عالی شاهرود

چکیده

در چشم انداز در حال تحول سریع امنیت سایبری، ادغام هوش مصنوعی (AI) بسیار حائز اهمیت شده است. این مقاله به بررسی تأثیر عمیق ابزارهای مبتنی بر هوش مصنوعی در تقویت دفاع‌های سایبری می‌پردازد و ضرورت آنها را در مقابله با تهدیدات سایبری پیچیده‌تر شده برجسته می‌کند. توانایی هوش مصنوعی در تحلیل مجموعه داده‌های عظیم با سرعت بی‌سابقه، امکان شناسایی آسیب‌پذیری‌ها و تشخیص ناهنجاری‌هایی که ممکن است به حملات احتمالی اشاره کنند را فراهم می‌آورد، اغلب قبل از اینکه این حملات شکل بگیرند. ابزارهای کلیدی هوش مصنوعی مورد بحث شامل سیستم‌های پیشرفته تشخیص تهدید، الگوریتم‌های یادگیری ماشین برای تحلیل پیش‌بینی‌کننده و مکانیسم‌های پاسخگویی خودکار به حوادث هستند. این ابزارها نه تنها کارایی و دقت تشخیص تهدید را افزایش می‌دهند، بلکه زمان پاسخگویی به حوادث سایبری را به طور قابل توجهی کاهش می‌دهند و در نتیجه آسیب‌های احتمالی را کاهش می‌دهند. مقاله همچنین به جنبه تاریک‌تر هوش مصنوعی می‌پردازد و بررسی می‌کند که چگونه بازیگران مخرب از هوش مصنوعی برای افزایش پیچیدگی حملات خود استفاده می‌کنند. بدافزارهای مبتنی بر هوش مصنوعی، طرح‌های فیشینگ خودکار و تاکتیک‌های مهندسی اجتماعی مبتنی بر هوش مصنوعی نشان‌دهنده مرز جدیدی از تهدیدات سایبری هستند، جایی که مهاجمان از هوش مصنوعی برای دورزدن اقدامات امنیتی سنتی بهره‌برداری می‌کنند. با برجسته کردن این جنبه‌های دوگانه هوش مصنوعی در امنیت سایبری، مقاله دیدگاهی جامع از وضعیت فعلی ارائه می‌دهد و بر نیاز حیاتی سازمان‌ها به پذیرش دفاع‌های مبتنی بر هوش مصنوعی برای پیشی گرفتن در مسابقه تسلیحات سایبری تأکید می‌کند. در نهایت، ادغام هوش مصنوعی در استراتژی‌های امنیت سایبری نه تنها یک گزینه بلکه ضرورتی برای اطمینان از حفاظت قوی در عصر دیجیتال است.

واژگان کلیدی: هوش مصنوعی (AI)، امنیت سایبری، تشخیص تهدید، یادگیری ماشین

مقدمه

با پیشرفت عصر دیجیتال، پیچیدگی و فراوانی تهدیدات سایبری افزایش یافته است و چالش‌های مهمی را برای اقدامات سنتی امنیت سایبری ایجاد می‌کند. مجرمان سایبری از فناوری‌های پیشرفته برای اجرای حملات پیچیده‌تر استفاده می‌کنند و مکانیسم‌های دفاعی متعارف را ناکافی می‌کنند. در این محیط پر خطر، هوش مصنوعی (AI) به عنوان یک نیروی دگرگون‌کننده در حوزه امنیت سایبری ظاهر شده است. ظرفیت هوش مصنوعی برای پردازش و تجزیه و تحلیل مقادیر زیادی از داده‌ها در زمان واقعی، همراه با توانایی آن در شناسایی الگوها و ناهنجاری‌ها، آن را به عنوان ابزاری حیاتی در مبارزه با جرایم سایبری قرار می‌دهد.

ادغام هوش مصنوعی در استراتژی‌های امنیت سایبری مزایای زیادی را ارائه می‌دهد. الگوریتم‌های یادگیری ماشینی می‌توانند رفتار غیرعادی را که ممکن است نشان‌دهنده نقض امنیتی باشد، اغلب قبل از اینکه آسیب قابل توجهی ایجاد کند، شناسایی کنند. سیستم‌های مجهز به هوش مصنوعی همچنین می‌توانند وظایف معمولی مانند نظارت بر ترافیک شبکه و مدیریت وصله‌ها را خودکار کنند و منابع انسانی را برای تمرکز بر مسائل پیچیده‌تر آزاد کنند. علاوه بر این، هوش مصنوعی با پیش‌بینی آسیب‌پذیری‌های بالقوه و بردارهای حمله، هوش تهدید را تقویت می‌کند و سازمان‌ها را قادر می‌سازد تا رویکردی پیشگیرانه به جای واکنشی برای امنیت اتخاذ کنند.

با این حال، پذیرش هوش مصنوعی در امنیت سایبری بدون چالش نیست. مسائلی مانند نیاز به حجم وسیعی از داده‌های با کیفیت بالا، سوگیری‌های احتمالی در الگوریتم‌های هوش مصنوعی، و خطر همیشه حاضر حملات خصمانه به خود سیستم‌های هوش مصنوعی باید مورد توجه قرار گیرد. همان‌طور که ما این پیچیدگی‌ها را بررسی می‌کنیم، برای سازمان‌ها ضروری است که چارچوب‌های حاکمیت هوش مصنوعی قوی را پیاده‌سازی کنند و از نظارت مستمر و به‌روزرسانی سیستم‌های هوش مصنوعی اطمینان حاصل کنند. با انجام این کار، آنها می‌توانند از پتانسیل کامل هوش مصنوعی برای ایجاد یک چشم انداز دیجیتال امن‌تر استفاده کنند.

در ادامه این پژوهش توضیحات کامل‌تری در رابطه با هوش مصنوعی، علل استفاده و کاربرد آن در امنیت سایبری، ارائه داده خواهد شد.

یادگیری هوش مصنوعی

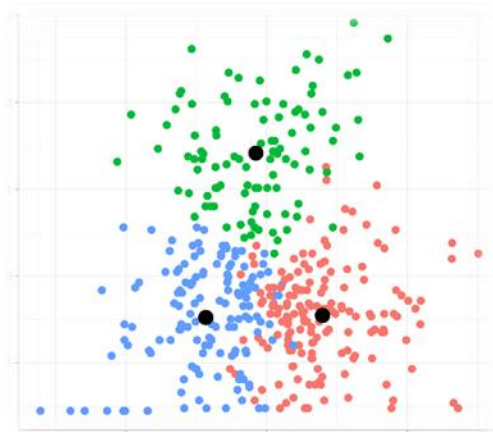
پیش از آنکه هوش مصنوعی بتواند در هر زمینه‌ای مورد استفاده واقع شود، بایستی در رابطه با آن موضوع یادگیری انجام دهد و تحت آموزش قرار گیرد. یادگیری هوش مصنوعی انواع مختلفی دارد و از آنجایی که در پژوهش به انواع یادگیری سیستم‌ها اشاره شده است، لازم دانستیم که به انواع آن اشاره نماییم.

• یادگیری نظارتی

در این نوع یادگیری، سیستم با استفاده از داده‌های برچسب‌گذاری شده، آموزش دیده و پس از آن به پیش‌بینی نوع داده‌های جدید و ارزیابی عملکرد پیش‌بینی بر اساس برچسب واقعی داده، می‌پردازد. الگوریتم SVM را می‌توان در این روش استفاده نمود. این الگوریتم عمل طبقه‌بندی (Classification) را انجام می‌دهد.

• یادگیری بدون نظارت

در صورتی که داده‌ها جهت آموزش فاقد هرگونه برچسب‌گذاری باشند، در این صورت از مدل‌هایی استفاده می‌شود که تنها بر اساس برآیند ویژگی داده‌ها، میانگین و داده‌های مرکزی را محاسبه نموده و تشخیص دهند. سپس بر طبق نتایج به دست آمده می‌توان داده‌های خطا و ناهنجاری را از داده‌های حقیقی تعیین و جدا نمود. مدل Kmeans از جمله الگوریتم‌های بدون نظارت است که به عمل خوشه‌بندی (Clustering) می‌پردازد.



تصویر ۱: نمودار مربوط به Kmeans

• یادگیری نیمه نظارتی

این روش پلی بین دو نوع نظارت شده و بدون نظارت است که دو کاربرد متفاوت دارد. اولین کاربرد برچسب گذاری است. در صورتی که مجموعه داده وسیعی وجود داشته باشد که بدون برچسب است، شما به صورت دستی نمی توانید آن ها را برچسب گذاری نمایید. از این رو می توان قسمت کوچکی از داده را به صورت دستی برچسب گذاری کرد و سپس سیستم با استفاده قسمت برچسب گذاری شده، سایر داده ها را برچسب گذاری نمود.

دومین کاربرد ارزیابی مدل های خوشه بندی است. هنگامی که این تصمیم اتخاذ گردد تا از یک مدل خوشه بندی بر داده های دارای برچسب اعمال گردد، می توان با استفاده از یک مدل، یادگیری بدون نظارت بر داده ها انجام شود. در ادامه نتایج به دست آمده از خوشه بندی را با برچسب داده ها مقایسه نموده تا بررسی نمود چه مقدار خوشه بندی به دست آمده نسبت به ویژگی های حقیقی داده ها دقت داشته است.

• یادگیری تقویتی

در این نوع یادگیری، هوش مصنوعی بدون داشتن هیچ اطلاعاتی از فضا و محیط داده ها، با استفاده از آزمون خطا و در نظر گرفتن دو تابع پاداش (در صورت به دست آمدن نتایج مفید) و مجازات (در صورت رخداد اشتباه از سوی Agent) به یادگیری کلی در رابطه با و داده های موجود پرداخته و به صورت صفر تا صد بدون هیچ گونه ارزیابی، این عمل صورت می پذیرد.

علل استفاده در امنیت سایبری

با گسترش روزافزون شبکه های شرکتی و سازمانی و افزایش چشمگیر IP ها، جمع آوری اطلاعات، یکپارچه سازی و بررسی آن ها، تست نفوذ به شبکه، تشخیص تهدیدات، بررسی و ایمن سازی شبکه از توان red team و blue team انسانی خارج شده و در صورت امکان زمان بر و نیازمند هزینه گزاف است. از طرفی آموزش نیروی انسانی متناسب با میزان تقاضا، تا رسیدن به سطح حرفه ای نیازمند پروسه ای طولانی است که نیاز بازار کار را رفع نمی کند. در حالت کلی می توان علل به کارگیری هوش مصنوعی را به صورت زیر شرح داد:

• تشخیص تهدید پیشرفته

هوش مصنوعی می تواند حجم وسیعی از داده ها را با سرعت بالا تجزیه و تحلیل کند و آن را قادر می سازد الگوها و ناهنجاری هایی را که ممکن است نشان دهنده حمله سایبری باشد، شناسایی کند. این می تواند به شناسایی فعالیت های مخرب، بدافزار یا رفتار شبکه مشکوک کمک کند و امکان شناسایی و پاسخ زود هنگام را فراهم کند.

- پاسخ بی درنگ به رخدادها

هوش مصنوعی می تواند فرایندهای واکنش به حادثه را خودکار انجام دهد و واکنش های سریع تر و کارآمدتر به نقض های امنیتی را ممکن می سازد. می تواند داده ها را از منابع مختلف تجزیه و تحلیل و مرتبط کند، تهدیدها را اولویت بندی کند و اقدامات فوری برای کاهش خطرات را آغاز کند.

- دفاع تطبیقی

هوش مصنوعی می تواند از حملات قبلی درس بگیرد و به طور مداوم مکانیسم های دفاعی خود را تکامل دهد. با مطالعه الگوها و تکنیک های حمله، سیستم های هوش مصنوعی می توانند توانایی خود را برای شناسایی و پیشگیری از تهدیدات آینده تطبیق داده و بهبود بخشند و دورزدن اقدامات امنیتی را برای مهاجمان دشوارتر می کنند.

- کاهش False Positive

سیستم های امنیتی سنتی اغلب هشدارهای خطر اشتباه تولید می کنند که منجر به اتلاف زمان و منابع می شود. الگوریتم های هوش مصنوعی می توانند از بازخوردهای انسانی بیاموزند و قابلیت های تشخیص خود را اصلاح کنند، میزان False Positive را به حداقل برسانند و به تیم های امنیتی اجازه دهند روی تهدیدات واقعی تمرکز کنند.

- آنالیز پیش بینی کننده

هوش مصنوعی می تواند داده های تاریخی و روندهای فعلی را برای پیش بینی آسیب پذیری های احتمالی و بردارهای حمله آینده تجزیه و تحلیل کند. این رویکرد پیشگیرانه به سازمان ها کمک می کند تا با رفع آسیب پذیری ها قبل از سوءاستفاده، موقعیت امنیتی خود را تقویت کنند.

- خطاهای انسانی کمتر

برخلاف کارمندان انسانی، یادگیری ماشینی بدون اینکه خسته شود، محافظت کاملی را در ۷ روز هفته و ۲۴ ساعته ارائه می کند. به علاوه، می تواند از مشاهدات و نتایج به دست آمده، بیاموزد تا به سرعت و دقت عملکرد خود بیفزاید. این بدان معناست که تیم های امنیتی می توانند عملیات بیشتری را به الگوریتم های بسیار آموزش دیده محول کنند و خطاهای انسانی را که به راحتی می توان از آن اجتناب کرد، کاهش داد.

به این نکته نیز باید توجه داشت که مداخله انسانی هنوز مورد نیاز است. سیستم های امنیت سایبری مبتنی بر هوش مصنوعی نمی توانند به طور کامل جایگزین متخصصان امنیتی شوند. استفاده از هوش مصنوعی در امنیت سایبری زمانی بهترین نتیجه را دارد که عنصر مداخله انسانی وجود داشته باشد. سیستم های هوش مصنوعی مانند یادگیری ماشینی به کارشناسان امنیتی کمک می کنند تا رفتارهای مخرب را شناسایی کرده و از وقوع آن جلوگیری کنند که خطرات امنیتی و نقض داده ها را کاهش می دهد. اساساً، ابزارهای هوش مصنوعی و تیم های امنیت سایبری باید مکمل یکدیگر باشند. تیم امنیتی باید از فناوری هوش مصنوعی با به روز نگه داشتن آن در مورد هر گونه تهدید شناخته شده و بررسی منظم عملکرد بهینه سیستم پشتیبانی کند. به نوبه خود، سیستم های امنیتی هوش مصنوعی تیم های امنیت سایبری را در مورد هرگونه رفتار مشکوک یا مخرب، الگوهای ناشناخته یا دیده نشده قبلی در داده ها و هر گونه آسیب پذیری امنیتی احتمالی هشدار می دهند.

کاربردها در حملات سایبری

علاوه بر تیم های مدافع (blue team)، حمله کنندگان و عاملین تهدید نیز در رابطه با بهبود سرعت، افزایش دقت در بررسی داده ها، افزایش کیفیت حمله و مدت زمان بقا و ماندگاری در شبکه از هوش مصنوعی در روند کارهای خود استفاده می کنند.

پیش از شرح بیشتر و ارائه توضیحات تکمیلی در زمینه حوزه‌های به کارگیری، نیاز است مقدمه‌ای در رابطه با دوند حملات بیان گردد که در ادامه به آن‌ها خواهیم پرداخت.

• روند حملات

چندین متدولوژی و استاندارد معروف وجود دارد که می‌توان از آن‌ها برای انجام تست‌های نفوذ استفاده کرد، مانند OSSTMM، OWASP، NIST، PTES، ISSAF. همه آن‌ها روندی از مراحل پیشبرد حملات سایبری را ارائه کردند که مراحل آن به ترتیب شرح داده می‌شود.

❖ تشخیص و جمع‌آوری اطلاعات

در طول این مرحله از حملات، عاملین تهدید سعی می‌کند با جمع‌آوری اطلاعات از منابع قابل دسترسی برای کشف پورت‌ها و سرویس‌هایی که باز هستند، تاحدامکان اطلاعات بیشتری درباره اهداف خود جمع‌آوری کنند. در پایان این مرحله، عاملین تهدید دانشی از اهداف خود خواهند داشت که شامل اطلاعاتی مانند نام Host، Domain، های هدف، سرویس‌های فعال، فناوری‌های موجود، نام کارمندان، ایمیل‌های کارکنان، مکان‌های فیزیکی، تصاویر مکان‌های فیزیکی، نام کاربری و رمز عبور و غیره است.

هوش مصنوعی و یادگیری ماشین می‌توانند به عاملین تهدید کمک کنند تا نه تنها تمام اطلاعات را به صورت خودکار جمع‌آوری کنند، بلکه آن‌ها را تجزیه و تحلیل کنند و دوره‌های مختلف عملیات را تعیین کنند. برای مثال، می‌توانند بر اساس اطلاعات جمع‌آوری شده بهترین حمله مهندسی اجتماعی را برای اجرا تعیین کنند. یا می‌توان از آن برای شناسایی میزبان‌های هدفی که باید ابتدا مورد حمله قرار گیرند استفاده کرد؛ زیرا احتمال موفقیت بیشتر است.

❖ بررسی و ارزیابی آسیب‌پذیری

در طول این مرحله، عاملین تهدید اسکن‌های آسیب‌پذیری عمیق‌تری را انجام می‌دهند تا تمام آسیب‌پذیری‌های بالقوه‌ای را که اهداف می‌توانند داشته باشند، مشخص کنند. در اینجا، هوش مصنوعی و یادگیری ماشین می‌توانند کمک کنند تا نتایج اسکن را با تجزیه و تحلیل آن و حذف هر چیزی که قابل اجرا نیست یا نویز ایجاد می‌کند، با در نظر گرفتن اطلاعات جمع‌آوری شده از مرحله قبل همراه با اطلاعات تهدید از منابعی مانند رسانه‌های اجتماعی، سوابق، دیپ و دارک وب درک کنند. همچنین، هوش مصنوعی و یادگیری ماشین می‌توانند با همبستگی همه اطلاعات و دانش جمع‌آوری شده، بهترین حالت و امکان حمله را تعیین نمایند.

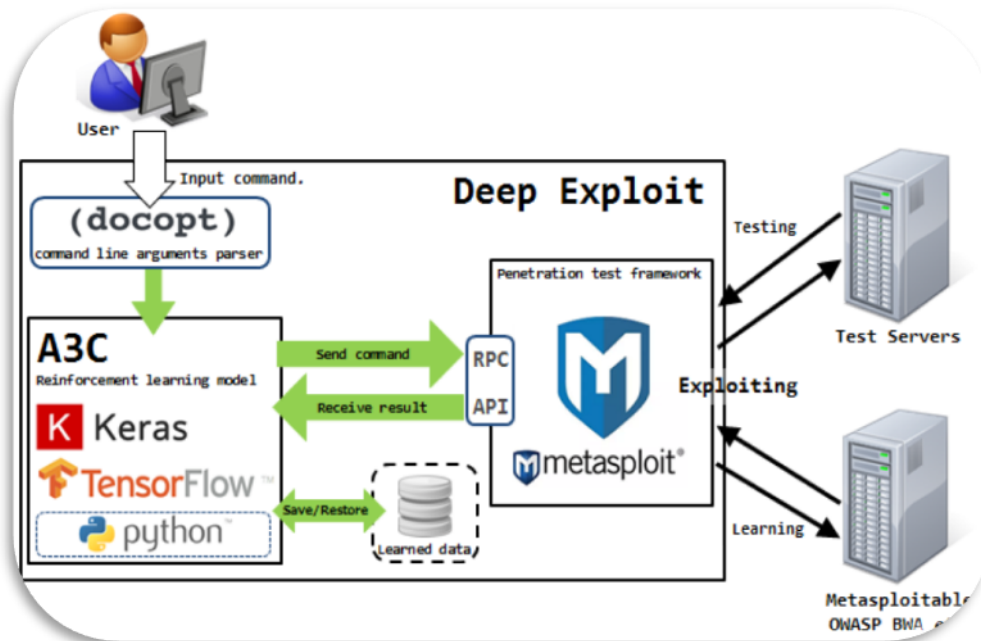
❖ بهره‌برداری

در این بخش سعی می‌شود عاملین تهدید بتواند به هدف دسترسی یابند، اختیارات کاربری (Privilege) را افزایش دهند، اطلاعات بیشتری جمع‌آوری کنند و دسترسی دائمی را حفظ کنند. هوش مصنوعی و یادگیری ماشین می‌توانند با تعیین بهترین مسیر عمل برای نفوذ به یک هدف کمک کنند، اما همچنین می‌توانند بهره‌برداری را به طور همزمان انجام دهند. نتایج این بهره‌برداری‌ها می‌تواند به مدل هوش مصنوعی بازخورد داده شود و به آن اجازه می‌دهد جایگزین‌های بهره‌برداری یا مسیرهای بهره‌برداری جدیدی که قبلاً در نظر گرفته نشده‌اند، تولید کند.

در حال حاضر ابزارهای open source در بازار وجود دارد که اجرای سه مرحله اول این روش را ترکیب می‌کند، مانند Deep Exploit در نشانی زیر قابل مشاهده است:

https://github.com/13o-bbr-bbq/machine_learning_security/wiki/deep-exploit

این یک ابزار تست نفوذ کاملاً خودکار است که از یادگیری ماشین نه تنها برای بهبود مرحله جمع‌آوری اطلاعات بلکه برای سوءاستفاده از آسیب‌پذیری‌ها استفاده می‌کند.



تصویر ۲: مدل روند کار Deep Exploit

• حوزه‌های به‌کارگیری

علاوه بر مواردی که در بخش روند حملات بیان و شرح داده شد، در این بخش حوزه‌ها و موارد دیگری را در این رابطه بیان خواهیم نمود. موارد جدید حالات پیشرفته و عمیق‌تری را در خود جای داده است.

❖ مسموم‌سازی داده‌ها

هوش مصنوعی می‌تواند داده‌های آموزشی مورد استفاده توسط سیستم‌های یادگیری ماشین را برای تصمیم‌گیری دست‌کاری کند که با دو روش امکان‌پذیر است:

تزریق داده: عاملین تهدید می‌توانند داده‌های مخرب یا گمراه‌کننده را به مجموعه داده‌های حقیقی مورد استفاده برای آموزش مدل‌های هوش مصنوعی تزریق کنند. با افزودن نمونه‌های نادرست یا دست‌کاری شده، فرایند یادگیری الگوریتم می‌تواند خراب شود. این عمل باعث به وجود آمدن مدل‌های مغرضانه یا نادرست می‌شود که پیش‌بینی‌ها یا تصمیم‌گیری‌های نادرست انجام می‌دهند.

شبکه‌های متخاصم مولد (GANs): نوعی الگوریتم هوش مصنوعی هستند که جهت تولید داده‌های مصنوعی از یک مجموعه داده حقیقی از آن‌ها استفاده می‌شود. عاملین تهدید می‌توانند یک GAN را برای تولید داده‌های مصنوعی، اما با تغییرات ظریف در برچسب داده‌ها (به هر کدام از داده‌ها برچسب نامرتبب تخصیص داده شود) آموزش دهند. سپس این داده‌های مصنوعی مسموم را می‌توان با داده‌های حقیقی مخلوط کرد و باعث به خطر افتادن مدل هوش مصنوعی حاصل شد. دست‌کاری یادگیری تقویتی: عاملین تهدید می‌توانند سیگنال‌های مربوط به پاداش، مجازات و محیط را دست‌کاری کنند تا سیستم را هنگام یادگیری به وسیله رفتارهای نامطلوب فریب دهند. با هدایت سیستم به سمت اقدامات مخرب، عاملین تهدید می‌توانند از سیستم هوش مصنوعی سوءاستفاده کنند.

❖ بدافزار

بدافزار مجهز به هوش مصنوعی می‌تواند شناسایی و دفاع در برابر حملات را برای سیستم‌های امنیتی سنتی چالش‌برانگیزتر کند. بدافزار می‌تواند تکامل یابد و از محیط خود یاد بگیرد و ریشه‌کن کردن آن را دشوارتر کند. این نوع بدافزارها، از رفتار تطبیقی هدف استفاده می‌کند. این رفتار می‌تواند بدافزار را قادر به تطبیق و تکامل بر اساس محیط خود کند. می‌تواند از تعاملات خود با سیستم‌ها درس بگیرد، اقدامات امنیتی را تجزیه و تحلیل کند و Source code خود را برای جلوگیری از شناسایی تغییر دهد. این امر، شناسایی و ریشه‌کن کردن بدافزار را برای آنتی‌ویروس یا دفاع شبکه چالش‌برانگیزتر می‌کند. الگوریتم‌های هوش مصنوعی می‌توانند حجم وسیعی از داده‌ها، از جمله نمایه‌های رسانه‌های اجتماعی، عادت‌های جستجو و فعالیت‌های آنلاین هدف را برای ایجاد حملات شخصی‌سازی شده تجزیه و تحلیل کنند. با تنظیم بدافزار به طور خاص بر اساس رفتار و علایق هدف، شانس نفوذ موفقیت‌آمیز و سازش را افزایش می‌دهد. همچنین هوش مصنوعی به بدافزار کمک می‌کند تا آسیب‌پذیری‌ها را در سیستم‌ها شناسایی کرده و به طور مؤثر از آن‌ها سوءاستفاده کند و همچنین الگوهای ترافیک شبکه، تنظیمات سیستم و رفتار کاربر را تجزیه و تحلیل کند تا بهترین زمان و روش برای شروع حمله را تعیین کند. این بدافزار را قادر می‌سازد تا اقدامات امنیتی را دور بزند و به اطلاعات حساس دسترسی غیرمجاز پیدا کند.

❖ مهندسی اجتماعی

این امکان وجود دارد که هوش مصنوعی را با تکنیک‌های مهندسی اجتماعی برای دست‌کاری و فریب افراد ترکیب نمود. هوش مصنوعی می‌تواند حجم وسیعی از داده‌ها را برای ایجاد ایمیل‌ها، پیام‌ها یا تماس‌های تلفنی برای حملات فیشینگ به صورت شخصی‌سازی شده و با قابلیت قانع‌کنندگی بالا تجزیه و تحلیل کند. پیام ایجاد شده توسط این سیستم قانع‌کننده‌تر به نظر برسند و احتمال گرفتار شدن قربانیان را افزایش دهند. هوش مصنوعی حتی می‌تواند آدرس‌های ایمیل واقعی یا شخصیت و هویت جعلی را برای فریب دادن افراد ایجاد کند. همچنین این قابلیت را دارد تا صداها و الگوهای گفتار انسان را تقلید کند، و امکان ایجاد حملات فیشینگ صوتی (vishing) پیچیده را فراهم کند. با استفاده از ضبط‌های صوتی تولید شده توسط هوش مصنوعی، عاملین تهدید می‌توانند هویت افراد یا سازمان‌های مورد اعتماد را جعل کنند و تلاش‌های مهندسی اجتماعی آن را متقاعدکننده‌تر و باورپذیرتر کنند. این نوع سیستم می‌تواند پست‌ها، نظرات و تعاملات رسانه‌های اجتماعی را برای شناسایی اهداف بالقوه برای مهندسی اجتماعی بررسی نمایند. با درک علایق، باورها و نقاط ضعف افراد، عاملین تهدید می‌توانند پیام‌های مناسبی برای سوءاستفاده از احساسات یا دست‌کاری اهداف ایجاد کنند. از این رو می‌توانند میزان موفقیت حملات را افزایش دهند و به جمع‌آوری اطلاعات حساس کمک کنند.

❖ DDoS

این امکان وجود دارد که با استفاده از الگوریتم هوش مصنوعی، حملات DDoS صورت پذیرد. سیستم می‌تواند الگوهای ترافیک شبکه را مشاهده و بررسی نماید، با سیستم دفاعی هدف سازگار شود، و موج عظیمی از ترافیک مخرب را برای غلبه بر سیستم‌های هدف هماهنگ کند. این می‌تواند منجر به اختلال در سرویس، زیان مالی و آسیب به اعتبار سازمان‌ها شود. همچنین می‌تواند با مدیریت و کنترل بات‌نت‌ها، حملات DDoS را راه‌اندازی نماید. این الگوریتم می‌تواند هماهنگی و توزیع ترافیک حمله را بهینه کند با کاهش اثر حمله، دفاع را چالش‌برانگیزتر نماید.

❖ شکستن گذرواژه

در صورتی که قدرت محاسباتی هوش مصنوعی با الگوریتم‌های پیشرفته ترکیب شود، به شکل مؤثرتری می‌توان انواع مختلف گذرواژه‌ها را شکست و یافت نمود. هوش مصنوعی می‌تواند الگوها، ساختارهای گذرواژه رایج را بیاموزد و حتی رفتار انسان را برای افزایش شانس شکستن موفقیت‌آمیز گذرواژه پیش‌بینی کند. از طرفی چنین سیستمی می‌تواند مقادیر زیادی از داده‌های مربوط به گذرواژه‌های نقل شده را برای شناسایی الگوها و روش‌های رایج مورد استفاده توسط افراد هنگام ایجاد گذرواژه را

بررسی کند. با یادگیری موارد فوق، هوش مصنوعی می‌تواند استراتژی‌های هدفمند و مؤثرتری برای شکست گذرواژه، از جمله حملات Dictionary، brute force یا حملات ترکیبی ایجاد کند. از دیگر قابلیت‌های این سیستم می‌توان به این نکته اشاره نمود که می‌تواند رفتار کاربر، اطلاعات شخصی و سایر داده‌های زمینه‌ای را برای پیش‌بینی دقیق گذرواژه‌های انتخاب‌شده توسط هدف را تحلیل و بررسی کند. الگوریتم‌های هوش مصنوعی با درک اینکه افراد چگونه فکر می‌کنند و گذرواژه ایجاد می‌کنند، می‌توانند حدس‌های دقیق‌تری ایجاد کنند و زمان موردنیاز برای شکستن گذرواژه را به میزان قابل‌توجهی کاهش دهند. از طرفی می‌توانند از سخت‌افزارهای تخصصی مانند GPU برای تسریع شکستن گذرواژه استفاده کنند. با استفاده از قدرت محاسباتی پردازنده‌های گرافیکی، هوش مصنوعی می‌تواند پردازش موازی را انجام دهد، چندین ترکیب گذرواژه را به طور هم‌زمان انجام دهد و روند شکستن گذرواژه را تا حد زیادی سرعت بخشد.

❖ DeepFake

از فناوری هوش مصنوعی برای ایجاد ویدئوها یا ضبط‌های صوتی Deepfake متقاعدکننده استفاده می‌شود. با ترکیب الگوریتم‌های هوش مصنوعی و یادگیری ماشینی، می‌توان محتوای رسانه‌ای را برای فریب‌دادن افراد یا انتشار اطلاعات نادرست دست‌کاری و تولید نمود. در برخی موارد مشاهده‌شده است که با استفاده از Deepfake صدا و تصویر مدیران ارشد برخی شرکت‌ها یا مسئولان دولتی را تولید نموده و از آن به‌عنوان یک سخنرانی قانع‌کننده در حملات Phishing استفاده شده است. از این‌رو می‌توان برای باج‌خواهی، افترا یا حتی برای دست‌کاری افکار عمومی استفاده نمود.

مقایسه حملات دستی، اتوماتیک و مبتنی بر هوش مصنوعی

می‌توان تفاوت‌هایی را میان حالات دستی، اتوماتیک و مبتنی بر هوش مصنوعی در حملات سایبری و انجام تست‌های نفوذ مقایسه نمود. به همین جهت جدول ۱ در رابطه با این زمینه تهیه شده است که مطالعه دقیق آن حالی از لطف نیست:

جدول ۱: مقایسه پیشبرد حملات سایبری

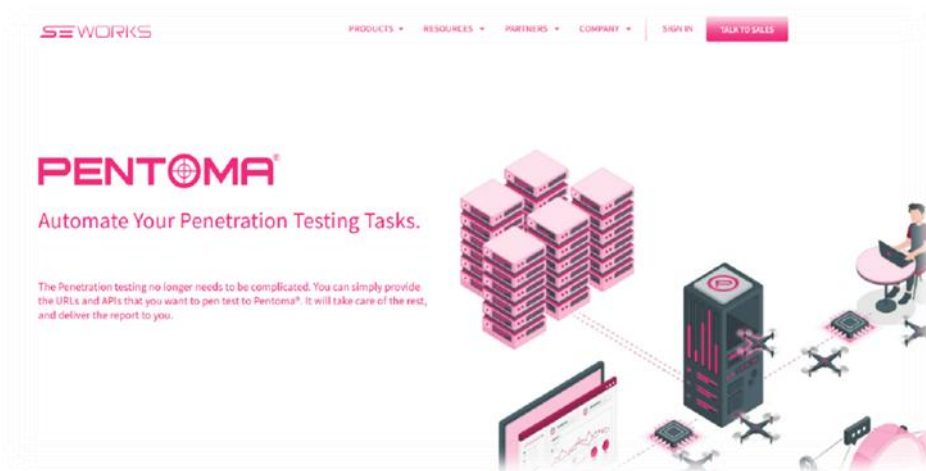
هوش مصنوعی	اتوماتیک	دستی
تست نفوذ فعال با هوش مصنوعی در مقایسه با تست خودکار دقیق است.	احتمال بازگشت False positive بیشتر است.	تست دستی همیشه به دلیل خطای انسانی دقیق نیست.
آزمایش با هوش مصنوعی زمان زیادی را صرف نمی‌کند. الگوریتم‌ها را می‌توان برای هزاران سیستم در یک لحظه مستقر کرد.	تست خودکار توسط ابزارهای نرم‌افزاری اجرا می‌شود، بنابراین به طور قابل‌توجهی سریع‌تر از روش دستی است.	تست دستی زمان‌بر است و منابع انسانی را به خود اختصاص می‌دهد.
هوش مصنوعی باعث صرفه‌جویی در سرمایه‌گذاری برای منابع انسانی در تست نفوذ می‌شود. نسبتاً می‌توان از همان کارمندان برای انجام کارهای کمتر تکراری و کارآمدتر استفاده کرد.	سرمایه‌گذاری برای تست ابزار موردنیاز است.	سرمایه‌گذاری برای نیروی انسانی موردنیاز است.
تست نفوذ مبتنی بر هوش مصنوعی در سازمان‌هایی با هزاران سیستم که برای صرفه‌جویی در زمان و منابع نیاز به آزمایش هم‌زمان دارند، عملی است.	تست خودکار زمانی عملی است که ابزارها، آسیب‌پذیری‌های تست را خارج از محدوده قابل‌برنامه‌ریزی پیدا کنند.	تست دستی تنها زمانی عملی است که موارد تست یک یا دو بار اجرا شوند و نیازی به تکرار مکرر نباشد.

ابزارها

علاوه بر ابزار DeepExploit که پیش از این در بخش روند حملات به آن اشاره شد، ابزارها و APIهای دیگری نیز وجود دارند که به آن‌ها خواهیم پرداخت که هر کدام مزیت‌ها و معایب خود را دارند.

• Pentoma

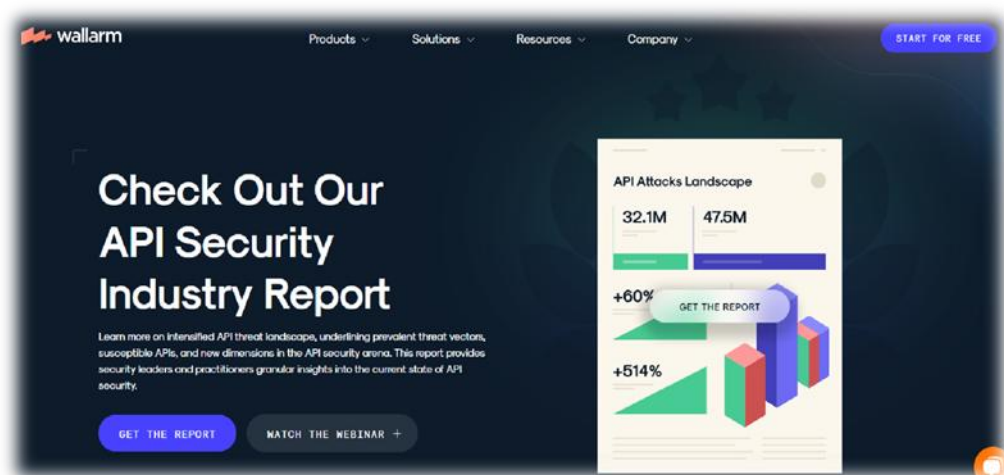
این ابزار با دریافت URL و APIها می‌تواند به صورت خودکار و مبتنی بر هوش مصنوعی تست نفوذ را بر برنامه‌ها و وب سرورها پیاده‌سازی نموده و نتایج به دست آمده به همراه نفوذپذیری‌های موجود را به کاربر تحویل دهد. نقاط حمله احتمالی را از دیدگاه مهاجم تجزیه و تحلیل می‌کند و تست‌های نفوذ را با شبیه‌سازی اکسپلویت‌ها انجام می‌دهد. تهیه این ابزار از طریق نشانی <https://se.works> به ثبت نام در سایت و انجام مذاکره از طریق مشاوران فروش قابل تهیه است.



تصویر ۳: صفحه مربوط به وبگاه se.works مربوط به Pentoma

• Wallarm

یکی دیگر از ابزارهای تست مبتنی بر هوش مصنوعی Wallarm است که منابع شبکه را کشف می‌کند، آسیب‌پذیری‌های رایج را اسکن می‌کند و واکنش برنامه‌ها را برای الگوهای رفتاری غیرعادی نظارت می‌کند. آسیب‌پذیری‌های خاص برنامه را به وسیله تأیید خودکار تهدیدات کشف می‌کند. محتوای یک درخواست مخرب مسدود شده برای ایجاد یک تست پاک‌سازی شده با همان بردار حمله استفاده می‌شود تا ببیند برنامه یا کپی آن در جعبه ایمنی چگونه پاسخ می‌دهد. این ابزار به صورت رایگان در نشانی <https://www.wallarm.com> قابل تهیه است؛ اما نیازمند به ثبت نام در سایت به وسیله ایمیل تجاری است.



تصویر ۴: صفحه اصلی wallarm.com

• Snyc DeepCode AI

از دیگر مواردی که می‌توان به آن اشاره نمود، پلتفرم DeepCode AI است. از طریق نشانی <https://snyc.io> قابل تهیه است. به‌وسیله Deepcode در حملات سایبری، می‌توان از قابلیت‌های آن برای یافتن آسیب‌پذیری‌ها در سیستم‌های نرم‌افزاری استفاده کنید. این پلتفرم می‌تواند نقاط ضعف و حفره‌های امنیتی را در برنامه‌ها، وب‌سایت‌ها یا شبکه‌های مختلف شناسایی کند. این به شما امکان می‌دهد از این نقاط ضعف سوءاستفاده کنید و دسترسی غیرمجاز به دست آورید، اطلاعات حساس را سرقت کنید یا به سیستم‌های هدف آسیب وارد کنید. علاوه بر یافتن آسیب‌پذیری‌ها، می‌توان از هوش مصنوعی Deepcode برای ساخت بدافزارهای پیچیده و اکسپلویت نیز استفاده نمود. با استفاده از این پلتفرم قدرتمند، می‌توان نرم‌افزار مخربی ایجاد کرد که می‌تواند به سیستم‌ها نفوذ کند، داده‌ها را بدزدد یا حتی کنترل کل شبکه‌ها را در دست بگیرد. این پلتفرم شامل سه پلن Free، Team و Enterprise است.

• Shennina

Shennina یک پلتفرم خودکار Host exploitation است. مأموریت این پروژه خودکارسازی کامل اسکن، اسکن و تحلیل آسیب‌پذیری و سوءاستفاده از آن‌ها با استفاده از هوش مصنوعی است. Shennina به همراه Metasploit و Nmap برای انجام حملات یکپارچه‌شده است و همچنین با یک سرور C&C داخلی برای استخراج خودکار داده‌ها از ماشین‌های در معرض خطر یکپارچه‌شده است. این پروژه بر اساس DeepExploit توسعه‌یافته است. این ابزار در نشانی <https://github.com/mazen160/shennina> در دسترس عموم قرار دارد و با سیستم‌عامل Kali سازگار است.

نتیجه

باتوجه به تحقیقات صورت‌گرفته، با پیشرفت تکنولوژی در زمینه هوش مصنوعی و ML، می‌توان چه در زمینه دفاع و امنیت سایبری و چه در زمینه حملات، تولید باج‌افزار و انجام مهندسی اجتماعی و Phishing از هوش مصنوعی استفاده نمود. با این حال در عمل به دلیل حساسیت حوزه حملات سایبری، ابزاری به دست نیامد؛ اما پلتفرم DeepCode AI را می‌توان به‌عنوان یک نمونه ابزار مفید در این زمینه معرفی کرد. از طرفی دیگر نیز ابزارها، پلتفرم‌ها و API‌های مختلفی در رابطه با حفظ امنیت در قبال حملات، رفتارهای غیرعادی، کلاهبرداری و Phish وجود دارد که به کمک ادمن شبکه‌ها و تیم‌های امنیتی سازمان‌ها و شرکت‌ها می‌آیند. این نکته نیز قابل‌ذکر است که در صورت استفاده از ابزارهای مبتنی بر هوش مصنوعی، همچنان به تیم‌های امنیتی انسانی نیاز است و ابزارهای هوش مصنوعی تنها برای کارآمدتر شدن عملکرد تیم انسانی مورد استفاده قرار می‌گیرد.



منابع

- [1] Gordon Gottsegen(Aug 07, 2023),Machine Learning in Cybersecurity: How It Works and Companies to Know,<https://builtin.com/artificial-intelligence/machine-learning-cybersecurity>
- [2] Andrew Froehlich(07 Apr 2020), West Gate Networks,AI pen testing promises delivers both speed and accuracy,<https://www.techtarget.com/searchsecurity/tip/AI-pen-testing-promises-delivers-both-speed-and-accuracy>
- [3] Andrew Froehlich(26 Sep 2019),West Gate Networks,When should I use breach and attack simulation tools?,<https://www.techtarget.com/searchsecurity/answer/When-should-I-use-breach-and-attack-simulation-tools>
- [4] Melisha Dsouza(October 21, 2018), How artificial intelligence can improve pentesting,<https://hub.packtpub.com/how-artificial-intelligence-can-improve-pentesting>
- [5] John Meah(13 March 2024),AI and Cybersecurity: Accelerate Your Defenses in 2024,<https://www.techopedia.com/ai-and-cybersecurity-benefits-and-threats>
- [6] Indre Raviv(Jun 17, 2021),4 ways AI can help us enter a new age of cybersecurity,<https://www.weforum.org/agenda/2021/06/4-ways-ai-new-age-of-cybersecurity>
- [7] Esteban Farao, ERMProtect, Director of IT Security Consulting,How Artificial Intelligence Will Drive the Future of Penetration Testing in IT Security,<https://ermprotect.com/blog/how-artificial-intelligence-will-drive-the-future-of-penetration-testing/>
- [8] Netacea(Feb 10, 2022),How Artificial Intelligence is Changing Cybersecurity,<https://medium.com/netacea/how-artificial-intelligence-is-changing-cybersecurity-cc91eb6b5eb>
- [9] TechByHeart Academy(Jul 30, 2023),ARTIFICIAL INTELLIGENCE (AI) IN CYBER SECURITY,<https://techbyheartacademy.medium.com/artificial-intelligence-ai-in-cyber-security-b5b7db5cead5>
- [10] Priyanshi Sharma(Jul 2, 2023),AI in Cybersecurity: A Match Made in Heaven, or a Recipe for Disaster?,<https://medium.com/@priyanshisharma1251/ai-in-cybersecurity-a-match-made-in-heaven-or-a-recipe-for-disaster-aef471bea41c>
- [11] Sciforce(Jan 16, 2020),Artificial Intelligence for Cyber-Security: A Double-Edge Sword,<https://medium.com/sciforce/artificial-intelligence-for-cyber-security-a-double-edge-sword-6724e7a31425>
- [12] Dmitrijs Trizna(Apr 21, 2023),Architecture of AI-Driven Security Operations with a Low False Positive Rate,<https://towardsdatascience.com/architecture-of-ai-driven-security-operations-with-a-low-false-positive-rate-a33dbbad55b4>
- [13] Ali Gündoğar(Sep 1, 2023),Kali Linux and Artificial Intelligence Integration,<https://salvacybersec.medium.com/kali-linux-and-artificial-intelligence-integration-f7c6da1f7d39>
- [14] R K(December 23, 2022),Shennina : Automating Host Exploitation With AI,<https://kalilinuxtutorials.com/shennina>



Application of Artificial Intelligence Tools in Cybersecurity

Mostafa Hosseini

Master's Degree of Software - Shahrood Higher Education Center

Abstract

In the rapidly evolving landscape of cybersecurity, the integration of Artificial Intelligence (AI) has become paramount. This article explores the profound impact of AI-driven tools in fortifying cyber defenses, underscoring their necessity in combating increasingly sophisticated cyber threats. AI's ability to analyze vast datasets at unprecedented speeds enables the identification of vulnerabilities and the detection of anomalies that could signify potential attacks, often before they materialize. Key AI tools discussed include advanced threat detection systems, machine learning algorithms for predictive analytics, and automated incident response mechanisms. These tools not only enhance the efficiency and accuracy of threat detection but also significantly reduce the response time to cyber incidents, thereby mitigating potential damage. The article also delves into the darker side of AI, examining how malicious actors leverage AI to enhance the sophistication of their attacks. AI-powered malware, automated phishing schemes, and AI-driven social engineering tactics represent a new frontier of cyber threats, where attackers exploit AI to bypass traditional security measures. By highlighting these dual aspects of AI in cybersecurity, the article provides a comprehensive overview of the current state of play, emphasizing the critical need for organizations to adopt AI-based defenses to stay ahead in the cyber arms race. Ultimately, the integration of AI into cybersecurity strategies is not merely an option but a necessity for ensuring robust protection in the digital age.

Keywords: Artificial Intelligence (AI), Cybersecurity, Threat Detection, Machine Learning