کاربردهای ابزارهای مبتنی بر GPT

در امنیت سایبری

زانیار کریمی

آذر ماه ۱۴۰۲

فهرست مطالب

۰۱

مقدمه

۰۲

امنیت سایبری، نقش مهمی در:

- حفاظت از اطلاعات حساس شخصی و مالی
- محافظت از افراد، سازمان‌ها و کشورها در برابر حملات و تهدیدات سایبری
- برقراری و اطمینان از صحت، یکپارچگی و قابل اعتماد بودن سیستم‌ها و داده‌های دیجیتال

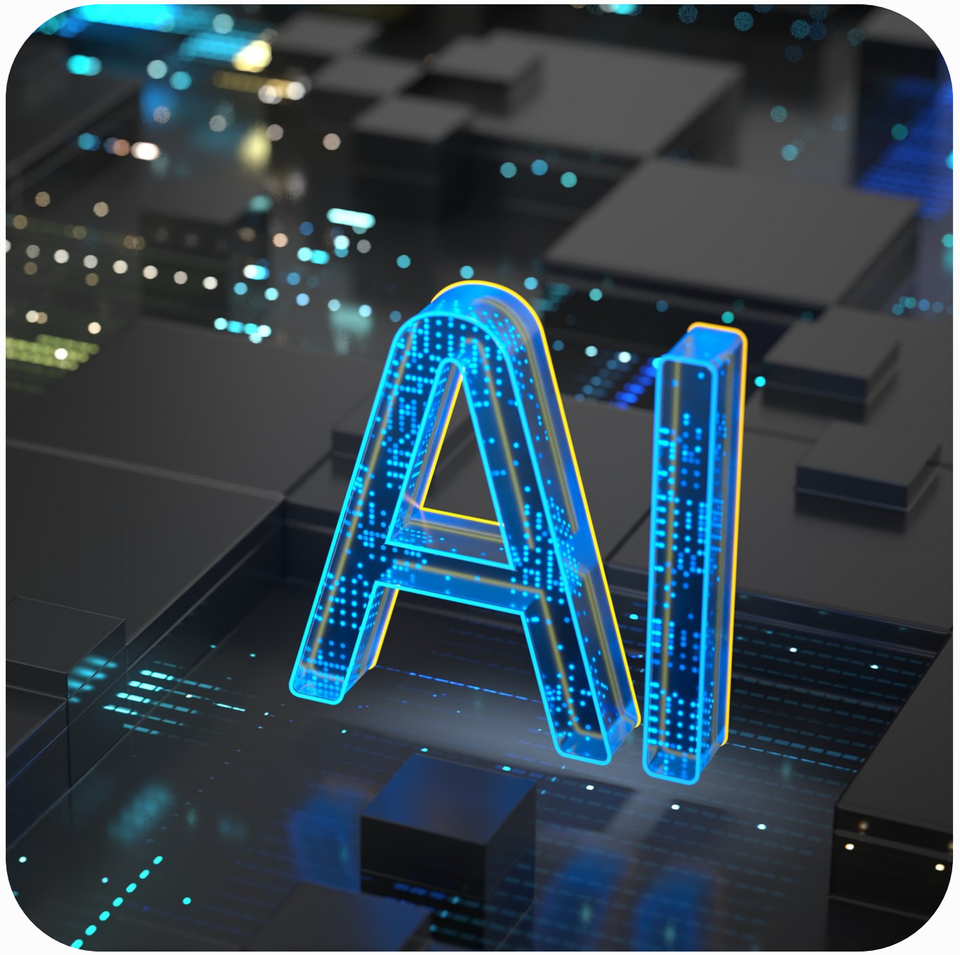
GPT چیست؟

Generative Pre-trained Transformer

«ترانسفورماتور از پیش آموزش دیده مولد»

۰۳

- یک مدل پردازش زبان طبیعی پیشرفته که زمینه تولید متن مبتنی بر هوش مصنوعی را متحول کرده است.
- استفاده از تکنیک‌های یادگیری عمیق برای درک و تولید متون شبه انسانی.
- پیش آموزش بر روی مقادیر وسیعی از داده‌های در دسترس عموم، یادگیری الگوهای اساسی، دستور زبان و محتوای زبانی.
- هدف توسعه هوش مصنوعی عمومی (AGI)



LLM (مدل زبانی بزرگ)

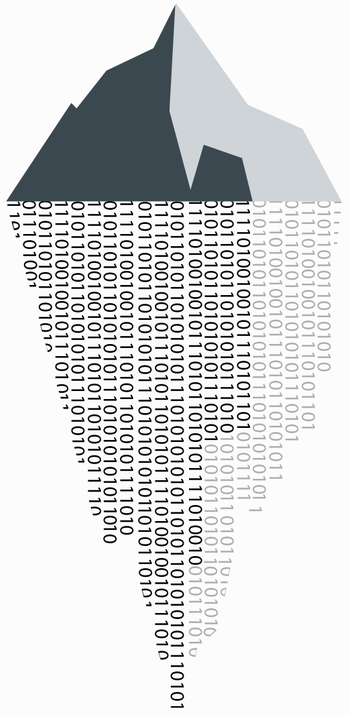
Large Language Model

۰۴

- سیستم‌های هوش مصنوعی پیچیده برای پردازش و تولید متن شبیه انسان.
- روی حجم وسیعی از داده‌ها از جمله کتاب‌ها، مقالات و وب‌سایت‌ها آموزش می‌بینند تا درک وسیعی از الگوهای زبان و دانش به‌دست آورند.
- **عموماً کاربرد در امور تحقیقات، دانشگاهی، روزنامه‌نگاری و صنایع تولید محتوا.**
- چند زبانه بوده و قادر به درک و تولید متن به چندین زبان هستند.
- وظایفی مانند ترجمه، خلاصه‌سازی، تجزیه و تحلیل احساسات و ...

DarkBert

- مدل زبان پیشرفته مبتنی بر ترانسفورماتور
- آموزش براساس یک فرآیند دقیق برای مدیریت حدود ۶/۱ میلیون صفحه دارک‌وب انگلیسی.
- توسط محققان KAIST و S2W توسعه‌یافته است.
- رمزگشایی لهجه‌های منحصربه‌فرد و پیام‌های رمزگذاری‌شده رایج در زوایای پنهان اینترنت، تلاش در راستای مبارزه با جرایم سایبری.
- عملکرد: نظارت بر دارک‌وب برای شناسایی تهدیدات در حال ظهور، کمک به اجرای قانون و تیم‌های امنیت سایبری و تولید محتوای آموزشی.



۰۵

تعدادی ابزار مبتنی بر GPT

بررسی برخی از ابزارهای مفید و مهم مبتنی بر GPT و کاربردهای آنها

در زمینه های مختلف:

۰۶

۰۷

انواع تهدیدات

بررسی تعدادی از رایج‌ترین و تاثیرگذارترین تهدیدات که توانسته‌اند در سالهای اخیر نتایج مخربی را به همراه داشته و باعث ضرر رساندن به سازمان‌ها، اشخاص و نیز حتی دولت‌های مختلف شده‌اند.

۰۱

• مهندسی اجتماعی

استفاده از معیارهای ساختاری و روانشناختی اجتماعی جهت دستیابی به اطلاعات اشخاص.

- فیشینگ
- جعل و سرقت هویت

۰۲

• حملات BadUSB

- شناسایی به عنوان HID
- انواع پیلود: باج‌افزار - صفحه ورود تقلبی - کی‌لاگر - DDoS
- میکروکنترلرهای پشتیبانی کننده:
  - ATtiny 85 (Digispark)
  - Teensy

۰۳

• حملات فیشینگ

- فیشینگ ایمیلی
- حمله مرد میانی (MitM)
- Vishing
- Smishing
- Pharming

۰۸

سناریو یک: حمله باج‌افزار

در این سناریو، مراحل ساخت یک باج‌افزار و رویکردهای استفاده شده در تولید باج‌افزارهای عمومی مورد بررسی قرار می‌گیرد:

- Encryption key generation
- File Encryption
  - Original file overwritten with random data & encrypted.
  - Encrypted data written back to the file.
- Directory Encryption
  - Traverse a directory and its subdirectories
  - Encrypt each file encountered
- Environment Check & execution (IF “sandbox” then exit; ELSE: execute)

سناریو دو: حملات BadUSB

بررسی تعدادی نمونه از انواع حملات که در سرقت اطلاعات حساس مورد استفاده قرار می‌گیرند:

- Keylogger
- USB Worm - Once connected to a computer, it copies itself onto other USB devices.
- Network Spoofer - acts as a rogue network adapter, intercepting and manipulating network traffic
- Firmware Infector
- Malicious Charger - O.MG Cable | secretly installs malware on the victim's device when connected.
- Ransomware Spreader
- Show the Wi-Fi password for a router commonly accessed via a desktop.

سناریو سه: حمله فیشینگ

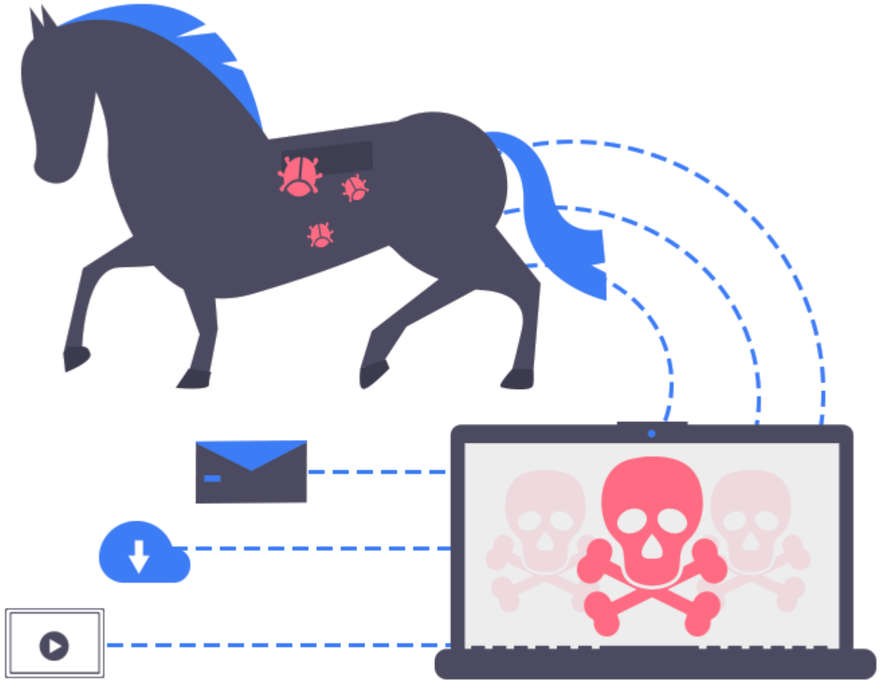
بررسی فیشینگ از طریق ایمیل و ساخت تعدادی سکریپت مخرب:

- Generate a basic phishing email.
- Antivirus and threat detection bypassing mechanisms.
- Generate a script based on JS, to automatically detect the browser fingerprint.
- Send sensitive documents and “.Docx” files from a victim to a web server.

سناریو چهار: ساخت R.A.T ویندوزی

به بررسی Remote Access Trojan و تعدادی از ویژگی‌های آن پرداخته‌ایم:

- Create a socket
- Connect to the specified IP address and port number
- Execute corresponding actions
- Encrypted data written back to the file.



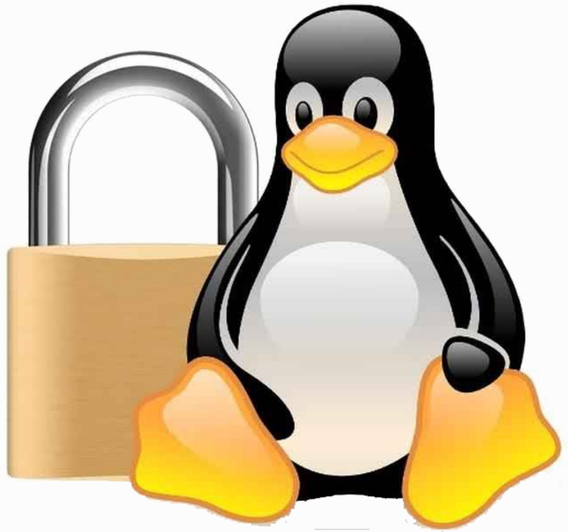
سناریو پنج: امن‌سازی ویندوز سرور

در این سناریو، یک رویکرد کامل برای امن‌سازی ویندوز سرور از طریق PowerShell اتخاذ شده است که به چند نمونه آن اشاره می‌شود:

- Disable services: Telnet service, FTP service, SNMP service, Remote Registry service
- Disable the Guest account
- Set a strong password policy
  - Minimum password length: 12
  - Password complexity: 1 (assumes complex passwords are required)
  - Password history size: 10
- Disable the built-in Administrator account
- Enable Windows Firewall

سناریو شش: فارنزیک در لینوکس

- Collect system information
- Gather event logs
- Capture running processes
- Retrieve network connections



سناریو هفت: ابزار فارنزیک تحت ویندوز

- در این سناریو، اطلاعات سیستم با استفاده از cmdletهای PowerShell جمع‌آوری می‌شود.
- گزارش‌های رویدادها، فرآیندهای در حال اجرا ضبط شده و کانکشن‌های شبکه بازیابی می‌شوند.

- Collect system information
- Gather event logs (Maximum of 1000 events retrieved)
- Capture running processes
- Retrieve network connections

با تشکر
از همراهیتان