



GMV SOLUCIONES GLOBALES INTERNET S.A.U.
© GMV 2023 – All rights reserved

The information contained within this document is considered as "GMV-Confidential". The receiver of this information is allowed to use it for the purposes explicitly defined, or the uses contractually agreed between the company and the receiver; observing legal regulations in intellectual property, personal data protection and other legal requirements where applicable.

Pentesting: Using AI and ChatGPT to compromise Computer Networks



GMV



Trusted Supplier of **Spanish MoD, Portuguese MoD** and **international Defense** organizations such as NATO and EDA.



Application of **groundbreaking artificial-intelligence technology** (dubbed “Artificial Immune Systems”) for **early fraud detection**.



GMV is chosen by the **European Space Agency (ESA)** to conduct an analysis of **cybersecurity risks** and set up a policy that establishes a series of control recommendations for the space missions.



GMV developed ***SimulIT***, the **only product of its category**. It calculates the resilience, the recuperation capacity of an information system asset by asset, with the objective of **protecting critical infrastructures** from possible cyber-attacks and guaranteeing the continuity of its activity.

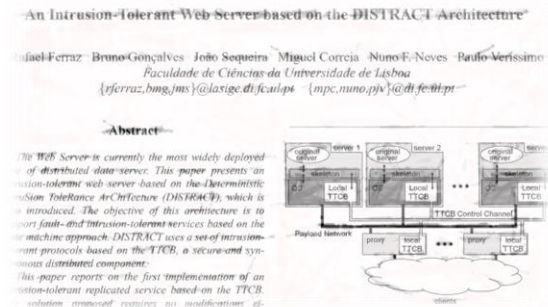
About Me



João Sequeira

**Director of SES -
Cybersecurity Unit Portugal**

- **Over 18 years experience in IT & Cybersecurity**
 - Unleashing hacker's mindset to fortify defenses.
 - Safeguarding applications with resilient measures.
 - Proactively mitigating vulnerabilities in the digital landscape.
 - Staying ahead of regulations, ensuring cybersecurity best practices.
- **Curious about AI**
 - Harnessing the power of artificial intelligence to assist Pentesters becoming more efficient and accurate identification of vulnerabilities.



The Challenge of Balancing Efficiency and Security

Embracing Proactive Cybersecurity Measures.

Technology has enhanced business communication, driving unparalleled efficiency. But new benefits also bring new risks, therefore companies need to adopt a proactive stance towards cybersecurity.



Why Penetration Testing

Simulate the actions an attacker could perform

One effective way to identify vulnerabilities and understand risk levels is through penetration testing.

Penetration testing provides valuable insights into potential weaknesses and entry points that malicious actors could exploit.

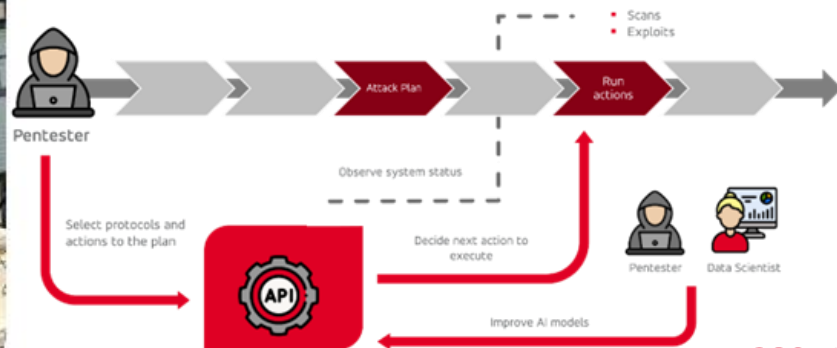


Leveraging AI for Penetration Testing

Train the system in a simulated scenario

The AI model is trained with reinforcement learning and integrated with hacking tools to execute actions

It learns from a vast array of attack scenarios and past pentesting plans, allowing it to adapt and evolve alongside emerging threats.



Enhancing Penetration Testing with LLMs

Increases efficiency, reducing *human* errors

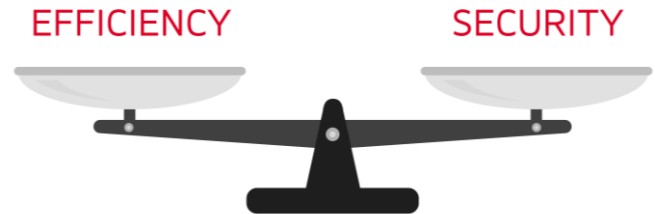
Facilitates Information Gathering

Helps phishing campaigns

Helps Generate Payloads for Exploitation

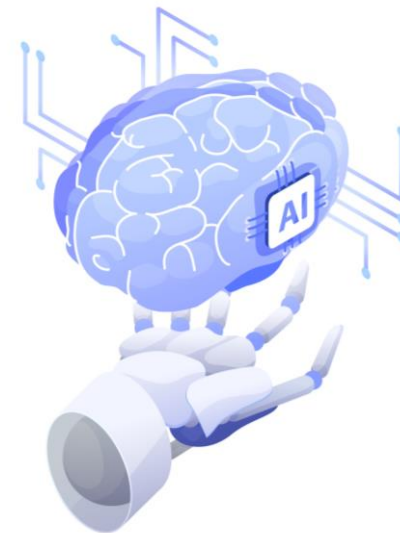
Vulnerability Assessment

Report Generation



Where LLMs Can Help

- Write convincing phishing emails for credential Harvesting
- Help create the web page
- Planning the tasks to be performed during an engagement
- Suggesting test tools and the next steps
- Suggesting tool parameters/commands to use
- Interpret and summarize the outputs
- Find Vulnerabilities in Code



Launch a Phishing Email



⚡ GPT-3.5

⚡ GPT-4 🔒

ChatGPT

Make up a story

about Sharky, a tooth-brushing shark superhero

Compare design principles

for mobile apps and desktop software

Suggest fun activities

to do indoors with my high-energy dog

Plan a trip

to explore the Madagascar wildlife on a budget

Send a message



Exploit Vulnerabilities



GPT-3.5

GPT-4

ChatGPT

Show me a code snippet
of a website's sticky header

Give me ideas
for what to do with my kids' art

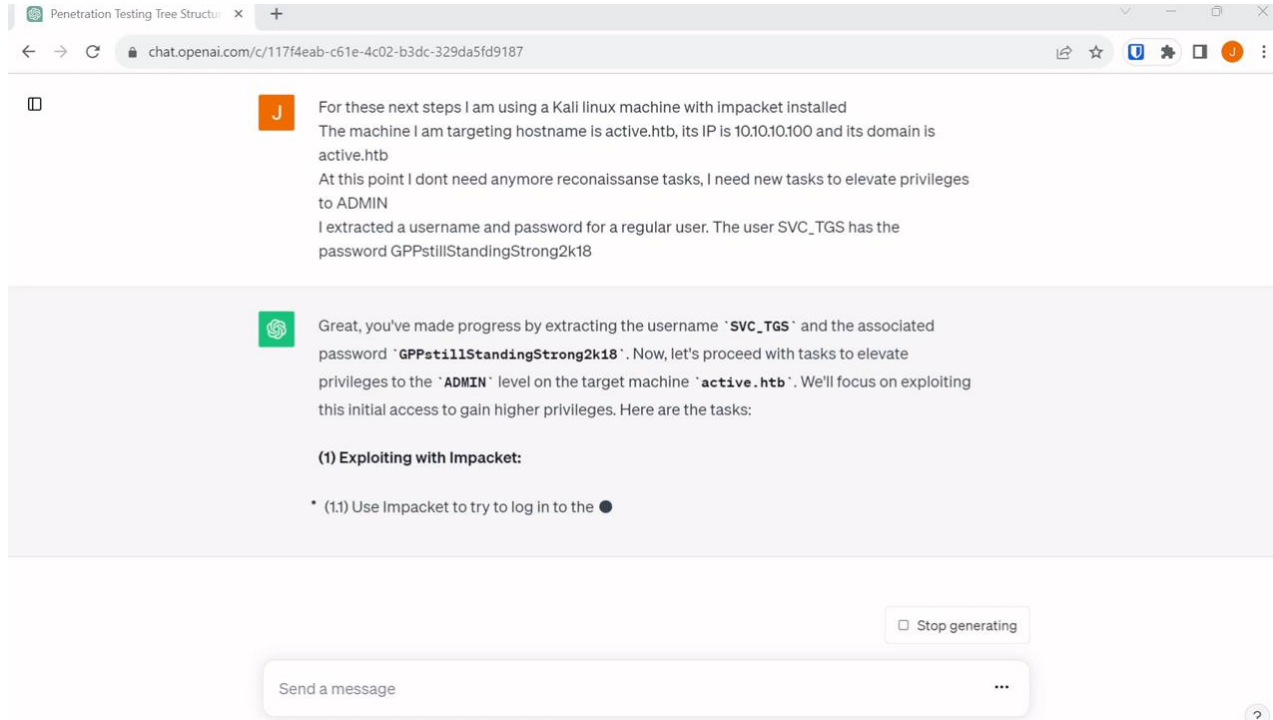
Design a database schema
for an online merch store

Make a content strategy
for a newsletter featuring free local weekend events

Send a message



Exploit a Domain Controller



Penetration Testing Tree Structure x

chat.openai.com/c/117f4eab-c61e-4c02-b3dc-329da5fd9187

J

For these next steps I am using a Kali linux machine with impacket installed
The machine I am targeting hostname is active.htb, its IP is 10.10.10.100 and its domain is active.htb
At this point I dont need anymore reconnaissance tasks, I need new tasks to elevate privileges to ADMIN
I extracted a username and password for a regular user. The user SVC_TGS has the password GPPstillStandingStrong2k18

GPT-4o

Great, you've made progress by extracting the username `'SVC_TGS'` and the associated password `'GPPstillStandingStrong2k18'`. Now, let's proceed with tasks to elevate privileges to the `'ADMIN'` level on the target machine `'active.htb'`. We'll focus on exploiting this initial access to gain higher privileges. Here are the tasks:

(1) Exploiting with Impacket:

- (1.1) Use Impacket to try to log in to the ●

Stop generating

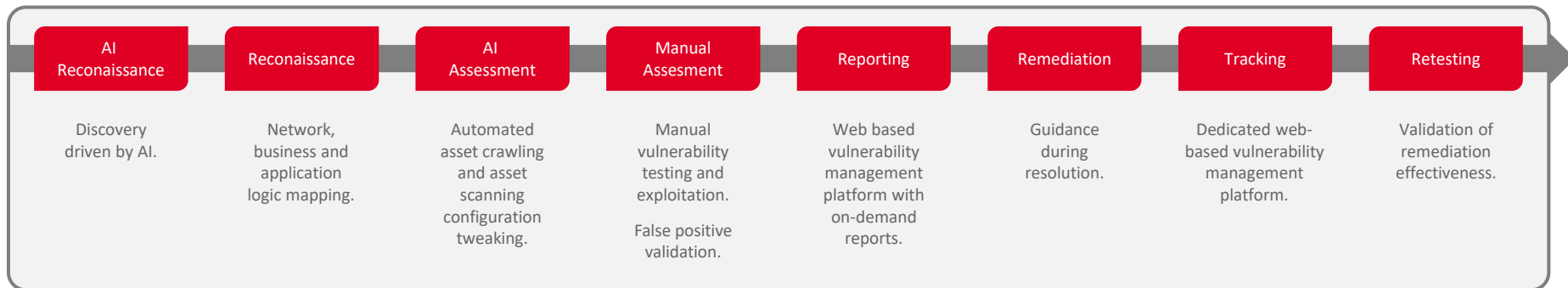
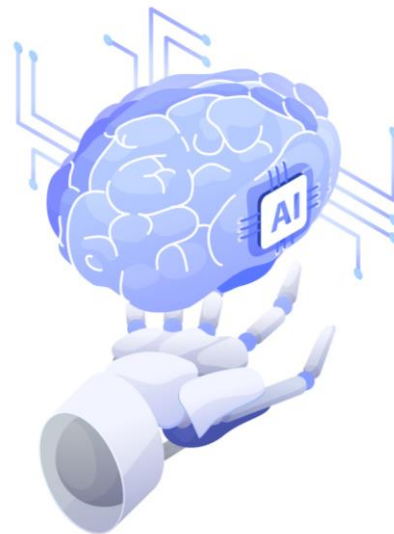
Send a message

AI-ASSISTED PENETRATION TESTING

GMV AI-enhanced approach

- GMV's AI-enhanced pentesting capabilities enable security teams to more efficiently surface threats and remediate vulnerabilities. Our approach significantly shortens the time required to conduct comprehensive assessments without compromising quality or accuracy.

This is done without compromising quality or accuracy, as AI only assists human testers - it does not replace them. By reducing the human hours needed through AI acceleration, we are able to package pentesting services competitively while maintaining our commitment to a first-class service with zero false positives.



Contact us

João Sequeira

joao.sequeira@gmv.com

Hall 7A - Booth Number 7A-220

