

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Social Engineering & Dark AI/NLP THROUGH KALI](#)

Tyr - November 13, 2024, 5:40 pm

Currently restructuring this post so that it reads well. Figured I would post it in the meantime because I would like true, educational, precise, and accurate data pertaining to cybersecurity to be available here. Anything highlighted in red is important to focus on if you already know the filler; i.e. program and tool names as well as basic TTP. This is a super rough draft that will be updated throughout the week.

PART 1.)

Context: Social engineering leverages psychological manipulation to exploit human error for gaining confidential information or access. With the advent of Natural Language Processing (NLP), attackers can automate and refine their tactics, making social engineering campaigns more convincing and scalable.

Step 1: Profiling the Target

NLP techniques can be used to gather and analyze public information about the target:

Data Extraction:

Use web scraping and NLP tools to collect social media posts, emails, and public documents.

Sentiment Analysis:

Understand the target's emotional state from their communication style.

Topic Modeling:

Identify topics they frequently discuss, e.g., hobbies, work-related issues, or personal interests.

Tools: Python libraries like BeautifulSoup for scraping, NLTK or spaCy for text analysis.

Step 2: Crafting Personalized Messages

Tone Adaptation: Use NLP models to mimic the writing style of a trusted contact or create messages that align with the target's tone. Those experienced with NLP also utilize a form of Language Generation to deploy models like GPT to craft believable phishing emails or chat messages. You may know this if you're experienced with AI but half of this was generated by AI querying for the tools I asked it to. Do not underestimate the power of behavioral analysis, applied.

Politeness/Professionalism Scoring: Tailor the message to be either formal or casual based on prior analysis.

Example: An email imitating a manager's tone asking for urgent file access. Play upon the following principalities and you will be successful if you can be persuasive: Urgency, intimidation, social proof (most usually done through familiarity), scarcity, and trust.

Step 3: Real-Time Interaction Using Chatbots

NLP-powered chatbots can simulate real-time conversations:

Conversational AI:

Chatbots can interact naturally, persuading the target to reveal information.

Dynamic Questioning:
Based on the target's responses, the chatbot can adjust its queries to gather sensitive details incrementally.

Tools: Rasa, Dialogflow for conversational agents.

Step 4: Exploiting Trust via Audio Synthesis

Text-to-Speech Synthesis: Convert written scripts into speech, mimicking a trusted individual.
Voice Cloning: Use recorded audio samples to create a realistic replica of someone's voice. This technique can be employed in vishing (voice phishing) to bypass suspicions. This is also known as SPIT if used appropriately for a replay data capture attack where you use telephony to capture the voice of a victim to replay in biometric authentication attack.

Tools: Descript, ElevenLabs.

Step 5: Reinforcing Credibility with Deepfake ContentVideo Deepfakes:

Create video content showing a trusted individual delivering false instructions.Facial Expressions Analysis:

My favorite of these; and the reason why I use a mini dot that slides over my phone camera is because of the following capabilities combined with psychological TTP that can be used for espionage related purposes. For example, NLP combined with computer vision can identify the target's trust indicators, ensuring the deepfake aligns emotionally.

Step 6: Evasion and AdaptationAdversarial Text Generation:

Avoid detection by anti-phishing tools through subtle variations in text.Feedback Loops:
Analyze the target's responses using NLP for continual improvement of scripts.

PART 2.) This hypothetical guide goes on to illustrate how NLP with specific programs contained can enhance social engineering techniques while using Kali Linux with a breakdown of some of the most popular tools for doing so.

Tools:

Recon-ng: Automates reconnaissance, collecting publicly available information (OSINT).

TheHarvester: Gathers email addresses, subdomains, and employee names from sources like LinkedIn and Google.

Maltego: Provides data visualization and mapping to establish connections between people, organizations, and infrastructure.

NLP Techniques:

Sentiment Analysis: Extract emotional context from social media posts using Python libraries such as NLTK or spaCy.

Named Entity Recognition (NER): Identify key entities like names, locations, and organizations from public communications.

Workflow:

Use TheHarvester to collect emails and domain data.

Analyze social media posts with sentiment analysis to understand tone and vulnerabilities.

Map relationships using Maltego to identify weak links for exploitation.

Step 2: Crafting Personalized Messages

Kali Linux Tools:

SET (Social-Engineer Toolkit): Facilitates crafting phishing emails and SMS messages.

Evilginx2: A man-in-the-middle attack framework, used for advanced phishing with real-time credential capture.

NLP Techniques:

Language Modeling: Use NLP models (e.g., GPT) to create persuasive, personalized messages.

Phishing Templates: Automate the generation of believable phishing emails or texts that match the target's communication style.

Workflow:

Use SET (social engineering toolkit) for SMS message crafting/creation. After this, deploy Evilginx2 to capture credentials via fake login pages on the other side. This is actually one of the best tools out there and with added configuration for GPT LLM's SET will be ahead of the ballgame if continued development team decides to implement this function.

Step 3: Real-Time Interaction Using Chatbots

Kali Linux Tools:

BeEF (Browser Exploitation Framework): Exploits the target's browser vulnerabilities and enables real-time interaction.

MSF (Metasploit Framework): Delivers payloads and maintains interaction once access is gained.

NLP Techniques through using Conversational AI to integrate chatbots with phishing campaigns to simulate trusted individuals.

Dynamic Responses: Adapt messages based on user behavior using Rasa or Dialogflow.

Workflow:

Exploit browser vulnerabilities via BeEF to establish a live session.

Use NLP chatbots to interact in real time, collecting sensitive information.

Step 4: Exploiting Trust via Audio and Video

Kali Linux Tools:

Gophish: A phishing framework to distribute multimedia-based attacks.

Cewl: Generates wordlists based on target profiles, useful for brute-forcing and password-related attacks.

NLP Techniques:

Voice Cloning: Use tools like Descript for phishing calls.

Deepfake Videos: Deploy pre-recorded messages that mimic trusted individuals.

Workflow:

Use Cewl to generate passwords based on targets' speech patterns or text usage.

Send multimedia phishing campaigns using Gophish.

Step 5: Reinforcing Credibility with Exploit Techniques

Blind SQL Injection (SQLi):

SQLmap (Kali Linux): Automates SQL injection attacks.

Example: Use NLP to identify potential SQL error messages in public data. Automate blind SQLi to extract data.

Types of XSS:

Stored XSS: Permanently inject malicious scripts.

Reflected XSS: Use phishing links to reflect payloads.

DOM-based XSS: Exploit JavaScript vulnerabilities on the client side.

Tool: XSSStrike to detect and exploit XSS vulnerabilities.

Remote File Inclusion (RFI):

Metasploit Framework: Exploits file inclusion vulnerabilities to execute remote scripts.

Step 6: Evasion and Adaptation

Kali Linux Tools: TorghostNG: Routes traffic through Tor for anonymity.

Proxychains: Chains multiple proxies for enhanced anonymity.

NLP Techniques:

Adversarial Text Generation: Generate phishing emails that bypass spam filters.

Feedback Loops: Use NLP to analyze the effectiveness of phishing campaigns and refine them

iteratively.

sammy1s - November 14, 2024, 9:08 am

Huge respect for this

Tyr - November 14, 2024, 12:43 pm

(Nov 14, 2024 10:08 AM)sammy1s Wrote: [\[CITE\]](#) Huge respect for this

Of course. I'm just trying to contribute some stuff that might help some of the more seasoned players out there but I will make some easier tutorials throughout the month. I just want to stress that this guide and many of the stuff I may post are not recommended for the beginner, lol.

CjSystem2030 - November 14, 2024, 2:56 pm

gracias por el contenido

Tyr - November 14, 2024, 7:17 pm

(Nov 14, 2024 03:56 PM)CjSystem2030 Wrote: [\[CITE\]](#) gracias por el contenido

No hay de qué! Please correspond in English though because other members may not understand.

Gawin - June 4, 2025, 10:17 am

Huge respect for this

Tyr - June 4, 2025, 10:51 am

(Jun 4, 2025 10:17 AM)Gawin Wrote: [\[CITE\]](#) Huge respect for this
u got it boss

7 - June 4, 2025, 11:13 am

Good write up.

Nice thread

alot of this could be automated.

HerrWinston - June 6, 2025, 9:49 am

I really like this tutorial, thanks for creating this thread man

Tyr - June 7, 2025, 2:07 am

(Jun 6, 2025 09:49 AM)HerrWinston Wrote: [\[CITE\]](#) I really like this tutorial, thanks for creating this thread man

You are welcome.

and ye, a lot, if not most, can be automated but that would be an entire new thread in of itself as we both know [7](#)

HerrWinston - June 7, 2025, 11:31 am

(Jun 7, 2025 02:07 AM)Tyr Wrote: [\[CITE\]](#) You are welcome.

and ye, a lot, if not most, can be automated but that would be an entire new thread in of itself as we both know [7](#)

yeah thats a whole different story and way to complicated for me lol

s1m0nc - June 21, 2025, 8:37 am

Thanks for your sharing

lincoln - July 11, 2025, 5:14 am

This feels like a cheat code

Tyr - July 16, 2025, 12:18 am

(Jul 11, 2025 05:14 AM)lincoln Wrote: [\[CITE\]](#) This feels like a cheat code
Indeed. My mind got carried away during it xd