

OSINT Project

Emily Jao, Aruzhan Yegemberdi, Sinanye Burton-
Captain



Cybersecurity: Pentesting



Definition & Technique

Overview:

Penetration testing is an OSINT tool that performs cyber-attacks on a company to find the weaknesses in the system. All the data searching, as part of the penetration test, culminates in a cyber-attack by targeting the domain, program, or individual.

Steps:

1. Performing extensive analysis through social media and metadata analysis, web scraping, and exploring public databases.
2. Flagging information and weak links that can be used to hack into the company's system.
3. Try to hack into the company by exploiting its weaknesses. One powerful tool used by cyber attackers is phishing emails.

Use Cases

1. Identify the social media pages of relevant employees, those working for the company.
2. Pages that share sensitive data related to the company are flagged down as a high priority.
3. One individual working in the IT department has shared sensitive information that identifies the type of program and software used to operate the company's system. Through this knowledge, the team performs a red teaming penetration test by hacking into the system through the use of the appropriate program.
4. Another scenario is that by analyzing human data, the hackers can send personalized phishing emails to break into the system.

It is important to educate employees on proper security measures and practices.

Ethical Considerations

- Companies need to give consent and have a full understanding of the process of penetration testing
 - Sign an NDA
 - Total transparency
- There is a fine line between ethical and unethical breach of personal data and information
- Teams performing such cybersecurity regulations need to follow all the laws and rules put forth

Web Scraping

The background is a dark, abstract digital space. It features numerous glowing orange and yellow lines that crisscross the frame, creating a sense of dynamic movement and data flow. Interspersed among these lines are various digital symbols, including binary code (0s and 1s) and stylized representations of data structures or code snippets. Some elements appear to be floating or falling, giving the impression of a 3D digital environment. The overall color palette is dominated by the warm tones of the glowing lines and the cool blues and greys of the background.

Technique and Definition

- What is web scraping?
 - An automated AI method that is often used to collect very large amounts of data from multiple websites

Use Cases

- The main use of web scraping is to collect troves of data
- For example, your web scraping program can collect the different prices of a specific item such as a blender from the multiple websites it is sold on
- You can also use web scraping to collect information on a person, such as the 19th president

Ethical Considerations

- **Web Scraping: Proceed with Caution**
 - Web scraping can be a useful tool, but it's important to approach it responsibly. While web scraping is legal, scraping for personally identifiable information and exposing it can be harmful.
 - Another consideration is the impact of exhaustive scraping on a website. Overloading a website can disrupt a company's business operations and affect other users.
- **Best Practices for Web Scraping:**
 - Use web scraping only when necessary.
 - Consider using a website's built-in API as an alternative.

Social Media Analysis



Definition & Techniques

- Definition
 - Social Media Analysis is a method that collects and checks information from various social media platforms, like Instagram and Facebook, to extract valuable insight.
 - This helps individuals and organizations take advantage of the large amount of information available online for their purposes.
- Techniques
 1. **Goal:** Define the information you want to explore.
 2. **Platform Selection:** Choose the social media platform for data collection.
 3. **Data Collection:** Gather relevant profile and post details.
 4. **Verification:** Cross-check the information with other sources for accuracy.

Use Cases

- Criminal Investigation

- Social media helps police gather evidence, track suspects, and solve cold cases.
- Posts and messages can reveal clues to locate missing persons.

- Global Event Monitoring

- Tracks real-time news and major events worldwide.
- Keeps people informed about natural disasters, political changes, and other critical incidents.

- Brand Monitoring

- Analyzes customer opinions about companies or products.
- Helps businesses understand public perception and improve services.

Ethical Considerations

- It is crucial in following these considerations:
privacy anonymity, legal issues, and ethical guidelines.
 - Firstly, during social media research, protecting one's identity and privacy secret is crucial. This is not to violate one's privacy rights and protect their identity while doing the work.
 - Secondly, when gathering information, it's important to recognize the legal rules, such as terms of service. By knowing these rules, anyone can avoid problems while collecting information.
 - Finally, one must follow guidelines for social media research. This means only gathering information from public sites or users, instead of hacking into one's system.

Sources

- Pentesting:
 - <https://www.blackduck.com/glossary/what-is-penetration-testing.html#:~:text=Definition,of%20weaknesses%20in%20a%20system.>
 - <https://www.rapid7.com/fundamentals/penetration-testing/>
 - <https://www.vaadata.com/blog/cybersecurity-osint-methodology-tools-and-techniques/>

ChatGPT Revision – Penetrative Testing

For a presentation about penetrative testing can you word this in a better format "Cases:

One specific scenario is that a company can hire a specific cybersecurity team to assess and perform a penetration test. The team first starts by identifying the social media pages of relevant employees, those working for the company. This information is further narrowed down by relevance. Pages that share sensitive data related to the company are flagged down as a high priority. One individual working in the IT department has shared sensitive information that identifies the type of program and software used to operate the company's system. Through this knowledge the team performs a red teaming penetration test by hacking into the system through the use of the appropriate program.

Another scenario is that by analyzing human data, the hackers can send personalized phishing emails to break into the system. In both cases, it is important to educate the employees on proper security measures. "

Sure! Here's an improved version of your cases section for a clearer and more professional presentation:

Cases:

One common scenario involves a company hiring a specialized cybersecurity team to conduct a penetration test. The team begins by identifying social media profiles of employees relevant to the organization. This data is then filtered for sensitivity, with particular focus placed on pages that disclose critical company information. For instance, an employee in the IT department may unknowingly share details about the software and programs used to run the company's systems. Using this information, the team conducts a red teaming exercise, simulating a real-world attack by exploiting the identified vulnerabilities and gaining unauthorized access to the system.

Another scenario focuses on leveraging human data to craft highly targeted phishing attacks. By analyzing personal information from social media or other sources, hackers can send convincing, personalized phishing emails to employees, which may lead to a breach of the company's network.

In both cases, the importance of educating employees on cybersecurity best practices is evident. Proper training can significantly reduce the risk of such attacks and mitigate the impact of any potential breaches.

For a presentation about penetrative testing can you word this in a better format "Overview:

Penetration testing is an OSINT tool that performs cyber-attacks on a company to find the weaknesses in the system. This cybersecurity technique utilizes OSINT tools using social media analysis and web scraping to look for weaknesses. Since companies are made up of employees, both technical and human data are collected to identify potential threats and vulnerabilities. All of the OSINT data searching culminates in a cyber-attack by targeting the domain, program, or individual. "

Sure! Here's a revised version of your overview for clarity and flow:

Overview:

Penetration testing is a cybersecurity practice that simulates cyber-attacks on an organization to identify vulnerabilities within its systems. It leverages Open Source Intelligence (OSINT) tools, such as social media analysis and web scraping, to gather information and uncover potential weaknesses. Since organizations consist of both technical infrastructure and human elements, penetration testing collects data from both domains to assess threats. This comprehensive approach leads to targeted cyber-attacks that focus on the company's network, applications, or individual personnel to pinpoint vulnerabilities.

Let me know if you need further adjustments or have other sections to work on!

For a presentation about penetrative testing can you word this in a better format "Ethical Consideration:

Essentially, the team performing a penetration test is hacking into the company's system. As such, they need to be fully aware of ethical considerations associated with such an action. The main concepts to be aware of are consent and breach of information. The team needs to make sure to obtain full consent from the company and sign an NDA. After the completion of the test, they need to be fully transparent and cooperative. All the laws and regulations on ethical hacking must be followed. "

Sure! Here's a refined version of your "Ethical Considerations" section:

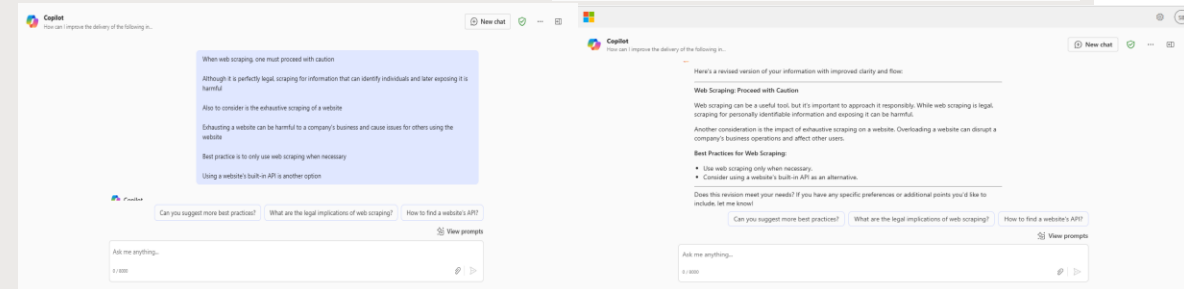
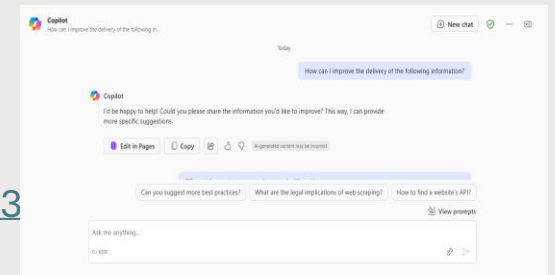
Ethical Considerations:

Penetration testing, by its nature, involves hacking into a company's systems, making it crucial for the testing team to be mindful of the ethical implications. The primary ethical concerns are obtaining proper consent and protecting sensitive information. Before starting the test, the team must secure explicit consent from the company and ensure that a non-disclosure agreement (NDA) is in place to protect any confidential data.

Once the test is completed, the team must maintain full transparency, providing detailed findings to the company, and cooperating fully in addressing any vulnerabilities discovered. Additionally, the team must adhere to all relevant laws, regulations, and ethical guidelines surrounding ethical hacking practices.

Sources

- Web Scraping:
 - <https://www.geeksforgeeks.org/what-is-web-scraping-and-how-to-use-it/>
 - <https://research.aimultiple.com/web-scraping-ethics/>
 - Microsoft Copilot Chat
 - <https://copilot.microsoft.com/?msocid=07e09e059635654c3323a>



Sources

- Social Media Analysis:

- <https://osintteam.blog/social-media-osint-a-comprehensive-guide-to-gathering-intelligence-from-social-media-platforms-b5dbb8d83f14>

- ChatGPT

- Chatgpt. (n.d.-a).

<https://chatgpt.com/>



hi ChatGPT, how can I better be concise and organized on how I phrase my key steps?:Key Steps:
Goal: Set a goal where one can determine what information is to be explored.
Preference: Choose a platform where one can start exploring.
Investigate: Gather data from the user's profile and posts, including important data or details needed.
Verify: Check if the information is accurate by comparing it to other resources.

Here's a clearer and more concise version of your key steps:

Key Steps:

1. **Goal:** Define the information you want to explore.
2. **Platform Selection:** Choose the social media platform for data collection.
3. **Data Collection:** Gather relevant profile and post details.
4. **Verification:** Cross-check the information with other sources for accuracy.

✅ This version is more streamlined and uses consistent, precise language. Let me know if you want further revisions!



hi ChatGPT, how can I better be concise on my phrasing and have it organized and hierarchal for my use cases? Use Cases:
This technique can be used for cases like criminal investigations, global events, and brand monitoring. Firstly, during criminal investigations, social media helps the police find information and evidence related to crimes. By looking through posts and text messages, they can obtain clues that help them to solve cold cases and find missing people. Secondly, for tracking global events, social media can keep an eye on global events with news and crucial events around the world. This helps people be informed about what is occurring from natural disasters to political changes. Finally, for brand monitoring, social media can keep account of what people say about a company or product. By listening to the opinion of customers, business can better understand how they are seen and if their services improved.

Here's a more concise, organized, and hierarchal version of your use cases:

Use Cases:

1. **Criminal Investigations:**
 - Social media helps police gather evidence, track suspects, and solve cold cases.
 - Posts and messages can reveal clues to locate missing persons.
2. **Global Event Monitoring:**
 - Tracks real-time news and major events worldwide.
 - Keeps people informed about natural disasters, political changes, and other critical incidents.
3. **Brand Monitoring:**
 - Analyzes customer opinions about companies or products.
 - Helps businesses understand public perception and improve services.

✅ This version uses clear, concise phrasing with a consistent structure, making it easier to read and follow. Let me know if you want further tweaks!

