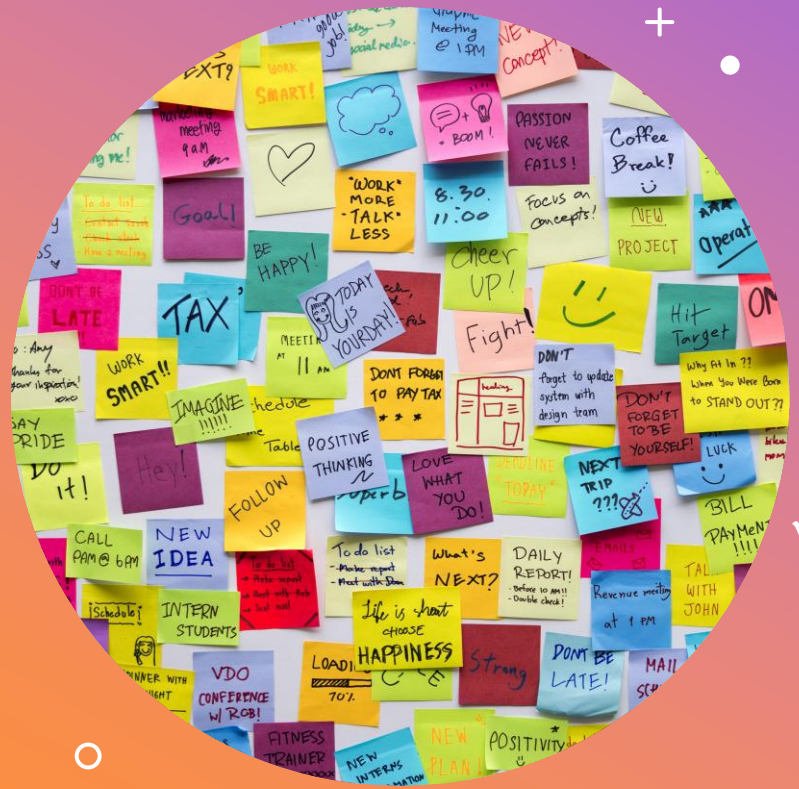
PART 0.1 TAKING NOTES AND SCREENSHOTS

Cracking OSCP: Your Roadmap to Ethical Hacking Success

YouTube : HackProKP – Kailash Parshad

LinkedIn : Kailash Parshad

TODAY'S AGENDAS



- ✓ How to take Proper Notes
- ✓ Why Note Taking is important for Ethical Hackers
- ✓ Which note-taking applications are good
- ✓ My recommendations (Note Taking Applications)
- ✓ Notes vs Reports
- ✓ Looking at Sample Notes and Report
- ✓ Why screenshots are important
- ✓ How Captions Below Screenshots Enhance Note-Taking
- ✓ Which screenshots applications are good
- ✓ My recommendations (Screenshot Applications)
- ✓ Summary

How to take “Proper Notes”

1. **Comprehensive Documentation:** Every action we take, whether it's running a command, modifying exploit code, or interacting with a graphical user interface (GUI), should be meticulously documented within our notes. This creates a detailed record of our hacking journey.
2. **Record Everything:** I will emphasize the importance of recording every detail. This practice is not just for the sake of documentation but as a safeguard against any potential regrets or oversights in the future
3. **Future-Proofing:** I will stress the significance of portability and structured formatting in note-taking. Having a standardized format for your notes is crucial. It ensures that even if you need to switch testers or collaborate with others, there's no room for confusion or errors when compiling reports.
4. **Understanding is Key:** At the end of the day, the true test of proper notes is your ability to understand and make use of them. Notes should not be a jumble of information but a coherent map of your hacking journey, providing clarity and guidance as you work through cybersecurity challenges.

WHY NOTE TAKING IS IMPORTANT FOR ETHICAL HACKERS

Taking Notes and Screenshots

1. **Client-Centric Focus:** The clients are ultimately paying for the comprehensive report, not just the penetration test itself. The report is the tangible output that provides value and insights to the client.
2. **Crucial for Report Preparation:** A detailed and well-structured report must be submitted to the client after a penetration test. This report should cover all aspects of the assessment, including what was done, what vulnerabilities and misconfigurations were discovered, and proposed solutions. Effective note-taking serves as the foundation for creating such a report.
3. **Memory Aid**: The practical aspect of note-taking serves as a memory aid. Even if you've taken extensive notes, it can be challenging to remember the specifics of the assessment later without well-organized and comprehensible notes.
4. **Ensuring Reproducibility**: The importance of coherence in note-taking is very important. Written and organized notes enable others, including colleagues or different testers, to reproduce the test and achieve the same results.
5. **Accessibility and Understanding**: The final report needs to be accessible and understandable to a wide audience, including those who may not have a technical background. the report should answer critical questions like what happened, why certain aspects are considered flaws or weaknesses, how threat actors could exploit them, what impact these vulnerabilities could have on the client's business, and how to address them effectively.

WHICH NOTE-TAKING APPLICATIONS ARE GOOD

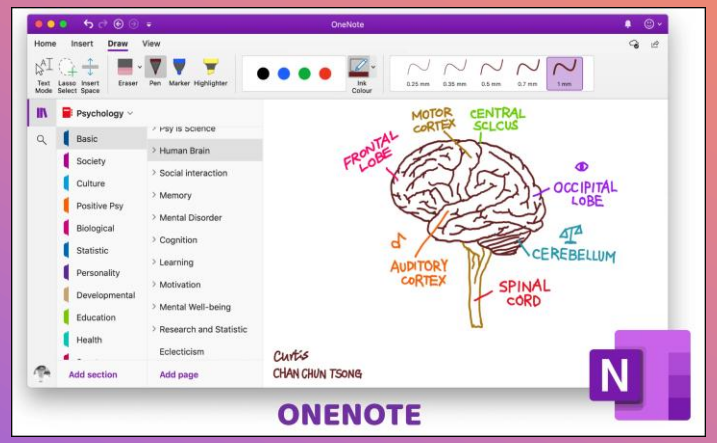
Taking Notes and Screenshots

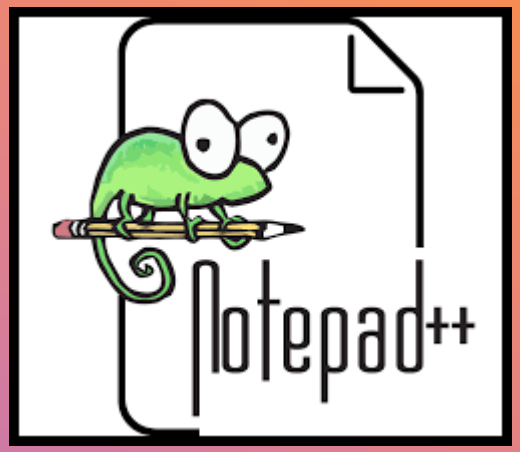
1. **Evernote:** Evernote is a versatile and feature-rich note-taking app known for its ability to organize notes effectively. It offers features like tagging, syncing across devices, and the ability to include various media types within your notes, making it a versatile choice for keeping track of your findings.
2. **OneNote:** Developed by Microsoft, OneNote is another powerful note-taking application. It's well-integrated with other Microsoft Office apps and offers a hierarchical notebook structure that can be useful for organizing your notes. It's also available on multiple platforms.
3. **Joplin:** Joplin is an open-source note-taking app that's gaining popularity for its security and privacy features. It supports end-to-end encryption, making it suitable for ethical hackers who prioritize data security.
4. **Notion:** Notion is a highly customizable note-taking and collaboration app. It allows you to create databases, boards, and tables within your notes, making it a versatile choice for organizing and structuring your findings and reports.
5. **Standard Markdown Editors:** Some ethical hackers prefer using plain text editors that support Markdown, a lightweight markup language. Applications like Notepad++, Visual Studio Code with Markdown extensions or dedicated Markdown editors offer simplicity and flexibility in note-taking.

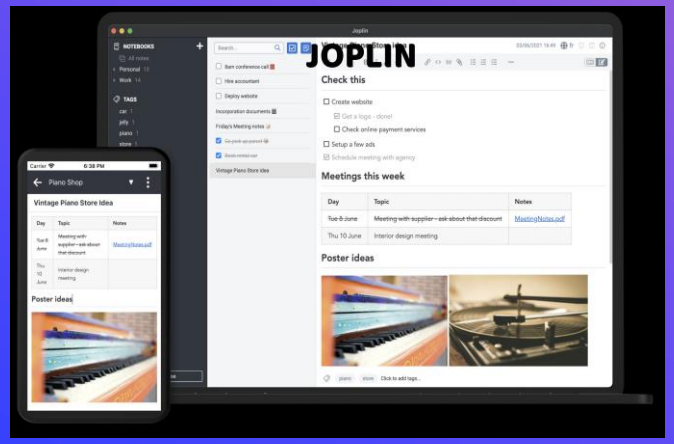
✓ More honorable mention:-

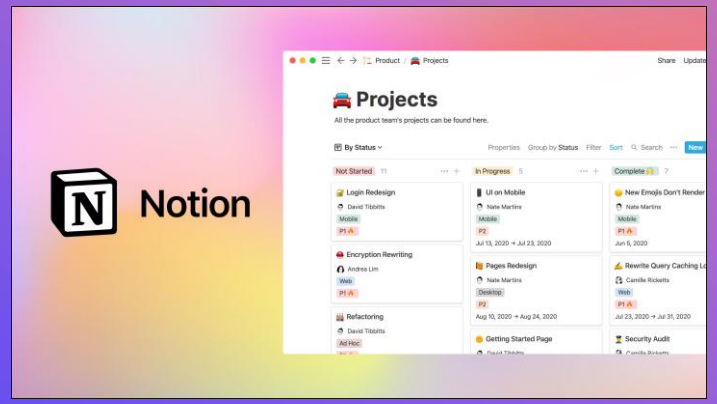
- **Google Keep:** Google Keep is a simple and intuitive note-taking application developed by Google. It's designed for quick and easy note-taking, list-making, and reminders. Keep allows users to create notes with text, images, and checkboxes. Notes are synchronized across devices if you have a Google account, making it easy to access your notes from anywhere.
- **Obsidian:** Obsidian is a versatile knowledge management and note-taking application that focuses on creating a network of interconnected notes. It is designed to create a personal knowledge base, and it encourages users to build links between their notes to explore relationships and patterns in their information. Obsidian supports markdown formatting and allows for the use of plugins to extend its functionality.
- **CherryTree:** CherryTree is an open-source hierarchical note-taking application that excels at organizing and structuring information. It allows users to create and manage notes in a hierarchical tree structure, making it suitable for detailed and structured note-taking. CherryTree supports rich text formatting, code blocks, syntax highlighting, and the ability to insert images and attachments.
- **Sublime Text:** Sublime Text is a highly customizable and feature-rich text editor primarily designed for code editing. However, it is also used for general text-related tasks, including note-taking. Sublime Text is known for its speed, responsiveness, and extensive package ecosystem. It offers features like multiple selections, syntax highlighting, and a distraction-free writing mode.
- **Keepnote:** Keepnote is an open-source note-taking application that allows users to organize information in notebooks and hierarchical folders. It offers features such as rich text formatting, file attachments, screenshots, and searching capabilities. Keepnote is especially suited for structured note-taking and research projects.

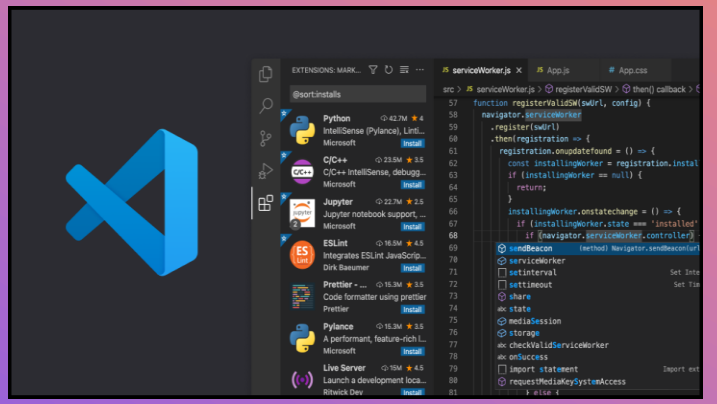
TAKING NOTES AND SCREENSHOTS





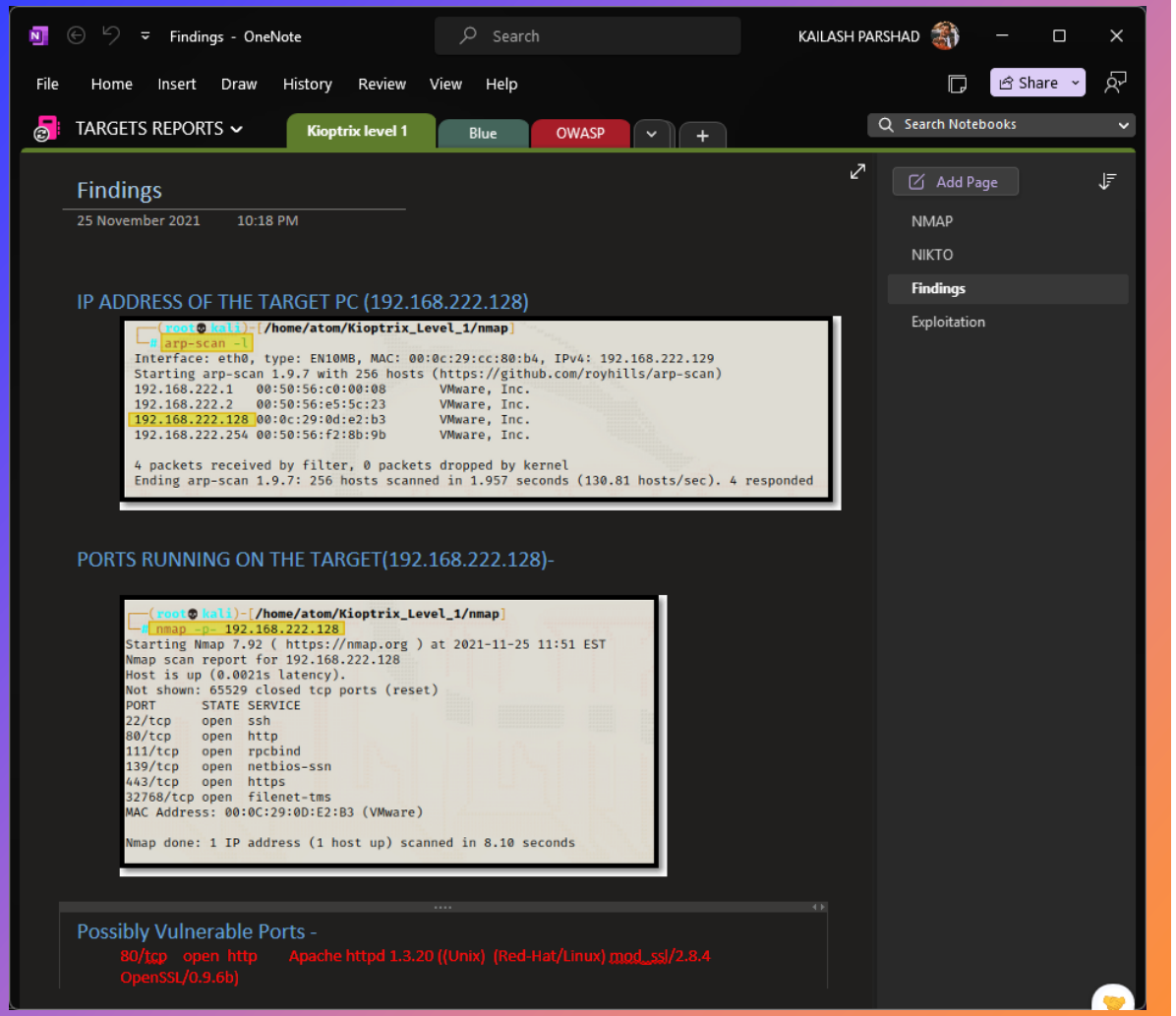






MY RECOMMENDATIONS (NOTE-TAKING APPLICATIONS)

Taking Notes and Screenshots



My choice is : -

OneNote:

- ✓ *Integration with Microsoft Ecosystem*
- ✓ *Cross-Platform Compatibility*
- ✓ *Organizational Flexibility*
- ✓ *Rich Note-Taking Features*
- ✓ *Collaboration and Sharing*
- ✓ *Syncing and Cloud Storage*
- ✓ *Search and Organization*
- ✓ *Security and Privacy*
- ✓ *Extensibility*

NOTES VS REPORTS

Taking Notes and Screenshots

• Notes:

1. **Informal Documentation:** Penetration test notes are typically informal and unstructured. They serve as a personal log or diary of actions taken during a security assessment.
2. **Real-Time Record:** These notes are created in real-time as the ethical hacker conducts tests, executes commands, and explores vulnerabilities. They capture every action, observation, and discovery during the test.
3. **Technical Details:** Pen test notes often include highly technical details, such as specific commands executed, IP addresses, network configurations, exploit code snippets, and log entries. They are intended to be a raw, technical record of the assessment.
4. **Quick Reference:** Ethical hackers refer to their notes during the assessment to backtrack, retest, or verify findings. It helps them maintain a clear understanding of what they've done and what still needs to be explored.
5. **Personal Use:** Penetration test notes are primarily for the personal use of the ethical hacker or the testing team. They aid in keeping track of the testing process and can help troubleshoot issues or revisit certain steps.

• Reports:

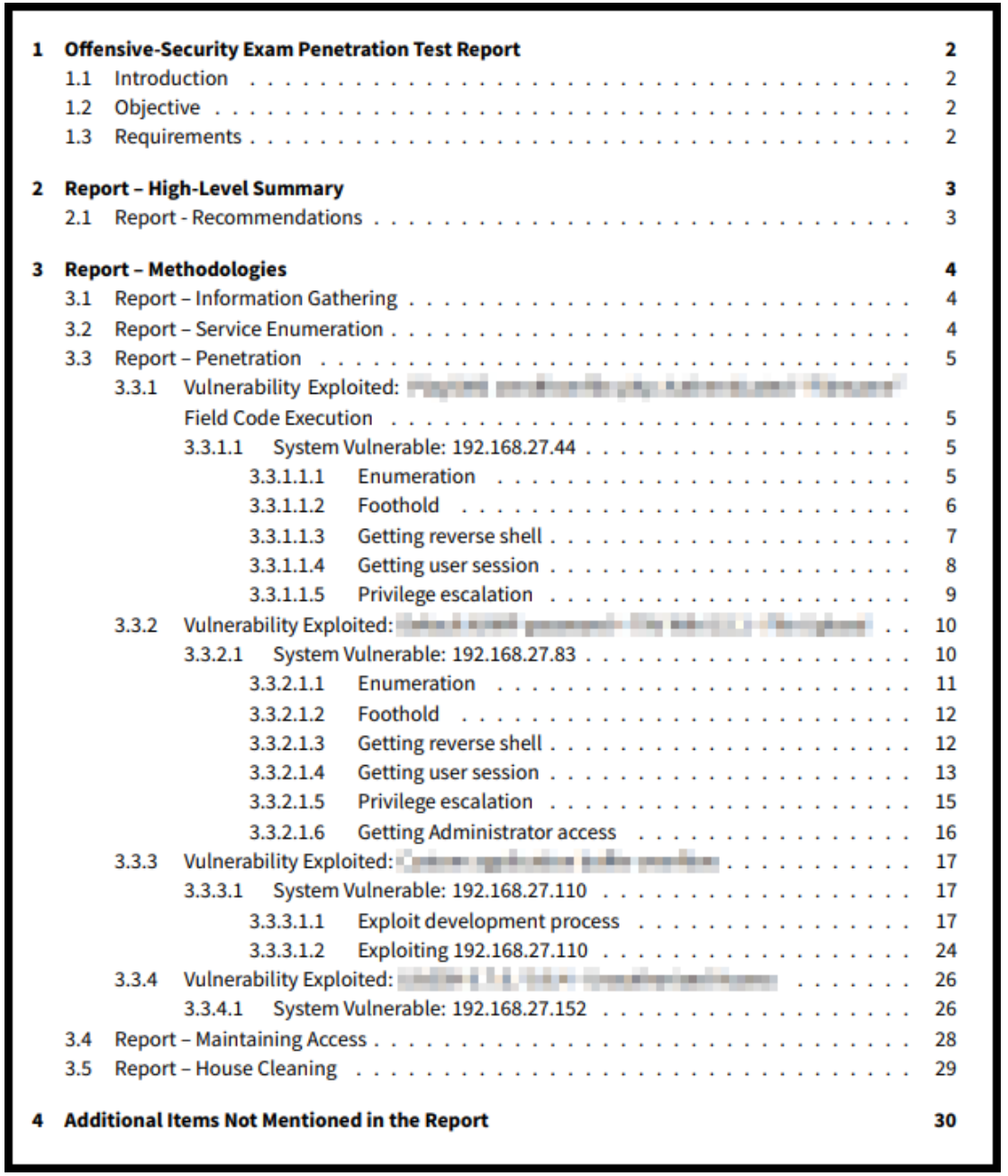
1. **Formal Documentation:** Penetration testing reports are formal and structured documents that summarize the results of a security assessment. They are intended for communication with clients and stakeholders.
2. **Post-Assessment:** These reports are created after the assessment is completed, once the ethical hacker has gathered and analyzed all the necessary data.
3. **Non-Technical Language:** Penetration testing reports are written in a way that is accessible to a broader audience, including non-technical stakeholders. They focus on explaining findings, risks, and recommendations in plain language.
4. **Summary of Findings:** Reports provide a concise summary of vulnerabilities, misconfigurations, and weaknesses discovered during the test. They prioritize and categorize issues based on severity.
5. **Recommendations:** Penetration testing reports include recommendations for mitigating identified vulnerabilities and improving overall security. These recommendations are actionable and guide risk reduction.
6. **Compliance and Decision-Making:** Reports are used by clients and organizations to make informed decisions about security improvements, compliance with industry standards, and risk management.

LOOKING AT SAMPLE NOTES AND REPORT

Taking Notes and Screenshots

Report Structure

Title Page
Table of Contents
Executive Summary
Introduction
Scope and Methodology
Findings and Vulnerabilities
Recommendations
Exploitation and Proof of Concept
Methodology and Tools
Appendices (if applicable)
Conclusion
Acknowledgments



https://www.offsec.com/pwk-online/OSCP-Exam-Report.docx

```
OSCP/
├── Offensive Security Lab Penetration Test Report
│   ├── Introduction
│   ├── Objective
│   └── Scope
├── High-Level Summary
│   └── Recommendations
├── Methodologies
│   ├── Information Gathering
│   ├── Service Enumeration
│   ├── Penetration
│   ├── Maintaining Access
│   └── House Cleaning
└── Findings
    ├── Box1 - 10.10.10.10
    ├── Box2 - 10.10.10.11
    ├── Box3 - 10.10.10.12
    ├── Box4 - 10.10.10.13
    └── Box5 - 10.10.10.14
```

1. Findings and Vulnerabilities

1.1. Vulnerability 1: SQL Injection
- Severity: Critical
- Description: A SQL injection vulnerability was discovered in the login module, allowing an attacker to execute arbitrary SQL queries.
- Impact: An attacker can potentially access, modify, or delete sensitive data from the database.

Recommendation:
- Implement input validation and parameterized queries to mitigate the SQL injection risk.
- Regularly patch the database management system and the web application framework.

[Screenshot: Insert screenshot here]

1.2. Vulnerability 2: Cross-Site Scripting (XSS)
- Severity: High
- Description: Multiple instances of reflected and stored XSS vulnerabilities were identified in the application.
- Impact: Attackers can execute malicious scripts within the context of the user's browser, potentially stealing session cookies and compromising user accounts.

Recommendation:
- Implement input validation and output encoding to prevent XSS attacks.
- Educate developers on secure coding practices to avoid introducing new XSS vulnerabilities.

[Screenshot: Insert screenshot here]

WHY SCREENSHOTS ARE IMPORTANT

Taking Notes and Screenshots

Screenshots play a crucial role in penetration testing for several reasons:

1. **Visual Documentation:** Screenshots provide visual documentation of the tester's actions and findings. They capture the exact state of the system or application at a specific moment, making it easier to understand and replicate the testing process.
2. **Evidence of Vulnerabilities:** Screenshots serve as concrete evidence of vulnerabilities, misconfigurations, or issues discovered during the assessment. They can be used to illustrate the impact of these findings on clients and stakeholders.
3. **Enhanced Communication:** Screenshots are a powerful tool for communication. They allow testers to convey their observations and findings more effectively to clients, fellow team members, or system administrators who need to understand the security risks.
4. **Troubleshooting and Validation:** In the event of an issue or unexpected behavior, screenshots help testers troubleshoot and validate their findings. They can refer to the screenshots to identify the exact conditions that led to a particular result.
5. **Documentation of Exploits:** If an ethical hacker successfully exploits a vulnerability, a screenshot can capture the successful execution of an exploit code or the compromise of a system. This visual evidence is invaluable for reporting and remediation.

HOW CAPTIONS BELOW SCREENSHOTS ENHANCE NOTE-TAKING

Taking Notes and Screenshots

Captions below screenshots provide context and clarity to the captured images. They serve to enhance the effectiveness of screenshots in note-taking:

1. **Contextual Information:** Captions explain what the screenshot depicts, providing context to the reader. This includes details about the system, the specific action taken, the tool or command used, and any relevant timestamps.
2. **Clarification:** Captions clarify the purpose of the screenshot. They help readers understand why the screenshot is included and what significance it holds in the assessment.
3. **Sequential Ordering:** Captions help maintain a logical sequence in the assessment notes. They ensure that the screenshots are presented in the correct order, aligning with the chronological flow of the testing process.
4. **Cross-Referencing:** When referencing screenshots in the report or notes, captions make it easy to cross-reference specific findings or actions with visual evidence. This aids in navigation and quick retrieval of information.
5. **Accessibility:** Captions make the notes and report more accessible to a wider audience, including non-technical stakeholders who may be reviewing the assessment. They provide a bridge between the technical content and a layperson's understanding.

WHICH SCREENSHOTS APPLICATIONS ARE GOOD

Taking Notes and Screenshots

Windows: -
Print Screen (PrtSc)
Alt + Print Screen
Windows + Shift + S

Windows

- PicPick: is a popular screenshot and image editing application.
- Snipping Tool: A built-in tool for capturing screenshots and annotating them.
- Lightshot: A lightweight, free, and easy-to-use screenshot tool.

Linux (GNOME): -
Print Screen
Alt + Print Screen
Shift + Print Screen

Linux

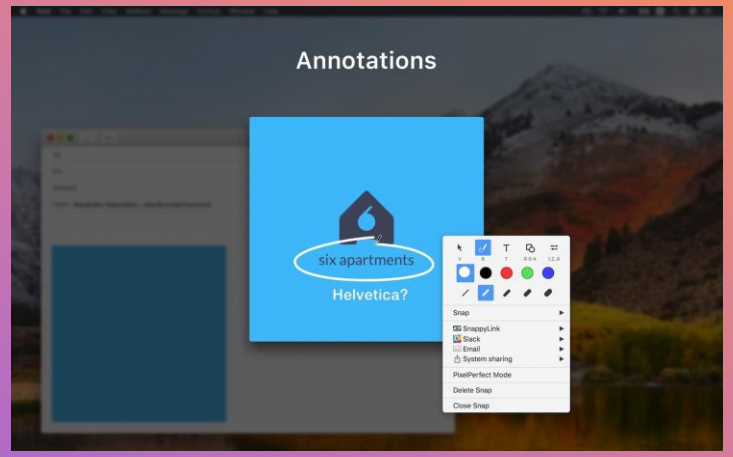
- GNOME Screenshot: It's simple but effective.
- Shutter: A powerful and feature-rich screenshot tool for Linux.
- Flameshot: A lightweight and customizable screenshot tool.

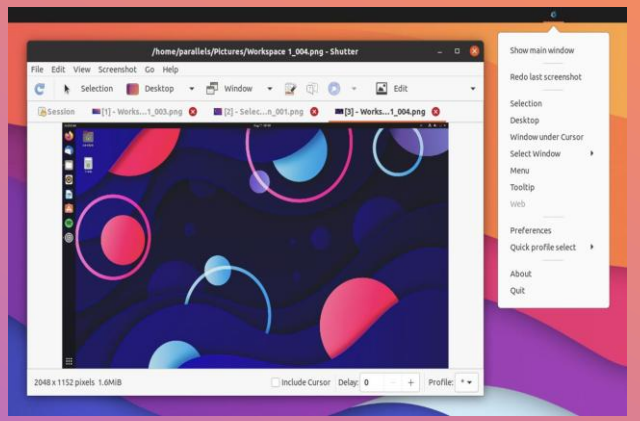
macOS: -
Command + Shift + 3
Command + Shift + 4
Command + Shift + 5

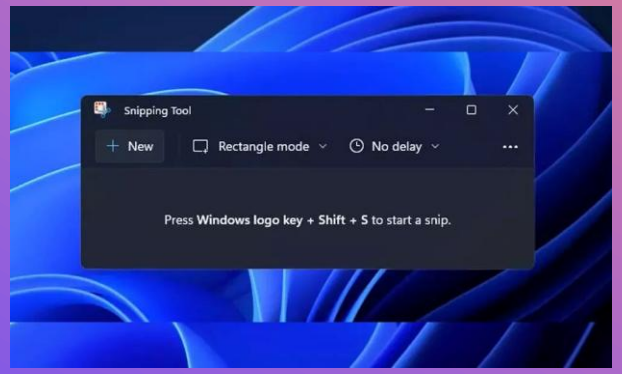
macOS

- Spectacle: A third-party open-source application for macOS that offers advanced screenshot options.
- Snappy: A lightweight, user-friendly screenshot tool for macOS with basic editing features.

TAKING NOTES AND SCREENSHOTS

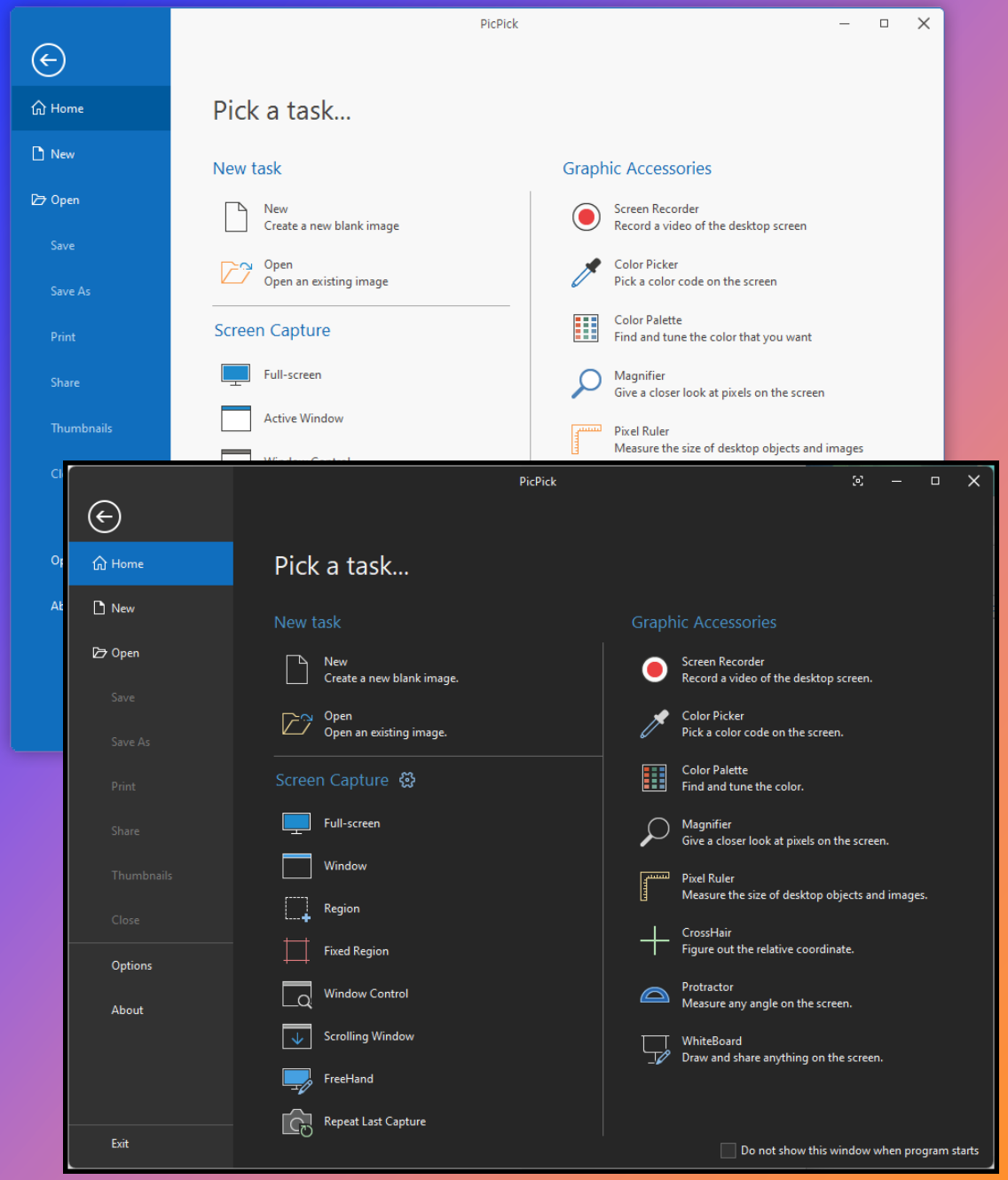






MY RECOMMENDATIONS (SCREENSHOT APPLICATIONS)

Taking Notes and Screenshots

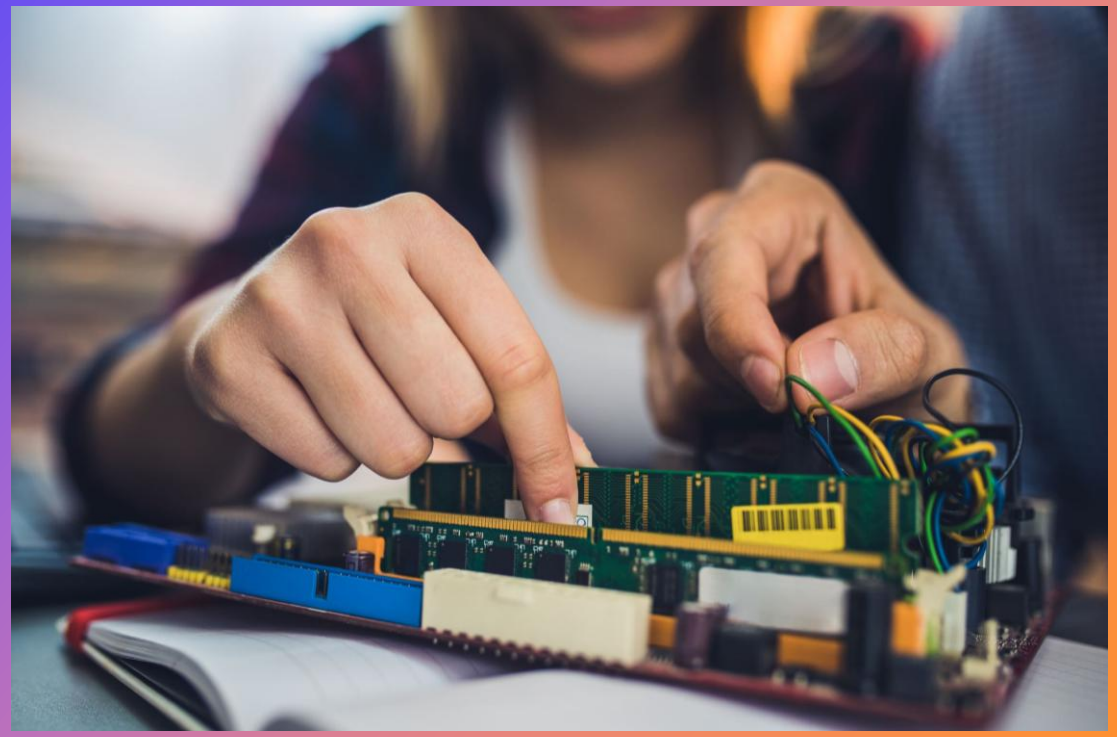


My choice is : -

PicPick

PicPick:

- ✓ *Feature-Rich*
- ✓ *Multiple Capture Modes*
- ✓ *Built-In Editor*
- ✓ *Color Picker*
- ✓ *Measuring Tools*
- ✓ *Crosshair Cursor*
- ✓ *File Sharing and Integration*
- ✓ *Free for Personal Use*
- ✓ *Compatibility*



Summary

- Effective note-taking is a critical step towards creating comprehensive and insightful reports in the field of ethical hacking.
- Utilizing a high-quality note-taking application is essential to ensure the best results in your assessments.
- For note-taking, I highly recommend using OneNote by Microsoft.
- The notes may start as rough drafts, your final reports must be polished and professional.
- In addition to textual notes, incorporating well-captured images with concise captions can convey complex information more effectively than words alone
- My top recommendation for a screenshot application that facilitates this is PicPick.
- It's a good practice to document everything during your assessments

THANK YOU

Please Like and Subscribe to never miss a video

And to help me with the Algorithm

And It's completely Free!!!

Love you guys

[YouTube : HackProKP – Kailash Parshad]

[LinkedIn : Kailash Parshad]