What is the purpose of penetration testing auditability?

Research questions

- What are the sources of penetration testing auditability data?
- What methods can be used to effectively audit these sources?
- What methods can be used to store these data efficiently and practically?
- How can penetration testing auditability enhance collaboration during penetration testing?
Penetration testing is characterised as an Art.

- It is not a standardised procedure meaning it cannot be fully automated.
- Penetration testing auditability can not be automated.
- Auditability though can be improved using a more structured methodology.
Identifying the sources of auditability data.

- **Manual Actions:**
  - Command Line
  - Other Actions

- **Automated Actions:**
  - Command Line tools
  - GUI tools
Identifying the methods that can be used to effectively audit and store these sources.

- Capture the command line streams
- Screen shots
- Screen casting
- Log files and reports of automated tools
- Manual notes
- Centralized storage space
Penetration testing auditability can enhance collaboration during penetration testing.

- Planning
- Task sharing
- File sharing
- Relation of files with tasks
Proposed Methodology / Framework

- **Action Recording**
  - Command Line Capture
  - Screen Shot
  - Screen Casting
  - Manual Notes
  - Storage Space

- **Planning**
  - Add / Edit / Delete a Plan
  - Add / Edit / Delete a Task

- **Data Sharing/Storage**
  - Centralized Storage Space
  - Storage Space

- **Chatting**
  - Global Chat
  - One to One Chat
  - Storage Space

- **Collaborative Documenting**
  - Create Document
  - Edit Document
  - Delete Document

- **Framework**
Prototype Architecture

Pen tester's machine
- Action Recording
  - Command Line Capture
  - Screen Shot
  - Screen Casting
  - Manual Notes
  - Storage Space
- Chatting
  - Global Chat
  - One-to-One Chat
  - Storage Space
- Collaborative Documenting
  - Create Document
  - Edit Document
  - Delete Document
  - Storage Space

Server
- Planning Data Sharing/Storage
  - Add/Edit/Delete a Project
  - Add/Edit/Delete a Plan
  - Add/Edit/Delete a Task
  - Upload/Download/Delete File From/To a Task
  - Storage Space
Prototype Implementation

VM: PEN TESTER'S MACHINE (Kali 2.0)
- Action Recording
  - Capture.py
  - Shutter
  - Vokoscreen
  - Tomboy

Chatting
- Iptux

Collaborative Documenting
- Gobby

VM: SERVER (Kali 2.0)
- Back-End
  - Database MySQL
  - File Directory Tree

Middleware
- PHP

Front-End
- PHP
- HTML
- CSS
- JavaScript
Results & Conclusion

Please rate how this system would improve the performance of pen testing auditability.

Mean: 7.75
Median: 8

Please rate how this system would improve the collaboration of pen testers.

Mean: 7.5
Median: 7.5

Please rate how this system would improve the quality and the quantity of pen testing auditability data gathered.

Mean: 7.625
Median: 8
References

- http://img10.deviantart.net/3ed0/i/2006/091/e/1/matrix_monanona_lisa_by_ninjakiller.jpg


- http://3vwuw21t7hbk3efr8u2h6dji.wpengine.netdna-cdn.com/wp-content/uploads/2013/03/software-security.jpg
