Record Keeping

Objectives

- Discuss need to keep records
- Understand what should be kept when you are “testing” your systems

This is not fun

- Record keeping is not fun
- Even though it’s not fun, it’s a necessary evil
- Record keeping allows a tester or administrator to understand what transpired, or if something went wrong, how to fix it so it doesn’t happen again
- Record keeping should be performed on all aspects of a pen test
- If you were ever asked to reproduce documentation, you will have it!

What should be collected

- Network logs
- Scripts
- Timelines
- Commands used
- Tools used
- Results
- Screen captures

Findings

- At the end of a pen test, you should have a final document
- The document should include:
  - Background
  - Procedure used
  - Risks identified
  - General findings
  - Recommendations
- A technical document on the pen test can also be helpful
  - Much more detailed
  - Can have technical findings

Warning

- When keeping records make sure to secure them
- An attacker might love to get their hands on a pen test, especially the technical findings
- These are like blueprints or instructions on how to break in
- Pen tests often take time to plan
- If records are not secured, attacker can easily just follow your report