Velkommen til

VikingScan reporting

Hack.lu

Henrik Lund Kramshj
hlk@security6.net

What is pentesting

Running a lot of tools

Running some more specialized tools

then doing some thinking and running more tools

Add some manual stuff like writing customized exploits

... but what about reporting results

Not very technical

Value add from companies - like mine :-)

Proposal

Create some tools to allow more or less automated reporting

Based on output from tools compile a report that can be edited

VikingScan

I have created the project VikingScan on Sourceforge, and started added and refining my various pieces

Feedback needed

Currently it uses Docbook XML, has various good things:

- Interoperable and can create RTF, HTML and PDF easily

and some bad things:

- Toolchain and templates/stylesheets can be pure hell

Current directions

Make easy offline generation from Nmap XML output into report working again

Go more into the database and provide solution based on:

- Postgresql - just one database for now
- Openjade
- LaTeX - only used for PDF currently
- Adding web fronted, proof of concept using Ravenous has initial steps and another project done by some students have more wizard like features. Probably needs complete rewrite, but WONT be PHP ;-)

Features needed:

- Basic import OK - proof of concept, data can be imported
- Extend database schema to allow merging data from multiple scans
- Extend database to allow integration with OSVDB (and nessus scans?)

Demo

Kind of a demo, showing the files and stuff

Tool writers

Consider making your tool output in XML

Yes, XML can be hard to decipher but has clear boundaries between fields