

Offensive and Defensive Techniques for Determining Web User Identity

Zachary Zebrowski

zakz@zakz.info

Approved for Public Release: 12-3046.

Distribution Unlimited

All materials are licensed under a Creative Commons "Share Alike" license

See <https://creativecommons.org/licenses/by-sa/4.0/>

Welcome

- I'm Zak Zebrowski.
- I'm a Forensic Database Engineer / "Data Miner" / and Perl guy.

Outline

- Characteristics of internet connections
- Ways of determining web user identity
- Preventing a web user identity from being determinable from an end user's perspective
- Finish

Ethics

- Reminder: Use for good not evil.
- I am not a lawyer.
- What you do is at your own risk.

Why Bother

- To determine who visits your website.
- Validate you are connecting from a known location versus an unexpected country.
- To hide your identity on the internet
- Note: Everything in this presentation is old. New technologies and techniques evolve over time which may be more (or less) intrusive.

Characteristics of Internet Connections

- What devices connect to the internet?
- When you connect to the ineternet.
- How you connect to the internet.

Why bother

- You can't escape these characteristics regardless of what you do.

What devices connect to the internet?