SSL Man-in-the-Middle Attacks with Dsniff

Rochester OWASP & ISSA Chapters
Ralph Durkee
Durkee Consulting, Inc.
rd@rd1.net
Ralph Durkee Background

- Founder of Durkee Consulting since 1996
- Founder of Rochester OWASP since 2004
- President of Rochester ISSA chapter
- SANS Instructor and course developer
- Application Security, development, auditing, PCI compliance, pen testing and consulting
- CIS (Center for Internet Security) – development of benchmark security standards – Apache, Linux, BIND DNS, OpenLDAP, FreeRadius, Unix, FreeBSD
- Rochester Area Security Consulting, Ethical Hacking and Auditing
dsniff- Suite of MITM tools

MITM = Man-in-the-Middle
Includes:

- **dsniff** - password sniffer
- **arpspoof** – Arp cache poisoning
- **macof** – flood switch with MAC addresses
- **dnsspoof** – DNS cache poisoning
- **webmitm** – HTTP / HTTPS MITM
- **tcpkill** – Kills TCP connections with RST
- **tcpnice** - Slows down TCP connection
More dsniff tools

Also includes:

- **filesnarf** – grabs files from NFS traffic
- **mailsnarf** – grabs emails from SMTP and POP3 traffic
- **msgsnarf** – grabs messages from IM traffic (AIM, ICQ, IRC, MSN, Yahoo)
- **urlsnarf** – grabs URLs from HTTP traffic
- **webspy** – sends sniffed URL’s from HTTP to local browser to spy on web traffic
- **sshmitm** – MITM on SSHv1 captures ssh passwords.
Resources - Rochester Non-Profit Groups & Events

OWASP Rochester Chapter Information
http://www.OWASP.org/rochester

Rochester Security Summit Oct 20-21, 2010
http://RochesterSecurity.org

Rochester ISSA Chapter
http://RochISSA.org
On-Line Resources

Dug Song’s dsniff
http://monkey.org/~dugsong/dsniff/

OWASP - Open Web Application Security Project
http://www.owasp.org/

OWASP Testing SSL
Thank You!

Rochester ISSA & OWASP Chapters
Ralph Durkee
Durkee Consulting, Inc.
rd@rd1.net