

DNS Security and Advanced Topics Hands on Training



© 2008 Men & Mice. All rights reserved.

This paper is for informational purposes only. Men & Mice does not make any warranty of any kind, either express or implied, in this document.

All Men & Mice product names and service names are trademarks of Men & Mice.

All other company and product names are trademarks or registered trademarks of their respective owners.

Men & Mice

E-mail: info@menandmice.com

Visit the Men & Mice web site at: <http://www.menandmice.com>

What Will You Learn?

- What kinds of threats your name servers are exposed to
- How to secure your name servers' configurations
- How to build a robust DNS and DHCP infrastructure
- How to secure your name servers' communications with other name servers and with clients
- How to configure your name servers to work with your Internet firewall
- How to configure and use BIND views
- How DNS works in an IP Version 6 network
- How ENUM works (the Telephone Number Mapping in DNS)
- How to leverage DNS to fight spam
- How to tune your internal DNS Environment

Why is this Course Important for You and Your Organization?

The Domain Name System (DNS) is a critical Internet infrastructure service. Without it, your customers can't get to your web site, your business partners can't send you email, and your employees can't use the Internet. Yet DNS is also one of the least well-understood and most vulnerable services on the Internet. BIND, the most popular implementation of the DNS protocol, has also been the source of some of the most dangerous vulnerabilities in the past.

The first part of this class will show you the range of attacks your name servers are subject to, how to secure your BIND name servers' configurations and the platforms on which they run, and how to secure your name servers' communications with other name servers. With this information, you can secure your DNS infrastructure and sleep better at night.

In the second part we will discuss in depth some of the more advanced features of the DNS System and of the BIND name server, like serving different DNS data based on the source a questions is coming from (BIND Views), DNS and IP version 6, secure interaction of DNS and DHCP, DNS and spam protection (SPF, DNS blacklists), DNS and Telephone Number Mapping (ENUM), DNS Tuning.

Who Should Attend?

Network engineers, network planners, system administrators – anyone who has anything to do with designing and administering DNS and TCP/IP networks. The Men & Mice DNS Security and Advanced Features course will give you a good understanding of the more advanced parts of this Internet service.

Why DNS Training with Men & Mice?

Men & Mice has specialized in DNS research, products and technology for 10 years. Our main focus is simplifying the management of DNS. The class material is written by some of the best DNS experts in the world and is updated regularly.

Course Outline

Threats

- Spoofing
- Denial of Services
- BIND Vulnerabilities

TSIG

- Theory
- Configuring TSIG
- Chroot and Least Privilege

DNS Security Extensions

(DNSSEC, new draft implementation in BIND)

- Theory
 - Public Key Encryption
 - RR Types
 - Chain of Trust (Delegation Signer Record)
- Practice
 - Generation a Zone Key
 - Signing a Zone Key
 - Submitting Your Key for Signing
 - Incorporating the Signed Key
 - Resigning a Zone

Infrastructure

- BIND Version / DNS Server Fingerprinting
- Restricting Zone Transfers
- Restricting Dynamic Updates
- Restricting Queries
- Avoiding Single Points of Failure
- Inside or Outside?
- "Split Service"

Views

- How BIND Views work
- Configuration of Views
- Views Best Practice
- Zone Transfers and Views

DNS and Firewalls

- Inside-out
 - Forwarding
 - Iterative Resolution
- Outside-in
 - Visibility

IP Version 6

- IP Version 6 Resource Records
- IPv6 DNS and Applications
- Dual-Stack BIND Configurations
- DNS and DHCPv6 Dynamic Updates

DNS and Spam Protection

- How Sender Authorization (SPF, Sender ID) works
- How to Create and Add Spam Protection to DNS Zones - Signing a Zone
- How DNS Blacklists work
- Blacklists Pro and Cons
- How to Check if Own IP Addresses are Blacklisted

DNS Tuning

- How to Monitor DNS Traffic
- Preventing Internal DNS from Leaking to the Internet

DNS and Telephone Number Mapping (ENUM)

- How ENUM Works
- The NAPTR Record
- ENUM Applications (VoIP, E-Mail ...)

Maintenance

- Automatic DNS Server Monitoring
- DNS Server Configuration Automation
- Mailing Lists and Newsgroups