COURSE OUTLINE

DNS Infrastructure Security

Intensive and Interactive – Led by an authorized instructor, this vendor-agnostic training course provides the much needed and updated information for the security-conscious DNS administrators in the modern enterprise. Several types of activities are used in the course to reinforce topics and increase knowledge retention, including questions from the instructor, demos, group discussions, and case studies.

Course Description	Understand security considerations for the modern DNS environment. This course covers major areas of the DNS infrastructure service, threats against each area, mitigations and defense options, and other security-related topics. Attendees will learn important protocol details that impact architecture design, and how to update their DNS infrastructure with industry best practices.
Target Audience	This training course is intended for experienced DNS professionals responsible for maintaining or designing an enterprise DNS infrastructure. The training is ideal for those working in or aspiring to Network Director/Manager, Network/System Engineer and Operator, and System Administrators.
Duration	1 day
Learning Style	Lecture, demo, and group discussions and activities
Available Modalities	Instructor-led, Virtual Instructor-led, On-Demand
Prerequisites	Attendees should have at least two years' hands-on DNS experience or have completed the DDI Professional course.
Training Credits	10
Course Topics	• DNS Security Overview • Threats Against DNS Availability • Data Accuracy • Trust Overview • DNSSEC on Authoritative Servers • DNSSEC on Recursive Servers • DNS as Authentication Source • Privacy Concerns • Encrypted DNS • Defense and Best Practices

20210709

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com

COURSE OUTLINE

DNS Infrastructure Security

Topics in Detail

1. DNS Security Overview
    - What is DNS Security?
    - Securing DNS Infrastructure
2. Threats Against DNS Availability
    - Threats Against DNS Service
    - Case Studies
    - Defense Options
3. Data Integrity
    - What is Data Integrity?
    - Data Accuracy and Case Studies
    - Dynamic Update
    - Change Authorization
    - Domain Hijacking
    - Defense Options
4. Trust Overview
    - TSIG and GSS-TSIG
    - Cache Poisoning
    - DNSSEC Overview
5. DNSSEC on Authoritative Servers
    - Deployment Tasks for Authoritative Servers
    - Working with Registrar
    - Algorithms and Key Management
    - Zone Signing and Record Types
    - Proof of Non-Existence
    - Uploading DS Record
6. DNSSEC on Recursive Servers
    - Deployment Tasks for Recursive Servers
    - Installing Trust Anchor
    - DNSSEC Validation Process
    - DNSSEC Lookup Tools
    - Negative Trust Anchor and Case Study
7. DNS as Authentication Source
    - Email Forgery Detection
    - Certificate Authorization
    - TLS Overview and Case Study
    - Out-of-band Authentication
8. Privacy Concerns
    - Privacy Concerns in DNS
    - Authoritative Data Privacy Concerns
    - Recursive Data Privacy Concerns
    - Mitigation Techniques
9. Encrypted DNS
    - Encrypted DNS Overview
    - Comparison and Considerations
    - Encrypted DNS in the Enterprise
10. Defense and Best Practices
    - Defense Strategies
    - Best Practices
    - Sample Architectures

20210709

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com