1. Record Nr. UNINA9910271030503321

Autore	Dooley Michael (Computer scientist)
Titolo	DNS security management / / Michael Dooley, Timothy Rooney
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley and Sons, Inc. Piscataway, NJ : , : IEEE Press, , [2017] [Piscataqay, New Jersey] : , : IEEE Xplore, , [2017]
ISBN	1-119-33139-0 1-119-33140-4 1-119-32829-2
Descrizione fisica	1 PDF : illustrations
Collana	IEEE Press series on networks and services management
Disciplina	005.8
Soggetti	Computer security Internet domain names - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	DNS Security Management; Contents; Preface; Acknowledgments; 1 Introduction; Why Attack DNS?; Network Disruption; DNS as a Backdoor; DNS Basic Operation; Basic DNS Data Sources and Flows; DNS Trust Model; DNS Administrator Scope; Security Context and Overview; Cybersecurity Framework Overview; Framework Implementation; Whats Next; 2 Introduction to the Domain Name System (DNS); DNS Overview -- Domains and Resolution; Domain Hierarchy; Name Resolution; Zones and Domains; Dissemination of Zone Information; Additional Zones; Resolver Configuration; Summary; 3 DNS Protocol and Messages DNS Message FormatEncoding of Domain Names; Name Compression; Internationalized Domain Names; DNS Message Format; DNS Update Messages; The DNS Resolution Process Revisited; DNS Resolution Privacy Extension; Summary; 4 DNS Vulnerabilities; Introduction; DNS Data Security; DNS Information Trust Model; DNS Information Sources; DNS Risks; DNS Infrastructure Risks and Attacks; DNS Service Availability; Hardware/OS Attacks; DNS Service Denial; Pseudorandom Subdomain Attacks; Cache Poisoning Style Attacks; Authoritative Poisoning; Resolver Redirection Attacks; Broader Attacks that Leverage DNS

Network ReconnaissanceDNS Rebinding Attack; Reflector Style Attacks; Data Exfiltration; Advanced Persistent Threats; Summary; 5 DNS Trust Sectors; Introduction; Cybersecurity Framework Items; Identify; Protect; Detect; DNS Trust Sectors; External DNS Trust Sector; Basic Server Configuration; DNS Hosting of External Zones; External DNS Diversity; Extranet DNS Trust Sector; Recursive DNS Trust Sector; Tiered Caching Servers; Basic Server Configuration; Internal Authoritative DNS Servers; Basic Server Configuration; Additional DNS Deployment Variants; Internal Delegation DNS Master/Slave Servers
Multi-Tiered Authoritative ConfigurationsHybrid Authoritative/Caching DNS Servers; Stealth Slave DNS Servers; Internal Root Servers; Deploying DNS Servers with Anycast Addresses; Other Deployment Considerations; High Availability; Multiple Vendors; Sizing and Scalability; Load Balancers; Lab Deployment; Putting It All Together; 6 Security Foundation; Introduction; Hardware/Asset Related Framework Items; Identify: Asset Management; Identify: Business Environment; Identify: Risk Assessment; Protect: Access Control; Protect: Data Security; Protect: Information Protection; Protect: Maintenance
Detect: Anomalies and EventsDetect: Security Continuous Monitoring; Respond: Analysis; Respond: Mitigation; Recover: Recovery Planning; Recover: Improvements; DNS Server Hardware Controls; DNS Server Hardening; Additional DNS Server Controls; Summary; 7 Service Denial Attacks; Introduction; Denial of Service Attacks; Pseudorandom Subdomain Attacks; Reflector Style Attacks; Detecting Service Denial Attacks; Denial of Service Protection; DoS/DDoS Mitigation; Bogus Queries Mitigation; PRSD Attack Mitigation; Reflector Mitigation; Summary; 8 Cache Poisoning Defenses; Introduction; Attack Forms

Sommario/riassunto

This work is an advanced Domain Name System (DNS) security resource that explores the operation of DNS, its vulnerabilities, basic security approaches, and mitigation strategies.