

Netzwerkemulation zur Untersuchung von Secure DNS

Inhaltsverzeichnis

Kurzfassung/Abstract I

Tabellenverzeichnis. IV

Abbildungsverzeichnis. V

1 Einleitung

1.1 Motivation

1.2 Zielsetzung der Arbeit

1.3 Aufbau der Arbeit

2 Grundlagen

2.1 IT-Sicherheit

2.2 DNS

2.3 DNSSEC

2.4 Netzwerk-und Kommunikationsprotokolle

2.5 OSPF-Routing-Protocol

2.6 Was ist der Unterschied zwischen: OSPF vs. EIGRP Protokolle

2.7 HTTP/HTTPS

2.8 SSL/TLS Protokoll

3 Kryptografische Grundlagen

3.1 Message Authentication (MAC)

3.2 Symmetrische/Asymmetrie Verschlüsselung

3.3 Public-Key-Infrastruktur (PKI)

3.3.1 Komponente einer Public-Key- Infrastruktur

3.3.2 Public-Key-Cryptography

3.3.3 Secret-key-Kryptographie

3.3.4 Digital Signatur

3.3.5 Hash Funktion

3.3.6 X.509 Certificate.

3.3.7 OpenSSL

4 Was ist GNS3?

5 DNS & BIND9

6 GNS3-basierte DNS Implementierung/Erprobung

6.1 DNS Architecture (Test Lab GNS3)

6.2 DNS Forwarding/ Delegation Configuration

7 Beispiel für erfolgreicher Angriff auf DNS

8 Beschreibung der DNSSEC Implementierung/Erprobung

8.1 DNSSEC-Configuration (GNS3 Test Lab)

8.2 Kryptographische Infrastruktur (PKI Schlüssel Verteilung)

8.3 DNSSEC Diagnostik und Tools (Nslookup/Dig)

8.4 Testergebnis und DNSSEC-Validation (Ad flag)

9 Beispiel für erfolgreich abgewertete Angriffe auf DNSSEC

10 Zusammenfassung und Ausblick

Literaturverzeichnis

Anhang

Erklärung