>> Lotus Notes/Domino 8.5

Hacking Lotus Domino

EGOS! the education company

Lotus Notes und Domino Server sind die Groupware Lösungen von IBM. Lotus Domino 8.5 zeichnet sich durch verbesserte E-Mail-Funktionen, eine größere Vielseitigkeit und Verwaltbarkeit und eine offene Anwendungsinfrastruktur aus.

Ihr Nutzen

Dieser Kurs zeigt aus der Sicht eines „Hackers“, wie Sicherheitslücken und Falschkonfigurationen in Lotus Domino für Angriffe genutzt werden können und wie man sich als Administrator/Entwickler gegen solche Angriffe schützt.

Voraussetzungen

Kenntnisse des Domino Administration.

Preis pro Teilnehmer

EUR 1185,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Hinweise

Die Kursinhalte beziehen sich auf Lotus Notes & Domino 8.5, sind aber auch auf ältere Versionen anwendbar.

Version: 8.5

Seminarinhalte

1. Tag
* Einleitung
- Ist Lotus Domino sicher?
- Übersicht über aktuelle Sicherheitslücken
- „Hacken“ - Begriffsdefinition
- Gute und böse Hacker
- Angriffe von innen und von außen
* Grundbegriffe
- Aufgriffe auf das Betriebssystem
- DoS-Attacken
- Buffer Overflows
- Viren, Würmer, Trojaner
- Weitere Hacker-Begriffe
* Notes-Ids hacken
- Domino Authentifizierung
- RSA-Verschlüsselung
- ID- Verschlüsselung
- Schlüsselstärken
- Eigenschaften von ID-Dateien
- ID Dateien Kennwortproblematik
- ID Dateien Problematik Ablaufdatum
- ID Vault
- Key Rollover
- ID Dateien Sicherheitsprobleme
- ID-Dateien „Best Practices“
- ID-Dateien Kennwortqualität
- ID-Dateien Kennwortüberprüfung
- Beispiel: Tool IPR
- Beispiel: Tool Lotus Notes Key
* HTTP Passwörter hacken
- „Sichere“ und „Sicherere“ Internetkennwörter
- HTTP Passwörter hacken
- Passwort-Synchronisation
- HTTP-Kennwörter - „Best Practices“

2. Tag
* Domino Sicherheit hacken
- Domino Sicherheitsmodell
- Die Serversicherheit
- Gruppen ohne Zugriff
- Administration mit voller Berechtigung
* Execution Control Lists
- ECL „Best Practices“
- Den Client wechseln
* Domino-Applikationen hacken
- Datenbanksicherheit
- ACL
- Übersicht: Möglichkeiten eine ACL zu ändern
- Beispiel: ACL mit Hex-Editor hacken
- Beispiel: ACL per LS ändern
- Hacken einer Datenbank mit Benutzertyp „Unbestimmt“
- Beispiel: PowerTools
- ACL - „Best Practices“
* Gestaltungssicherheit
- Falsch implementierte Sicherheit
- Leserfelder
- Agenten-Sicherheit
- Beispiel: Verstecktes Design via LS einblenden
- Verstecktes Design mit HEX-Editor einblenden
- „Stored Form“ - Attacke
- „Stored Form“-Attacke - Gegenmaßnahmen
- Zugriff via API
- Empfehlungen
* Angriff aus dem Internet
- Benutzer-Authentifizierung im Web
- Web Authentifizierung
- Standard-Authentifizierung (Basic Authentication)
- Sitzungs-Authentifizierung
- Internet Password Lockout
- Anonyme Benutzer
- Hackerangriff mit Google
- Catalog.nsf – Ein offenes Buch für Hacker
- Angriffe auf das Domino Verzeichnis
- Weitere „offene“ Datenbanken
- URL-Attacken - Allgemein
- *DefaultView
- ?ReadDesign
- ?ReadViewEntries
- Einrichten einer URL-Umleitung

3. Tag
* Angriffe per E-Mail
- Mögliche Attacken - Übersicht
- Mail-Attacke per OLE-Steuerelement
- Beispiel: Bösartiger Code
- Beispiel: Mail-Spoofing mit Telnet
- Beispiel: Mail-Bombe mit LS-Agent