# Kurs-Agenda „Hack Proofing Lotus Domino“

| | |
|---|---|
| Beschreibung | Dieser Kurs zeigt aus der Sicht eines „Hackers“, wie Sicherheitslücken und Falschkonfigurationen in Lotus Notes & Domino für Angriffe genutzt werden können und wie man sich als Administrator/Entwickler vor solchen Angriffen schützt. |
| Zielgruppe | Fortgeschrittene Administratoren & Entwickler |
| Dauer | 3 Tage |
| Inhalte | Der Kurs bezieht sich auf Lotus Notes Domino 8.5.<br><br>**Einleitung**<br>- Ist Lotus Domino sicher?<br>- Übersicht über aktuelle Sicherheitslücken<br>- „Hacken“ - Begriffsdefinition<br>- Gute und böse Hacker<br>- Angriffe von innen und von außen<br><br>**Grundbegriffe**<br>- Aufgriffe auf das Betriebssystem<br>- DoS-Attacken<br>- Buffer Overflows<br>- Viren, Würmer, Trojaner<br>- Weitere Hacker-Begriffe<br><br>**Notes-IDs hacken**<br>- Domino Authentifizierung<br>- RSA-Verschlüsselung<br>- ID- Verschlüsselung<br>- Schlüsselstärken<br>- Eigenschaften von ID-Dateien<br>- ID Dateien Kennwortproblematik<br>- ID Dateien Problematik Ablaufdatum<br>- ID Vault<br>- Key Rollover<br>- ID Dateien Sicherheitsprobleme<br>- ID-Dateien „Best Practices“<br>- ID-Dateien Kennwortqualität<br>- ID-Dateien Kennwortüberprüfung<br>- Beispiel: Tool IPR<br>- Beispiel: Tool Lotus Notes Key |

| | |
|---|---|
| | **HTTP Passwörter hacken**<br>- „Sichere" und „Sicherere" Internetkennwörter<br>- HTTP Passwörter hacken<br>- Passwort-Synchronisation<br>- HTTP-Kennwörter - „Best Practices"<br><br>**Domino Sicherheit hacken**<br>- Domino Sicherheitsmodell<br>- Die Serversicherheit<br>- Gruppen ohne Zugriff<br>- Administration mit voller Berechtigung<br><br>**Execution Control Lists**<br>- ECL „Best Practices"<br>- Den Client wechseln<br><br>**Domino-Applikationen hacken**<br>- Datenbanksicherheit<br>- ACL<br>- Übersicht: Möglichkeiten eine ACL zu ändern<br>- Beispiel: ACL mit Hex-Editor hacken<br>- Beispiel: ACL per LS ändern<br>- Hacken einer Datenbank mit Benutzertyp „Unbestimmt"<br>- Beispiel: PowerTools<br>- ACL - „Best Practices"<br><br>**Angriff aus dem Internet**<br>- Benutzer-Authentifizierung im Web<br>- Web Authentifizierung<br>- Standard-Authentifizierung (Basic Authentication)<br>- Sitzungs-Authentifizierung<br>- Internet Password Lockout<br>- Anonyme Benutzer<br>- Hackerangriff mit Google<br>- Catalog.nsf – Ein offenes Buch für Hacker<br>- Angriffe auf das Domino Verzeichnis<br>- Weitere „offene" Datenbanken<br>- URL-Attacken - Allgemein<br>- $DefaultView<br>- ?ReadDesign<br>- ?ReadViewEntries<br>- Einrichten einer URL-Umleitung |

| | |
|---|---|
| | **Angriffe per E-Mail**<br>- Mögliche Attacken - Übersicht<br>- Mail-Attacke per OLE-Steuerelement<br>- Bespiel: Bösartiger Code<br>- Beispiel Mail Spoofing mit Telnet<br>- Mail Spoofing mit dem Notes-Client<br>- Mail-Bomben<br>- Beispiel: Mail-Bombe mit LS-Agent<br>- Verhindern von Mail Relaying<br>- AntiVirus-Produkte für Lotus Domino<br>- Penetrationstest<br>- TLS<br>- Produkte zur Abwehr<br><br>**Gestaltungssicherheit**<br>- Falsch implementierte Sicherheit<br>- Leserfelder<br>- Agenten-Sicherheit<br>- Beispiel: Verstecktes Design via LS einblenden<br>- Verstecktes Design mit HEX-Editor einblenden<br>- „Stored Form" - Attacke<br>- „Stored Form"-Attacke - Gegenmaßnahmen<br>- Zugriff via API<br>- Empfehlungen<br><br>**Domino & Firewalls (optional)**<br>- Firewall-Typen<br>- Regeln<br>- Proxy-Dienste<br>- Proxy-Server-Arten<br>- Von Domino unterstützte Proxies<br>- Domino Durchgangsserver als Proxy<br>- Domino Proxy-Konfiguration<br><br>**Secure Sockets Layer (SSL - optional)**<br>- SSL: Grundlagen<br>- SSL: Zertifizierungsstellen<br>- SSL und Domino<br>- SSL: Domino CA<br>- SSL: Erstellen einer Domino CA<br>- SSL: Erstellen des Server-Schlüsselrings<br>- SSL: Konfiguration Domino Server<br>- SSL: Client-Authentifizierung via Internetzertifikat<br>- Client-Authentifizierung via SSL einrichten |