NetScaler Web Application Firewall - Deep Dive

GEEK COURSES

OBJECTIFS

> Identifier le differentes failles au niveau applicatif et les attaques les plus repandues
> Configurer et administrer les differents modes du NetScaler Application Firewall pour proteger les applications et les services hebergés par la plateforme.
> Sécuriser l'accès aux applications et aux données pour les connexions utilisateurs.
> Répondre aux exigences réglementaires au niveau sécurité et protection des données privées.
> Pouvoir comprendre et analyser le trafic analyser et corriger les comportements du WAF

Qui ?

Administrateurs réseaux et systèmes

Pré-requis

Maîtriser les fonctionnalités de base de NetScaler

Durée

2 jours (14 heures)

Dates

Sur demande

Intervenant

Leopoldo Torres @1leotorres
Senior consultant
IT Applications

Formations connexes

Curscus NetScaler 10.5

Coût

1 600 € HT

Contact formation

chloe.manen@d2-si.eu

PROGRAMME

#CasPratique #Conférence #Échange

APPLICATION ATTACKS

- Application Attack Description
- Goals of Application Attacks
- Most Common Types of Web Application Attacks
- The Application Firewall Solution
- Business Problems

THE BENEFITS OF APPLICATION FIREWALL

- Application Layer Protection
- Security Models
- Deep Stream Inspection
- Adaptive Learning Engine
- Web Application Vulnerabilities
- Security Audits and Application Firewalls

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

- Importance of PCI
- Common Coding Vulnerabilities
- PCI-DSS Report
- Packet Processing and Inspection

IceLab BY D2SI

NetScaler Web Application Firewall - Deep Dive

PROGRAMME (suite)

DEPLOYMENT CONSIDERATIONS PROFILES AND POLICIES

- Profile Types
- Policy Creation
- Policy Binding

ENGINE SETTINGS ATTACKS AND PROTECTIONS

- Common Security Checks
- HTML Security Checks
- XML Security Checks
- Request-Side and Response-Side Checks
- Buffer Overflow
- Parameter Manipulation Example
- Server Misconfiguration
- Deny URL Protection

SQL INJECTION

- How SQL Injection Works
- HTML SQL Injection Protection
  - > SQL Keywords and Special Characters
  - > Modifying SQL Injection Action Settings
  - > XML SQL Injection Security Check

CROSS-SITE SCRIPTING

- How Cross-Site Scripting Attacks Work
- Cross-Site Scripting Protection settings
- Relaxations
- Command Injection Examples

FIELD FORMAT PROTECTION

- Field Types and Field Formats configuration
- Confidential Fields

COOKIE TAMPERING AND POISONING

- Cookies and Attack
- Cookie Consistency Protection
- Relaxations

FORM/HIDDEN FIELD MANIPULATION

- Example of Hidden Field Manipulation
- Form Field Consistency Protection

FORCEFUL BROWSING

- Forceful Browsing Protection
- Start URLs
- Backdoors and Misconfigurations
- URL Closure

CREDIT CARD PROTECTION

- Predefined Credit Cards
- Credit Card Settings
- Protecting Credit Cards
- Errors Triggering Sensitive Information Leaks

ADAPTIVE LEARNING FOR SECURITY

- Learning Over Time and Thresholds
- Generalized and Simple Rules
- Managing Learned Rules

APPLICATION FIREWALL TROUBLESHOOTING

- HTTP Headers
- HTML Comment Stripping
- Configuration Issues
- Policy Issues
- Profile Issues

IceLab BY D2SI