Training: F5
Mitigating Vulnerabilities with NGINX App Protect

TRAINING GOALS:

This course gives participants a functional understanding of how to deploy and operate NGINX App Protect (WAF and DoS) to protect their web applications from the most common web application vulnerabilities and Layer 7 denial of service attacks.

This course features hands-on labs and discussion about detecting and mitigating threats from different threat vectors.

Audience

The target audience is personae new to DevOps and SecOps, along with anyone in DevOps where exposure to app security knowledge is limited. Application developers responsible for adding NGINX App Protect to their ecosystems are also encouraged to attend this class.

CONSPECT:

- Chapter 1: Introduction
  - Visualize an application as an assembly of elements and resources across the client, network and server environments
  - Make the connection between clients, application, and data
  - Visualize the architecture of the application we will secure
- Chapter 2: Overview of HTTP Communication
  - Overview of web application communication elements
  - Overview of HTTP message structure
  - Exploiting the document object model
  - Overview of web application implementation paradigms
- Chapter 3: Overview of Web Application Vulnerabilities
  - Assessing how web applications might be vulnerable
  - Common exploits against web applications
  - Exploiting the document object model

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Reviewing the Open Web Application Security Project® Top 10 list
- Chapter 4: Applying Security Concepts and Enabling NGINX App Protect
  - Differentiating a web application firewall from other security solutions
  - Defining a security policy
  - Exploring attacks at Layer 7 of the OSI model
  - Differentiating between positive and negative security
  - Defining attack signatures and threat campaigns
  - Defining Enforcement Mode
- Chapter 5: Logging Security Events in NGINX App Protect
  - Logging with NGINX
  - Reviewing the default security log configuration
  - Using custom logs
  - Understanding security log variables
- Chapter 6: Setting Policy
  - Review default policy protections
  - Examine the default policy configuration file
  - Review attack signature sets and blocking settings
  - Examine the strict policy
- Chapter 7: Policy tuning and working with multiple policies
  - Use cases for multiple policies
  - Policy tuning
  - Working with external policy reference files
- Chapter 8: Updating Attack Signatures and Threat Campaigns
  - Outline steps for attack signature and threat campaign updates
  - Setting email options for role and business needs
  - Testing a Threat Campaign violation
- Chapter 9: Mitigating Denial of Service Attacks
  - Understanding stress inducing client behaviors
  - Examining denial of service activity
  - Connecting NGINX App Protect DoS Directives and Policy
  - Overview of logging DoS events
- Chapter 10: Troubleshooting
  - Common errors
  - Using native troubleshooting
  - Ways to collect information before reaching out to technical support
  - Review how to update NGINX Plus and NGINX App Protect

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Chapter 11: Final Project
  - Create a policy based on real-world requirements without guidance

REQUIREMENTS:

Before taking this course, make sure you have completed one of the following:

- Administering NGINX for Web Services

The course assumes a basic understanding of networking, web servers, HTTP, load balancing, caching, proxying, and related concepts. Hands on labs are performed in a Linux environment. You will need to be able to navigate the file system from the command line and edit configuration files using VI/VIM. Additional experience with Linux environments will be helpful.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by F5 (course completion).

This course helps prepare participants for the F5 Certified Administrator, NGINX (F5-CA, NGINX) certification. The certification requires candidates to pass four exams: NGINX Management (F5CAN1); NGINX Configuration: Knowledge (F5CAN2); NGINX Configuration: Demonstrate (F5CAN3); and NGINX Troubleshoot (F5CAN4).

More information: https://education.f5.com/learning-path/view/24

TRAINER:

Certified F5 Networks Trainer

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310