OVERVIEW

Course Level:

Intermediate

Format:

Instructor-Led Training

Prerequisite Knowledge:

Completing the following Arbor Security Academy on-demand courses is recommended:

- Introduction to DDoS
- Getting Started with Arbor Edge Defense (AED)

Target Audience:

Anyone who owns, operates, or administers a NETSCOUT® Arbor Edge Defense (AED) platform.

Duration:

16 course hours

Defending Against DDoS Attacks Using NETSCOUT Arbor Edge Defense (AED)

Course Description

This course focuses on using NETSCOUT Arbor Edge Defense (AED) for protection from availability threats such as volumetric, state-exhaustion, and application-layer Distributed Denial of Service (DDoS) attacks.

NOTE: This course is also appropriate for anyone who has deployed Arbor's Availability Protection System (APS).

The goal of the course is to build your confidence to take action to mitigate DDoS attacks against your critical network infrastructure. Through extensive use of hands-on attack scenarios, you will learn and practice attack detection, strategizing an appropriate response, and analyzing the outcome of the response. Throughout the experience, you will learn about the different types of DDoS attacks and see them in action. You will also discover the broad set of inbound and outbound protections AED can apply to the malicious traffic, and how to apply those protections and monitor network traffic.

Course Objectives

- Use NETSCOUT Arbor Edge Defense to identify DDoS threat activity
- State the characteristics of volumetric, state exhaustion, and application layer DDoS attacks
- Create and tune Protection Groups used to protect critical network resources
- Apply AED-defined countermeasures to mitigate DDoS threats
- Verify DDoS attacks have been mitigated

Course Syllabus

Module 1: NETSCOUT Arbor Edge Defense (AED) Overview

- NETSCOUT AED architecture and functional overview
- Establish UI familiarity and workflow
- Verify current AED operational status
- Establish perspective by identifying current traffic characteristics
- Lab: Protection Group Setup and Tuning

Module 2: Configuring NETSCOUT AED For Your Network

- Using blacklists and whitelists
- Filter traffic with FCAP fingerprint expression language
- Lab: Use blacklists and filtering to block unwanted traffic

Module 3: Defend Against Layer 3/4 State-Exhausting Attacks

- Identify characteristics of the Invalid Packet protection and view the traffic types that it drops
- Describe and configure protections used to drop or block layer 3/4 misuse traffic
- Discuss common layer 3/4 DDoS attack vectors
- Lab: Mitigate state-exhaustion attacks

Module 4: Engage Cloud Signaling Services

- Define Arbor AED cloud signaling
- Describe when to use AED cloud signaling
- Distinguish between different cloud signaling requests
- Configure AED to connect to your provider's cloud-based services
- Use and monitor your cloud-based mitigation
- Lab: Configuring and engaging cloud signaling

Module 5: Defend Against an Outbound Attack

- Identify the use of and characteristics of the Outbound Threat Filter
- Monitor and view indicators of outbound threats generating from within your network
- Enable and configure the Outbound Threat Filter
- How to use NETSCOUT AED to protect from outbound attacks
- Lab: Blocking outbound traffic on your network
- Lab: Mitigating Protocol Attacks

Module 6: Defend Against an Application-Layer Attack

- Apply application layer protections for common servers and services
- Discuss common application-layer DDoS attack vectors
- Lab: Mitigate Application-layer Attacks
- Lab: Mitigate Multi-vector Attacks

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

TCI_078_EN-2001 09/2020