OVERVIEW

Course Level:

Basic

Format:

Instructor-Led

Course Code:

SP-TRAIN-OPER

Target Audience:

Security Operations Center (SOC) Operators, Network Operations Center (NOC) Operators with a security focus, and any staff responsible for monitoring a network for security-related events and taking action to minimize the impact of offending traffic against the network.

Duration:

16 course hours, 1.6 CEUs

Arbor SP/TMS Operator Course

Course Description

This course focuses on using Arbor SP and TMS to monitor network traffic, identify and react to alerts, and create an appropriate remediation plan to quell an attack. Participants will learn about the different types of DDoS attacks and how to use Arbor SP to monitor and analyze DoS alerts. Through a series of hands-on simulations, participants will experience different types of DDoS attacks and learn the skills to create an appropriate mitigation strategy. Participants will then configure the necessary TMS countermeasures to drop or block the misuse traffic.

Course Objectives

- Check the status of the Arbor deployment
- Monitor and analyze network and customer traffic
- Identify and analyze security events
- Mitigate DDoS threats in the network

Course Syllabus

Module 1: Getting to Know Your Arbor SP Deployment

- Identify the different Arbor SP and TMS appliances and know the roles of each in a deployment
- Access and navigate the Arbor Web User Interface (UI) and identify key elements of the UI
- Check the status of the Arbor deployment, appliances, and routers
- Recognize signs of operational issues that impact the operation of the Arbor deployment
- Check and analyze alert and security status

Module 2: Investigating Traffic

- Use dashboards to quickly view the most commonly needed data about your network
- Use network, router, and customer reports to analyze the network, monitored routers, and customer traffic
- View and understand network events using Explore pages and queries

Module 3: Analyzing DDoS Alerts

- Access a DoS alert and view summary details to identify the characteristics that triggered the alert
- View further alert details and traceback the origin traffic
- Add traffic data to an Alert Scratchpad for later use
- Modify alert classification and add further annotations
- Use various reports to identify if the alert is a possible attack or false-positive
- Investigate the raw flows database to further analyze major traffic events

Module 4: Identifying and Mitigating Volumetric DDoS Attacks

- Describe the characteristics and impact of a volumetric attack
- Identify the techniques available to Arbor SP to drop or block malicious traffic
- Use the TMS to launch and monitor a mitigation
- Use filter Lists and TMS countermeasures to mitigate a volumetric attack
- Identify deployment issues with a running mitigation
- Identify when to blackhole an attack and create a SP-triggered blackhole mitigation
- Create and use a SP-triggered Flow Specification mitigation

Module 5: Protecting Against TCP State Exhaustion DDoS Attacks

- Describe the characteristics and impact of a TCP State-Exhaustion attack
- Use the TMS to launch and monitor a mitigation
- Identify and use countermeasures to best protect against a TCP state-exhaustion attack

Module 6: Stop an Application-layer DDoS Attack

- Describe the characteristics and impact of application-layer attacks including DNS, HTTP, SIP, and SSL
- Analyze the DoS alert then use the TMS to launch and monitor a mitigation
- Identify the TMS countermeasures to use to protect against a specific type of application-layer attack

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_077_EN-1801 04/2018