

Nessus version used for training: 4.4.1



## Course Structure

### Chapter 1: Introduction to Nessus and Vulnerability Scanning

Students will learn about Nessus' historical development, where Nessus sits within Tenable's Unified Security Monitoring architecture, vulnerability scanning fundamentals and Nessus's architecture and scanning process.

---

### Chapter 2: Nessus Install and Registration

Students will observe the installation and registration steps of a Professional Feed scanner.

---

### Chapter 3: Basic Nessus Scan Operation

Students will be introduced to the scanner's graphical user interface. The main areas of interest are highlighted, configuration options explained and details on how to use scan results given.

**Lab 1:** Students. Connect to a remote scanner with NessusClient, create basic scan policies, view scans results, and use filtering expressions to identify data of interest.

---

### Chapter 4: Nessus Credentialed Scanning

Students will learn the benefits of scanning hosts and applications with credentials. In addition they will be made aware of the types of scan emanating from using credentials as well as configuration options specific to these.

**Lab 2:** Students will configure credentialed scans against UNIX and Windows targets to perform patch audits and analyze scan data that is only available using credentialed scans.

**Lab 3:** Students will create a bespoke credentialed scan that satisfies the exercise's prerequisites.

---

### Chapter 5: Resources

Students will be made aware of the various online resources available to them: forums, blogs, portal...

---

### Chapter 6: Report customisation

Students will discover how to tweak out-of-box reports to accomplish standard customisations. They will also be introduced to additional report templates available from the older NessusClient.

**Lab 4:** Students will gain insight into general report customisations and how to accomplish them.

## Chapter 7: Introduction to compliance

Student will learn how Nessus can help with your compliance audits ranging from legal standards such as PCI to your own custom internal policies.

---

## Chapter 8: Windows System Auditing

Students will be introduced to the Nessus configuration audit mechanism with regards to Windows.

**Lab 5:** Students will create a Windows configuration audit scan.

---

## Chapter 9: UNIX System Auditing

Students will be introduced to the Nessus configuration audit mechanism with regards to Unix.

**Lab 6:** Students will create a Unix configuration audit scan.

---

## Chapter 10: Content Auditing

Students will be introduced to the Nessus configuration audit mechanism with regards to detecting sensitive content at rest.

**Lab 7:** Students will create a sensitive content audit scan.

---

## Chapter 11: Nessus Database auditing

Students will be introduced to the Nessus configuration audit mechanism with regards to database auditing.

---

## Chapter 12: Web Application testing with Nessus

Student will be shown the two approaches that Nessus can provide when testing web applications. The essential configuration options will be discussed.

**Lab 8:** Students will create a barebones web app testing scan and launch against a vulnerable web server.

To register please email [training@satisnet.co.uk](mailto:training@satisnet.co.uk) or phone 01582 434320.