Introduction to configuration management & session management

Unit objectives

After completing this unit, you should be able to:

- Gain insight on configuration management
- Understand the basics of session management

Introduction to configuration management & session management (1 of 2)

- Configuration management requires the understanding of the following:
  - Basics of configuration management

Introduction to configuration management & session management (2 of 2)

- Configuration management requires the understanding (cont.) of the following:
  - Configuration management vulnerability
  - Protection from configuration management issues
  - Requirements of configuration management

Unauthorized access to administration interfaces (1 of 3)

- Configuration management requires the understanding of the following:
  - Basics of unauthorized access to administration interfaces

Unauthorized access to administration interfaces (2 of 3)

- Configuration management requires the understanding (cont.) of the following:
  - Detailed description of unauthorized access to administration interfaces

Unauthorized access to administration interfaces (3 of 3)

- Configuration management requires the understanding (cont.) of the following:
  - Black box testing
  - Grey box testing

Unauthorized access to configuration stores

- Unauthorized access to configuration stores requires the understanding of the following:
  - Basics of unauthorized access to configuration stores
  - Protection of configuration stores
  - Retrieval of plaintext configuration secrets

Retrieval of clear text configuration data

- Retrieval of clear text configuration data requires the understanding of the following:
  - Basics of retrieval of clear text configuration data

Lack of individual accountability

- Lack of individual accountability requires the understanding of the following:
  - Basics of lack of individual accountability

Over-privileged process and service accounts

- Over-privileged process and service accounts requires the understanding of the following:
  - Basics of 0ver-privileged process and service accounts

Basics of Session Management (1 of 2)

- Session management requires the understanding of the following:
  - Basics of session management
  - Control objectives of session management

Session-Management-Diagram

Basics of Session Management (2 of 2)

- Session management requires the understanding (cont.) of the following:
  - Broken authentication and session management vulnerability
  - Protection from broken authentication and session management

Hijacking attack

- Hijacking attack requires the understanding of the following:
  - Basics of hijacking
  - Protection from session hijacking

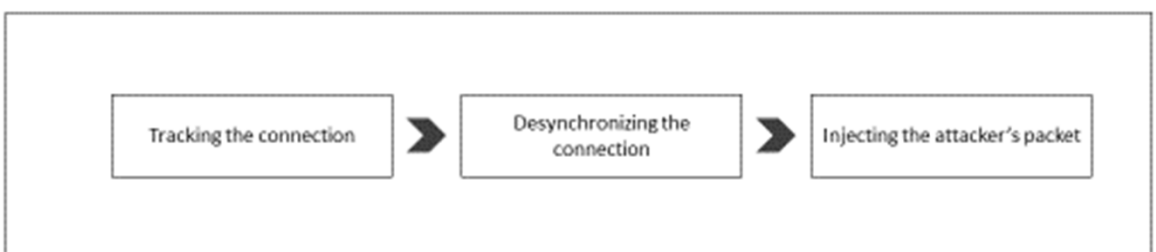

Figure: Session Hijacking Technique

Session replay attack

- Session replay attack requires the understanding of the following:
  - Basics of session replay attack

Man in the middle attack

- Man in the middle attack requires the understanding of the following:
  - Basics of man in the middle attack

Checkpoint

1. Which of the following is not a configuration management threat?
   A. Unauthorized access to administration interfaces
   B. Unauthorized access to configuration stores
   C. Lack of individual accountability
   D. Under-privileged process and service accounts

2. Full form of DCOM:
   A. Distributed Component Object Model
   B. Directory Component Object Model
   C. Direct Computer Oriented Method
   D. Distributed Computer Object Model

Checkpoint

3. HMACs stands for?
   A. High Media Access Controls
   B. Hashed Minute Authentication Codecs
   C. Hashed Message Authentication Codes
   D. Hashed Message Authorization Codes

4. A session ID should be:
   A. Complex
   B. Lengthy
   C. Unpredictable random numbers
   D. All of the above

Checkpoint

5. A session ID should not be stored in?
   A. Hidden HTML fields and HTTP headers
   B. Persistent Cookies and URLs
   C. Both A and B
   D. Neither A nor B

6. Applications should not store secret data in:
   A. Clear Text
   B. Cypher Text
   C. Enciphered Text
   D. Coded Text

Checkpoint

7. Which of the following testing mechanism is used in administrator interfaces?
   A. Green box testing
   B. Blue box testing
   C. Both A and B
   D. Neither A nor B

8. By avoiding XSS vulnerability you can protect your web application from broken authentication and session management.
   A. True
   B. False

Checkpoint

9. _____ is used to compare the true value and the arrived value in order to validate the non-tampering of the data
   A. HMACs
   B. MACs
   C. XML
   D. Matching

10. A perpetrator can steal your session through?
   A. Hijacking
   B. Session Replay Attack
   C. Both A and B
   D. Neither A nor B

Checkpoint solutions

1. D
2. A
3. C
4. D
5. C
6. A
7. D
8. A
9. A
10. C

Unit summary

After completing this unit, you should be able to:

- Gain insight on configuration management
- Understand the basics of session management