目录

Last update: 2024/03/25 05:32	b.理论储备:07.安全从业资格:sc	https://www.zhangzt315.com/doku.php?id=b.%E7%90%86%E8%AE%BA%E5%82%A8%E5%A4%87:07.%E5%AE%89%E5%85%A8%E4%BB%8E%E4%B8%9A%E8%B5%84%E6%A0%BC:sc

IPv6

几个特殊地址

IPv6的Global Unique Address相当于IPv4的单播地址(即Global Address),是以001开头的,所以2001:满足.

LoopBackAddress则类似于IPv4的127.0.0.1,在IPv6中是::1

攻击手法和对策

20240324 SC模拟考试解答讲义笔记

问1:

CRYPTREC□推奨暗号方法（**アルゴリズム**）

参照**ファイル**

電子政府推奨暗号**リスト**

共通鍵暗号方式

- **ブロック**暗号□AES□**ブロック**長128**ビット**/鍵長、256**と192ビット**□□Camellia
- **ストリーム**暗号□KCipher-2□電子政府推奨暗号**リストにストリーム**暗号**として**唯一記載**されている アルゴリズムです**。

認証付**き**暗号□AEAD□□TLS1.3**で**登場**する**。 認証**は、**改**ざんのチェックです**。

AEADの例　AES-GCMとAES-CCM

鍵共有**アルゴリズム**□DH,ECDH

共通鍵

前方秘匿性(PFS),用于TLS1.3,形成了DHE和ECDHE这两种加密方式.

问2:

MAC:□**メッセージ**認証符号

HMAC:□鍵付**きハッシュ**関数（共通鍵利用）