SEGURANÇA

Segunda parte da matéria a negrito ⬆2 ⬇0

Abaixo de cada questão estará as duas opções V e F, à frente de cada opção estará (x) em que x será o número de concordâncias, **quem concordar com a resposta adiciona uma unidade**, se calhar assim teremos uma melhor perceção de qual será a resposta certa, existem questões duplicadas com respostas diferentes.

Atenção, os números à frente de cada resposta não querem dizer nada! Se acharem que a maioria está errada, justifiquem!

O mecanismo de two-phase commit garante sempre a conclusão de uma transação? - V s
F (1) - Confirmado no elearning O mecanismo refere se ao mecanismo no global (intenção + commit) e pode falhar na intenção source-> https://en.wikipedia.org/wiki/Two-phase_commit_protocol
(ele deve ter traduzido o nome e ficou isso "two phase commit" == "two-phase update")

É possível concretizar a autenticação de uma pessoa com vários métodos alternativos com PAM (Pluggable Authentication Modules)? - Acho que sim (unificação de diferentes mecanismos de autenticação para diferentes aplicações)
V (6) - CONFIRMADO
F (0)

Pode-se usar criptografia assimétrica para calcular um MAC (Message Authentication Code)?

Uma JVM (Java Virtual Machine) permite que uma aplicação redefina as classes pertencentes à hierarquia java.*?
V (0)
F (3) Confirmado no elearning

Uma entidade pode ter mais do que um certificado para a sua chave pública?

Um item no CVE (Common Vulnerabilities and Exposures) dá algumas indicações sobre como a vulnerabilidade pode ser explorada?
V (0)F (0)

A cifra de células numa base de dados deverá usar parâmetros secretos diferentes por cada célula?
V (7) (Confirmed True)
F (0)

A sanitização dos conteúdos guardados num servidor é fundamental para evitar ataques XSS (Cross-Side Scripting) por reflexão?

Os conceitos de confusão e difusão são fundamentais para o desenho das cifras assimétricas?

O sistema de ficheiros base do unix permite impedir que um ficheiro seja apagado? -V
V (4) CONFIRMADO
F (0)

A autenticação com pares de chaves assimétricas obriga ao uso de certificados das respectivas chaves públicas ?
O conhecimento da data em que se realizou uma assinatura digital é crítico para a sua validação?
V (0)
F (0)

É normal os sistemas de cifra de volumes de armazenamento usarem modos de cifra com realimentação, de forma a não evidenciarem padrões?
V (0)
F (2) -> Confirmado no elearning slide 14

O modo de cifra ctr (counter) permite acesso aleatório uniforme -apenas na decifra -tanto na cifra como na decifra

O princípio do privilégio mínimo serve para escolher mecanismos de segurança?
V (0)
F (5) Confirmado no elearning
Existe uma questão quase igual a esta, só que muda ***escolher*** *para* ***modelar****, será uma rasteira ? Muda para modelar POLÍTICAS não mecanismos* **V (3) F (0)**
O principio do privilégio minimo serve para escolher mecanismos de segurança?
F(1) Confirmado no Elearning
V(0)

É possível definir uma política de segurança para uma JVM, independentemente da aplicação que executar?
V (3) (Confirmed True)
F (0)

O paradoxo do aniversário define um nível de resistência máximo de uma função de síntese à
a) descoberta de colisões **V (0)**
b) descoberta de uma pré-imagem **V (0)**

Um procedimento a seguir em caso de emergência é um mecanismo de segurança?
V (0)
F (3) (Confirmed False)

Uma assinatura digital é realizada com recurso a uma função de síntese para aumentar a sua segurança?

O PAM é uma componente do núcleo do sistema operativo Linux?
V (1) - “The goal of these exercises is to explore the functionalities of PAM infrastructure present in current Linux distributions. “ retirado do guião da aula prática -- Mas o PAM está em user space e não faz parte do kernel. Source: https://stackoverflow.com/questions/10768111/relationship-between-linux-pam-and-the-kernel

F (4) Confirmado no elearning PAM é uma biblioteca que fornece uma API que permite a integração de múltiplos esquemas de autenticação num único host ou em aplicações.

O sistema de ficheiros EFS usa uma simétrica diferente por ficheiro?
V (5) (Confirmed True)
F (0)

Os problemas de XSS são causados por deficiências nos mecanismos de segurança dos navegadores?

A definição da lista de utentes de uma máquina numa organização é um mecanismo de segurança?
V(0)
F(1) Confirmado no elearning

Pode-se gerar uma assinatura com uma chave privada de Diffie-Hellman?

Uma aplicação java pode redefinir a sua política de segurança usando uma instância da classe Policy?
V (4) - CONFIRMADO ELEARNING source :
"Can be overwritten (void Policy.setPolicy(Policy))"
https://stackoverflow.com/questions/11737971/programmatically-grant-permissions-without-using-policy-file

(Retirado de apontamentos de Segurança)
Ele (JRE) mantém e tem instalado políticas de segurança específicas em ficheiros de configuração, que determinam o conjunto de autorizações permitidas ou negadas. O JRE mantém sempre uma política por definição, sendo possível instalar outras (requer permissão getPolicy) ou escrever por cima das que existem (requer permissão setPolicy).

F (1) - Um JRE pode ter um gestor de segurança cujo objetivo é ajudar a implementar políticas de segurança em aplicações. O gestor por definição é o SecurityManager do Java.lang

Questão retirada dum exame passado
18. No Java, uma política de segurança(secure policy) (escolhe a resposta errada):
- *a. É um conjunto de autorizações dadas e negadas*
- *b. Possui um conjunto de valores iniciais especializados? em ficheiros de configuração*
- *c. é algo que existe sempre em qualquer execução de uma jvm*
- *d. Não pode ser programaticamente alterado a partir de uma aplicação*

Está repondida a d)

O princípio do privilégio mínimo serve para modelar políticas de segurança?
*Existe uma questão **quase** igual a esta mais acima. -- Mas esta está verdadeira, não tem a rasteira que a outra tinha*
V (8) (Confirmed True)
F (0)

A técnica de K-anonimato permite reduzir a possibilidade de identificação de pessoas?
V (9) (Confirmed True)
F (0)

A autenticação com pares de chaves assimétricas obriga ao uso de certificados das respectivas chaves públicas?

O modo de cifra CFB permite transformar uma cifra contínua (stream) numa cifra por blocos?

Um item no CVE indica a forma como uma vulnerabilidade pode ser explorada?

A system call chroot serve para mudar a noção que o sistema operativo Linux tem da diretoria raiz do seu sistema de ficheiros?

V (0)
F (4) (Confirmed False) Muda a noção do root para o PROCESSO e não para o sistema. “A chroot on Unix operating systems is an operation that changes the apparent root directory for the current running process and its children.”

Os conceitos de confusão e difusão são fundamentais para o desenho das cifras assimétricas?

Um ataque de ARP Poisoning permite alterar o endereço IP de uma máquina na mesma rede local?
V (0)
F (5) - Confirmado no elearning Altera os MACs - tecnicamente não alteras o MAC a ninguém. A vitima é que vai pensar que és alguém que não és.
Vais dizer a alguém que um determinado IP tem um MAC (que não é o correto), de forma a enganar a vítima.

---

1 - Um item no CVE (Common Vulnerabilities and Exposures) indica o nível de gravidade de uma vulnerabilidade?
2 - Um certificado x.509 indica obrigatoriamente o fim a que se destina a chave pública que certifica?
3 - Os conceitos de confusão e difusão são fundamentais para o desenho das cifras assimétricas?

6 - A formação regular dos empregados de uma organização acerca dos cuidados a ter com a segurança é uma política de segurança?
V (0)
F (0)

8 - No âmbito da autenticação biométrica um falso positivo é um evento
- **a)** Grave para a segurança do sistema **V (8) | F (0) CONFIRMADO NO ELEARNING**
- **b)** Desagradável para quem se está a autenticar **V (0) | F (8)**

9 - No desenho de uma função de síntese é fundamental usar o conceito de:
- a) Difusão

b) Confusão

10 - A criptografia simétrica permite gerar assinaturas digitais de forma mais eficiente?
V (0)
F (0)

12 - Pode-se usar criptografia assimétrica para calcular um MAC?
14 - O modo de cifra CFB (Cipher Feedback) permite transformar uma cifra contínua (stream) numa cifra por blocos?

15 - **Um módulo PAM tem de concretizar todas as funcionalidades previstas pela arquitetura PAM?**
V (0)
F (3) (Confirmed False) - Not all functions need to be implemented (Slides)

16 - **Uma cache ARP só é atualizada por mensagens ARP?**
V (0)
F (4) (Confirmed False) - Hosts cache information directly from all packets received

17 - Os problemas de XSS são causados por deficiências nos mecanismo de segurança dos navegadores?
V (0)
F (0)

18 - **O princípio do privilégio mínimo é fundamental para a definição de papéis num sistema que use RBAC?**
V (5) - Confirmado no elearning "Each subject should have, at any given time, the exact privileges required to the assigned tasks" - access control models, slide 5 // acho que se relaciona bem com as roles (RoleBasedAC)
F (0)

O comando chmod serve para mudar o bit set-uid de um processo?
V (4)
F (0)

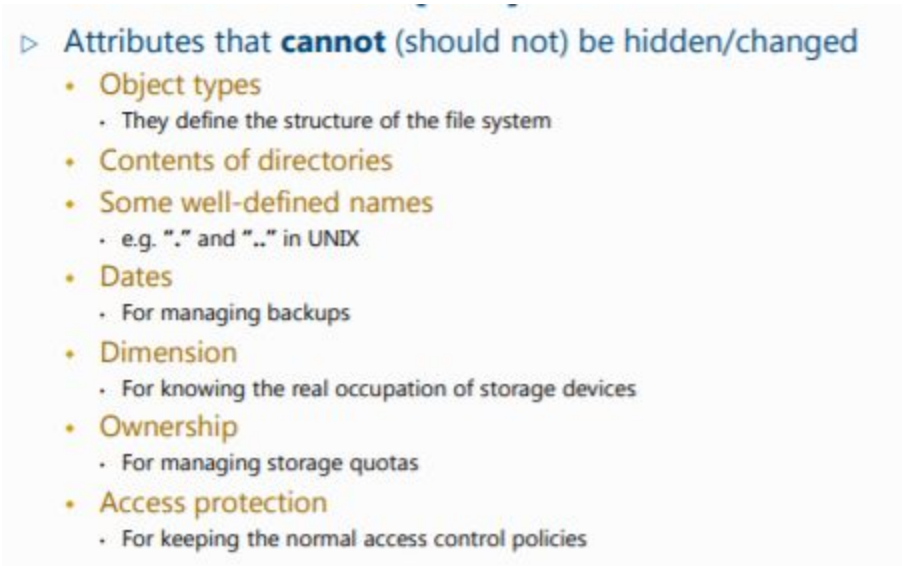
A aproximação CBC-MAC (*Cipher Block Chaining Message Authentication Code*) pode usar chaves simétricas de qualquer dimensão?
V (0)
F (0)

A autenticação com senhas descartáveis (otp) é imune a ataques com dicionários?
V (0)
F (1) - Confirmado no elearning Não é garantido, mas se as cotações das respostas no trial

tiverem bem, esta é falsa. (Nós testamos responder só a quatro que tínhamos a certeza e deu 4 valores, depois respondemos só a esta a dizer que era imune e descontou um valor) Continuo a achar ridiculo tho. Isto é só prova empírica. Há uns tempos tirei esta dúvida com o zuq: Pergunta: Nos slides diz que o RSA SecurID e os protocolos desafio-resposta com uma chave partilhada são robustos contra ataques com dicionário, isto quer dizer que é mesmo impossível um ataque com dicionário ser bem sucedido ou é apenas improvável? Resposta: Em princípio, são impossíveis. Os ataques com dicionários exploram o facto de se escolherem menos senhas (ou chaves) do que o universo de escolhas possíveis.Isso acontece quando a escolha é feita por humanos. Quando é um programa de computador a fazer uma escolha, e ele escolhe um valor de N bits aleatoriamente, só existe uma limitação do universo de chaves possíveis se o algoritmo de geração tiver um defeito. Se não tiver ... os ataques com dicionários são impossíveis, porque não se conseguem fazer dicionários.

Os problemas de XSS (Cross-Side Scripting) são causados por deficiências nos mecanismos de segurança dos navegadores?

Um sistema de ficheiros permite sempre distinguir um ficheiro cujo conteúdo está cifrado?
V (0) - tinha aqui um voto, mas se ta confirmado ta confirmado i guess vou estudar q me fodo guga(?) - não está (nada?) explícito nos slides, foi mesmo com o elearning só, também estava na dúvida. Resumo: português é fodido
F (3) - Confirmado no elearning (distinguir as in conteúdo cifrado vs não cifrado)



Penso que nenhum destes atributos permite distinguir qual o ficheiro.

A resistência de uma função de síntese à descoberta de uma pré-imagem é crítica para as assinaturas digitais?

Os computadores aceitam mensagens ARP Response mesmo que não tenham enviado o correspondente ARP Request?
V (3) - Confirmed
F (0)

Pode-se gerar um MAC (Message Authentication Code) usando apenas uma função de síntese?
V (0)
F (0)

As cifras simétricas modernas são cifras de:

a) Substituição
b) Transposição

Qual dos seguintes modos de cifra propaga erros no criptograma na decifra?

a) CFB (Cipher FeedBack)
b) OFB (Output FeedBack)

Uma cifra contínua, ou de fluxo (stream) é uma aproximação prática da cifra de Vernam (One-Time Pad)?
V (0)
F (0)
F

O mecanismo de proteção de CORS (Cross-Origin Resource Sharing) permite controlar o acesso a um recurso de um domínio Web a partir de recursos de outros domínios Web?
V(0)
F(0)