Segurança Informática e nas Organizações

Exame Recurso
29 de Janeiro de 2016

João Alegria | 68661

Segurança Informática e nas Organizações

1º Semestre, 2015/16

Exame de Recurso

29 de janeiro de 2016

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3h.

1. Os processos em Linux possuem um UID (User IDentifier), um EUID (Effective User IDentifier) e um GID (Group IDentifier) associado. Explique o que são e para que servem.

2. No âmbito da utilização do SSH, qual o propósito de se utilizarem chaves pré-distribuídas?

3. Descreva quais os riscos típicos que a segurança informática aborda.

4. Explique a diferença que existe entre defesa de perímetro e defesa em profundidade.

5. No contexto de segurança da Informação qual o propósito das medidas de recuperação?

6. Descreva qual o papel de ferramentas como a MetaSploit do ponto de vista de um programador e de um atacante.

7. Uma cifra polialfabética não reproduz na sua saída os padrões do texto original. Explique porquê.

8. Explique como funciona o modo de cifra n-bit OFB (Open FeedBack), tanto na cifra como na decifra.

9. Descreva como pode construir um MAC (*Message Authentication Code*) recorrendo principalmente a:
   a. Uma cifra por blocos
   b. Uma síntese

10. A assinatura digital de um documento não tem existência autónoma como uma assinatura manual clássica, i.e. não pode ser "copiada" entre documentos. Explique porquê.

11. Qual o papel das Entidades Certificadores (CA) num acesso a uma página Web?

12. Considere um processo de autenticação com desafio-resposta.
    a. Explique como é que opera.
    b. Explique como é que o mesmo pode ser usado para autenticar pessoas titulares de um Cartão de Cidadão.

13. No contexto de um *smartcard* usando PKCS#11, distinga os tipos de sessões típicos e as operações disponíveis em cada tipo.

14. Descreva os diferentes tipos de prova utilizados para autenticação e o mais adequado para autenticar o acesso a uma zona restrita de um edifício.

15. Descreva o papel do atributo SRES utilizado na rede GSM e como este é processado pelas diferentes entidades.

16. A função CRC-32, usado no WEP para controlo de integridade, não pode ser considerada uma função de síntese. Explique porquê, tendo em conta os 3 requisitos que as funções de síntese têm de cumprir.

17. Discuta um problema e uma vantagem das *Firewalls* pessoais.

18. Qual a utilidade do mecanismo *chroot* na construção de *honeypots*?

19. Descreva os *backups* de informação em relação ao nível a que são realizados.

20. A probabilidade de um sistema falhar na globalidade é proporcional ao número de discos que compõem um volume RAID5. Explique porquê.

Segurança 2015/2016
Exame Recurso - 29 Janeiro 2016

1. Os processos em Linux possuem um UID (user IDentifier), um EUID (effective user IDentifier) e um GID (Group IDentifier) associado. Explique o que são e para que servem.

UID → para um SO, um utilizador é um número estabelecido durante o operação de login. As atividades executadas num computador fazem-se sempre associadas a um UID. Este, por sua vez, permite estabelecer o que é permitido/negado as atividades.

GID → É um conjunto de utilizadores. Um utilizador pode pertencer a diferentes grupos, onde os seus privilégios são determinados através do conjunto de privilégios atribuídos a si e aos grupos a que pertence.

EUID → É um utilizador efetivo, no qual permite determinar o acesso a determinados ficheiros.

2. No âmbito da utilização do SSH, qual o propósito de se utilizarem chaves pré-distribuídas?

O propósito é que para autenticar o cliente, este apenas precisa de saber uma senha: a que protege a sua chave privada. Se essa senha for comprometida, é apenas necessário alterá-la no sistema onde a chave privada está guardada.

3. Descreva quais os riscos típicos que a segurança informática aborda.

- Eliminação ou Alteração de informação
- Confidencialidade: Acesso não autorizado à informação
- Privacidade: Recolha de dados de caracter privado
- Disponibilidade de Recursos
- Personificação de pessoas ou serviços
- Uso abusivo de sistemas alheios privilegiados

4. Explique a diferença que existe entre defesa em profundidade e defesa de perímetro.

A <u>defesa de perímetro</u> consiste em definir um perímetro protegido englobando um conjunto de máquinas e redes, e em evitar interações indesejáveis entre os dois lados desse perímetro.

O perímetro divide o universo de máquinas e redes em dois: num é onde estão os recursos a proteger e noutro é onde estão os possíveis abusadores desses recursos.

A <u>defesa em profundidade</u> é útil para detetar problemas internos, ou seja, atua em todos os níveis e não apenas nas fronteiras.

→ A diferença entre estas duas fases é que a defesa em profundidade é mais complexa de gerir, mas teoricamente mais eficaz que a do perímetro.

5. No controlo de segurança de Informação qual o propósito das medidas de recuperação?
O propósito destas medidas é poderem recuperar a informação, caso tenha havido algum problema ou ataque.
A informação pode estar armazenada redundantemente em vários discos; realizar cópias de segurança periódicas (backups) ou recuperação forense.

6. Descreva qual o papel de ferramentas como o Metasploit do ponto de vista do programador e de um atacante.
Metasploit é um projeto de segurança de informação com o objetivo de análise de vulnerabilidades de segurança a facilitar testes de intrusão e no desenvolvimento de assinaturas para sistemas de deteção de intrusos. ⊗1

7. Uma cifra polialfabética não produz na sua saída os padrões do texto original. Explique porquê.
Porque um caráter do alfabeto original pode ser substituído por diferentes caracteres dos alfabetos de substituição (pode ser mais que um) numa operação de cifra/decifra.
Os alfabetos são usados de forma cíclica, onde a frequência de letras individuais e de "consoantes dobradas" são menores relativamente às cifras monoalfabéticas.

⊗1 Ou seja, no ponto de vista do programador é testar a intrusão de ataques, enquanto que no ponto de vista do atacante é a tentativa de ataque.

8. Explique como funciona o modo de cifra n-bit OFB (Open feedback), tanto na cifra como na decifra.
O modo de cifra OFB transforma uma cifra por blocos numa cifra contínua.
Método base: O gerador de cifra contínua é recolhido por uma função de cifra por blocos, por dois registos com o comprimento do bloco, R_i e R_0 e por uma função de realimentação.
A função cifra o conteúdo de R_i e guarda-o em R_0. Desse resultado, os n bits mais significativos são usados para cifrar os dados.
São essenciais três fatores: - valor inicial de R_i
- da função de cifra e da chave utilizada
- da função de realimentação
Nota: No OFB, a realimentação é feita a partir do criptograma
Quem cifra e decifra este modo tem de usar o mesmo valor de R_i.

9. Descreva como pode construir um MAC (Message authentication code) recorrendo principalmente a:

a. Uma cifra por blocos.

Através do CBC-MAC é possível um MAC que é um conjunto de bits do último bloco do criptograma gerado com uma cifra por blocos em modo CBC. Ou através do DES-MAC que gera um MAC que é um conjunto de bits do último bloco do criptograma gerado com DES em modo CBC ou CFB de 64 bits. No caso do CBC o VI é nulo enquanto que CFB o VI é o primeiro bloco da mensagem.

b. uma síntese

Através de keyed-MDs que gera um MAC aplicando uma função de síntese a um bloco formado pela concatenação de uma chave com a mensagem

Através do HMAC que gera um MAC aplicando a função de síntese 2 vezes: uma chamada interior (onde são processadas a chave e a mensagem) e outra exterior (onde é processada a síntese interior e a chave).

10. A assinatura digital de um documento não têm existência autónoma como uma assinatura manual clássica, i.e. não pode ser "copiada" entre documentos. Explique porquê.

As assinaturas digitais são sempre únicas consoante o documento que autenticam enquanto as assinaturas manuscritas tendem a ser muito semelhantes (para a mesma pessoa) independentemente do documento que autenticam.

Logo, uma assinatura digital não serve de nada se não acompanhar o documento que autentica, já por outro lado, as assinaturas manuais têm existência própria e podem por isso ser copiadas entre documentos.

11. Qual o papel das Entidades Certificadoras (CA) num acesso a uma página Web?

As CAs têm um papel básico de garantir a correspondência entre a identidade e a chave pública de uma determinada entidade.

Uma CA é capaz de realizar todos os processos de emissão de certificados, verificação de validade, armazenamento, publicação e acesso online, revogação e arquivamento para verificação futura. Estes certificados permitem que as transações sejam seguras, garantem autenticidade e integridade à página web a que estão associados.

Os browsers mantêm uma lista de todas as CA que são confiáveis e quando se acede a uma página segura esta deve apresentar o seu certificado digital ao browser e se estiver dentro da validade e pertence a uma CA confiável então o acesso à página decorre sem avisos de segurança.

12. Considere um processo de autenticação com desafio-resposta

a. Explique como opera

É lançado um desafio pelo autenticador, onde a entidade a ser certificada transforma o desafio usando as suas credenciais de autenticação. Esse resultado é enviado ao autenticador, que verifica o mesmo, produzindo um resultado próprio usando o mesmo aproximação e verificando a igualdade entre os dois.

Deve ser utilizada sempre que o meio de comunicação possa ser escutado, pois é mais complexa. Tem como vantagem não expor credenciais de autenticação e como desvantagens o facto das pessoas precisarem de ter meios para calcular as respostas a partir dos desafios e o facto de o autenticador armazenar os segredos partilhados sendo vulneráveis a ataques com dicionários antecipados que usam pares desafio-resposta.

b. Explique como é que o mesmo pode ser usado para autentica pessoas titulares de um cartão cidadão.

Através do desafio-resposta com smartcards, onde as credenciais de autenticação são as do CC, a chave privada no cc e o pin de acesso à chave privada. O autenticador sabe a chave pública correspondente.

Nesta aproximação, o autenticador gera um desafio aleatório e o dono do CC cifra o desafio com a sua chave privada, enviando posteriormente ao autenticador. Este último, decifra o resultado com a chave pública respetiva; se o resultado for igual ao desafio a autenticação teve sucesso.

13. No contexto de um smartcard usando o Pkcs#11, distinga os tipos de sessões típicos e as operações disponíveis em cada tipo.

- Sessão pública de leitura
  - Acesso de leitura aos objetos públicos
  - Acesso de leitura/escrita aos objetos de sessão públicos

- sessão pública de leitura e escrita
  - Ler e escrever todos os objetos públicos

14. Descreva os diferentes tipos de prova utilizados para autenticação e o mais adequado para autenticar o acesso a uma zona restrita de um edifício.

Existe 3 tipos de prova:

- o que se sabe? - Uma entidade prova a sua autenticidade mostrando que conhece uma determinada informação secreta (ex: senha). Se a senha for conhecido pelos intervenientes diretos no processo de autenticação, pode provar que o interlocutor é quem afirma ser.

- o que se possui? - Uma entidade prova a sua autenticidade mostrando que possui um determinado dispositivo de segurança ou que é dono legítimo desse dispositivo de segurança.

- o que se é? - Neste paradigma é apresentado alguma característica que permite diferenciar dos demais. Normalmente este paradigma é aplicado a humanos e às características diferenciadoras são obtidas pela biometria.

Estes três paradigmas podem ser usados isoladamente ou combinados para reforçar a prova de identidade. Para o acesso a uma área restrita é possível combinar estes três paradigmas através da junção de uma senha pessoal de acesso + um cartão + leitura de impressão digitais.

15. Descreva o papel do atributo SRES utilizado na rede GSM e como este é processado pelas diferentes entidades.

16. A função CRC-32, usada no WEP para controlo de integridade, não pode ser considerada uma função. Explique porquê, tendo em conta os 3 requisitos que as funções de síntese têm de cumprir.

Os 3 requisitos das funções de síntese são:

- resistência à descoberta de um texto - dado um valor produzido por uma função de síntese é muito difícil encontrar um texto que produza o mesmo valor

- resistência à descoberta de um 2º texto - dado um texto, é difícil encontrar um segundo texto com a mesma síntese

- resistência à colisão - é difícil encontrar 2 textos com a mesma síntese

O WEP usa um mecanismo de controlo de integridade não criptográfico baseado no CRC-32. Não pode ser considerado uma função de síntese pois não cumpre estes 3 requisitos dado que a integridade dos dados é verificada comparando o ICV extraído do frame com a soma de controlo calculada com base CRC-32 a partir dos dados obtidos após a decifra.

17. Discuta um problema e uma vantagem das Firewalls pessoais.

Firewalls pessoais não são nada mais do que firewalls que se destinam a proteger uma única máquina e fazem parte do seu sistema. Uma firewall pessoal normalmente é um sistema de software que é executado na mesma máquina que se quer proteger, ou seja, a firewall e o perímetro protegido é a mesma máquina.

Tem como vantagem minimizar o comprometimento de máquinas alheias no mesmo perímetro de segurança. No entanto tem a desvantagem de que nem todos os utentes são especialistas em segurança de redes e a variedade de interações leva a um grande número de regras.

18. Qual a utilidade do mecanismo chroot na construção de honeypots?

Um método de criar um honeypot é usando o chroot. O chroot basicamente limita um utilizador a uma área específica do sistema mas ao mesmo tempo dá a impressão de que ele está no nível máximo de acesso de ficheiros. Isto permite criar um pequeno ambiente simulado numa área do sistema que não afeta nada. Após isto, cria-se um servidor simulado para ver o que o atacante tenta fazer.

19. Descreva os backups de informação em relação ao nível a que são realizados

• Nível Aplicacional - onde a extração dos dados da aplicação representa uma vista consistente para a aplicação.

• Nível de Ficheiros - onde a cópia de ficheiros individuais permite copiar qualquer aplicação

• Nível do Sistema de ficheiros - onde a criação de registos de alterações periódicas permitem recuperar ficheiros individuais ou não

• Nível dos Blocos - cópia dos blocos do suporte de armazenamento, que pode ser realizado pela infraestrutura de armazenamento.

20. A probabilidade de um sistema falhar na globalidade é proporcional ao número de discos que compõem um volume RAID 5. Explique porquê.

Num sistema RAID 5, a probabilidade do sistema falhar na globalidade é devido à repartição da informação por todos os discos, uma vez que cada disco tem um fragmento de paridade.