EscolhasMultiplas

1. **Autenticação no GSM, indique a resposta errada:**
    a. Permite autêntica os terminais móveis mas não permite autenticar a rede
    b. Usa um protocolo de autenticação multimétodo
    c. Baseia-se no conhecimento mútuo de uma chave secreta
    d. Não é imune a ataques com dicionários
        i. **É imune porque usa senhas do user**
2. **Autenticação de utentes com S/Key, indique a resposta errada:**
    a. O autenticador tem acesso à senha original dos clientes
        i. **Autenticador sabe "raíz, última OTP usada (OTPn) e n (índice).**
    b. Os autenticados precisam de reinstalar as suas credenciais de autenticação após um determinado número de utilizações
    c. As senhas descartáveis são geradas a partir de uma senha
    d. Permite que, para o mesmo utente, a mesma senha produza senhas descartáveis diferentes para sistemas diferentes
3. **Autenticação com desafio-resposta, indique a resposta errada:**
    a. Não é tipicamente aplicável a autenticações biométricas
    b. É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam
    c. Visa proteger as credenciais usadas no processo de autenticação
    d. Não permite uma fácil implantação de protocolos de autenticação mútua
4. **Autenticação de utentes com RSA Secure ID, indique a resposta errada:**
    a. É imune a ataques com dicionários
    b. As senhas descartáveis são geradas a partir de uma chave secreta
    c. Obriga a que os que utentes usem um equipamento próprio (ou uma aplicação)
    d. A chave secreta de cada utente é gerada a partir de uma senha
        i. **A senha é que é gerada com um chave secreta.**

5. **Arquitetura PAM (escolha a resposta errada):**

A ***pluggable authentication module (PAM)*** is a mechanism to **integrate multiple low-level authentication schemes** into a **high-level API**. It allows **programs** that rely on **authentication** to be **written independent** of the **underlying authentication scheme**.

   a. Permite adicionar novos mecanismos de autenticação sem alterar as aplicações
   b. Permite customizar mecanismos de autenticação
   c. É uma forma de separar a forma de autenticar da necessidade que as aplicações têm que ela ocorra
   d. Permite que as aplicações programaticamente orquestrem a forma como querem concluir os seus processos de autenticação
      i. **Permite configurar autenticação sem modificação das apps mas não permite que estas alterem as autenticações programaticamente**

6. **A não observância do princípio do Privilégio Mínimo (escolha a resposta errada):**

O ***princípio do menor privilégio*** é uma estratégia de segurança que se baseia na ideia de **conceder autorizações apenas** quando realmente sejam **necessárias** para o desempenho de uma atividade específica.

   a. Permite que os utentes se possam exceder nas suas actividades
   b. Permite abusos
   c. Abre caminho a problemas causados involuntariamente
   d. É perfeitamente aceitável caso haja um sistema robusto de auditoria

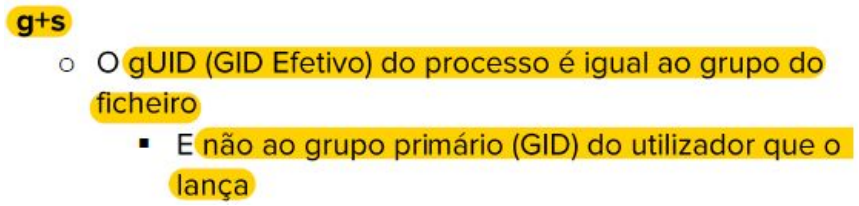
7. **Autenticação de utentes baseados em senhas descartáveis, indique a resposta errada:**
    a. Pode envolver a troca de um desafio para indicar a senha descartável a ser usada.
    b. Exige que o utente tenha de ter algo para memorizar ou gerar as senhas descartáveis.
    c. É imune a ataques com dicionários
        i. **Pode não ser imune caso use senhas do utilizador para gerar a OTP**
    d. Tipicamente não permite autenticação mútua.
8. **Autenticação no GSM, indique a resposta errada:**
    a. Permite autenticar os terminais móveis mas não permite autenticar a rede.
    b. A posse do módulo SIM onde está a chave secreta é normalmente suficiente para um terminal móvel se autenticar
        i. **Precisa de SIM (A3 e A8) e da Baseband (A5).**
    c. Permite delegar a autenticação dos terminais móveis noutras redes
    d. Baseia-se no conhecimento mútuo de uma chave secreta
9. **Autenticação de utentes do UNIX/Linux indique a resposta errada:**
    a. Usa senhas memorizadas
    b. Usa valores guardados em ficheiros inacessíveis aos utentes comuns.
    c. Não deverá ser usada para criar sessões remotas sobre comunicações não seguras
    d. Usa uma aproximação desafio-resposta
        i. **Aproximação direta**

10. Autenticação no SSH indique a resposta errada:

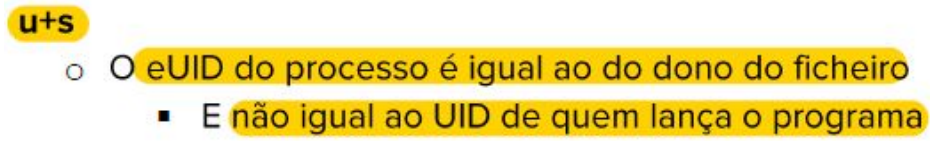
a. Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor
b. Permite que os utentes se autentiquem de forma flexível
c. Protege a autenticação dos clientes realizando-a no âmbito de uma comunicação segura
d. Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou o nome DNS)
    i. **Autenticação de servidores é feita com um par de chaves assimétricas**

11. Considerando um mecanismo de Set-UID / Set-GID, qual é a afirmação verdadeira:

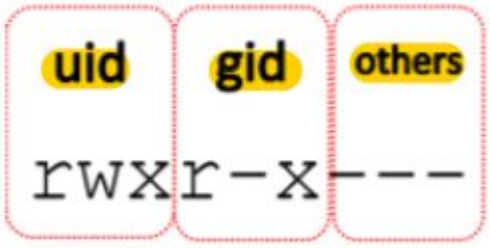
a. Um processo possui as permissões do grupo com o real GID associado ao processo
b. A permissão do Set-GID altera o GID associado a um ficheiro



c. O mecanismo Set-UID não permite que um utilizador obtenha mais permissões do que as que já possui.
d. Um ficheiro com permissão Set-UID irá executar com as permissões do UID do dono do ficheiro



12. **No UNIX/Linux, caso um ficheiro tenha a proteção -wx rwx --x, qual dos seguintes acessos é negado?**



UID: Dono do file

a. Execução por um processo com um GID igual ao do ficheiro
b. Execução pelo dono
c. Leitura pelo dono
    i. -wx rwx --x
d. Alteração do bit Set-UID pelo dono

13. **No UNIX/Linux relativamente ao comando sudo, qual das seguintes afirmações é falsa?**

a. Permite realizar uma elevação de privilégios por comando
b. É um comando especial que é reconhecido como tal pelo núcleo do sistema operativo.
    i. **É uma aplicação com SET-UID e o dono é a ROOT (UID = 0)**
c. É um comando que serve para concretizar elevação de privilégios pontuais, logo é útil para concretizar políticas de privilégio mínimo.
d. Permite que os comandos realizados para fins de administração sejam registados em nome de quem os executou.

14. **No UNIX/Linux qual dos seguintes direitos está sempre vedado ao dono de um ficheiro (excepto se for root)?**

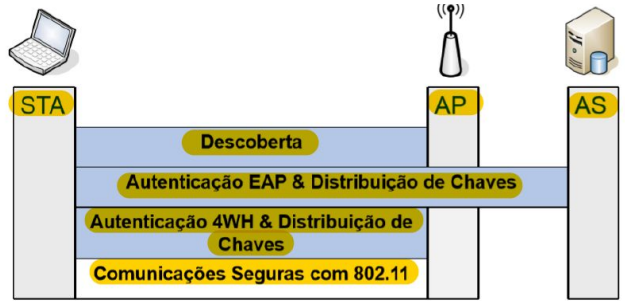
a. Alterar o seu dono
b. Alterar a proteção relativa ao seu dono
c. Eliminar o nome de um ficheiro
d. Alterar o seu grupo

15. **Qual das seguintes afirmações é falsa relativamente à cifra de ficheiros usando aplicações?**
    a. a) Não existe um método padrão de identificar se um ficheiro está cifrado
    b. b) Permitem cifras diferentes em cada ficheiro
    c. c) Permite que os ficheiros partilhados em rede circulem de forma cifrada
    d. d) A partilha de utentes por vários utentes é simples
        i. **Devido ao facto da encriptação ser feita por aplicações autónomas**

Perguntas SIO

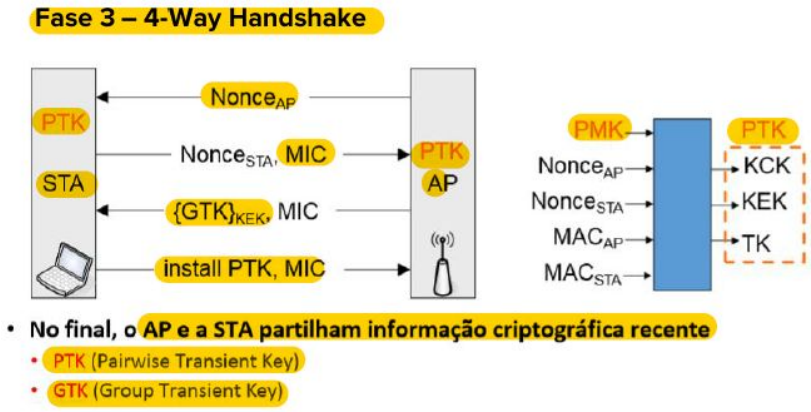
1. **45. Uma ACL (Access Control List) escolha a opção errada:**
    a. É uma informação de controlo de …
    b. É uma informação que pode ter dimensão fixa ou variável
    c. Permite verificar que direitos de acesso tem um sujeito a um objecto
    d. É uma parcela de matriz de controlo de acesso usada por um monitor de controlo de acesso
2. **53. Relativamente à autenticação no SSH indique a resposta errada:**
    a. Pode criar problemas de decisão aos clientes quando se mudam as credenciais dos servidores
    b. É vulnerável a ataques de interposição (man in the middle)
    c. Permite que os utentes se autentiquem de forma flexível
    d. Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor
3. **109. Autenticação de utentes através de senhas descartáveis:**
    a. É sempre imune a ataques por dicionário (falsa)
    b. Exige que o utente tenha de ter algo memorável ou gerar as senhas descartáveis
    c. Tipicamente permite autenticação mútua
    d. Evita todos os problemas decorrentes da captura de senhas trocadas em claro
4. **110. Autenticação do WPA no acesso de um terminal à rede:**
    a. Elimina apenas o modo OSA do WEP
    b. Segue os princípios do padrão 802.1X
    c. Depende sempre de um serviço ….
    d. Realiza sempre uma autenticação

5. **111. Protocolo vulnerável a ataques por dicionário?**
    a. Linux
        i. **John The Ripper**
    b. SSH (servidor)
    c. TLS (servidor)
    d. TLS (cliente)
6. **113. Firewall Pessoal**
    a. Só atua com Packet Filter
    b. Só atua com Circuit Gateway
    c. .... chamada defesa de perímetro
    d. controlo do tráfego de aplicações concretas
7. **114. O que ocorre na 2ª etapa do 802.1**



    a. Distribuição de chaves entre o suplicante e o Servidor
    b. Distribuição chaves entre suplicante e o Autenticador
    c. Autenticação do Autenticador
8. **115. Qual das seguintes deficiências <u>não</u> existe no WEP?**
    a. Não autêntica AP
    b. Tem um algoritmo de autenticação que não é robusto
    c. Não separa chaves de autenticação de chaves de cifra de mensagens
    d. Não permite distinguir os utentes que acedem
        i. **Permite distinguir**

9. **116. iptables**
    a. É do tipo filtro de pacotes (Packet Filter)
    b. É do tipo filtro de circuitos (circuit Gateway)
    c. Packet filter com contexto?
10. **118. A que é que o dono de um ficheiro (exceto root) está vedado:**
    a. Alterar nome ficheiro
    b. Ler o conteúdo caso não tenha permissão de leitura
    c. Retirar todas as permissões ao dono do ficheiro
    d. Alterar o bit do setUID
11. **124. O que acontece na etapa 4 hand shake do 802.1x:**



    a. Distribuição de chaves criptográficas para ao autenticador
    b. Apenas autenticação para o suplicante
    c. Apenas autenticação do servidor de autenticação
    d. Distribuição de chaves criptográficas para o servidor
12. **126. Protocolo vulnerável a ataques por dicionário?**
    a. S/Key
    b. GSM
    c. SSL
    d. RSA SecurID

13. 130. Four handshake, o que acontece:

a. Distribuição de chaves entre o suplicante e o Servidor
b. Distribuição chaves entre suplicante e o Autenticador
c. Só Autenticação do Autenticador
d. Só Autenticação do Suplicante

14. Controlo de acesso discricionário (Discretionary Access Control DAC)

a. É um meio de restringir o acesso a objetos com base na ***identidade*** dos sujeitos e/ou grupos aos quais eles pertencem. Os controles são ***discricionários*** no sentido de que o sujeito com uma ***certa permissão de acesso seja capaz de passar esta permissão*** (talvez indiretamente) para ***qualquer outro sujeito*** (a menos que seja restringido pelo ***controle de acesso obrigatório***).
b. Utilizadores podem definir regras para controlo de acesso
    i. **Podem ser definíveis apenas pelo dono/utilizador:** Esta limitação é em si um Acesso Mandatório. *(EX: ACL)*

15. Controle de acesso obrigatório

a. tipo de controle de acesso pelo qual o sistema operacional restringe a capacidade de um sujeito ou iniciador de acessar ou, geralmente, realizar algum tipo de operação em um objeto ou destino.
b. Existem inúmeros casos de controlo de acesso obrigatório num sistema operativo
    i. Fazem parte da lógica do modelo computacional
    ii. **Não são moldáveis pelos utentes e administradores:** A menos que alterem o comportamento do núcleo

16. UNIX/Linux relativamente ao UID e GID

a. **UID:**

i. **Para um SO um utilizador é um número:** Estabelecido durante a operação de login

ii. **Atividades executadas fazem-se sempre associadas a um UID:** O UID permite estabelecer o que lhes é *permitido/negado.* UIDs *especiais* podem permitir acesso privilegiado

b. **GID:**

i. Também existem identificadores de grupo:

1. Um grupo é um conjunto de utilizadores
2. Um grupo pode ser definido à custa de outros grupos

ii. Um utilizador pode pertencer a diversos grupos:

1. Direitos = Direitos *UID* + Direitos *GIDs*

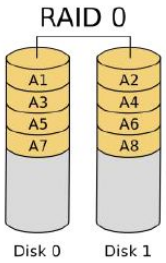
iii. Em Linux as atividades executam associadas a um conjunto de grupos

1. **1 Grupo primário:** utilizado para definir pertencia de ficheiros criados
2. **Vários grupos secundários:** utilizados para condicionar o acesso

c. **Processos** são Associado à identidade de quem o lançou (UID e GIDs)

17. 100. Qual desperdiça menos espaço de armazenamento (RAID)?

a. RAID 0. Não há desperdício, discos estão em paralelo



18. **101. Qual desperdiça maior espaço de armazenamento (RAID)?**
    a. RAID 0+1, precisa pelo menos 4 discos
19. **102. Condição de paragem do RAID 0**
    a. Não há, porque perde-se toda a informação do disco
20. **103. Condição de paragem no RAID 1**
    a. N-1, sem perda de dados
21. **104. Condição de paragem no RAID 0+1/1+0**
22. **105. Em que RAID o desperdício de armazenamento não segue uma proporcionalidade direta com o número de discos**
    a. RAID 0

23. **106. Firewall do tipo Packet Filter**
    a. Rejeitam interações não autorizadas segundo o conteúdo dos datagramas IP
    b. Podem analisar comportamento de fluxos
    c. Transparente para as aplicações responsáveis pelos fluxos que avalia

24. **107. Autenticação no SSH**
    a. Permite os clientes autenticarem-se de forma flexível
    b. Vulnerável a ataques man-in-the-middle
    c. Protege a autenticação dos clientes
    d. **Autenticação das entidades intervenientes:** Suportado por vários métodos
    e. **Servidor: Um par de chaves assimétricas e não certificadas**
    f. **Clientes: Autenticação parametrizável**

25. 108. Autenticação no TLS

a. Autenticação das entidades intervenientes
    i. Serviços, sistemas, sujeitos, etc…
    ii. Assegurado por chaves assimétricas e certificados X.509
b. **Confidencialidade e integridade da comunicação:** Distribuição de chaves, negociação de cifras, sínteses e outros mecanismos
c. Autenticação dos clientes não é opção dos mesmos
d. **Autenticar Servidor** - cliente usa a chave pública do servidor para cifrar dados que são usados para calcular a chave secreta

26. Effective UID/GUI e Real UID/GUID

a. Fundamental para efeitos de controlo de acesso do processo
b. Pode ser igual à identidade de quem lançou o processo
c. O effective UID (euid) e o effective GID (egid) afetam a criação e o acesso de arquivos. Durante a criação do arquivo, o kernel define os atributos do proprietário do arquivo para o UID efetivo e o GID efetivo do processo de criação. Durante o acesso ao arquivo, o kernel usa o UID efetivo e o GID efetivo do processo para determinar se ele pode acessar o arquivo.

27. Pergunta de SKA e OSA

a. WEP (Wired Equivalent Privacy)
b. OSA: Open System Authentication: Sem qualquer autenticação
c. SKA: Shared Key Authentication:
    i. Desafio resposta entre STA e AP
    ii. Chave distinta por cliente (Endereço MAC) ou rede
        1. Autenticação unilateral da STA
        2. AP não é autenticado

28. Em que consiste a autenticação biométrica

a. **Avaliações biométricas:** Uma pessoa autentica-se usando medidas do seu corpo
b. **Referência biométrica:** Estas medidas são comparadas com um registo pessoal similar

29. O que é a rede DMZ

a. DeMilitarized Network ou Perimeter Network
b. Rede insegura
c. Contém servidores expostos ao mundo
    i. Por vezes necessário para utilizar serviços/aplicações específicas

30. SecurID

a. Dispositivo de Autenticação Pessoal (ou software)
b. Valor único calculado com base numa chave, instante temporal, etc.
c. Robusto contra dicionários

31. **Vantagens do NAT (Extensa)**
    a. **NAT (Network Address Translation):** Masquerading e Port forwarding
    b. Reescrever, utilizando-se de uma **tabela hash**, os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior
    c. **Vantagens:**
        i. As entradas no NAT são geradas apenas por pedidos dos computadores de dentro da rede privada. Sendo assim, um pacote que chega ao router vindo de fora e que não tenha sido gerado em resposta a um pedido da rede, ele não encontrará nenhuma entrada no NAT e este pacote será automaticamente descartado, não sendo entregue a nenhum computador da rede.
        ii. Isso impossibilita a entrada de conexões indesejadas e o NAT acaba funcionando como um **firewall**.
32. **Esquema de iptables com as cadeias identificadas com letras, e pedia qual a cadeia correspondente a uma determinada letra**

33. **131. [Pergunta Extensa] O que é um ataque com dicionários e como pode ser evitado?**
    a. **Definição:** Ataque de dicionário é um tipo de ataque de força bruta destinado a burlar uma cifra ou mecanismo de autenticação com o objetivo de descobrir uma senha tentando centenas ou, algumas vezes, milhões de possibilidades, como por exemplo, palavras de um dicionário.
    b. **Prevenção:**
        i. Using a passphrase
        ii. choosing a password that is not a simple variant of a word found in any dictionary
        iii. listing of commonly used passwords

Content teste 2 2019

1. iptables
2. chaves assimétricas com desafio-resposta
3. S / key
4. senhas descartáveis
5. RSA SecurID
6. Firewall pessoal
7. Filtro aplicacional
8. RAID - condições de paragem

Content recurso 2019

1. certificados X509
2. raids, probabilidade de perda P^N condições de paragem
3. camadas de núcleo dos sistemas operativos anéis
4. s/key
5. fórmula do CTR qd o AES é 128
6. [extensa] padding, e ataques com dicionários

Revisão recurso 2019

1. apparmor
2. condições de paragem do RAID 1: N-1
    a. P^N raid 1
3. esquema das iptables, a resposta era output
4. Senhas descartáveis, pode envolver a troca de um desafio
5. Autenticação do wpa permite o modelo para redes de pequena dimensão
6. Firewall IP tables serve para aceitar ou rejeitar que passam através de uma máquina

7. **Tipo packet filter pode ser concretizada com uma aplicação genérica configurada**
8. **Aplication gateway obriga a que existam múltiplas aplicações uma para cada tipo de tráfego**
9. **O processo pode alterar livremente o seu efetive user ID para o valor do user ID**
10. **ACLs, mandatórias e discricionárias**