

**1. As políticas de segurança:**

- a) ~~São as tecnologias que permitem implementar um determinado objetivo de segurança.~~
- b) ~~São regras que definem o mecanismo a utilizar de forma a obter segurança.~~
- c) ~~São constituídas pelas leis que definem o âmbito do crime informático.~~
- d) São normas, regulamentos e orientações que definem o modelo de proteção num determinado domínio de segurança


**2. Um ataque do dia zero é :**

- a) ~~um ataque lançado no início do ano~~
- b) ~~um ataque inovador usando uma combinação de vulnerabilidades conhecidas~~
- c) ~~um ataque novo para uma vulnerabilidade conhecida~~
- d) um ataque que explora uma vulnerabilidade até aí desconhecida


**3. Qual das seguintes afirmações é falsa tendo em conta o que é um registo CVE (Common Vulnerabilities and Exposures)**

- a) Um registo CVE refere a potencial gravidade de um ataque face a uma vulnerabilidade.
- b) Um registo CVE pode dar indicações acerca do erro que originou uma vulnerabilidade
- c) Um registo CVE nunca descreve um problema de configuração
- d) Um registo CVE descreve como pode ser realizado um ataque a um software vulnerável

**4. Num ataque XSS (Cross site scripting) de armazenamento onde é executado o código malicioso?**

- a) No computador da vítima
- b) No servidor 
- c) ~~Num equipamento de rede (eg. roteador)~~
- d) ~~No computador do atacante~~

**5. No processo de manipular o endereço MAC de uma interface local é denominado de:**

- a) ARP Resolution
- b) ARP Spoofing 
- c) ARP corruption
- d) ARP Poisoning

**8. Tendo em conta as recomendações relativas ao uso de cifras contínuas, qual não é necessariamente crítico?**

- a) Não usar o mesmo estado inicial no gerador de cifra para mensagens diferentes
- b) O criptograma deverá incluir um mecanismo de controlo de integridade
- c) O valor da chave contínua numa determinada posição, não deverá permitir calcular outros valores da mesma, tanto antes como depois
- d) Não se devem cifrar mensagens com um comprimento elevado

**9. Quando se usa cifra tripla é normal usar o modo EDE (encrypt, decrypt, encrypt). Porquê?**

- a) porque caso se usasse 3 cifras seria mais simples descobrir as 3 chaves
- b) porque se usasse 3 cifras ficaria menos eficiente
- c) porque se pode anular uma cifra com a decifra ou vice versa
- d) porque usar uma decifra entre cifras aumenta a confusão do processo de cifra

**10. Para enviar uma mensagem confidencial a um destinatário, usando criptografia assimétrica, deve:**

- ~~a) cifrar a mensagem usando a sua (remetente/ originador) chave pública~~

- b) ~~cifrar a mensagem usando a sua (remetente/ originador) chave privada~~
- c) cifrar a mensagem usando uma síntese da sua (remetente/ originador) chave pública
- d) cifrar a mensagem usando uma cifra híbrida com a chave simétrica aleatória e a chave pública do destinatário

**11. Qual dos seguintes modos de cifra não permite um acesso aleatório constante na decifra?**

- a) ECB
- b) OFB
- c) GCM (Galois/Counter Mode)
- d) CBC

**12. Qual dos seguintes modos de cifra realiza uma cifra monoalfabética?**

- a) GCM
- b) CFB
- c) ~~OFB~~
- d) ECB

**13. Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é falsa?**

- a) se for reduzida, representa um risco caso a função seja usada num MAC.
- b) se for reduzida, o autor de uma assinatura digital poderá produzir vários documentos para a mesma assinatura
- c) se for reduzida, uma entidade terceira poderá produzir um texto alternativo compatível com a assinatura de outro texto
- d) é definida apenas pela dimensão do resultado da função, de acordo com o paradoxo do aniversário



**14. Um MAC é calculado com uma chave secreta**

- a) porque a mensagem autenticada com o MAC precisa de ser confidencial
- b) porque é necessário garantir o seu secretismo
- ~~c) porque usa uma função de cifra~~
- d) para impedir que terceiros possam gerar um MAC válido para outra mensagem

**15. Um dos objetivos das assinaturas digitais é o não-repúdio que consiste em:**

- a) Forçar o uso de smartcards na geração de assinaturas
- b) Impedir o acesso não autorizado ao conteúdo das mensagens/documentos
- c) Garantir que uma mensagem, no documento, não sofreu qualquer alteração, isto é, esta tal e qual como quando foi gerada
- d) Impedir que uma entidade que produziu uma mensagem/documento assinada(o) o possa negar

**16. A assinatura digital de um documento:**

- a) garante que é possível detetar qualquer adulteração do mesmo após a sua assinatura
- ~~b) deixa de ser válida quando o par de chaves do assinante expira~~
- ~~c) impede que o documento possa ser compreendido por quem não estiver autorizado~~
- ~~d) pode, em certos casos, ser realizada com chave simétrica~~

**17. Um Entidade Certificadora raiz é confiável porque:**

- a) Certifica muitas outras Entidades Certificadoras
- b) Está no topo de uma cadeia de certificação
- c) Tem um certificado autoassinado

d) Confiamos na correção da sua chave pública

**18. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?**

- a) a data do certificado é válida
- b) o certificado não está listado na CRL
- c) não é de todo possível
- d) existe uma Entidade Certificadora (CA) intermédia confiável no caminho da certificação

**19. Tendo em conta o uso de CRL qual destas é falsa?**

- a) as listas delta completam as listas base
- b) quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior
- c) as CRL indicam a data de revogação dos certificados revogados
- d) as CRLs delta incluem certificados expirados, mas as CRL base não

ÉPOCA NORMAL 2016/2017

**21.Os mecanismos de segurança:**

- a) São as máquinas que desempenham um papel ativo na proteção de infraestruturas computacional
- b) são as tecnologias que permitem implementar um determinado objetivo de segurança
- c) são os procedimentos que devem ser seguidos numa situação de emergência
- d) ~~são as normas e regulamentos que regem a proteção de um domínio de segurança~~

**22. Uma vulnerabilidade é um estado de um sistema que permite (escolha a resposta errada):**

- a) que um atacante aceda a dados que não está autorizado a aceder
- b) que um atacante se apresenta com outrem
- c) que um atacante negue a prestação de serviços
- d) que um atacante consiga apagar o rasto da sua ação

MENINOS ECT

**23. Qual das seguintes afirmações é falsa tendo em conta o que é um registo CVE?**

- a) Um registo CVE dá algumas indicações de como uma vulnerabilidade pode ser explorada
- b) Um registo CVE refere a potencial gravidade de um ataque face a uma vulnerabilidade
- c) Um registo CVE descreve uma vulnerabilidade num software
- d) Um registo CVE descreve como pode ser realizado um ataque a um software vulnerável

**24. O processo de manipulação da cache ARP de um sistema remoto designa-se por:**

- a) ARP Resolution
- b) ARP Spoofing
- c) ARP Poisoning
- d) ARP Corruption

**25. Qual das seguintes respostas corresponde a uma vantagem introduzida pelos processos de randomização de chaves assimétricas? (OAEP)**

- a) O mesmo valor, cifrado várias vezes com a mesma chave assimétrica, produz sempre o mesmo valor
- b) Permite fazer um controlo de integridade do criptograma, após a sua decifra
- c) Impede a criptanálise de valor conhecidos cifrados com chaves privadas
- d) Permite acelerar as cifras assimétricas

**26. Qual dos seguintes modos de cifra não propaga erros do criptograma para outros bits que não os correspondentes do texto recuperado?**

- a) GCM (Galois/Counter Mode)
- b) ~~CFB~~
- c) ECB

d) ~~CBC~~



**27. Qual das seguintes propriedades de uma função de síntese não é seguramente vital para assegurar a qualidade de uma assinatura digital?**

- a) ~~Resistência à colisão~~
- b) Resistência à procura de um texto original
- c) Resistência à procura de um segundo texto original
- d) Elevado desempenho

**28. No cálculo de um MAC qual dos seguintes tipos de funções é normalmente usado?**

- a) Cifra de Vernam
- b) Cifras simétricas por blocos
- c) Cifras assimétricas
- d) Cifras simétricas contínuas

**29. Para se verificar uma assinatura digital de um documento é preciso:**

- a) ~~A chave privada do assinante~~
- b) ~~O certificado de chave pública do verificador~~
- c) ~~O certificado de chave privada do assinante~~
- d) O certificado de chave pública do assinante

**30. Uma Entidade Certificadora raiz é confiável porque**

- a) Confiamos na correção da sua chave pública
- b) Ninguém certifica o seu certificado
- c) Tem um certificado autoassinado
- d) Certifica muitas outras Entidades Certificadoras

**31. Tendo em conta o período de validade de um certificado, qual destas afirmações é falsa?**

- a) Serve para limitar, no tempo, o uso da correspondente chave privada


- ~~b) Impede que a chave privada possa ser usada fora desse período~~
- ~~c) Não pode ser usado para validar assinaturas feitas fora desse período~~
- ~~d) Pode ser encurtado caso seja revogado~~

TESTE 2 2017 (teste desfocado, pode haver erros) ECT

**32. Relativamente à autenticação de utentes baseada 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**
- d) Tipicamente não permite autenticação mútua

**33. Relativamente à autenticação no GSM (Global System For Mobile Communications) 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
- c) **Permite delegar a autenticação dos terminais móveis noutras redes**
- d) Baseia-se no conhecimento mútuo de uma chave secreta

**34. Relativamente à 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~~

opção está correta




d) Usa uma aproximação desafio-resposta

**35. Relativamente à 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 autenticuem 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(excepto o endereço IP, ou o nome DNS)

**36. 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 

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

- a) Execução por um processo com um GID igual ao do ficheiro
- b) Execução pelo dono
- c) Leitura pelo dono
- d) Alteração do bit Set-UID pelo dono

**38. 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.
- c) É um comando que serve para concretizar elevações 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.

**39. 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

**44. Relativamente à autenticação de utentes com desafio-resposta e pares de chaves assimétricas indique a resposta errada**

- a) Não há o risco de ocorrerem ataques com dicionário
- b) ...
- c) ...
- d) ...

**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

**46. Relativamente à 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

**47. Relativamente à autenticação de utentes com S/Key, indique a resposta errada:**

- a) O autenticador tem acesso à senha original dos clientes
- 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

**48. Relativamente à 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

**49. Relativamente à 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

**50. A arquitetura PAM (escolha a resposta errada):**

- 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**

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

- 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

**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 autenticuem de forma flexível
- d) Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor

**54. O controlo de acesso discricionário (Discretionary Access Control DAC )**

- a) ...
- b) ...
- c) ...
- d) ...

**55. Qual dos seguintes atributos de um ficheiro / diretoria pode ser cifrado sem que isso crie problemas?**

- a) ? Diretoria de acesso ao ficheiro
- b) Dimensão do ficheiro

- c) Data de modificação do ficheiro
- d) Nome da diretoria

**57. Os dados numa base de dados podem ser sensíveis porque (escolha a opção errada):**

- a) Provêm de uma fonte sensível
- b) Revelam a estrutura da base de dados
- c) Permitem em conjunto com mais dados inferir ...clusões indesejadas
- d) Foram declarados sensíveis

**58. Numa base de dados a integridade dos seus dados significa:**

- a) Assegurar a correção e coerência dos dados
- b) Dar acesso aos dados corretos
- c) Assegurar a execução sequencial de transações correntes
- d) Garantir a partilha dos dados

**59. No UNIX/Linux relativamente ao UID e GID de um processo qual das seguintes afirmações é verdadeira?**

- a) ...

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

RAID 0

**101. Qual desperdiça maior espaço de armazenamento (RAID)?**

RAID 0+1, precisa pelo menos 4 discos

**102. Condição de paragem do RAID 0**

Não há, porque perde-se toda a informação do disco

**103. Condição de paragem no RAID 1**

N-1, sem perda de dados

**104. Condição de paragem no RAID 0+1/1+0**

**105. Em que RAID o desperdício de armazenamento não segue uma proporcionalidade direta com o número de discos**

**106. Firewall do tipo Packet Filter**

Transparente para as aplicações responsáveis pelos fluxos que avalia

**107. Autenticação no SSH**

Permite os clientes autenticarem-se de forma flexível

Vulnerável a ataques man-in-the-middle

Protege a autenticação dos clientes

**108. Autenticação no TLS**

Autenticação dos clientes não é opção dos mesmos

Autenticar Servidor- cliente usa a chave pública do servidor para cifrar dados que são usados para calcular a chave secreta

**109. Autenticação de utentes através de senhas descartáveis: (parecem todas certas)**

- a) É sempre imune a ataques por dicionário
- 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

**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

**111. Protocolo vulnerável a ataques por dicionário?**

- a) Linux
- b) SSH (servidor)
- c) TLS (servidor)
- d) TLS (cliente)

**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

**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

**115. Qual das seguintes deficiências não existe no WEP?**

- a) Não autentica 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

**116. iptables**

- a) É do tipo filtro de pacotes (Packet Filter)
- b) É do tipo filtro de circuitos (circuit Gateway)
- c) ...
- d) ...

**117. Effective UID/GUI e Real UID/GUID**

**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

**119. Pergunta de SKA e OSA**

**120. Em que consiste a autenticação biométrica**

**121. O que é a rede DMZ**

**122. Na DMZ**

- a) Está sempre o Gateway Bastião
- b) Não me lembro das outras



**123. SecurID**

**124. O que acontece na etapa 4 hand shake do 802.1x:**

- a) Distribuição de chaves criptográficas para o autenticador
- b) Apenas autenticação para o suplicante
- c) Apenas autenticação do servidor de autenticação
- d) Distribuição de chaves criptográficas para o servidor

**125. Vantagens do NAT (Extensa)**

**126. Protocolo vulnerável a ataques por dicionário? nenhum**

- a) S/Key
- b) GSM
- c) SSL
- d) RSA SecurID

**127. A autenticação com RSA SecurID:**

- a) Obriga à aquisição de um equipamento (ou aplicação)
- b) Requer a memorização de de uma senha
- c) ...

**128. Qual dos seguintes não autentica mutuamente:**

- a) SSH
- b) SSL
- c) Biometria
- d) ...

**129. Esquema de iptables com as cadeias identificadas com letras, e pedia qual a cadeia correspondente a uma determinada letra**

**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

**131. [Pergunta Extensa] O que é um ataque com dicionários e como pode ser evitado?**

TESTE 2 2019

**132. iptables**

**133. chaves assimétricas com desafio-resposta**

**134. S / key**

**135. senhas descartáveis**

**136. RSA SecurID**

**137. Firewall pessoal**

**138. Filtro aplicativo**

**139. RAID - condições de paragem**

RECURSO 2019

**141. certificados X509**

**142. raids, probabilidade de perda  $P^N$   
condições de paragem**

**143. camadas de núcleo dos sistemas operativos anéis**

**144. s/key**

**145. fórmula do CTR qd o AES é 128**

**146. [extensa] padding, e ataques com dicionários**

REVISÃO DO RECURSO 2019:

**147. apparmor**

**148. condições de paragem do RAID 1: N-1**

**P^N raid 1**

**149. esquema das iptables, a resposta era output**

**150. resistência das funções síntese, a falsa é a do mac**

**151. A assinatura digital de uma mensagem, a falsa é a que obriga que a mensagem contenha o certificado da chave pública do assinante**

**152. O conjunto de certificado que um programa deve validar para poder confiar cadeia de certificação**

**153. validação incompleta**

**O certificado ainda não expirou mas validação da cadeia de certificação foi inicialmente baseada em algo**

**154. Senhas descartáveis, pode envolver a troca de um desafio**

**155. Autenticação do wpa permite o modelo para redes de pequena dimensão**

**156. Firewall IP tables serve para aceitar ou rejeitar que passam através de uma máquina**

**157. Tipo packet filter pode ser concretizada com uma aplicação genérica configurada**

**158. Application gateway obriga a que existam múltiplas aplicações uma para cada tipo de tráfego**

**159. Está negado ao dono ler o conteúdo se não tiver direitos de leitura**

**160. sudo falsa é um comando especial**

**161. O processo pode alterar livremente o seu efetivo user ID para o valor do user ID**

#### **ALGUMAS RESPOSTAS**

**4 - a, mas pode ser de outra acena que não armazenamento e aí é um link**

**5 - o Poisoning utiliza o Spoofing. O Spoofing manipula o MAC, sendo que o Poisoning depois trata da manipulação da cache ARP**

**8 - noutra pergunta a resposta: Não é necessariamente crítico o período ser periódico**

**9 - c**

**38 - b**

**118 - b**

#### **EXTRAORDINÁRIA - Extensas**

- Diffie-Hellman**
- ataques com dicionários, o que são e como podem ser evitados**
- ACLs, mandatórias e discricionárias**
- Difusão e confusão explicar, e como atuam nas cifras contínuas**