24. Protocolo vulnerável a ataque por dicionário?
SSH (servidor

25. O que ocorre na 2ª etapa do 802.1x?
Autenticação do autenticador

26. A que é que o dono de um ficheiro (exceto root) está vedado:
Retirar todas as permissões ao dono do file

27. O que acontece no 4º handshake do 802.1x?
Distribuição de chaves criptográficas entre o suplicante e o servidor

28. Qual dos seguintes não autentica mutuamente
Biometria (SSH e SSL geralmente incluem uma troca de chaves criptográficas e permite a autenticação mútua).

29. Protocolo vulnerável a ataques por dicionário?
S/Key -> Desafio resposta
GSM - não é vulnerável
SSL - pouco vulnerável
RSA SecureID - não é vulnerável

10. O mecanismo Set-UID / Set-GID, resposta VERDADEIRA:
Um ficheiro com permissão Set-UID irá executar c/ as permissões do UID dono do ficheiro

11. No UNIX/LINUX qual dos seguintes direitos está sempre vedado ao dono do ficheiro (excepto se for root)
Alterar o seu dono

12. relativamente ao comando sudo, resposta errada:
É um comando especial que é reconhecido como tal pelo SO.

13. Relativamente à autenticação de utentes baseados em senhas discretáveis, ERRADA:
É imune a ataques c/ dicionários

14. Relativamente à autenticação no GSM, ERRADA:
A posse do módulo SIM onde está a CHAVE secreto é normalmente suficiente para um terminal móvel se autenticado.

15. Autenticação de utentes do UNIX/LINUX, ERRADA:
USA UMA APROXIMAÇÃO DESAFIO-RESPOSTA

16. Autenticação no SSH, ERRADA:
ESTÁ bem adaptado para a autenticação de servidores dos quais nada se conhece

17. Qual dos seguintes atributos de um ficheiro / directorio pode ser cifrado sem que isso crie problemas?
Nome do directorio

18. Os dados numa BASE DE DADOS podem ser sensíveis porque, ERRADA
Revelam a estrutura da BD

19. NUMA BD a integridade dos seus dados significa:
Assegurar a correcção e coerência dos dados,

20. UMA ACL (ACCESS CONTROL LIST), ERRADA:
É uma informação de controlo de ...

21. Autenticação no SSH, ERRADA:
Pode CRIAR problemas de Decisão aos clientes qd se mudam as credenciais dos servidores

22. DAC (Discretionary ACCESS CONTROL) é um modelo de segurança:
onde os Donos dos recursos TÊM A CAPACIDADE de controlar quem tem acesso a estes recursos

23. Autenticação do WPA no ACESSO de um terminal à rede:
Segue os princípios do padrão 802.1X

Ataques com Dicionário -> são uma classe de ataques exaustivos onde o atacante procura ser eficaz (ou seja, ter sucesso) através da exploração de um conjunto de elementos de prova + reduzido do que o teoricamente possível, daí esse conjunto se dê o nome de dicionário.

Por outras palavras, se a probabilidade de ocorrência de cada um dos elementos de prova não for independente e igualmente distribuída, o ataque procurá encontrar e testar os elementos de prova + prováveis para, dessa forma, maximizar a probabilidade de sucesso na descoberta do elemento de prova efetivo.

A designação de ataque d/ Dicionário capta a analogia q existe entre o facto das pessoas usarem conjuntos de letras c/ uma determinada estrutura como forma de memorização. Este ataque afeta protocolos de autenticação baseados em senhas memorizadas escolhidas pelos seus donos (há senhas + prováveis q outras)

Como evitar?

A forma + simples e abrangente, na qual se deve investir maior esforço, consiste em evitar q as pessoas escolham senhas vulneráveis a tais ataques / senhas fracas. Ex: usar frases em vez de palavras simples, misturar caracteres minúsculos c/ maiúsculos, usar algarismos, caracteres de pontuação, símbolos do teclado.

UID GID others
-wx rwx --x
dono só consegue escrever e executar

Questions:

1. Relativamente à autenticação no GSI, resposta errada:
   Não é imune a ataques c/ dicionário.
2. Relativamente à autenticação de clientes c/ S/Key, resposta errada:
   O autenticador tem acesso à senha original dos clientes
3. Relativamente à autenticação c/ desafio-resposta, resposta errada:
   Não permite uma fácil implantação de protocolos de autenticação mútua
4. Autenticação RSA Secure ID, resposta errada:
   É imune a ataques c/ dicionários
5. Autenticação no SSH:
   Vulnerável a ataques de interposição (man in the middle)
6. A arquitetura PAM (Pluggable Auth module), resposta errada:
   Permite que as aplicações programaticamente orquestrem a forma como querem conduzir os processos de Auth
7. A não observância do princípio de privilégio mínimo, resposta errada:
   É perfeitamente aceitável caso haja um sistema Robusto de auditoria.