INE5680 – Segurança da Informação e de Redes – Prova B - Prof. Bosco (4,00)

Aluno: _____

1. (Ambiente Cooperativo) (0,50) – Quatro fatores que influenciam no crescimento da segurança de redenecessária em um ambiente cooperativo (ter necessidade de se colocar mais segurança):

   (Verdade/Falso) Diminuição (Aumento) das perdas devido a falhas de segurança.
   (Verdade/Falso) Crescimento de números de conexões de Internet.
   (Verdade/Falso) Crescimento do número de aplicativos permitidos para a rede.
   (Verdade/Falso) Tráfego de rede expandido.

2. (Scanner de Vulnerabilidades) (0,75) – Após o mapeamento das portas e serviços que são executados, as vulnerabilidades específicas para cada serviço serão procuradas por meio de um *scanning* de vulnerabilidades. Estes procuram falhas de segurança em protocolos, serviços, aplicativos ou sistemas operacionais. Assinale, sublinhando o mais indicado:

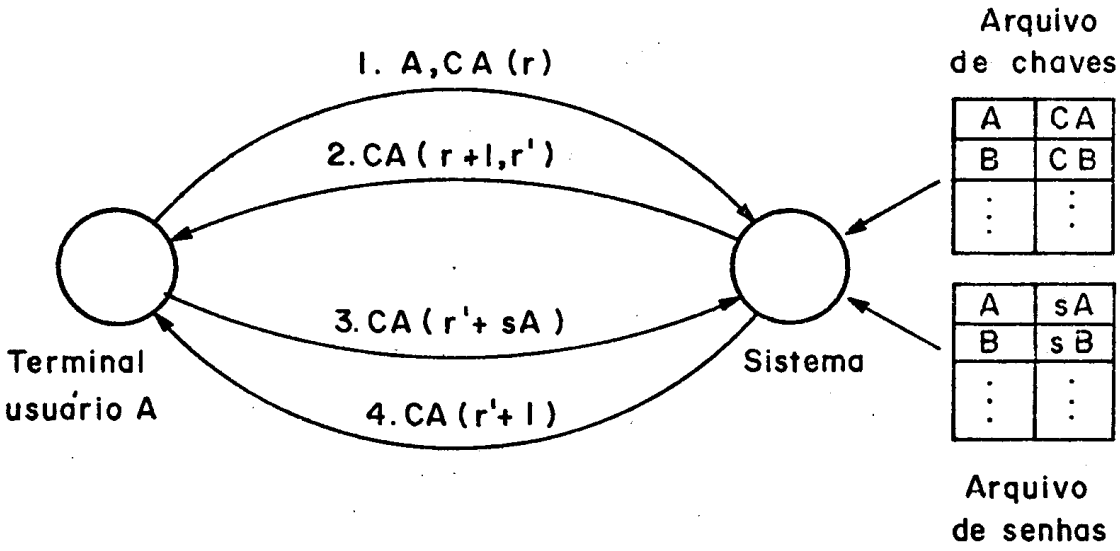
   (a) (Fragilidade da tecnologia/Fragilidade de configuração/Fragilidade da Política de Segurança) (0,50) - Se um servidor Web é escaneado para vulnerabilidades e o resultado apresenta uma vulnerabilidade relacionada à programação de uma linguagem para Web (por exemplo, PHP) no lado do servidor, que propicia a alteração de um BD. A fragilidade se dá pelo uso incorreto da linguagem. É preciso configurar algum parâmetro da linguagem usada, que não foi feito corretamente. Na fragilidade da tecnologia, o problema seria a linguagem em si e não se teria nem como configurar corretamente.

   (b) (Verdade/Falso) (0,25) - Supondo o caso anterior, uma configuração/programação incorreta pode ter sido realizada, no uso da linguagem.

3. (Scanner de Portas) (0,75) - Os scanners de portas são ferramentas utilizadas para obtenção de informações referentes aos serviços que são acessíveis e definidos por meio do mapeamento das portas TCP e UDP. Além de cumprir o papel a que se destina, um scanner de portas pode, em alguma circunstância, trazer consequências para seus alvos.
   (a) (Ameaça/Ataque) (0,25) - Se no ato do *scanning*, um serviço do SO é desabilitado.
   (b) (Ameaça/Ataque) (0,25) - Se um software de servidor travar quando um *scanning* é realizado.
   (c) (Verdade/Falso) (0,25) - TCP Connect é a técnica de "escanear" portas mais básica que tem e você executou no *nmap* em aula de laboratório. Ela é usada para abrir uma conexão nas portas do alvo. Uma atacante (A) tenta fazer uma conexão com um alvo (T). Se T aceita a tentativa de conexão de A, então a porta está fechada (aberta) , o serviço não (existe) em T, e pode ser utilizada para o ataque. Se T não aceita a tentativa de conexão vinda de A, então a porta está aberta (fechada). Uma vantagem deste método é que não é necessário nenhum privilégio especial para

sua utilização. Em contrapartida, ele é facilmente detectado, se existir algum firewall, pois basta ver as conexões em cada porta.

4. Altere o protocolo da figura abaixo, que descreve o protocolo com criptografia simétrica, para mostrar como se pode descrever o protocolo de autenticação com criptografia de chave pública. Suponha que o terminal é uma entidade *T*, que suporta um usuário A, e o sistema central é uma entidade S. Considere que o terminal *T* gera, para uma sessão do usuário A, um par (PU_A, PR_A) e o par (PU_S, PR_S) de chaves pública e privada é gerado pelo sistema central. (2,0)



Uma abstração da solução :

0. Suponha que A e S tenha seus pares de chaves pública-privada: (PU_A, PR_A) e (PU_S, PR_S).

1. O usuário A envia sua chave pública PU_A para o sistema S.
2. O sistema S envia sua chave pública PU_S para o usuário A.
3. O usuário A envia a mensagem 1, A,PU_S(r), cifrando r.
4. O sistema S recebe A,PU_S(r) e decifra r com PR_S. S gera r+1 e r´.
5. O sistema S envia a mensagem 2, PU_A(r+1,r´). A recebe a mensagem 2 e decifra r+1 e r´ com a sua chave privada PR_A, verificando que r+1 é maior do que o valor r por ele gerado.
6. O usuário A envia a mensagem 3, PU_S(r´+SA), para o sistema S.
7. O sistema S decifra com a sua PR_S, o valor r´ e a senha SA, e de posse de r´ S determina a senha SA e o sistema S, verifica que SA é a senha de A.
8. O sistema S envia um mensagem de sucesso, cifrada com a chave pública do usuário PU_A(r´+1).
9. O terminal decifra a mensagem PU_A(r´+1) com sua chave privada PR_A, e verifica que r´+1 é maior que r´ e aceita o usuário como se fosse A.

Obs: Na aula-prática sobre GnuPG (chaves, criptografia, assinatura), será visto uma melhor prática de como as chaves públicas PU_A e PU_S podem ser disponibilizadas.