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

Aluno: _____

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

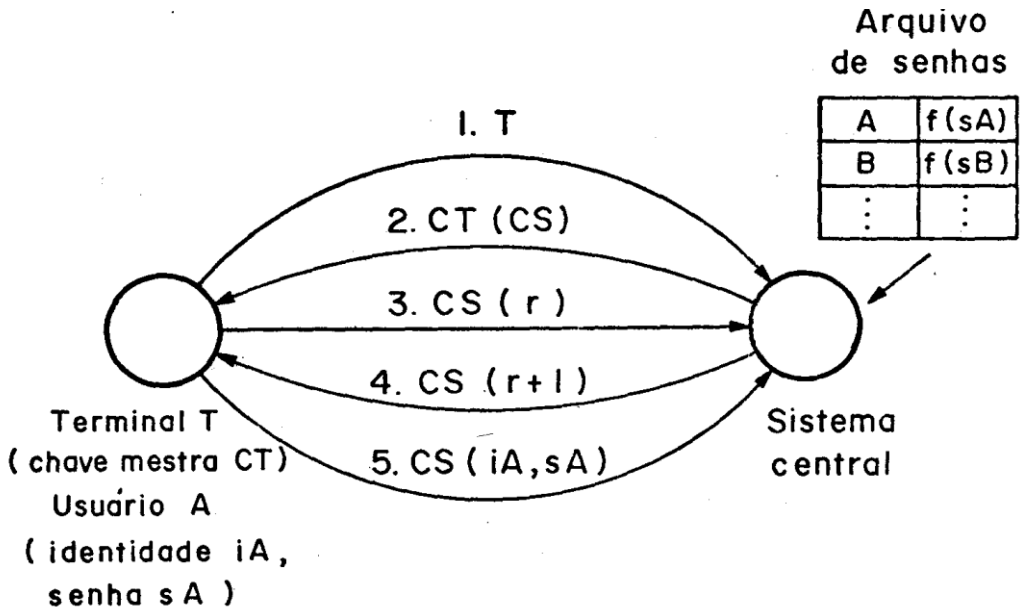
   (Verdade/Falso) Tráfego de rede expandido.
   (Verdade/Falso) Crescimento de números de conexões de Internet.
   (Verdade/Falso) Crescimento do número de aplicativos permitidos para a rede.
   (Verdade/Falso) Diminuição (Aumento) das perdas devido a falhas de segurança.

2. (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.

3. (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 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.

4. Altere o protocolo da figura abaixo, que descreve o protocolo com criptografia simétrica, para mostrar como se pode especificar o protocolo de autenticação com criptografia de chave pública, para criptografar a chave de sessão *CS*, ao invés da chave mestra CT de T. e usar a criptografia de chave simétrica para o restante. Suponha que o terminal é uma entidade *T* e o sistema central uma entidade S. Considere que o terminal *T* gera, para cada sessão de usuário, um par (PU_T, PR_T) e o par (PU_S, PR_S) de chaves pública e privada é gerado pelo sistema central. (2,0)



Observações:

a) A **criptografia de chave pública** substituirá a *CT* (chave mestra de *T*).

b) A **criptografia simétrica**, com uma chave de sessão *CS* é usada no procedimento de autenticação.

c) Uma chave de sessão CS de criptografia simétrica, quando cifrada por uma chave pública (PUT) e decifrada por uma chave privada (PRT), tem-se os uso da criptografia simétrica para cifrar a comunicação, e usa a chave pública (PUT) para cifrar e repassar a chave de sessão (CS). Esta chave de sessão (CS) é temporária, só serve para aquela sessão de um usuário, e deve ser descartada ao término de cada sessão. Sessão, aqui, é com dois `s´, pois tem a conotação de tempo.

Uma abstração da solução é:

0. Considere que o sistema central conheça as chaves públicas dos vários terminais *T* (PU_T). E que esses conheçam a chaves pública do sistema central.

1. O protocolo se inicia quando o terminal envia sua identificação *T* para o sistema central. Alguém está querendo usar o terminal.

2. Pelo protocolo da figura, o sistema central deve enviar uma chave de sessão *CS* para o terminal *T* poder criptografar os dados do usuário (usando criptografia simétrica com a chave de sessão *CS*), através da chave mestra *CT*, a qual não é necessário mais e será substituída pela chave pública de T (PU_T).

3. Mas, para se usar criptografia de chave pública, o sistema central, agora, se utilizará da chave pública do terminal T (PU_T), enviando uma chave de sessão *CS* criptografada por (PU_T), para *T.* Com sua chave privada (PR_T), o terminal *T* decifra a chave de sessão *CS*.

4. O passo 3 da figura continua. Com *CS*, o terminal *T* pode cifrar os números *r,* supostamente aleatório gerado por *T,* e enviá-los ao sistema central.

5. De posso do número *r*, o sistema central modifica esse número *r,* adicionando 1, cifrando-o com *CS* e enviando para *T*. Lembrem que os números *r* e *r+1* são usados apenas uma vez, para evitar ataques de repetição no procedimento de autenticação de um usuário do terminal *T*. Daí o termo *nonce*, em inglês, para denominar esses números.

6. O terminal envia sua identificação *iA* e a senha *sA* para o sistema central poder autenticar usando o arquivo de senhas, contendo os valores *hash* das senhas dos usuários do sistema.