INE 5680 – Segurança de Rede e da Informação – Prova 2 – 2014.2 - 21/11/2014 – Prof. Bosco

Nome : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. POLÍTICA DE SEGURANÇA – (1.0)
2. (Verdade/Falso) - Uma política de uso aceitável define o que uma corporação (irá ou) não irá tolerar em termos de acesso interno e externo à corporação., uso de software e hardware e quaisquer outras restrições exigidas por leis ou regulamentos. Explique sua resposta. (0.25)

Falso. Uma política de uso aceitável irá ou não tolerar em termos de acesso interno e externo à corporação., uso de software e hardware e quaisquer outras restrições exigidas por leis ou regulamentos. Porque o documento de política de segurança fala em usos aceitáveis da rede e usos inaceitáveis da rede (página 654 do material fornecido para a Empresa XYZ).

1. Escreva uma frase sobre a política de segurança, para usuários que precisam acessar os recursos de computação de forma remota de sua corporação XYZ. Ou seja, de que forma se pode garantir a segurança, entre a máquina remota do usuário e o servidor que atende os acessos remotos na corporação. (0.25)

Os usuários da corporação XYZ, deverão estabelecer uma VPN entre sua máquina e o sistema remoto da corporação, apropriado para ser um gateway VPN.

1. (Verdade/Falso) - Uma política de acesso à Internet contempla: o acesso de saída à Internet, uma política de Firewall e uma política de serviços públicos, uma DMZ, a qual restringe o acesso de entrada da Internet à rede da corporação, através de um host de segurança para tráfego de email, HTTP, FTP e outros tráfegos de Internet necessários. Comente. (0.25)

A política de acesso à Internet define as diretrizes relacionadas à Internet, tanto para sair (acesso interno) da corporação para fora, quanto para entrar (acesso externo) da Internet para a corporação.

1. Uma DMZ (Desmilitarized Zone) é uma rede semi-protegida de proteção de uma rede corporativa, , que tem um IP próprio, diferente do IP da rede corporativa, e que serve para expor os serviços mais públicos de uma corporação. Que recursos de computação, geralmente, aparecem colocados numa DMZ ? (0.25)

São servidores com conteúdo público de informações a clientes, tais como Email, Servidor Web com HTTP, Serviço FTP, Servidor de Banco de Dados, Sistema de Detecção de Intrusão, ...

( X ) Serviço de FTP ( X ) Servidor Web ( X ) Serviço de DNS ( ) Ambiente de Nuvem
( X ) Serviço de Email ( X ) Proxy de Web ( X ) Banco de Dados

Como um host de segurança é uma máquina somente, e um ambiente de nuvem requer um conjunto de máquinas específicas, não é considerado um ambiente de nuvem dentro de uma DMZ,que, inclusive, esse ambiente de nuvem pode ser privado, contradizendo a ideia de serviços públicos de uma DMZ.

1. **R**ECONHECIMENTO E COLETA DE INFORMAÇÕES - Indique Verdade/Falso (1,0)

(Verdade/Falso) - Uma analisador de vulnerabilidades (como o OpenVAS) que fornece essencialmente, um relatório mostrando as portas e serviços de uma máquina, além de descobrir o sistema operacional da máquina remota “escaneada”. Explique sua resposta.

Falso. O que é mostrado é um relatório onde constam vulnerabilidades, classificadas de acordo com seu nível de severidade. (0.5)

(Verdade/Falso) - Uma ferramenta de reconhecimento e coleta de informações, como Nmap, fornece um relatório dos problemas de segurança de um sistema, mostrando as vulnerabilidades, classificando-as em seus níveis de severidade. Explique sua resposta.

Falso. Uma ferramenta de reconhecimento e coleta de informações, fornece uma lista de portas e serviços associados a essas portas, com status de ativos, inativos, filtrados, ou não conhecido. (0.5)

1. AUDITORIA DE SEGURANÇA - (1.0)
2. Uma auditoria de segurança de rede e sistemas é formada por algumas fases, e envolve ferramentas específicas para uso nessas fases. Ordene as fases de uma auditoria de segurança, e mencione os nomes das ferramentas de seu conhecimento adquirido nas tarefas práticas. (0.5)

( 3 ) Análise de vulnerabilidades sobre serviços encontrados, enumeração e
 escolhendo seus alvos. OpenVAS

( 2 ) Reconhecimento e coleta de informações usando técnicas avançadas. Nmap

( 1 ) Planejamento do escopo de testes de penetração.

( 4 ) Exploração remota de vulnerabilidades. Metasploit

( 6 ) Relatório final sobre a rede e sistemas auditada.

( 5 ) Pós-exploração (após ter conseguido invadir) Metasploit, SET (Engenharia
 Social), outras.

1. (Verdade/Falso) - *Metasploit Framework* é uma ferramenta desenvolvida para se realizar testes de penetração (ou tentar ataques) contra máquinas-alvo, proporcionando um código de *payload* e um código de *exploit*, no sentido de tentar penetrar na máquina testada, através de uma vulnerabilidade conhecida em algum serviço. Para que serve o código de *payload* no contexto de um teste de penetração ? Explique sua resposta. (0.5)

Verdade. Você usou Metasploit, a ferramenta para fazer um teste de penetração, a partir de uma VM Backtrack contra um VM Windows Server 2008. Um código de *payload* foi usado pelo Metasploit para forçar uma conexão com a máquina-alvo sendo testada.

4) Protocolo KERBEROS (2.0, sendo 0.25 cada ítem correto)

Sejam A = usuário de um serviço, B = servidor rodando um serviço, KDC um centro de distribuição de chaves de sessão, KA é a chave mestra entre A e KDC, KB é a chave mestra entre B e KDC, t um rótulo de tempo, L um tempo de vida da mensagem, KSé uma chave de sessão que deve existir entre A e B, onde B pode ser um servidor que mantém um serviço de interesse de A, que precisa ser acessado.

Codifique o protocolo, usando a notação formal que reproduza as etapas seguintes do protocolo:

1. A envia uma mensagem ao KDC com sua identidade IDA e a identidade de B, IDB.

 A → KDC : [ IDA, IDB ]

(2) KDC toma o rótulo de tempo t, o tempo de vida L, a chave de sessão e a identidade de B, e encripta esta com a chave que ele compartilha com A.

 KDC : EKA ( t || L || KS || IDB )

1. KDC gera uma mensagem com os seguintes itens concatenados: um rótulo de tempo t, um tempo de vida L, uma chave de sessão KS, e a identidade de A (IDA), e encripta esta mensagem com a chave-mestra que o KDC compartilha com B:

KDC : ( t || L || KS || IDA )

KDC : EKB ( t || L || KS || IDA )

(4) KDC gera a mensagem de concatenação das duas mensagens anteriores:

 ( EKB ( t || L || KS || IDA ) || EKA ( t || L || KS || IDB ) )

(5) KDC envia ambas as mensagens encriptadas e concatenadas para A:

 KDC → A : ( EKB ( t || L || KS || IDA ) || EKA ( t || L || KS || IDB ) )

(6) A gera uma mensagem com sua identidade IDA e o rótulo de tempo t, encripta esta com
 a chave KS e a envia para Bob. A também envia para B, a mensagem de KDC, encriptada
 com a chave mestra KB de Bob compartilhada com KDC: (0.25)

 A → B : ( EKS ( IDA, t ) || EKB ( t || L || KS || IDA ) )

(7) B cria uma mensagem consistindo do rótulo de tempo t adicionado a 1, encripta com a
 chave KS e envia para A: (0.25)

 B : ( t+1 )

 B → A : EKS ( t+1 )

(8) O que pode ocorrer no funcionamento do KERBEROS, caso os clocks de A e B não estejam sincronizados com o KDC ? (0.25)

Se os clocks de A e B não estiverem sincronizados com o KDC, existe a possibilidade de ataques surgirem contra o protocolo. Um atacante pode interceptar uma mensagem a partir de A para B, e repetí-la mais tarde, quando o rótulo de tempo t tornar-se corrente (atual) no clock do receptor B.

As condições necessárias entre A, B e KDC, para o protocolo KERBEROS funcionar:

Este protocolo funciona, mas assume que os clocks de A e B sejam sincronizados com o clock do KDC. Na prática, o efeito é obtido por sincronizar os clocks num intervalo de poucos minutos, usando um servidor (seguro) de tempo, e detectando repetições dentro do intervalo de tempo.

(9) (Verdade/Falso) - O protocolo KERBEROS provê um serviço de autenticação de usuários de serviços acessados em um servidor, utilizando-se de um centro de distribuição de chaves (KDC). Explique sua resposta, detalhando mais a arquitetura básica do KDC. (0.5)

Basicamente, *Kerberos KDC* é constituído de duas partes: uma que, inicialmente, autentica o identificador do usuário que está na máquina-cliente num servidor de autenticação (AS), o qual fornece um ticket de concessão de ticket e mais uma chave de sessão, e outra parte, um *servidor de concessão de ticket (TGS)* que fornece um ticket para um servidor S remoto ser acessado, e mais uma chave de sessão. Após estas etapas, o usuário da máquina-cliente solicita o serviço ao servidor remoto S.

5) Protocolo de Votação Eletrônica com Assinaturas Cegas
 (2.5, sendo 0,5 para cada ítem correto)

É necessário, de alguma forma, dissociar, o voto, do eleitor, enquanto, ainda, se mantém a autenticação deste.

Considere o que é uma assinatura cega (*blind signatures*) e o protocolo seguinte sobre assinaturas cegas:

Veja no que segue, o módulo de ocultar mensagens para se obter Assinaturas Cegas, onde A = eleitor, B = CTF, KRB é a chave privada de B=CTF, KUB é a chave pública de B = CTF.

 1. A : k \* M // ( k = fator de ocultação, M é uma mensagem = um voto)

1. A → B : ( k \* M ) // B tem M com o fator de ocultação.
2. B → A : SKRB ( k \* M ) || KUB // B assina digitalmente a mensagem ocultada. O *hash* da
 // assinatura, aqui, é abstraído.

 A : KUB e VKUB ( k \* M ) // A tem que receber a KUB e verifica a assinatura de B,
 // obtendo tem seu voto ocultado.

 A : SKRB ( k \* M ) // A, gerador da mensagem, tem a sua mensagem **assinada às
 cegas** por B, porque A, agora, tem a mensagem com o fator k
 de ocultação, assinado com a chave privada de B.

1. Se A : ( k \* M ), então A : ( k \* M ) / k ou seja A : M // A pode ter a mensagem original, ou seja, seu voto de volta.

O Protocolo:

 (1) Cada eleitor gera uma mensagem, correspondente ao seu voto. Cada mensagem contém também um número de identificação gerado aleatoriamente, grande o suficiente para evitar duplicações com outros eleitores.

(2) Cada eleitor “cega” a mensagem de seu voto (com o módulo descrito acima) e envia, com seu fator de ocultação a um CTF (Central de Apuração de Votos).

 (3) O CTF, que recebe votos ocultados, com o fato *k* de ocultação, verifica a sua base de dados para garantir que o eleitor não apresentou, ainda, seus voto “ocultado”. Em seguida, CTF assina digitalmente, a mensagem do voto ocultado. CTF envia o voto ocultado de volta para o eleitor, armazenando o nome do eleitor em sua base de dados.

(4) O eleitor desfaz as assinaturas cegas das mensagens, e fica com seu voto assinado pelo CTF. O voto é assinado digitalmente, mas não criptografado, para que o eleitor possa ver facilmente que o voto é realmente o que ele deu.

(5) O eleitor pega seu voto e criptografa com a chave pública do CTF.

(6) O eleitor envia seu voto ao CTF.

(7) A CTF decifra o voto com sua chave privada, verifica a sua assinatura sobre o voto ocultado e verifica o seu banco de dados para alguma duplicata da numeração de identificação, guarda esse número de série e tabula os votos. CTF publica os resultados da eleição, juntamente com o número de identificação (que só o eleitor pode ter) e seu voto associado.

Questões:

1. O protocolo garante que seu voto é único ? Explique sua resposta.

Sim, se um eleitor tentar enviar o mesmo voto duas vezes, o CTF notará a duplicidade do número serial de identificação na etapa (7) e rejeitará o segundo voto.

1. Se um eleitor tenta múltiplos votos na etapa (2), o que ocorre na etapa (3) ?

Se ele tenta obter múltiplas votos assinados na etapa (2), o CTF descobrirá na etapa (3).

1. Pode um eleitor malicioso gerar seu próprio voto ?

 Um eleitor malicioso não pode gerar seus próprios votos, porque ele não sabe a chave
 privada do CTF. Ele não pode interceptar e mudar votos de outras pessoas, pela mesma
 razão.

1. Pode um CTF malicioso calcular como eleitores individuais votaram ?

Não. Porque o protocolo de assinatura cega previne o CTF de ver os números seriais de identificação sobre os votos, antes deles serem lançados. O CTF não pode ligar o voto cego que ele assinou com o voto eventualmente lançado. Publicando uma lista de números seriais e seus votos associados, permite eleitores confirmarem que seus votos foram tabulados corretamente.

1. Que problema pode surgir na etapa (6) ?

Na etapa (6) - o eleitor envia seu voto criptografado com a chave pública do CTF – o voto é protegido na comunicação, mas ao chegar no CTF, como existe anonimato (a assinatura sobre o voto ocultado), o CTF não pode descobrir quem votou em quem. Contudo, se CTF recebe o voto numa urna lacrada e então computa os votos mais tarde, ele, também, não pode descobrir quem votou em quem. Também, enquanto, o CTF não pode ser capaz para ligar votos a indivíduos eleitores, ele pode gerar um grande número de votos válidos assinados e fraudar, submetendo aqueles próprios (seria o caso do nosso TSE mudar os votos). Se um eleitor descobre que seu voto foi mudado, ele não tem nenhum meio de provar este fato.

6 ) Protocolo de Votação Eletrônica com duas centrais de votação
 (2.0, sendo 0,25 cada ítem correto)

O seguinte protocolo usa as facilidades de duas centrais: CLA (Central Legitimization Agency) e uma separada CTF (Central Tabulating Facility).

Parte I: **Legitimização do eleitor**

1. Cada eleitor ao chegar na sua seção eleitoral, apresenta seu título de eleitor e requisita um **número de validação**.
2. O CLA fornece de volta ao eleitor, um número de validação aleatório. O CLA mantém uma lista de **números de validação**.
3. O CLA envia uma lista atualizada de **números de validação** ao CTF.

Parte II: **O eleitor votando**

1. Cada eleitor escolhe um número de identificação aleatório. Ele cria uma mensagem com esse número de identificação, o número de validação que ele recebeu do CLA e seus votos (1 para cada cadeira: presidente, senador, deputado federal, deputado estadual, prefeito e vereador. Ele envia esta mensagem ao CTF.
2. O CTF verifica o número de validação recebido com o voto, contra a lista de que ele recebeu de CLA na etapa (3). Se o número de validação existe, o CTF marca ele, para proibir alguém de votar duas vezes. O CTF adiciona o número de identificação à lista de eleitores que votaram para um candidato particular e adiciona 1 ao registro de votos.
3. Após todos os votos terem sido recebidos. O CTF publica o resultado, bem como, as listas de números de identificação e para os quais candidatos os eleitores votaram.

Questões:

1. O CLA é uma autoridade confiável ? Ele pode certificar eleitores que não podem votar múltiplas vezes ? Se é verdade, como esse risco pode ser minimizado ?

O que diz o livro *Applied Cryptography, Bruce Schneier*:

Um atacante, quem não seja um eleitor admissível pode tentar fraudar, por advinhar um número de validação. Esta ameaça pode ser minimizada por fazer o número de possíveis números de validação muito maior do que os números de validação reais. Ou seja, o universo de geração desses números é bem maior do que os reais números gerados: números de 100 dígitos para 1 milhão de eleitores, por exemplo. É claro que números de validação devem ser gerados aleatoriamente.

Apesar disso, o CLA é uma autoridade confiável em alguns aspectos. Ela pode certificar eleitores que não podem votar. O CLA pode certificar eleitores admissíveis múltiplas vezes. Este risco será minimizado se CLA publicar uma lista de eleitores certificados, mas não seus números de validação. Se o número de eleitores sobre esta lista é menor do que o número de votos tabulados, então alguma coisa está errada. Se mais eleitores foram certificados do que os votos tabulados, provavelmente significa que alguns eleitores certificados não se preocuparam com a votação. Muitas pessoas que são registradas para votar, não se preocupam em votar.

1. O que acontecerá se o CTF encher a urna de votos suspeitos ?

O CTF não pode encher uma urna com votos suspeitos, porque ele está sendo fiscalizado pelo CLA. O CLA sabe quantos eleitores tem sido certificados e seus números de validação, e detectará quaisquer modificações.

1. Para que servem os números de validação e os números de identificação ?

O número de validação serve para certificar que um eleitor é autorizado a votar.

Enquanto o número de identificação identifica o eleitor para ele saber, depois, que seu voto foi computado corretamente.

1. CLA e CTF são entidades independentes, mas pertencentes a um único sistema de votação. Ambas entidades tem suas bases de dados. O que pode ocorrer se CLA e CTF se juntam e correlacionarem suas bases de dados ?

Este protocolo é vulnerável ao “conluio” entre CLA e CTF. Se as duas entidades, CLA e CTF, se juntarem, elas podem correlacionar suas bases de dados e descobrir quem votou para quem, comprometendo, assim, o sigilo do voto.

1. Como pode o eleitor ter certeza de que seu voto foi contado ?

Cada eleitor, ao final da votação, pode conferir as listas de números de identificação e encontrar o seu próprio. Isto dá a prova de que seu voto foi computado. Isto não ocorre no boletins de urna publicados pelo nosso TSE.