Ine5680 - Segurança de Informação e de Rede - Prova de Recuperação – 2012.1 – 30%

Aluno: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Considere o seguinte cenário: suponha que você trabalha como um Home Office para uma corporação. Por questão de segurança, você estabelece uma VPN entre sua máquina e o gateway VPN de sua organização. Uma possibilidade perigosa que abre possibilidade de um ataque é a de existir na Internet um intruso e utilizar sua máquina em casa (um cliente VPN) como uma ponte entre a Internet (porque você está ligado via um modem) e a rede interna da organização. O seu equipamento passa a ter duas conexões, uma com a Internet (sujeita a ataques externos) e outra, via tunelamento VPN com a rede de sua organização, que você precisa para trabalhar de forma segura. Dessa maneira, um intruso (cracker) pode utilizar uma conexão via Internet e passar para a outra (o túnel VPN), e alcançar, assim, a rede de sua organização.

Entretanto, as considerações de segurança envolvidas no cenário acima, podem ser preocupantes, pois o cliente está disponível (mas não deve estar aberto) a todo universo na Internet.

Um dos métodos para fazer com que sua máquina (cliente VPN) atue como uma ponte entre a Internet e a rede de sua empresa, é por meio de roteamento de pacotes TCP/IP. Se a máquina-cliente VPN tiver capacidade de roteamento de pacotes, o intruso pode enviar pacotes à sua máquina, que por sua vez, rotearia esses pacotes para a rede de sua organização. Isto porque, o cliente VPN age sobre a pilha TCP/IP de sua máquina, de modo que todo pacote endereçado à rede de sua organização é transformado em um pacote VPN, que são pacotes válidos e autenticados pelo gateway VPN de sua empresa.

Indique verdade ou falso para as afirmações sobre medidas de segurança simples que podem se tomadas no seu cliente VPN.

1. (Verdade/Falso) A capacidade de roteamento depende de configurações do sistema operacional (Windows, Linux, Unix, ...) em uso em sua máquina cliente VPN. Uma possibilidade de forçar o roteamento em sua máquina cliente VPN é a utilização de uma funcionalidade do TCP/IP, e você deve desabilitar essa funcionalidade em seu sistema operacional, que torna sua máquina atuando como um *host* roteador. Assim, o cliente VPN não deve permitir rotear pacotes para a rede interna da organização. Ou seja, rotas-padrão para a rede interna devem ser evitadas a todo custo. (0,25)
2. (Verdade/Falso) Outra possibilidade de invadir a rede de sua organização, através de sua máquina é por meio do controle desta por algum atacante, por exemplo, usando alguma ameaça como um Cavalo-de-Tróia. Para evitar ataques a sua máquina, e consequentemente, que sua VPN seja usada por um atacante, é conveniente que um scanner vulnerabilidades revele as portas abertas com serviços em seu sistema operacional que funcionam como portas de entrada, e que um scanner de portas revele e enumere vulnerabilidades nos serviços encontrados em portas TCP. (0,25)
3. Escreva políticas de segurança, que sua empresa deve seguir, para as questões (a) e (b), sendo cada valendo 0,5.

Política (a): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Política (b):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 2. Suponha que você é um profissional da área de segurança, responsável por implantar os
 níveis apontados na política de segurança num ambiente cooperativo de uma empresa
 XYZ. Então, indique, visualizando a rede XYZ desprotegida na figura abaixo, como a
 política de segurança pode ser implementada para se ter (desenhe ou descreva):

 (a) Uma segurança de perímetro definindo uma DMZ mais externa. Ou seja, em que
 pode consistir a DMZ mais externa ? (1,0)

 

 (b) Uma política segura de acesso, supondo que clientes remotos tem acesso
 via linha telefônica até chegar no servidor NAS (Servidor de Acesso de Rede)
 colocados nos segmentos de vendas e engenharia. Ou seja,
 como a empresa XYZ pode aumentar a segurança de acesso remoto ? (0,5)