INE5680 – SEGURANÇA DA INFORMAÇÃO E DE REDES – PROVA 2 – 14/12/2012 (50%)

Prof. Bosco - Prova Avaliada com peso de 50%

Classifique os seguintes ataques: (0,25 cada)

a) *IP Spoofing* é uma técnica na qual o endereço real do atacante fica oculto, de forma a evitar que ele seja encontrado. Um ataque na camada de rede , pelo qual um grande tráfego de pacotes *ping* é enviado para o endereço IP de broadcast da rede (então, todos da rede enviam as respostas da requisição para o alvo), tendo como origem o endereço IP do alvo (isto é *IP Spoofing*), ou seja, IP Spoofing é realizado, como se o alvo requisitasse a resposta e o alvo deixa de fornecer serviço.

IP Spoofing: Ataque ativo contra o TCP/IP;
DoS: Negação de Serviço com pacotes do ICMP (comando ping).

b) Um ataque onde o usuário na *web* é iludido a pensar que está em uma página autêntica, que na verdade é falsificada e ele é induzido a fornecer suas informações pessoais ao falso servidor. Note a camada de protocolo onde o ataque é feito.

Ataque no Nível da aplicação, Web: Phishing

c) Considere o seguinte fluxo de ataque e classifique o ataque:

1. Um atacante manda um SPAM com uma notícia (email com um link malicioso) para diversos usuários e uma delas clica num link malicioso recebido, com uma URL que é como sendo uma fonte confiável (para iludir o usuário).
2. Ao clicar no link, o usuário será redirecionada para um site, e como resposta, receberá a página da "notícia" mais o código malicioso de um script embutido.
3. Se o script é reconhecido pelo navegador da vítima, o mesmo irá executar o script e algum ataque estará consolidado. Informações, para o host do atacante, poderão ser enviadas, ou *cookies* podem ser manipulados e o atacante roubar a sessão da vítima. Ataque no Nível da Aplicação, XSS não persistente (nada fica armazenado na aplicação (servidor).

d) *Sniffing* de pacotes, *scanning* de portas, *scanning* de vulnerabilidades em serviços e *Firewalking*, são ataques classificados como:
Ataques para a Obtenção de Informações: portas abertas com serviços e descobrir vulnerabilidades nos serviços, para posterior ataque.

2. 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 o atacante na 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 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. (0,50 cada)

a) Escreva a **política de segurança**, que sua empresa deve seguir para exigir que todo funcionário em Home Office bloqueie este ataque.

Todo funcionário, trabalhando em Home Office deverá estabelecer em sua máquina , uma VPN para acesso remoto à empresa. A configuração de roteador de sua máquina deve ser bloqueada.

b) Cite uma característica de uma VPN e explique como a sua empresa pode se beneficiar diretamente desta.
Tunelamento, criptografia, autenticação mútua por certificados entre clientes e servidor VPN. Confidencialidade é garantida por criptografia. Mas, uma VPN pode até ter somente o tunelamento e não existir criptografia. Neste último caso, garantindo o acesso remoto de um cliente à empresa, no que esse usa a VPN para usufruir do ambiente de sua organização como se estivesse localmente nela.

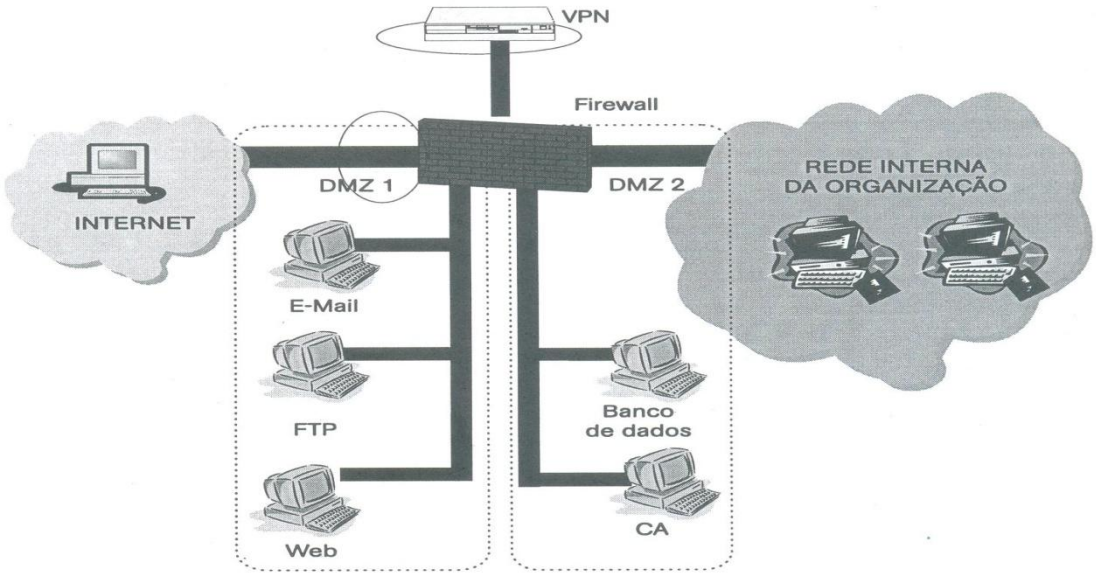
c) O que caracteriza uma VPN com criptografia simétrica ?

Uma chave é gerada para ser compartilhada entre cliente e servidor VPN, através de um acordo de chave, ou uma cópia da chave é gerada ou enviada pelo servidor para um cliente. Criptografia simétrica é usada, para garantir sigilo no tunelamento VPN.

d) O que caracteriza uma VPN com criptografia assimétrica ?

Geração de uma chave privada e do certificado de uma AC. Chaves públicas e privadas são geradas para cliente e servidor VPN. AC assina os certificados com chaves públicas para autenticar múltiplos clientes e servidor VPN. Criptografia de chave pública é usada para garantir sigilo no tunelamento VPN.

3. Seja a **arquitetura de um firewall cooperativo** como mostrado na figura seguinte:



Um **modelo de segurança** define cinco níveis hierárquicos de defesa são definidos para auxiliar na definição das proteções para os três tipos de recursos num ambiente cooperativo (públicos, privados e internos): recursos públicos, disponibilizados para acesso via Internet e localizados na DMZ-1; recursos privados, disponibilizados para acesso via Internet e localizados na DMZ-2 e recursos internos, localizados na rede interna e acessados externamente via VPN. Um **firewall cooperativo** é uma arquitetura de segurança que inclui tecnologias de segurança, e considerando cinco níveis, facilita a definição e a implementação das medidas de segurança necessárias para a estratégia de segurança de uma organização. Uma **DMZ** é uma rede intermediária entre a rede corporativa e a Internet, criada para disponibilizar recursos públicos ou privados aos usuários de uma corporação. **CA** é uma autoridade certificadora privada que a empresa utiliza. (0,25 cada)

a) Indique nos parênteses **a ordem dos cinco níveis de defesa**, considerando o modelo hierárquico de níveis em uma arquitetura de um firewall em uma ambiente cooperativo.

- Autenticação dos usuários para acesso aos serviços internos. (**4**)
- Autenticação do usuários para acesso aos serviços públicos na DMZ-1. (**2**)
- Filtragem de pacotes TCP/IP pelo firewall, antes de serem encaminhados aos níveis 2 ou 3. Descarta pacotes de serviços que não são permitidos. Protege contra ataques *IP Spoofing* e Negação de Serviços. (**1**)
- Sistemas IDS podem ser disponibilizados para proteger segmentos da rede interna da corporação. (**5**)
- O acesso à DMZ-2 e para o acesso à rede interna da organização são tratadas por regras do firewall mais complexas em que usuários terão acesso apenas às informações e aos serviços pertinentes a ele. (**3**)

b) Indique (Verdade/Falso) : Uma arquitetura de firewall cooperativo reúne e integra conceitos e tecnologias como firewall, DMZ, VPN, PKI, SSL, IDS, NAT. (0,75)