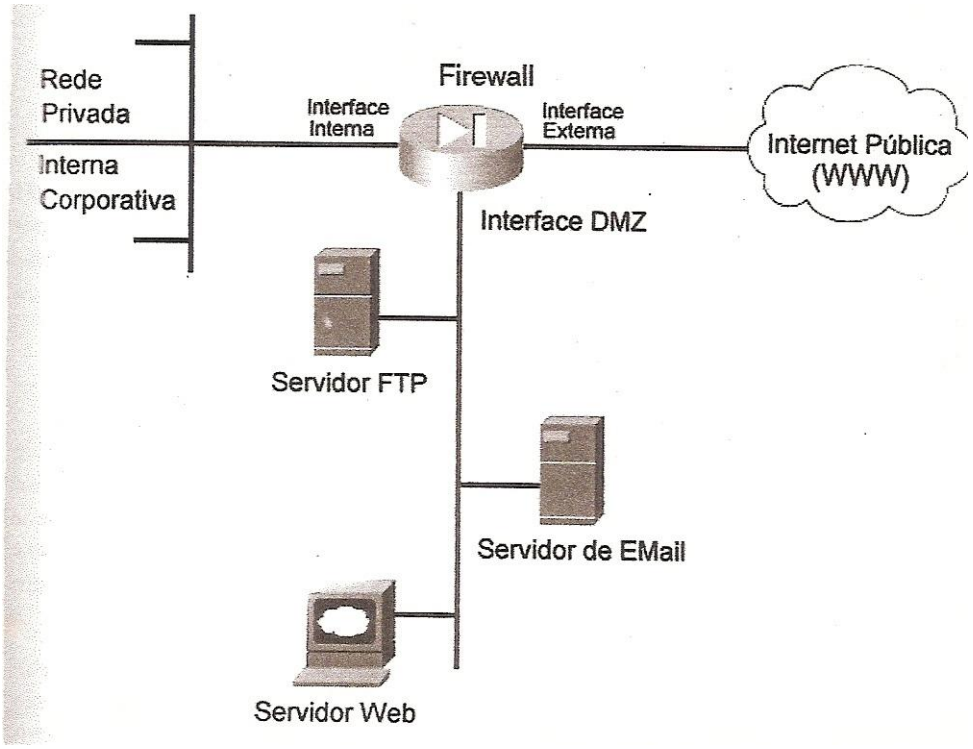
INE5680 – Segurança da Informação e de Redes - Prova 1B – 03/05/2013

Aluno: _____Gabarito Prova 1B_____

1. (**Firewall e NAT**) – Esta questão você deve entregar, hoje, **por impresso**, pois foi solicitada para ser feita em casa. (vale 1,0, se feita de forma aceitável)

2. Um segmento de rede **DMZ**, de uma rede corporativa, está configurado como na figura abaixo: (vale 1,0)

a) **(Verdade/Falso)** O tráfego de Internet será sempre permitido viajar pelos servidores da rede privada. Os IPs, destas redes, interna e privada e da DMZ são os mesmos. Explique, brevemente, sua resposta. (0,25)



Uma outra solução, para que o tráfego de Internet não seja permitido viajar pelos servidores da rede privada, é que os servidores FTP, Web e Email (os bem públicos) são anexados ao segmento DMZ. Eles não devem ter duas interfaces de rede, a não ser a interface para o segmento DMZ.

A existência da DMZ é exatamente no sentido de não permitir, por medida de segurança, que sempre, a rede privada, interna, seja acessada. Essas redes tem seus IPs distintos. Normalmente, uma DMZ tem um IP exclusivo que difere do IP da rede corporativa, privada, interna. Pode ocorrer que a DMZ seja a única que pode ser vista de fora. A rede corporativa tem um IP público e a rede DMZ pode ter um IP privado, definido na interface DMZ no firewall.

b) **(Verdade/Falso)** Uma equipe de TI deve garantir que o tráfego recebido da Internet, permanecerá confinado ao segmento contendo os servidores numa DMZ . Explique, brevemente, sua resposta. (0,25)

Regras de conectividade configuradas no Firewall permitirão que todo tráfego externo para serviços na DMZ, será mantido confinado apenas ao segmento DMZ.

c) **(Verdade/Falso)** Os servidores armazenando as informações públicas, como FTP, Web e Email, serão anexados ao segmento DMZ. (0,25)

É conveniente colocar o que for mais público numa DMZ.

d) **(Verdade/Falso)** Para ocultar a rede interna privada de uma empresa XYZ , do tráfego recebido da Internet, a interface DMZ, definida no Firewall, deverá ter um roteador que permita esse tráfego. Explique, brevemente, sua resposta. (0,25)

A interface DMZ não tem a necessidade de ter um roteador para ocultar a rede interna privada. No caso da figura acima, para ocultar a rede interna, deve ser suficiente configurar NAT com MAQUERADE no firewall, para a interface que vai para a rede interna, e liberar via firewall, o tráfego na interface de rede da DMZ.

O cenário real não está completo na figura. O que é bastante usado é um roteador protegendo a entrada da rede corporativa, situado entre a Internet e o Firewall, mas não dentro da DMZ, o qual seria um primeiro nível de segurança. Este roteador é chamado roteador de perímetro ou de borda. Neste caso, o roteador definiria a DMZ, para compor um sistema de proteção de perímetro composto pelo roteador, pelo firewall e pela DMZ.

Esse roteador normalmente tem um primeiro nível de segurança, ele define a DMZ, faz a filtragem de pacotes via ACL na camada de rede IP que protege ele próprio, funcionando como um sistema de alarme, caso alguém tente invadi-lo (um IDS para ele), protege os hosts de segurança na DMZ. Este roteador é chamado roteador de perímetro ou de borda. Neste caso, o roteador compõe um sistema de proteção de perímetro composto pelo roteador, pelo firewall e pela DMZ.

ACL = Access Control Lists IDS = Intrusion Detection System

Uma rede corporativa é basicamente de responsabilidade de alguém e, como resultado, se pode determinar o que é permitido em tal rede.

O roteador de perímetro pode definir uma DMZ semi-protegida.

Recursos básicos de segurança no roteador de perímetro permitem, também, a autenticação e autorização de outros roteadores de mesmo nível, protegem contra endereços de origem/destino desconhecidos ou indesejáveis, oculta endereços IP internos da exibição pública (NAT quando traduzem endereços IPs e PAT quando traduzem endereços de portas), rastreiam a atividade dentro e fora do roteador (registrando logs), controlam ataques DoS (Denial of Service) , e permitem que administradores implementem a segurança amparada por política no perímetro.

O roteador de perímetro, essencialmente, utiliza regras de filtragem de pacotes via ACL, para restringir o acesso a serviços TCP/IP e aplicativos. Numa ACL, já pode aparecer uma primeira implementação de política de segurança, a *Política de Menor Privilégio (Policy of Least Privilege)*, "bloquear tudo, e permitir apenas o que é necessário para conduzir os negócios".

A DMZ pode ser um ambiente parcialmente protegido por um host de segurança (um host protegido que fornece serviços a usuários externos e internos, tais como FTP, Web, DNS, SMTP que é serviço de recepção de email para entregar email à empresa). No caso da figura, esses serviços estão separados em servidores próprios. Mas, veja a figura A-2 do Apêndice A sobre o Cenário do Estudo de Caso da Empresa XYZ.

O firewall pode ser usado para criar uma DMZ protegida, colocando-se, também, hosts de segurança nessa DMZ criada na interface do firewall.

3. (Verdade/Falso) Para a **Identificação e Análise de vulnerabilidades**, usamos a ferramenta OpenVAS. Essa ferramenta propicia, dentre outras coisas, as vulnerabilidades em serviços encontrados rodando em portas fechadas (o correto é abertas), quantificando e classificando-as em níveis de severidade (graus de danos, alto, médio e baixo), gerando relatório enfatizando os riscos envolvidos e orientando alguma solução para eliminar as vulnerabilidades. (1,0)

Nas portas encontradas abertas, é que possuem serviços sendo executados, usando algum protocolo.

4. (Verdade/Falso)) Há numerosos benefícios práticos para o exame regular de suas redes. O mais evidente destes é a segurança. Um dos princípios centrais de segurança de redes é a redução do número e complexidade dos serviços oferecidos reduzirá a oportunidade dos atacantes irromperem. O que pode acontecer quando um exame do **Nmap** é executado: (1) **Enumeração de alvos**, quando pesquisa os especificadores de hospedeiros fornecidos pelo proprietário da rede. (2) **Descoberta de hospedeiro** (ping) (3) **Resolução de DNS inversa**, ou seja, ao partir de IPs, chega-se aos nome DNS, (4) **Exame de Portas**. (5) **Detecção de versões dos serviços encontrados em portas abertas.** (6) **Detecção de SO** em máquinas remotas, quando o SO é identificado. (7) **Traceroute**, quando pode encontrar rotas de rede para hospedeiros. (8) **Exame de Script**, quando pode descobrir backdoors e outros malwares. Dos itens mencionados, nós verificamos o item 4, sobre exame de portas abertas, fechadas e filtradas por firewall, a operação fundamental do Nmap. (Vale 1,0)

Nesta questão, está resumido tudo o que a ferramenta Nmap pode fazer. Na aula prática, só examinamos portas e alguns testaram a detecção de SO da máquina sendo examinada. Nos exemplos mostrados, algumas poucas vulnerabilidades puderam ser mostradas, enfatizadas num relatório provido pela ferramenta, mostrando a quantidade e seus níveis de severidade.

5. Indique a ordem das etapas. Suponha que você tenha que prestar um serviço de auditoria de redes sistemas e aplicações, numa empresa. Uma das metodologias existentes para tal é por Testes de Invasão. Neste caso, você deve seguir algumas etapas do processo de auditoria. Ordene, as etapas que você teria que realizar para prestar seu serviço. (Vale 1,0)

(**3**) Sondagem e mapeamento: por exemplo, usando a ferramenta Nmap. (0,20)

(**4**) Identificação e análise de vulnerabilidades: por exemplo, usando a ferramenta OpenVAS.

(0,20)

(**1**) Planejamento e preparação: o Escopo do Teste, Detalhes da Infraestrutura. (0,20)

(**5**) Testes de Invasão através da simulação de ataques, usando ferramentas apropriadas existentes, como na máquina virtual do Backtrack 5. (0,20)

(**2**) Obtenção de Informações sobre a rede, sistemas, serviços e aplicações a ser auditado: Engenharia social, Buscas na Internet, Cópia de WebSite. (0,20)

Consulte, no final do dia 05/05/2013, o gabarito na página disciplina, Prof. Bosco