Segurança de Rede - Prova A

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

1. Lembre da figura sobre anatomia de ataques por *crakers* (hackers não éticos). Que tipos de ferramentas (não são os nomes das ferramentas) mostradas no laboratório são utilizadas na fase de *footprint* ?

 a) -----------------------------------------------------------

 b) -----------------------------------------------------------

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. Ou seja, 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. Veja a figura seguinte:

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 o 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) O cliente VPN pode estabelecer uma VPN sem segurança, apenas para se conectar à sua empresa, via tunelamento, e utilizar serviços como se estivesse acessando localmente dentro do próprio ambiente da empresa.
2. (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.
3. (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.
4. Sobre a figura abaixo, quanto à relação entre um firewall e um IDS (Sistema de Detecção de Intrusão) pode-se afirmar que:



1. (Verdade/Falso) Um firewall de pacotes verifica os campos de endereçamento dos pacotes de rede, ou seja, para onde os pacotes se destinam, podendo bloquear ou não, o pacote.
2. (Verdade/Falso) Enquanto um IDS verifica todo o pacote na busca de ataques, incluindo o campo de dados (mensagem da camada superior) de um pacote.
3. (Verdade/Falso) O IDS libera/bloqueia conexões e o firewall pode detectar e notificar a forma de tráfego.
4. (Verdade/Falso) Um IDS pode responder com falsos negativos (não detectar ataques reais) ou falsos positivos (achar que comportamentos normais são ataques).