|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nome**:** |  | | | | Número: |  |
| **Nas questões de escolha múltipla assinale com V (verdadeiro) ou F (falso).** | | |  | **Docente: NC 🞎 PR 🞎** | | **Duração: 1 Hora** |
|  | | | | | | |
|  |  |

1. Em relação ao IEEE 802.11 indique:
   * V O anexo 802.11g é retro compatível com o 802.11b
   * F No anexo 802.11n o *interframe space* mais curto é o SIFS
   * V No anexo 802.11b os canais 13 e 8 ocupam bandas rádio que não se sobrepõem
   * V Os débitos físicos suportados pela norma original são de 1 e 2Mbit/s
2. Em relação aos problemas que afectam a IEEE 802.11 indique:
   * V Quando todas as estações que participam numa BSS se escutam entre si, não faz sentido o uso de protecção RTS/CTS
   * V O problema do terminal exposto ocorre quando a emissão de uma estação distante (no mesmo canal) impede a emissão de outra que, ao assumir o canal como ocupado, não o irá usar, quando na prática a sua emissão até iria decorrer sem problemas pois o sinal distante não iria interferir no destino
   * V O problema *Near-and-Far* ocorre em situações em que as estações emissoras envolvidas se encontram a operar em canais sem sobreposição de banda
   * F O mecanismo *CTS-to-self* consegue de uma forma mais eficiente que o RTS/CTS resolver o problema do nó escondido
3. As tramas de dados IEEE802.11 destinadas a endereços MAC de grupo têm menor fiabilidade
   * X Porque não podem ser fragmentadas
   * V Porque não são confirmadas com ACK
   * F Porque são transmitidas num débito *basic-rate*
   * V Porque não podem ser protegidas por RTS/CTS
4. Relativamente à adenda IEEE802.11n:
   * F Introduz a possibilidade de agregação de canais consecutivos num único de até 80MHz
   * V Aumenta a eficiência ao permitir negociar períodos comunicação com ACK em bloco
   * V Nem todos os equipamentos que suportam a norma são compatíveis com células 802.11a
   * V Define a possibilidade de operação com 1 a 4 fluxos (*spatial streams*)
5. Em relação à segurança das redes sem fios IEEE802.11
   * F A validação do endereço MAC cliente numa ACL é considerada uma forma adequada de segurança
   * F É possível descobrir a chave usada numa cifra WEP realizando um ataque de “força bruta” a partir da informação obtida durante o acesso de um cliente legítimo
   * F É possível descobrir a chave usada na segurança WPA2-PSK/AES obtendo grandes quantidades de tráfego cifrado e derivando os bits da chave a partir dos IV (*initialization vectors*) usados na cifra de cada trama individual
   * V No WPA2-PSK/AES a melhor segurança obtém-se usando uma chave hexadecimal aleatória de 256bit
6. Considere um AP configurado com um *RTS Threshold* de 500 e um *Fragmentation Threshold* de 500. Considere o tempo total durante o qual uma trama de 900 bytes circula entre duas estações no mesmo BSS e que não existem erros na entrega. As estações têm os parâmetros de *RTS Threshold* e *Fragmentation Threshold* por omissão.
   * V Circulam 3 tramas que contêm dados
   * F Vão existir 4 ACKs
   * V Vão existir 2 fragmentos e três ACKs
   * V Vai existir um RTS
7. Considerando uma estação IEEE 802.11-2012 em poupança de energia, indique:
   * V Existe sempre uma trama de PS POLL por cada trama armazenada no AP
   * V Não é necessário o envio de PS-POLL se as tramas a receber forem de *Broadcast*
   * F As tramas de dados enviadas em resposta a um PS-POLL dispensam o ACK
   * F As estações em poupança de energia que queiram enviar dados só o podem fazer após o próximo *beacon* em que o TIM tenha o AID da estação
8. No acesso de uma estação a uma rede sem fios IEEE802.11
   * V A autenticação ocorre antes da associação
   * F A autenticação tipo OPEN não é recomendada pois permite a associação de qualquer estação à BSS
   * F A pesquisa de rede é feita exclusivamente enviando mensagens *ProbeRequest*
   * V O AP só aceita o acesso se o cliente suportar todos os débitos definidos como *basic rates*
9. As ACLs da cisco podem ser utilizadas para:
   * V Filtragem de pacotes
   * V Filtragem de rotas
   * F Manipulação de pacotes quando utilizada também para filtragem de pacotes
   * F Abrir automaticamente acessos a ligações de dados auxiliares como no caso do FTP
10. Em relação às listas de acesso *standard* da Cisco, indique:
    * V Só permitem duas acções *accept* ou *deny*
    * F Só permitem verificar endereços de destino
    * V Por omissão, quando é aplicada uma acção *deny* é gerada uma mensagem *ICMP Unreachable*
    * F A opção *reflect* permite avaliar o tráfego numa lista no sentido inverso
11. Em relação às listas de acesso *extended* da Cisco, indique:
    * F Uma ACE com a *keyword* *fragments* sucede apenas no primeiro fragmento de um datagrama
    * F As ACEs com a *keyword* *established* sucedem em todos os pacotes que não tenham o SYN activo
    * F A keyword time-range verifica o *timestamp* das mensagens *ICMP Timestamp*
    * V A opção *evaluate* permite avaliar o tráfego que tenha passado anteriormente numa lista no sentido inverso
12. Em relação aos diferentes pontos de intercepção do *iptables*, indique:
    * F A tabela de NAT só está disponível para tráfego gerado localmente
    * V A tabela de *Mangle* pode ser interceptada em INPUT e OUTPUT
    * V A tabela de *Filter* está disponível em FORWARD, INPUT e OUTPUT apenas
    * V É possível filtrar tráfego gerado localmente, após ser manipulado na tabela *Mangle*
13. Um *router* realiza a protecção de uma rede local usando o *netfilter* (Linux), a Internet é ligada à interface eth0 e a rede local à eth1. O módulo *helper* de filtragem de FTP se encontra-se activo e as regras abaixo aplicadas. Quando numa máquina interna for iniciada uma ligação FTP (modo passivo), ilustrada na figura abaixo, com o objectivo de publicar um ficheiro num servidor da Internet, que regras serão aplicadas a cada uma das mensagens do diagrama?

1) -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT

2) -A FORWARD -i eth0 -j da\_internet

3) -A FORWARD -o eth0 -j para\_internet

4) -A FORWARD -j LOG

5) -A FORWARD -j DROP

6) -A da\_internet -m conntrack --ctstate RELATED -j ACCEPT

7) -A para\_internet -m conntrack --ctstate RELATED -j ACCEPT

8) -A para\_internet -p tcp -m tcp --dport 21 -j LOG

9) -A para\_internet -p tcp -m tcp --dport 21 -j ACCEPT

