a) Porque terminam nestes certificados?

b) Quem define quem são estes certificados?

A.4 Vulnerabilidades em máquinas

1. Considere os ataques por esmagamento da pilha (*stack smashing attacks*) contra programas escritos em C.

   a) Explique qual é a vulnerabilidade que exploram.

   b) Indique por que razão não são possíveis com Java.

2. Descreva o modo como se processa um ataque por esmagamento da pilha (*stack smashing attack*).

3. Considere o sistema de proteção de endereços de retorno com canários do *StackGuard* e a proteção de memória de uma pilha proibindo execução. Explique a complementaridade entre estes dois mecanismos de proteção.

4. A ferramenta `nmap` permite identificar portos de transporte disponíveis numa máquina e o sistema operativo da mesma. Explique qual o interesse que tem para um atacante:

   a) Conhecer os portos.

   b) Conhecer o sistema operativo.

5. O sistema de identificação de sistemas operativos do `nmap` recolhe características operacionais da pilha de protocolos TCP/IP para conseguir distinguir os sistemas. Explique:

   a) Por que razão as opções do TCP são muito úteis para esta identificação.

   b) Por que razão essas mesmas opções podem ser facilmente uma fonte de ilusão para o processo de identificação.

6. A ferramenta de deteção de vulnerabilidades `nmap` usa técnicas de identificação de características da pilha de comunicações de uma máquina para reconhecer o respetivo sistema operativo. Explique como poderia contrariar esse reconhecimento protegendo a máquina com uma *firewall* (admitindo que a máquina a proteger pode disponibilizar um conjunto limitado de serviços públicos via TCP ou UDP) e qual o tipo de *firewall* que usaria.

7. Considere as diversas formas de deteção de portos TCP abertos pela ferramenta `nmap`. Indique quais as vantagens e desvantagens de usar:

   a) Pedidos de ligação normais.

b) Meios-pedidos de ligação (sem resposta ACK).

c) Sondas furtivas (segmentos FIN).

8. A utilização por administradores de redes de ferramentas de deteção de vulnerabilidades como o OpenVAS (ou Nessus) deve ser precedida de um aviso aos utentes das máquinas/redes inspecionadas. Explique porquê.

9. Considere os ataques por esmagamento da pilha (*stack smashing attack*) contra programas escritos em C. Explique com pormenor como os mesmos podem ser mitigados alterando o endereço base de início da pilha de cada vez que um programa inicia a sua execução.

10. Considere os ataques por esmagamento da pilha (*stack smashing attack*) contra programas escritos em C.

    a) Explique com pormenor como atuam.

    b) Indique como podem ser detetados com canários.

A.5 Vulnerabilidades em redes

1. Um ataque de envenenamento de tabelas ARP (*ARP poisoning attack*) explora um determinado tipo de vulnerabilidade. Explique:

    a) Em que consiste essa vulnerabilidade.

    b) Que consequências podem advir de um ataque deste tipo.

2. Considere o problema da personificação de máquinas usando IP *spoofing*. Explique porque é que não é fácil de efetuar a mesma na iniciação de ligações TCP.

3. Um dos tipos de vulnerabilidades dos sistemas computacionais é a não previsão de cenários absurdos ou, à partida, impossíveis em condições normais de operação. Indique duas dessas vulnerabilidades e ataques que as explorem.

4. Os datagramas IP permitem que se use uma funcionalidade designada por *Source Route*, mas a mesma é normalmente contrariada pelos *routers* por motivos de segurança. Explique porquê.

5. Explique como funciona um ataque de envenenamento da *cache* ARP (*ARP poisoning attack*).

6. Explique como se realiza um ataque de interposição (*meet-in-the-middle attack*) através de envenenamento da *cache* ARP (*Address Resolution Protocol*).

7. Considere o problema de envenenamento de *caches* DNS (*Domain Name System*). Explique de que maneira os mecanismos do IPSec (IP *Security*), ESP (*Encapsulating Security Payload*) ou AH (*Authentication Header*), podem ou não evitar esse problema (considere apenas o IPSec em modo transporte).

A.6 *Firewalls*

1. Uma *firewall* do tipo filtro de pacotes é especificada usando uma lista de regras. Considere a *firewall* `iptables`, do Linux, onde as regras são empacotadas em cadeias (*chains*). Explique:

   a) Para que servem cada uma das seguintes cadeias: INPUT, OUTPUT e FORWARD.

   b) Que diferença existe entre as decisões DROP e REJECT tomadas por uma regra?

2. Uma *firewall* do tipo filtro de pacotes é especificada usando uma lista de regras.

   a) Qual é a estrutura-base de cada uma dessas regras?

   b) De que forma essas regras são usadas para realizar a missão da *firewall*?

3. Explique para que fim se usa atualmente o conceito de DMZ (*DeMilitarized Zone*).

4. Explique de que forma uma *firewall* (de rede, não pessoal) permite minimizar as vulnerabilidades de uma rede informática.

5. Quando se fala em segurança importa considerar duas vertentes: políticas e mecanismos. Indique, justificando, como é que o mecanismo normalmente designado como *firewall* pode aplicar a política conhecida como princípio do privilégio mínimo.

6. Considere o conceito de Zona Desmilitarizada ou DMZ. Explique:

   a) Qual o significado original do conceito em termos topológicos.

   b) Qual a sua principal utilidade.

7. Uma política de segurança aconselhável para minimizar riscos consiste na aplicação do princípio do privilégio mínimo. No âmbito da configuração de uma *firewall* explique como os seguintes mecanismos podem ser usados para implantar essa política:

   a) DMZ.

   b) Filtragem de datagramas.
   c) NAT dinâmico (*masquerading*).

8. As *firewalls* são normalmente usadas com dois propósitos: (i) proteção de uma rede por isolamento e (ii) controlo de interações entre redes. Indique, justificando, dois exemplos claros de atuação de uma *firewall* que evidenciem claramente cada um dos propósitos referidos.

9. Indique e descreva sumariamente os três tipos funcionais base de *firewalls*.

10. Indique dois tipos de vulnerabilidades de uma rede organizacional que podem ser minimizados por uma *firewall* do tipo filtro de datagramas.

11. Indique dois tipos de vulnerabilidades de uma rede organizacional que podem ser minimizados por uma *firewall* do tipo filtro aplicacional.

12. Imagine que tem uma rede local com N servidores públicos localizados em DMZ e que existe alguma interação normal e conhecida entre os servidores. As DMZ são sub-redes ligadas a uma *gateway* que dispõe de uma *firewall* do tipo filtro de pacotes. Discuta as vantagens e desvantagens das seguintes alternativas topológicas:

    a) Todos os servidores numa única DMZ.
    b) Um servidor por DMZ.

13. Explique por que razão as *firewalls* do tipo filtro de pacotes não são as ideais para procurar vírus em dados trocados entre redes.

14. As *firewalls* podem ser de três tipos: filtros de datagramas, filtros de circuitos ou filtros aplicacionais. Indique que tipos escolheria para resolver os seguintes problemas e porquê:

    a) Deteção de vírus em ficheiros descarregados por HTTP.
    b) Controlo de acesso de utilizadores da rede protegida a recursos públicos na rede exterior.
    c) Prevenção de ataques à prestação de serviços que explorem vulnerabilidades da pilha de protocolos dos sistemas operativos (por exemplo, SYN *flooding attack*).

15. Considere os SYN *flooding attacks*. Explique:

    a) Como são efetuados e quais as consequências para as máquinas-vítima.
    b) Como é que um sistema NIDS (*Network-based Intrusion Detection System*) com acesso a todo o tráfego das máquinas-vítima pode detetar o ataque e contrariá-lo.

16. Considere o problema dos SYN *flooding attacks*.

    a) Explique como são efetuados.

    b) Indique três formas diferentes de redução do seu impacto.

17. Compare as *firewalls* do tipo filtro de datagramas e filtro aplicacional quanto aos seguintes aspetos:

    a) Flexibilidade (capacidade de adaptação a diferentes interações remotas).

    b) Capacidade de deteção e eliminação de conteúdos perigosos (ciberpragas, etc.)

18. Compare as *firewalls* do tipo filtro de datagramas e filtro aplicacional quanto aos seguintes aspetos:

    a) Capacidade de interposição de mecanismos adicionais de autenticação de utilizadores.

    b) Capacidade de intervenção em protocolos com portos de transporte dinâmicos (FTP, Sun RPC, protocolos P2P, etc.)

19. As *firewalls* do tipo filtro de pacotes têm algumas limitações relativas à gestão de estado, o que motivou a sua evolução no sentido de alternativas designadas como "filtros de pacotes com estado". Dê dois exemplos desse estado mantido e usado por estas *firewalls*.

20. A sobrefragmentação de datagramas IP ou ICMP é uma fonte de problemas para as *firewalls* do tipo filtro de pacotes. Explique:

    a) Porque é que são um problema.

    b) Como se pode resolver esse problema de forma eficaz.

21. Considere uma DMZ numa arquitetura de rede de uma *firewall*. Explique:

    a) O que é e para que serve.

    b) Indique duas alternativas topológicas de implantação de uma DMZ e discuta as vantagens e desvantagens relativas.

22. Por que razão se colocam servidores públicos, dentro do perímetro protegido por uma *firewall*, numa DMZ?

23. Quais os benefícios de definir uma DMZ como uma rede isolada ligada às restantes redes, pública e privada, através de uma *gateway* bastião?

24. Considere as *firewalls* do tipo filtros de circuitos. Indique, justificando:

a) Em que situações operacionais é necessário usar este tipo de *firewalls* em vez de qualquer um dos outros tipos (filtros de datagramas ou filtros aplicacionais)?

b) Quais as desvantagens operacionais decorrentes do seu uso?

25. Indique duas razões para aplicar filtros aplicacionais numa *firewall* para processar tráfego de dentro para fora do perímetro protegido.

26. Considere que uma rede apenas dispõe de um endereço IP público para suportar o acesso das suas máquinas à Internet. Para esse fim pode usar NAT (*Network Address Translation*) dinâmico (*masquerading*) ou um filtro de circuitos SOCKS, ambos operando na máquina que possui o IP público. Explique quais as vantagens e desvantagens relativas de ambas as aproximações.

27. Explique por que razão os mecanismos de NAT podem ser úteis para concretizar uma política de privilégio mínimo.

28. Quais as vantagens, para a segurança de uma rede privada ligada à Internet, de usar NAT dinâmico na *gateway* de interligação?

29. O mecanismo NAT é, por vezes, considerado como um auxiliar importante para garantir alguns atributos de segurança de uma rede privada. Indique:

a) Os riscos que são evitados quando o NAT é dinâmico (*masquerading*).

b) Os riscos que não são evitados quando o NAT é estático (*port forwarding*).

30. Indique, justificadamente, como é que numa *firewall* do tipo filtro de pacotes se aplica a política "tudo o que não é proibido é negado".

31. Quais são as vantagens e desvantagens, em termos de impacto no uso e proteção da rede protegida, da concretização das seguintes políticas numa *firewall* do tipo filtro de pacotes:

a) "Tudo o que não é proibido é negado".

b) "Tudo o que não é proibido é autorizado".

A.7 Sistemas de deteção de intrusões

1. Explique de que forma se conseguem detetar ataques automatizados (isto é, não conduzidos pessoalmente por um atacante, mas autonomamente por um programa) na Internet.

2. Considere um sistema de deteção de intrusões (IDS – *Intrusion Detection System*). Explique:

a) O que é um falso positivo ou um falso negativo.

b) Quais os riscos de cada um dos erros para a eficácia do sistema.

3. Os IDS usam dois métodos alternativos de deteção: deteção de anomalias ou deteção de usos incorretos. Explique:

   a) Como funciona cada um deles.

   b) Quais as vantagens e desvantagens de cada um relativamente à ocorrência de erros (falsos positivos ou falsos negativos).

4. Explique a diferença entre os seguintes métodos de deteção dos IDS:

   a) Baseados em conhecimento.

   b) Baseados em comportamento.

5. Imagine que possui um sistema NIDS numa rede protegida capaz de detetar SYN *flooding attacks* a qualquer das máquinas da rede. De que modo é que o sistema NIDS poderia reagir automática e corretamente de forma a contrariar o ataque?

6. Considerando os métodos de deteção acima referidos indique as vantagens e desvantagens relativas no que toca a:

   a) Geração de falsos positivos.

   b) Deteção de ataques desconhecidos.

7. Considere a exploração da sobrefragmentação de datagramas para a camuflagem de ataques ou para ludibriar sistemas de defesa. Discuta as vantagens e desvantagens relativas dos sistemas NIDS e HIDS (*Host-based Intrusion Detection System*) na:

   a) Deteção da sobrefragmentação.

   b) Reação defensiva à sobrefragmentação.

A.8 Redes Privadas Virtuais (VPN – *Virtual Private Networks*)

1. As chaves de sessão usadas em comunicações seguras devem ser usadas de forma limitada. Indique por que razão se devem impor os seguintes limites:

   a) Tempo máximo de utilização.

   b) Número máximo de octetos cifrados com a chave.

2. Explique os conceitos de:

   a) Chave de sessão.

   b) Chave de cifra de chave (KEK – *Key Encryption Key*).

3. No âmbito da distribuição de chaves de sessão explique o que significa o conceito de segurança futura perfeita.

4. Indique qual a técnica base de distribuição de chaves que permite garantir segurança futura perfeita e explique porquê.

5. O algoritmo de negociação de chaves Diffie-Hellman é um dos poucos que permite negociar chaves simétricas entre duas partes que assegurem segurança futura perfeita. Explique:

   a) O que significa uma chave assegurar segurança futura perfeita.

   b) Quais os requisitos na utilização do algoritmo Diffie-Hellman necessários para que a chave resultante assegure segurança futura perfeita.

6. Considere o problema da personificação de máquinas usando IP *spoofing*. Explique como é que os mecanismos AH e ESP do IPSec podem contribuir para reduzir a relevância desse problema (considere os mecanismos separadamente e ambos os modos de transporte e túnel).

7. O algoritmo de Diffie-Hellman permite distribuir chaves de sessão entre interlocutores que à partida só partilham valores públicos. Explique:

   a) Como funciona o algoritmo.

   b) Quais os valores públicos acima referidos.

   c) Como se pode atacar o algoritmo através de interposição (*meet-in-the--middle attack*).

8. Para que servem as associações seguras no âmbito do IPSec e como se usam após a sua criação?

9. Considere as associações seguras do IPSec. Explique:

   a) Qual o conteúdo de uma associação segura.

   b) Como se relaciona uma associação segura com um datagrama IPSec recebido?

10. Considere os cabeçalhos extra do IPSec. Explique:

    a) Para que serve o campo SPI (*Security Parameter Index*) presente em cada um deles?

b) Explique o processo de escolha do valor desse campo para um dado datagrama IPSec.

11. O IPSec pode usar duas formas de autenticação entre máquinas/redes: chaves secretas partilhadas ou pares de chaves assimétricas com certificação da componente pública. Indique cenários operacionais concretos onde cada uma das formas de autenticação é mais vantajosa.

12. Explique para que serve o cabeçalho ESP do IPSec.

13. Explique, ilustrando a sua resposta, a diferença entre os modos de transporte e de túnel IPSec.

14. Numa VPN (*Virtual Private Network*) as técnicas de encapsulamento (*tunnelling*) e cifra/controlo de integridade estão muitas vezes associadas, mas servem propósitos diferentes. Explique em que consiste o ESP em modo túnel do IPSec e qual a vantagem do seu uso face ao ESP em modo transporte, o modo mais simples de usar o ESP no IPSec.

15. O cabeçalho IPSec AH em modo transporte pode ser substituído pelo cabeçalho IPSec ESP em modo túnel. Explique:

    a) Discuta as vantagens e desvantagens relativas dos dois métodos.

    b) Discuta o uso alternativo do cabeçalho ESP em modo transporte (em vez do modo túnel).

16. Indique, justificando, qual dos modos IPSec, transporte ou túnel, faria sentido escolher para criar as seguintes VPN:

    a) Rede-rede.

    b) Rede-máquina.

17. Considere uma VPN rede-rede usando IPSec em modo túnel. Indique:

    a) Quem gere as associações seguras IPSec usadas pela VPN.

    b) Como se processa a aplicação e validação dos mecanismos do IPSec numa comunicação entre quaisquer duas máquinas em redes distintas ligadas através da VPN.

18. Por que razão existem problemas quando os datagramas IPSec atravessam uma *gateway* que aplica mecanismos de NAT? Considere, na resposta, todas os cenários relativos ao uso de AH ou ESP e dos modos transporte e túnel.

19. Considere o protocolo PPTP (*Point-to-Point Tunneling Protocol*):

a) Explique de forma sintética a sua evolução face ao PPP (*Point-to-Point Protocol*).

b) Explique por que razão no PPTP não se deve usar o protocolo de autenticação PAP (*Point-to-point Authentication Protocol*).

20. O protocolo de autenticação PAP era considerado suficientemente seguro em ligações *dial-up* PPP em redes telefónicas, mas já não é aconselhável ser usado em VPN PPTP na Internet. Explique porquê.

21. As VPN podem atuar em níveis protocolares distintos: nível 2 (PPTP, L2TP – *Layer 2 Tunneling Protocol*, etc.), nível 3 (IPSec), níveis acima do 4 (SSH – *Secure SHell*, etc.). Discuta as vantagens e desvantagens de atuar a um nível mais baixo ou mais alto.

22. Por que razão uma comunicação segura IPSec com cabeçalhos ESP aumenta a latência e diminui o desempenho em comunicações sobre *modems* analógicos com capacidade de compressão.

23. A compressão de dados é uma das opções de muitos protocolos de comunicação segura (SSL (*Secure Sockets Layer*), SSH, PGP, etc.). Indique as vantagens que advêm da sua utilização.

24. Os protocolos de comunicação segura de mais alto nível, como o SSL, o SSH e o PGP, podem optar por comprimir os dados antes de os tornar seguros, enquanto os protocolos de mais baixo nível, como o IPSec, não possuem tal opção. A que se deve esta diferença de atuação?

25. Qual a vantagem para a segurança das comunicações de utilizar encapsulamento (túneis IPSec, multiplexagem SSH, etc.).

26. O encapsulamento é uma das tecnologias normalmente usadas pelas VPN (por exemplo, PPTP). Explique porquê.

27. Que modos de transporte do IPSec escolheria para atravessar uma *gateway* que aplica mecanismos de NAT? Considere, na resposta, todas os cenários relativos ao uso dos cabeçalhos AH ou ESP.

28. Considere a multiplexagem de várias comunicações através de um único canal de comunicação seguro. Indique:

a) Quais são as vantagens da multiplexagem para a segurança.

b) Dois protocolos que permitem obter essa multiplexagem.

29. Considere a multiplexagem de vários fluxos de comunicação através de um único canal de comunicação seguro. Indique:

a) Quais são as vantagens da multiplexagem para a segurança.

b) Explique como o pode fazer com SSH.

30. Considere os conceitos de segurança na ligação (*link security*) e segurança entre extremos (*end-to-end security*). Explique por que razão uma VPN pode associar-se com os dois conceitos (considere, por exemplo, uma VPN PPTP).

31. Considere dois tipos de VPN: PPTP e SSL. Compare-os quanto a:

    a) Abrangência (protocolos abrangidos pela VPN).

    b) Facilidade de configuração e utilização.

32. A comunicação segura entre duas máquinas usando IPSec e o protocolo de negociação de chaves IKE (*Internet Key Exchange*) segue os seguintes passos: (1) estabelecimento de uma SA (*Security Association*) IKE, (2) estabelecimento das SA IPSec e (3) transmissão de dados usando IPSec. Explique:

    a) Para que serve cada passo.

    b) Que cenários operacionais concretos levam à sua execução.

A.9 Segurança em redes sem fios 802.11 (WLAN ou Wi-Fi)

1. Considere o controlo de integridade de tramas usado no WEP (*Wired Equivalent Privacy*), baseado na função CRC-32.

    a) Explique como funciona.

    b) Explique de que forma pode ser facilmente contornado por atacantes que queiram modificar uma trama.

2. Considere os mecanismos de segurança introduzidos pelo TKIP (*Temporal Key Integrity Protocol*).

    a) Indique qual é a relação entre o TKIP e o WEP.

    b) Indique dois mecanismos usados pelo TKIP que eliminam vulnerabilidades existentes no WEP.

3. Considere o processo de autenticação SKA (*Shared Key Authentication*) do WEP.

    a) Explique como é que opera.

    b) Explique como pode ser atacado.

4. Considere o controlo de integridade de tramas usado no WEP, baseado na função CRC-32.

a) Explique como funciona.

b) Explique de que forma pode ser facilmente contornado por atacantes que queiram modificar uma trama.

5. Considere a autenticação de rede nas comunicações sem fios 802.11.

   a) Indique como funcionam os mecanismos de autenticação OSA (*Open System Authentication*) e SKA do WEP.

   b) Explique os princípios gerais da autenticação com 802.1X e EAP (*Extensible Authentication Protocol*).

6. Em comunicações sem fios há que considerar diversas vulnerabilidades que não existem em infraestruturas cabladas. Indique:

   a) Quais são essas vulnerabilidades.

   b) De que modo no 802.11 elas são evitadas.

7. O facto de se usar segurança entre extremos (*end-to-end*) em comunicações sensíveis é razão para se abandonar, sem mais, a segurança de ligação (*link security*) em comunicações sem fios subjacentes? Explique porquê.

8. Considere a arquitetura de autenticação WEP usada em redes sem fios 802.11. Explique:

   a) Quais são os modelos possíveis de autenticação.

   b) Por que razão é possível um cliente ser enganado por um AP (*Access Point*) falso.

9. Considere a arquitetura de autenticação WEP usada em redes sem fios 802.11. Explique:

   a) Como funciona o protocolo de autenticação SKA.

   b) Em que casos é preferível usar o protocolo de autenticação OSA.

10. As chaves de sessão usadas em comunicações seguras devem ser usadas de forma limitada e os limites podem ser (i) um número máximo de octetos cifrados com a chave ou (i) um tempo máximo de utilização. Explique, com uma explicação resumida, por que razão:

    a) O modelo de gestão de chaves de sessão do WEP não é o adequado.

    b) O modelo de gestão de chaves de sessão do WPA (*Wi-Fi Protected Access*) e do 802.11i são os adequados.

11. O controlo de integridade do WEP usa CRC-32, que não é criptográfico. Que problemas podem advir desse facto?

12. O WEP não faz um uso correto das chaves simétricas partilhadas entre os (utentes dos) equipamentos móveis e (a administração d)os AP. Indique:

    a) Qual, ou quais, o(s) uso(s) incorreto(s) a que nos referimos.

    b) Um ataque concreto que explore vulnerabilidades criadas devido às incorreções antes referidas.

13. O WEP não define qualquer política de gestão dos valores VI (Vetor de Iniciação) usados nas tramas protegidas. Explique, recorrendo a exemplos ilustrativos, que problemas podem resultar dessa omissão.

14. O WEP não usa chaves contínuas diferenciadas consoante o sentido da comunicação. Explique:

    a) Como é que isso poderia ser feito de forma fácil (sem reduzir outros critérios de segurança).

    b) Que vantagens adviriam desse facto.

15. Considere a arquitetura de autenticação 802.1X usada em redes sem fios 802.11. Explique:

    a) Qual a vantagem de usar EAP na autenticação dos Suplicantes.

    b) Qual o papel do Autenticador e do Servidor de autenticação.

    c) Para que serve a autenticação em quatro passos entre o Suplicante e o Autenticador.

16. Considere o mecanismo de autenticação e distribuição de chaves 802.1X, usado no WPA e 802.11i. Descreva as suas três fases e o propósito de cada uma delas.

17. O 802.1X fornece um serviço de autenticação ao nível 2 da pilha de protocolos. Por que razão foi necessário usar um serviço a este nível e não um outro qualquer para gerir a autenticação e o controlo de acesso a uma rede sem fios 802.11?

A.10 Protocolos de autenticação

1. Explique por que razão a autenticação de entidades é normalmente um requisito fundamental para a concretização de políticas de autorização.

2. Considere os protocolos de autenticação com desafio-resposta e segredo partilhado.

    a) Explique de uma forma genérica como funcionam.

b) Explique como podem ser desenhados para facultar autenticação mútua (com um mínimo de mensagens trocadas).

3. Considere o conceito de autenticação com senha descartável.

   a) Que cenários operacionais justificam o seu uso?

   b) Escolha um protocolo de autenticação com senha descartável e descreva o seu funcionamento

4. A autenticação de máquinas no SSH é feita recorrendo a chaves públicas pré-partilhadas.

   a) Explique por que razão esta é uma aproximação válida, por contraponto ao recurso a chaves públicas certificadas.

   b) Explique como é realizada normalmente a distribuição das chaves públicas partilhadas.

5. Considere um processo de autenticação biométrica de pessoas.

   a) Explique como é que opera (**Sugestão: tenha em consideração as ações de recenseamento e autenticação do titular**).

   b) Explique que vantagens e desvantagens podem advir da dificuldade de transferir credenciais de autenticação para terceiros.

6. Imagine que pretende usar o Cartão de Cidadão para fazer autenticação local numa máquina Linux. Explique como o poderia fazer usando o par de chaves assimétricas de autenticação do titular do cartão. (**Sugestão: tenha em consideração as ações de recenseamento e autenticação do titular**).

7. A autenticação de máquinas pode-se fazer com chaves públicas certificadas (por exemplo, SSL) ou com chaves públicas não certificadas (por exemplo, SSH).

   a) Explique as vantagens e desvantagens de cada uma das aproximações.

   b) Explique a razão das opções tomadas no SSL e no SSH face a esta questão.

8. Considere um processo de autenticação com desafio-resposta.

   a) Explique como é que opera.

   b) Explique como é que o mesmo pode ser usado para autenticar pessoas titulares de um Cartão de Cidadão.

9. Considere o processo de autenticação de utentes do Linux.

   a) Explique como é que opera.

b) Explique, justificando, de que forma devem ser protegidos os recursos usados nesse processo.

10. Considere o conceito de autenticação multifator.

    a) Em que consiste?

    b) Explique como a mesma é obtida no caso da autenticação de subscritores de serviços GSM.

11. A distribuição de chaves com autoridades terceiras confiáveis (KDC – *Key Distribution Centers*) pressupõe a autenticação das entidades a quem as chaves são distribuídas perante uma ou duas dessas autoridades. Explique como no Kerberos, que é um exemplo de uma dessas autoridades, se resolve o problema quando as duas entidades, por exemplo um cliente e um servidor, são conhecidas (ou seja, identificadas e autenticadas) por dois serviços Kerberos diferentes (assumindo o cenário mais simples).

12. O mecanismo de autenticação com senhas descartáveis S/Key é vulnerável a ataques com dicionários, muito embora nunca se transmita a mesma senha entre autenticado e autenticador. Explique como.

13. O Kerberos é constituído por dois serviços: o serviço de autenticação (AS – *Authentication Service*) e o serviço de distribuição de bilhetes (TGS – *Ticket Granting Service*). Explique para que fim são contactados pelas aplicações-clientes que usam autenticação Kerberos.

14. A distribuição de chaves de sessão simétricas entre pares de interlocutores é um problema complexo que pode ser resolvido através de entidades terceiras confiáveis designadas como Centros de Distribuição de Chaves. A utilização destes centros pressupõe que os mesmos são seguros e que atuam corretamente. Explique a necessidade destes dois pressupostos.

15. A distribuição segura de chaves de sessão requer a autenticação das entidades envolvidas e a autenticação dos dados trocados (correção e frescura). Explique o objetivo de cada um dos requisitos.

16. Explique em que é que consiste um ataque com dicionário e mostre como o mesmo pode ser efetuado contra o modelo-base de autenticação do UNIX.

17. A arquitetura PAM (*Pluggable Authentication Modules*) permite adaptar os princípios gerais da autenticação (prova de autenticidade, alteração dos elementos de prova, autorização para iniciar uma sessão e salvaguarda de credenciais) às necessidades reais de autenticação de sistemas ou aplicações específicas. Explique como.

18. Explique o modelo de operação da autenticação S/Key.

19. Um Centro de Distribuição de Chaves (KDC – *Key Distribution Center*) é muito prático para fazer uma distribuição autenticada de chaves de sessão entre dois interlocutores que nada partilham entre si. Explique, no caso concreto do Kerberos:

    a) Como se garante a autenticação mútua dos interlocutores (*principals*).

    b) Que segredos têm esses interlocutores de partilhar com o Kerberos para conseguir usufruir dos seus serviços.

20. Um dos aspetos relevantes da tecnologia atual de autenticação biométrica é a afinação das taxas de erros do processo de autenticação: falsos positivos ou falsos negativos. Explique o que significam objetivamente esses erros (não confundir com a consequência da sua ocorrência).

21. A autenticação biométrica normalmente não permite derivar uma chave de autenticação, ao contrário do que acontece com a autenticação tradicional com senhas. Porquê?

22. Os sistemas UNIX atuais dispõem de uma infraestrutura de autenticação de utentes designada por PAM. Explique, de forma sucinta mas completa:

    a) Como é que as aplicações que requerem a autenticação usam o PAM.

    b) Como é que o PAM permite incorporar diferentes mecanismos de autenticação de pessoas (por exemplo, com senha ou com biometria).

23. Os sensores biométricos permitem normalmente ser afinados para controlar duas taxas de erros: FAR (*False Accept Rate*) e FRR (*False Reject Rate*). Explique:

    a) Por que razão existem esses erros.

    b) Que compromissos se fazem quando se afinam os sensores.

24. O serviço Kerberos possui dois subserviços: AS e TGS. Explique as vantagens operacionais desta subdivisão:

    a) Para a comodidade e segurança dos clientes.

    b) Para a gestão das chaves secretas guardadas pelo Kerberos.

25. Por que razão a utilização de autenticação Kerberos entre aplicações cliente-servidor kerberizadas obriga as máquinas das entidades que a usam (*principals*) a manter relógios bastante sincronizados?

26. No GSM (*Global System for Mobile communication*) os equipamentos móveis possuem algoritmos criptográficos implantados em locais diferentes: (i) a cifra das comunicações com A5 é feita pelo equipamento móvel e (ii) a geração de respostas a desafios para autenticação e de chaves de sessão, com A8, A3 ou COMP128, é feita pelo cartão SIM (*Subscriber Identification Module*). Indique as vantagens que advêm desta separação:

    a) Para a segurança do utente.

    b) Para a gestão das operadoras.

27. A arquitetura PAM permite adaptar os princípios gerais da autenticação (prova de autenticidade, alteração dos elementos de prova, autorização para iniciar uma sessão e salvaguarda de credenciais) às necessidades reais de autenticação de sistemas ou aplicações específicas. Explique como.

28. O serviço Kerberos gere dois tipos de bilhetes: bilhetes para o TGS, conhecidos como TGT (*Ticket Granting Ticket*) e bilhetes para outros serviços. Explique:

    a) Qual a diferença entre estes bilhetes ao nível da sua estrutura interna e modelo de utilização.

    b) O modo como é obtido cada um deles (ou seja, como é formulado o pedido dos mesmos e processada a resposta em termos protocolares).

29. Considerando o mecanismo de autenticação de utentes Kerberos, indique quais os problemas que teria que resolver para o integrar com mecanismos de autenticação biométrica.

30. No GSM os equipamentos móveis usam diversos algoritmos criptográficos, os quais são realizados por componentes diferentes: (i) cartão SIM ou (ii) equipamento móvel. Indique:

    a) Quais as operações criptográficas realizadas por cada um.

    b) Como é que essa separação aumenta a segurança e operacionalidade na exploração do GSM.

31. O protocolo Kerberos é vulnerável a ataques com dicionários. Explique como faria exatamente um ataque com dicionário ao Kerberos (quais as mensagens a capturar, os testes a efetuar para dar por concluído com sucesso o ataque, etc.).

32. Considere a afinação de um sistema de autenticação biométrica não ideal, onde é preciso equilibrar taxas de aceitação falsa (FAR) e rejeição falsa (FRR). Explique como efetuaria a mesma:

a) Num sistema de relógio de ponto.

b) Num sistema de acesso a um cofre forte de uma instituição bancária.

33. Considere o protocolo de autenticação com senhas descartáveis S/Key. Explique:

a) Qual o seu propósito.

b) Como funciona.

c) Quais as suas vulnerabilidades.

34. A versão 5 do Kerberos possui um campo na mensagem inicial do utente para o servidor AS (*preauthenticated data*) que consiste numa marca temporal cifrada com a chave (derivada da senha) do utente. Este campo destina-se a minimizar o risco de ataques com dicionários. Indique, justificando:

a) Que tipos de ataques com dicionários são evitados.

b) Que tipos de ataques com dicionários são, mesmo assim, possíveis.

35. Considere o modelo de autenticação de utentes no GSM. Explique:

a) Como é que o mesmo funciona de forma a permitir acesso em *roaming* de utentes.

b) Para efeitos de autenticação, qual a confiança que tem que existir entre o utente e operador que o aceita em *roaming*?

36. Considere os protocolos de autenticação com desafio-resposta. Explique, ilustrando com um diagrama, como pode realizar um protocolo unilateral desse tipo usando as operações de cifra assimétricas do Cartão de Cidadão (do autenticado).

37. O protocolo de autenticação S/Key é vulnerável a ataques com dicionários à senha do autenticado? Justifique, considerando duas situações distintas:

a) Acesso do atacante aos dados mantidos pelo autenticador.

b) Acesso do atacante aos dados trocados remotamente entre autenticador e autenticado.

38. Indique duas vantagens da autenticação biométrica face aos demais mecanismos de autenticação de pessoas.

39. Explique como funciona o mecanismo de autenticação do Linux.

40. Considere os paradigmas de autenticação com apresentação direta de credenciais e com desafio-resposta. Explique:

a) Qual é a diferença fundamental entre as mesmas?

b) Em que situações pode (deve) ser explorado cada um deles?

41. Considere o conceito de autenticação com senha descartável. Explique:

a) Em que consiste?

b) Quais as suas vantagens e desvantagens?

42. Considere o modelo de autenticação GSM. Explique:

a) Como funciona?

b) Que riscos podem advir de uma personificação de uma BTS (*Base Transceiver Station*) por um atacante?

43. O GSM usa um processo de autenticação em que se usa, simultaneamente, algo que se tem e algo que se sabe. Explique porquê, complementando a sua explicação com um diagrama.

44. Considerando que o Cartão de Cidadão não realiza decifras com as suas chaves privadas, mas apenas assinaturas, como o usaria para realizar uma autenticação remota através de desafio-resposta?

45. Considere os protocolos de autenticação com desafio-resposta. Explique: Por que razão o desafio tem de ter um valor nunca antes usado (*nonce*)? Como podem ser realizados estes protocolos usando o Cartão de Cidadão?

46. Explique como funciona o protocolo de autenticação S/Key, nomeadamente os seguintes aspetos:

a) Iniciação dos dados no autenticador (ou servidor de autenticação).

b) Execução da autenticação.

47. Considere os protocolos de autenticação com segredo partilhado. Explique:

a) Em que consiste um ataque com dicionário?

b) Por que razão o protocolos do GSM e do RSA SecurID não são vulneráveis a este tipo de ataques?

48. Explique o modelo geral de exploração do PAM do Linux.

49. Descreva e dê exemplos dos três modelos genéricos de autenticação de pessoas.

50. Descreva como funciona o modelo de autenticação do GSM, focando todas entidades e trocas de dados envolvidas.

51. Imagine que pretende controlar o acesso a áreas protegidas usando fechaduras ativadas através do Cartão de Cidadão. Indique que cuidados deve ter, na interação com o Cartão de Cidadão, para tornar o controlo de acesso tão fidedigno quanto possível.

A.11 Integração de conceitos

1. A função CRC-32, usada no WEP para controlo de integridade, não pode ser considerada uma função de síntese. Explique porquê, tendo em conta os 3 requisitos que as funções de síntese têm de cumprir.

2. As cifras contínuas são normalmente as preferidas para atuar ao nível da transmissão física sem fios de sinais digitais cifrados (por exemplo, WEP, GSM). Explique porquê.

3. Tanto um mecanismo de NAT como um mecanismo de túnel IPSec servem para atingir um mesmo objetivo: necessitar de apenas um endereço IP público numa rede local para aceder à Internet. Compare os dois mecanismos quanto às seguintes questões:

   a) Facilidade na interação IN-OUT (iniciada pelas máquinas da rede local, tendo como alvo quaisquer outras máquinas na Internet).

   b) Facilidade na interação OUT-IN (iniciada por outras máquinas na Internet tendo como alvo quaisquer máquinas da rede local).

4. Considere uma tentativa de intrusão por adivinhação de senha via SSH. Quais as vantagens e desvantagens de usar os seguintes IDS para detetar o ataque:

   a) NIDS.

   b) HIDS.

5. Considere uma rede de máquinas continuamente monitorizada por sistemas independentes de deteção de intrusões, tanto HIDS como NIDS. Explique o que aconteceria em cada um desse tipos de sistemas IDS se, nessa rede de máquinas, se procurasse por vulnerabilidades usando uma aproximação semelhante à do OpenVAS (ou Nessus).

6. Qual o problema de usar uma ferramenta como o OpenVAS (ou Nessus) para detetar problemas numa rede de máquinas individualmente monitorizadas por HIDS ou globalmente monitorizadas por NIDS?

7. É possível que surjam falsos positivos quando se usa uma ferramenta como o OpenVAS (ou Nessus) para detetar problemas numa rede de máquinas individualmente monitorizadas por sistemas `Tripwire` (HIDS)? Justifique pormenorizadamente, incluindo uma descrição sumária do funcionamento de cada uma das ferramentas, OpenVAS e `Tripwire`.

8. Os sensores dos IDS tipicamente podem recolher dois tipos de dados. Indique

   a) De que tipos de dados estamos a falar.

   b) Quais as vantagens e desvantagens de cada um relativamente à deteção de atividades ilícitas exploradas através de canais seguros (por exemplo, propagação de vírus sobre canais SSH).

9. As versões mais recentes do PGP permitem dois tipos de tecnologias para suportar comunicação confidencial e assinaturas digitais: (i) RSA e (ii) Diffie-Hellman + ElGamal (DH/DSS). O ElGamal usa valores públicos e privados semelhantes aos do Diffie-Hellman, mas serve apenas para gerar e validar assinaturas digitais. Explique como, a partir a conjugação destas duas técnicas, se efetua no PGP a troca de uma mensagem confidencial entre as entidades A e B.

10. Quando se implanta uma VPN há que associá-la a algo que funcione como uma *firewall*, de modo a autenticar utilizadores legítimos da VPN, aos quais será possível atravessar a fronteira imposta pela *firewall*. A *firewall* pode ser um servidor SSH, um servidor RAS (*Remote Access Server*), ou mesmo uma componente mais complexa instalada ao nível de um sistema operativo de uma máquina. Para o caso do SSH indique, justificando, qual é o tipo da *firewall*: filtro de datagramas, filtro de circuitos ou filtro aplicacional.

11. Por que razões os servidores de VPN são muitas vezes integrados com máquinas *gateway*-bastião que protegem perímetros protegidos?

12. Discuta como em termos arquiteturais se pode integrar uma *firewall* do tipo filtro aplicacional com túneis (de saída) de uma VPN SSH e quais as limitações que se podem colocar à *firewall*. Use diagramas para ilustrar, da melhor maneira possível, a sua resposta.

13. A utilização obrigatória de IPSec num servidor tem alguma influência na sua vulnerabilidade a ataques por inundação de segmentos SYN (SYN *flooding attacks*)?

14. Considere a utilização conjunta de NAT dinâmico (*masquerading*) e IPSec em modo transporte com AH. Explique:

a) Em que situações podem surgir problemas pela conjugação dos dois mecanismos?

b) Como é que os mesmos podem ser conjugados de forma a evitar esses problemas?

15. Um dos problemas de autenticidade na Internet consiste na falsificação de endereços IP de origem (IP *spoofing*). Considerando o IPSec e os seus dois modos de operação (transporte e túnel), discuta aprofundadamente a contribuição que os seguintes cabeçalhos dão para evitar IP *spoofing*:

a) AH.

b) ESP (com e sem autenticação).

16. O protocolo de Diffie-Hellman não inclui autenticação das partes negociantes. Indique, com diagramas, que alterações faria ao protocolo, mas assegurando segurança futura perfeita da chave resultante, de forma que a autenticação fosse feita:

a) Com uma chave secreta partilhada de longa duração partilhada entre as partes.

b) Com dois pares de chaves assimétricas, um por cada uma das partes.

17. O GSM e o WEP são aparentemente muito semelhantes em termos de tecnologia de cifra (ver tabela abaixo), mas a exploração do primeiro é muito mais segura no que diz respeito à privacidade dos dados cifrados. Explique porquê (assuma transmissão de dados, e não voz, no caso do GSM).

	Cifra		VI
	Algoritmo	Chave	
GSM	A5	54 *bits*	22 *bits*, índice da mensagem
WEP	RC4	40 *bits*	24 *bits*, escolhido *ad hoc* pelo emissor

18. Considere o problema da distribuição de chaves de sessão entre entidades que, à partida, nada partilham entre si. Indique, justificando, vantagens e desvantagens de usar o protocolo de Diffie-Hellman ou o Kerberos para resolver este problema.

19. Explique como se processa a autenticação entre entidades (*principals*) registadas em domínios Kerberos distintos.