EXAME PERGUNTAS POSSIVEIS

GRUPO I

1.1 – Indique e descreva os principais objetivos da segurança informática numa organização?

- Proteger e possibilitar o acesso apenas a entidades que podem aceder a recursos informáticos: Informação (dados) e serviços, Equipamento que suportam a informação e serviços
- Impedir o acesso a informação/recursos a restantes entidades sem autorização: intrusos, concorrentes, inimigos e espiões
- Garantir disponibilidade da informação/serviços e equipamentos
- Garantir a comunicação segura de informação privada
- Garantir boa reputação do detentor dos recursos informáticos

1.1 Indique e descreva os principais requisitos para garantir a segurança das comunicações na internet?

- Autenticação e Controlo de Acessos: 2,5/4
  - Possibilitar acesso a recursos informáticos apenas a entidades identificadas, autenticadas e autorizadas
- Confidencialidade: 2,5/4
  - Garantir que dados privados (confidenciais) transmitidos entre 2 entidades (originador & destinatário) não são legíveis/compreendidos por terceiras entidades (sem autorização) => Comunicação de dados com encriptação
- Gestão de chaves de encriptação 2,5/4
  - Garantia de distribuição segura de chaves
- Integridade: 2,5/4
  - Garantir que dados transmitidos não são alterados:
    - Acidentalmente por erros de transmissão
    - Propositadamente por terceira entidades sem autorização
  - Não-Repudiação: impossibilidade de negação de identidade

1.1 – Indique quatro das principais ameaças correntes à segurança de uma organização e respetivas medida/soluções para reduzir a probabilidade de sucesso dessas ameaças?

- Exploração de vulnerabilidades conhecidas: 2,5/4
  - Solução: atualizações periódicas de SW
- Receção e leitura de e-mails maliciosos com links HTML para sites com malware:2,5/4
  - Solução: não clicar em links de e-mails desconhecidos/estranhos
- Uso indevido da internet com acesso a sites com malware: 2,5/4
  - Solução: usar configurações de segurança em browsers + antivírus atualizados
- Dispositivos portáteis perdidos ou roubados: 2,5/4
  - Solução: gestão centralizada para controlo de dispositivos portáteis, com planeamento de ação a executar em caso de perda

(podiam ser indicadas outras ameças)

1.2 – Descreva de forma resumida como se poderá proceder o ataque por DNS Spoofing (resolução errada de nomes DNS) e quais as medidas a adotar para minimizar o sucesso do mesmo?

Spoofing é um tipo de falsificação tecnológica que procura enganar uma rede ou pessoa, fazendo acreditar que a fonte de informação é confiável, quando na verdade não é.
As medidas a adotar são:

- Usar autenticações baseadas em troca de chaves entre as máquinas da rede
- Usar uma lista de controlo de acesso para negar acesso a IPs privados na interface de downstream
- Implementar a filtragem de tráfego tanto nas portas de entrada como de saída
- Configurar os routers e switches para rejeitar pacotes que sejam originados fora da rede local, que supostamente estão com o endereço da rede interna
- Ativar sessões de criptografia no router, para que os hosts confiáveis que estão fora da rede possam comunicar de forma segura com os hosts locais.

1.2- Descreva de forma resumida como se poderá proceder o ataque por *MAC spoofing* (obtenção errada da endereços MAC) e quais as medidas a adotar para minimizar o sucesso do mesmo?

Cada sistema operativo guarda cache ARP (Address Resolution Protocol) com mapeamento entre endereços IP/MAC. Tabela com conteúdo dinâmico em função de respostas a novos pedidos ARP (para associar endereço MAC a IP).

- Procedimento de envenenamento de cache ARP:
  - Atacante altera mensagem ARP response e coloca endereço falso para onde as mensagens originadas no terminal requisitante do endereço serão redireccionadas
    2,5/2
    - Tipo de ataque MITM (Man In The Middle)
- Soluções:
  - Restringir a possibilidade de alterações de endereços MAC de terminais de redes fixas apenas aos seus administradores:
    2,5/4
    - Nas redes wi-fi públicas é difícil controlar acesso por MAC
  - Monitorização da rede para detecção de cenários estranhos: 2,5/4
    - Uso de IDS: Monitorização de tráfego em nós centrais que encaminham tráfego, ex. switches
      - Verificação de conteúdo de respostas ARP não solicitadas
      - Maior latência em fluxos de mensagens na rede

1.2 – Indique os principais requisitos que devem ser satisfeitos pelos protocolos para garantir a segurança das comunicações na internet?

- Autenticação de entidades 2,5/4
- Confidencialidade dos dados transmitidos 2,5/4
- Controlo de integridade de dados transmitidos 2,5/4
- Gestão de chaves de criptografia 2,5/4

GRUPO II

2.1 – Indique as razões da importância da implementação de mecanismos de segurança para os fornecedores de serviços na nuvem?

- Fiabilizar e credibilizar o uso desses serviços 2,5/2
  - Garantir boa reputação do fornecedor de serviços na nuvem
- Nível de segurança deverá ser igual ou superior ao cenário de rede com infraestrutura própria 2,5/2

2.1 – Indique e exemplifique estratégias que poderão ser usadas para efetuar ataques distribuídos para negação de serviço (DDoS)?

- Usar redes Botnets (rede de robots):

- Redes de computadores controladas por malware, que atacam terminais da rede sem serem detectados pelo utilizador legítimo

- Terminais infectados podem efectuar ataques coordenados à mesma vítima;

- Usar mecanismos de amplificação de tráfego de várias frentes

- Explorando as funcionalidades dos protocolos -> Ex: Endereços de difusão

- Explorando os mecanismos de pergunta/resposta -> Ex: Serviços de resolução de nomes DNS

2.1 – Descreva o procedimento de ataques distribuídos para negação de serviço (DDoS) e indique e exemplifique uma estratégia que poderá ser usadas pelos mesmos?

- Objectivo de DDoS: amplificar efeito de ataque DoS por ter origem em várias frentes de forma coordenada 2,5/2
- Usando redes Botnets (rede de robots): 2,5/2
  - Redes de computadores controlados por worms, que atacam máquinas remotas sem conhecimento do utilizador legítimo das mesmas
  - Possibilitar a worm interagir com servidor e explorar as suas vulnerabilidades ao nível da camada de aplicação
- Usando mecanismos de amplificação de tráfego: 2,5/2 (alternativa a botnets)
  - Explorando de funcionalidade dos protocolos
    - Ex. Endereços de difusão
  - Explorando mecanismos de pergunta/resposta
    - Ex. Serviços de resolução de nomes DNS

2.1 – Indique e exemplifique estratégias de ataques que poderão causar o efeito de negação de serviço (DoS)?

- Exploração de vulnerabilidades que provocam falhas no sistema 2,5/3
  - Ex. Ping-of-Death, enviar mensagem ping com grande dimensão (formato incorreto) para sobrecarregar terminal de vítima
    - Pacote IP c\ mensagem ICMP Echo Requet com dimensão superior a tamanho máximo suportado pelo IP: 64K
- Sobrecarga dos servidores com excesso de pedidos de acesso 2,5/3

Sobrecarga de rede de acesso a servidores com tráfego “inútil”

2.2 – Os IDS podem desempenhar uma função importante na segurança dos sistemas informáticos. Indique e descreva as principais funcionalidades dos IDS, que os distinguem das *firewalls* de rede?

- Além do tráfego externo, podem monitorizar o tráfego interno 2,5/3
- Não impedem ataques, mas geram notificações/comprovativos 2,5/3
- Ataques internos são menos prováveis, mas têm mais facilidade em causar danos
  2,5/3

2.2 – Indique os principais riscos de segurança da nuvem e as soluções a adotar para os minimizar?

- Garantir comunicação segura de dados privados: 2,5/5

o Solução => uso de VPN, se acesso for via redes públicas (internet):

- Autenticação
- Encriptação
- Controlo de integridade

- Controlo de acessos a recursos na nuvem: 2,5/5
  - o Soluções =>
  - Uso de Firewall de rede para controlo de acessos externo
  - Garantir isolamento de recursos de diferentes clientes

* Permissões com autenticação nos acessos =>

Impedir acessos a dados privados de outros clientes

* Uso de VLANs para separação de fluxos de tráfego de diferentes clientes

- Indisponibilidade de serviços / Isolamento de falhas
  2,5/5
  - Soluções (podem ter custo adicional para cliente):
    - Usar redundância de recursos
    - Realizar backups periódicos de dados
- Perda de Controlo 2,5/5
  - Solução: comprometer fornecedor a cumprir contrato
- Interface de gestão 2,5/5
  - Soluções:
    - Controlo de acessos rigoroso (*Firewall* aplicacional)
    - Uso de anti-virus actualizado

2.2 – Indique e descreva de forma resumida os elementos de rede que utilizaria para evitar o sucesso dos ataques que referiu na questão anterior?

- Firewalls: Implementação de política de segurança para defesa de perímetro da rede ⇔ recursos informáticos de uma organização: 2,5/2
    - Proteção/Defesa por "isolamento" de máquinas da rede interna:
        - Contra acessos externos não autorizados ao perímetro da rede
    - Controlo de acesso, fluxo e conteúdos
        - De interações autorizadas entre as redes interna e externa
- IDS: Deteção e notificação de atividades suspeitas: 2,5/2
    - Atividades anormais que possam corresponder a intrusões:
        - tentativas de acesso (externo ou interno) não autorizado a recursos da rede protegida => possibilidade de comprometer a integridade, confidencialidade ou disponibilidade de um recurso
    - Possibilidade de tomada de ações reativas contra intrusões detetadas

2.2 – As firewalls devem ser utilizadas para evitar o sucesso dos ataques informáticos. Descreva de forma resumida as principais funcionalidades das firewalls?

- Sobrecarga dos servidores com excesso de acesso

- Exploração de vulnerabilidades que provocam indisponibilidade nos sistemas

- Sobrecarga de rede de acesso a servidores com tráfego inútil

GRUPO III

3.1 – Indique e descreva os objectivos e vantagens de se utilizarem comunicações com VPNs?

* Possibilitam a interligação de redes privadas através de canais de comunicação seguros e virtual/ dedicados de redes públicas 2,5/3

* Redução de custos: 2,5/3

* Substituição de linhas dedicadas na interligação de LANs e WANs, por uso de internet

* Poupança de deslocações físicas

* Impulsionadas pela cada vez maior facilidade e velocidade de acessos a internet: 2,5/3

3.1 - O protocolo SSL/TLS é constituído por 4 sub-protocolos. Indique e descreva as principais funcionalidades do sub-protocolo de registos?

- Fragmentação de dados em bloco => adaptação de formato de transporte de dados a protocolos das camadas inferiores 2,5/5
- Compressão de blocos de dados => maior rapidez no transporte de dados 2,5/5
- Calcula e adiciona MAC a cada bloco, usando algoritmo e chave de encriptação definidos em *Handshake* => autenticação de origem de bloco de dados 2,5/5
- Encripta bloco com MAC (criptograma), usando algoritmo e chave de encriptação definidos em *Handshake* => garantir confidencialidade de bloco de dados 2,5/5

Entrega de criptograma a TCP (Nível 4) para serem transmitidos para a rede => transporte de dados na rede

3.1 – O protocolo SSL/TLS é constituído por 4 sub-protocolos. Indique e descreva as principais funcionalidades do sub-protocolo Handshake?

- Autentica as entidades em comunicação - Inicializa e sincroniza os estados das sessões e ligações a proteger - Estabelece os parâmetros de controlo da sessão

- Chaves de cifra e MAC

- Vetores de inicialização

- Números de sequência

- Negoceia os algoritmos usados pelo Protocolo de Registos

- Encriptação, controlo de integridade e compressão.

3.1- Indique e descreva o principal risco de segurança associado às comunicações sem fios e as medidas a adoptar para o minimizar?

 Meio de transmissão não guiado => mensagem difundida por uma determinada área de propagação do sinal da mensagem => facilitar interceção da mesma por outros utilizadores localizados nessa área e não apenas o destinatário da mensagem 2,5/2

 Transmissão de mensagens encriptadas com chave secreta apenas do conhecimento do emissor e receptor, de modo a que apenas este a possa desencriptar: 2,5/2

3.1 - O protocolo SSL/TLS (*Secure Socket Layer*/*Transport Layer Security*) é constituído por 4 sub-protocolos. Indique e descreva as principais funcionalidades do sub-protocolo de Registos (do SSL/TLS)?

- Fragmentação de dados em blocos 2,5/5
- Compressão de blocos de dados 2,5/5

Calcula e adiciona MAC a cada bloco, usando algoritmo e chave de encriptação definidos em *Handshake*

- Encripta bloco com MAC (criptograma), usando algoritmo e chave de encriptação definidos em *Handshake* 2,5/5
- Entrega de criptograma a TCP (Nível 4) para serem transmitidos para a rede 2,5/5

3.2 – Indique e descreva os principais melhoramentos introduzidos no protocolo WPA2 relativamente ao protocolo WPA (Wi-Fi *Protected Access*)?

WPA2 (WPA não tem estas características) possibilita maior segurança:

- WPA2 possibilita uma comunicação com maior segurança 2,5/3
- Encriptação mais forte (AES)*:* 2,5/3

Controlo de integridade de cabeçalho e dados mais forte

3.2 – Indique e fundamente o protocolo de segurança que melhor suporta o acesso via VPN de forma mais flexível e especifica a elementos de uma rede corporativa?

- SSL/TLS: 2,5/3
- Na rede corporativa o controlo de acesso é feito também no servidor, além da Firewall =>
    - poder ser usada para controlo de tráfego externo e interno 2,5/3
- Clientes poderão ou não utilizar SW e terminal corporativo 2,5/3
- Ex. webmail não necessita de SW específico e possibilita acesso de qualquer terminal, mesmo não corporativo via browser

3.2 – Indique e descreva as principais diferenças entre os protocolos WEP e WPA?

WPA (WEP não tem estas características):

 Diferentes chaves para autenticação, encriptação e integridade 2,5/4

 Encriptação de dados com recurso a chaves temporárias e diferentes para cada bloco de mensagens 2,5/4

- TKIP: Temporal Key Integrity Protocol

 Possibilidade de autenticação mútua entre STAs e APs 2,5/4

 Controlo de integridade com recurso a algoritmo de síntese MIC (Message Integrity Code) com chave específica: 2,5/4

GRUPO IV

4.1 – Indique e descreva as principais funcionalidades de segurança disponibilizadas pelo GSM (2G), suportadas pelo uso de cartões SIM (*Subscriber Identity Module*)?

* Autenticação da identidade do utilizador: 2,5/4
    - Para impedir o acesso à rede a utilizadores não autorizados, sempre que um TM pretender aceder à mesma, a sua identificação é requisitada e verificada
* Confidencialidade dos dados do utilizador: 2,5/4
    - Para proteger e garantir a confidencialidade dos dados contra intrusos, todas as mensagens dos utilizadores transmitidas na interface rádio são encriptadas
* Verificação de identificação do equipamento (IMEI): 2,5/4
    - Para impedir a utilização de equipamento não autorizado ou roubado, o operador pode verificar a identificação do mesmo (IMEI)
        - por exemplo, quando o correspondente utilizador efetuar uma tentativa de chamada
* Anonimato do utilizador: 2,5/4
    - Para impedir a identificação de um utilizador, a rede utiliza uma identificação temporária (TMSI) nas mensagens de sinalização transportadas na interface rádio
    - O TMSI é atribuído pelo VLR, após cada procedimento de *Location Update*

4.1 – Descreva as principais funcionalidades do protocolo IPSec?

Estabelecimento de associações de segurança (SA: Security Association) entre as entidades comunicantes

Garantia de autenticidade e integridade da informação, ao nível do IP: 2,5/3

Garantir que a fonte do pacote é de fato a indicada no cabeçalho

Garantir que o cabeçalho não foi alterado durante a transmissão

=> Inserção de cabeçalho de Autenticação (AH: *Authentication Header*) para garantir 1& 2.

Garantia de confidencialidade e integridade, ao nível do IP: 2,5/3

Garantir que nenhuma 3ª entidade maliciosa consiga ler ou alterar os dados transmitidos nos pacotes IP

=> Inserção de cabeçalho de segurança de dados/conteúdo encapsulado (ESP: *Encapsulation Security Payload*)

Suporte a dois modos de operação: 2,5/3

Modo Transporte: proteção de dados do utilizador (*payload*)

Modo Túnel: proteção de todo o pacote

4.2 – Descreva as principais caraterísticas que definem as "Associações de Segurança" no IPSec?

Conjunto de regras e parâmetros que possibilitam o estabelecimento de uma comunicação segura IPSec (autenticada + encriptada) entre 2 máquinas comunicantes:

Regras de segurança acordadas:
2,5/3

Algoritmo de encriptação (ESP)

Algoritmo de autenticação (AH)

Parâmetros relevantes especificados: 2,5/3

Chaves de cifra a usar

Vetores de inicialização

Identificador de SA: *Security Parameter Index* (SPI)

Endereço IP destino, para identificar direção de AS (unidirecional)

Modo do protocolo: túnel ou transporte

4.2 – Indique as principais funcionalidades de segurança introduzidas no UMTS (3G), suportadas pelo uso de cartões USIM (Universal Subscriber Identity Module), que o diferenciam do GSM?

- Algoritmo de encriptação reforçado (baseado em AES) e estendido à interface Nó-B/RNC - Proteger o troço Nó-B/RMC por se encontrar fora das instalações do operador

- Autenticação da rede para com o utilizador - Encriptação e controlo de integrdade e de mensagens de sinalização/controlo dos utilizadores

- Utilização de cinco parâmetros de autenticação e encriptação (quintets) com cartão USIM, em vez de três do GSM (triplets) com cartão SIM.