

### 1.a)

O fator humano é explorado em quase todas as fases de um ataque. Na aquisição de conhecimento, os atacantes utilizam engenharia social, phishing ou exploração de informações públicas. Durante a infiltração, são comuns técnicas como spear phishing, uso de macros maliciosas ou exploits em navegadores que dependem de erro humano. Na propagação, o fator humano permite elevação de privilégios devido a práticas inseguras, como passwords fracas ou reutilização de credenciais. Na fase de exfiltração, a falta de vigilância e de formação leva à não deteção de comportamentos anómalos, como uploads fora do normal para serviços legítimos.

### 1.b)

Para mitigar ataques baseados em fator humano, devem ser implementadas autenticação forte (802.1X), segmentação da rede com VLANs, microsegmentação com firewalls internas e políticas de Zero Trust. O uso de sistemas de deteção de intrusões (IDS/IPS), aliado a SIEM com análise de comportamento, permite identificar atividades atípicas. As portas devem ser protegidas com autenticação, e o acesso a recursos sensíveis deve requerer autorização centralizada (AAA). A filtragem de tráfego baseado em políticas nas firewalls e a inspeção de conteúdo TLS/HTTPS ajudam a detetar uso malicioso de canais legítimos.

### 2.a)

A arquitetura deve isolar logicamente as zonas com funções distintas:

- **DMZ pública**, contendo os servidores Web e de Email acessíveis da Internet.
- **Datacenter B**, zona interna para a Intranet, acessível apenas pelas VLANs 5 e 6.
- **Datacenter C**, zona de backups, acessível unicamente pelos servidores Web HTTPS e por um IP externo autorizado.

Devem ser colocadas firewalls entre a DMZ e os restantes domínios, e entre os Datacenters. A proteção contra DDoS exige balanceadores de carga à entrada da DMZ, filtros de tráfego baseados em volume e aplicação, e limitação de sessões. Recomenda-se ainda o uso de IPS inline na fronteira da DMZ. O tráfego entre zonas deve ser validado por firewalls stateful com regras específicas.

### 2.b)

Regras de firewall (nível alto):

1. Permitir TCP 443 de Internet para DMZ (servidores Web públicos).
2. Permitir TCP 465 de Internet e rede interna para os servidores de Email na DMZ.

3. Permitir TCP 443 da VLAN 5 e 6 para o servidor Web da Intranet no Datacenter B.
4. Permitir TCP 5001-5002 dos servidores Web HTTPS para Datacenter C.
5. Permitir TCP 5001-5002 de um único IP externo pré-definido para Datacenter C.
6. Bloquear por defeito qualquer tráfego não especificado.

Estas regras devem ser aplicadas em F3 (entre rede interna e DMZ), F4 (entre Datacenter B e C), e nas firewalls de borda.

### **3.**

Para garantir confidencialidade no tráfego entre os servidores para o Datacenter C via WAN, deve-se implementar túneis IPsec com modo túnel (gateway-to-gateway), usando encapsulamento ESP para garantir encriptação e integridade. A negociação das SAs pode ser feita com IKEv2 com autenticação por certificados digitais. Este túnel deve encapsular tráfego TCP nas portas 5001 e 5002 dos servidores Web HTTPS até ao Datacenter C. As firewalls devem ser configuradas para permitir ESP (protocolo 50) e UDP nas portas 500 e 4500 (IKE + NAT-T), com regras específicas para o tráfego IPsec entre os IPs internos das zonas envolvidas. A interface VTI pode facilitar a gestão do tráfego encapsulado.

#### **4.a)**

Para detetar acessos não autorizados a objetos nos servidores HTTPS, o SIEM deve integrar logs de servidores Web (como Apache/Nginx), com regras como:

- Alerta se forem feitas múltiplas tentativas de acesso a URLs protegidos com status 403 ou 401 num curto intervalo.
- Alerta se um utilizador tentar aceder a diretórios administrativos (ex: /admin, /config) sem estar autenticado.

#### **4.b)**

Para deteção de DDoS:

1. Alerta se houver mais de 100 conexões TCP simultâneas por segundo vindas do mesmo IP.
2. Alerta se for excedido o número normal de SYNs por segundo para os servidores da DMZ.
3. Alerta para padrões de tráfego anómalos com alta entropia (payloads randômicos).

#### **4.c)**

Para atividade de botnet:

- Alerta quando múltiplos terminais iniciam conexões para domínios dinâmicos ou recém-criados com baixa reputação.
- Alerta se forem detetadas conexões persistentes para hosts externos sem função normal conhecida.
- Alerta se for identificado tráfego outbound com payloads cifrados para portas não standard.

#### **4.d)**

Para exfiltração stealth:

- Alerta se um terminal envia dados de forma regular para serviços como Dropbox, Google Drive ou OneDrive, fora do horário normal ou com volume atípico.
- Alerta se houver uso de esteganografia em pacotes HTTPS (ex: uploads frequentes de imagens sem contexto funcional).
- Alerta se a taxa de transferência cumulativa por terminal ultrapassar o padrão diário médio com destino a serviços autorizados, mas fora do perfil típico do utilizador.