# 1 [**Q1962708**](https://www.qconcursos.com/questoes-de-concursos/questoes/ba670fd2-34)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2022 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[SEFAZ-AM](https://www.qconcursos.com/questoes-de-concursos/institutos/sefaz-am) **Prova:**[FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Tarde](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2022-sefaz-am-analista-de-tecnologia-da-informacao-da-fazenda-estadual-tarde)

Com relação à segurança dos contêineres Docker, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) Possuem isolamento no nível do processo no sistema operacional e isolamento adicional, usando recursos especiais tais como *namespaces* e *cgroups*.

( ) Aproveitam-se dos mecanismos *interprocess communication* padrão, tais como sinais, *pipes*e*sockets*, onde cada contêiner possui a sua própria *network stack*.

( ) Os contêineres possuem um *multi level security* no sistema operacional do *host* e os recursos físicos que são gerenciados por um *hypervisor* compartilhado.

As afirmativas são, na ordem apresentada, respectivamente,

**A** F – V – V. **B** F – F – V. **C** V – F – V. **D** V – F – F. **E** V – V – F.

baby\_yoda\_ti

26 de Outubro de 2022 às 23:17

**Com relação à segurança dos contêineres Docker, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.**

**(V) Possuem isolamento no nível do processo no sistema operacional e isolamento adicional, usando recursos especiais tais como *namespaces*e *cgroups*.**

**VERDADEIRO**

Um conteiner, seja ele qual for, é utilizado para isolar, ou encapsular, algumas partes do SO para que uma aplicação possa ser executada dentro do conteiner. Com o Docker não é diferente.

Esse conteiner permite isolar um conteiner do outro e também isolar recursos do sistema, tanto para limitar a quantidade de recursos que um conteiner pode utilizar, quanto para restringir ou permitir recursos a outros.

O recurso que é utilizado para gerenciar os recursos do sistema é conhecido como *cgroup*. O que isola as características do conteiner é conhecido como *namespace*.

**(V) Aproveitam-se dos mecanismos *interprocess communication* padrão, tais como sinais, pipes e sockets, onde cada contêiner possui a sua própria *network stack*.**

**VERDADEIRO**

Interprocess communication (IPC) é uma forma de comunicação interna entre os processos executados dentro de um conteiner. Esse processo de comunicação interna pode ser feito via sinal, em que um conteiner envia um sinal específico para um outro conteiner. Pode ser feito por meio de pipes, em que a saída de um processo é direcionado para a entrada de outro. E pode ser feito por meio de sockets, nesse caso, é possível a comunicação entre conteiners na mesma máquina, como ligados por uma rede.

Tudo isso é possível, pois cada conteiner possuia sua própria pilha de protocolos (*network stack*).

**(F) Os contêineres possuem um *multi level security* no sistema operacional do host e os recursos físicos que são gerenciados por um *hypervisor*compartilhado.**

**FALSO**

Volta e meia há uma comparação acontencendo entre Conteiners e VMs. Neste há hypervisor, naquele não há. Por conta disso, os conteiners são mais leves e mais rápidos de serem executados, ao passo que as máquinas virtuais demoram um pouco mais em sua execução.

Enfim não existe hypervisor em conteiners.

A ordem que temos é **V - V - F**.

# 2 [**Q1928124**](https://www.qconcursos.com/questoes-de-concursos/questoes/17260a1b-f1)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2022 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[MPE-GO](https://www.qconcursos.com/questoes-de-concursos/institutos/mpe-go) **Prova:**[FGV - 2022 - MPE-GO - Assistente Programador](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2022-mpe-go-assistente-programador)

Devido ao crescente número de ataques *ransomware* aos sistemas de uma empresa, a Chefe da Informática elaborou um documento com orientações de segurança para seus colaboradores que trabalham em home office.

Para proteção específica a contra-ataques *ransoware*, a Chefe da Informática orientou corretamente seus usuários a

**A** utilizar conta de usuário com perfil de administrador e restringir o máximo possível o uso de contas de usuário comum.

**B** manter o sistema operacional, antivírus e todos os demais programas instalados no computador em suas versões mais recentes.

**C** fazer backup dos dados regularmente e manter uma cópia armazenada no computador para agilizar o procedimento de recuperação caso necessário.

**D** configurar o software de correio eletrônico para que a auto execução de anexos dos e-mails esteja habilitada.

**E** configurar o antivírus para bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador.

Leandro Henrique

26 de Outubro de 2022 às 09:22

**GAB B**

**c)** O backup precisa ser armazenado em outro computador/rede

**e)** Tá falando de firewall (Q1955030)

Gabriel Veras

19 de Setembro de 2022 às 21:21

Não entendi direito por que a E estaria errada. Resposta B me parece mais certa porque é mais senso comum do que a E.

# 3 [**Q1902445**](https://www.qconcursos.com/questoes-de-concursos/questoes/a5a3ecf1-c7)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2022 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[PC-AM](https://www.qconcursos.com/questoes-de-concursos/institutos/pc-am) **Prova:**[FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2022-pc-am-perito-criminal-4-classe-processamento-de-dados)

Para tentar esconder evidências de um comprometimento de um sistema Windows 10, o invasor apagou alguns arquivos que estavam no disco C, que foram para a lixeira do Windows. Posteriormente, na análise forense desse sistema, o perito procurou verificar o caminho original desses arquivos e a data em que foram removidos.

O perito pode conseguir essas informações

**A** nos arquivos do diretório C:\Windows\RECYCLE.

**B** no arquivo com o nome C:\$Recycle.BIN\INFO2, contendo todos os metadados dos arquivos que estão na lixeira.

**C** nos arquivos com nomes iniciados com I$, localizados abaixo do diretório C:\$Recycle.BIN\\*.

**D** no arquivo com o nome C:\NTUSER.DAT, contendo todos os metadados dos arquivos que estão na lixeira.

**E** no Registry do Windows.

Patrick Coelho

20 de Setembro de 2022 às 00:28

Alguém pode comentar/explicar essa resposta, por gentileza?

# 4 [**Q928005**](https://www.qconcursos.com/questoes-de-concursos/questoes/31143d0b-b1)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2018 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[AL-RO](https://www.qconcursos.com/questoes-de-concursos/institutos/al-ro) **Prova:**[FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e Comunicação](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2018-al-ro-analista-legislativo-infraestrutura-de-redes-e-comunicacao)

A maior segurança dos sistemas operacionais, por exemplo, do sistema operacional Microsoft Windows 10 para, especificamente, reforçar o mesmo contra ameaças que exploram vulnerabilidades presentes nas distribuições originais do respectivo sistema operacional, pode ser alcançada por meio de

**A** análise de pacotes na rede.

**B** reinstalação do sistema operacional.

**C** instalação de *patches* de segurança.

**D** desconectar o computador hospedeiro do sistema operacional da rede de computadores.

**E** instalação de máquinas virtuais.

Rodrigo G. Marcelo

12 de Setembro de 2018 às 12:04

O processo de aplicação de patches de segurança rápido e robusto é uma contramedida absolutamente essencial para manter o ambiente seguro , apesar de nunca podemos levar em considerão 100%, porém essa ação já contribui para evitar possíveis danos.

Ibsen Maciel vulgo "Perito"

09 de Fevereiro de 2019 às 17:45

Gabarito C

As atualizações de software desempenham diferentes funções. Elas estão disponíveis para o sistema operacional e para programas de software individuais. A realização dessas atualizações implantará várias revisões em seu computador, como a adição de novos recursos, a remoção de recursos desatualizados, a atualização de drivers, a distribuição de correções para bugs e, o mais importante, a correção das brechas de segurança recém-descobertas.

# 5 [**Q899878**](https://www.qconcursos.com/questoes-de-concursos/questoes/f4655b80-63)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2018 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[Banestes](https://www.qconcursos.com/questoes-de-concursos/institutos/banestes) **Prova:**[FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2018-banestes-analista-em-tecnologia-da-informacao-suporte-e-infraestrutura)

Considere as seguintes permissões de acesso para a pasta intranet em um sistema operacional Linux:

drwxrw---- 2 root root 58 Mar 25 07:01 intranet

Para que os usuários do sistema pertencentes ao grupo intranet possam escrever na pasta em questão, é necessário executar o comando:

**A** chmod a-w intranet **B** chmod 765 intranet **C** usermod -a -G intranet intranet

**D** chown -R root:intranet intranet **E** chown root intranet

Vulgo Jhow

12 de Junho de 2018 às 10:35

Questão boa pra pegar os desatentos.

À principio, você julga que é preciso alterar as permissões, quando na verdade se deve alterar o grupo.

Sidnei Almeida

07 de Junho de 2018 às 20:01

**GABARITO: D**

**COMANDO *CHOWN***

**O comando chown executado pelo root permite alterar o proprietário ou grupo do arquivo ou diretório, alterando o dono do arquivo ou grupo.**

Priscila da Silva Moreira

18 de Abril de 2019 às 19:57

O “-R” no exemplo faz com que a alteração seja aplicada de forma recursiva, afetando todos os arquivos e sub-pastas. Sem ele, a alteração seria aplicada apenas à pasta propriamente dita, mas não ao seu conteúdo.

Luiz Ortiz - Max Q

20 de Agosto de 2018 às 12:39

Complementando ainda mais os comentários abaixo;

Sobre alguma possível dúvida da utilização dos  **dois pontos(:)** no gabarito da questão.

*"Para alterar o dono e o grupo deveremos utilizar o comando chown. O nome do dono deverá estar separado do nome do grupo por um ponto(.) ou por dois pontos(:)*"

Fonte: Descobrindo o Linux - João Mota Filho

Leandro Henrique

04 de Setembro de 2020 às 20:40

drwx**rw-**--- 2 **root (proprietário) root (grupo)** 58 Mar 25 07:01 intranet

Observe que o diretório não pertence ao grupo intranet. Por isso, é necessário alterar o grupo por meio do chown.

**A) chmod a-w intranet**: remove permissão de escrita do diretório intranet para todas as classes de usuários.

**B) chmod 765 intranet**: adiciona permissão rwx para o owner (root), rw para o grupo (root), rx para os demais.

**C) usermod -a -G intranet intranet**: adiciona o usuário intranet ao grupo com o mesmo nome.

**D) chown -R root:intranet intranet**: sintaxe é user:group, portanto, altera o owner novamente para root e o grupo passa a ser intranet. -R faz isso recursivamente aos demais subdiretórios.

**E) chown root intranet**: altera o proprietário novamente para root

# 6 [**Q873291**](https://www.qconcursos.com/questoes-de-concursos/questoes/8cf58f19-26)[Windows ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/windows)[Segurança de sistemas operacionais ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais)[Windows Server 2012](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/windows-server-2012) **Ano:**2018 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[Câmara de Salvador - BA](https://www.qconcursos.com/questoes-de-concursos/institutos/camara-de-salvador-ba) **Prova:**[FGV - 2018 - Câmara de Salvador - BA - Analista de Tecnologia da Informação](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2018-camara-de-salvador-ba-analista-de-tecnologia-da-informacao)

Maria, analista de suporte, utiliza ferramentas diversas para avaliar os riscos de segurança, identificar as atualizações de segurança ausentes e gerenciar o processo de segurança dos servidores de aplicações e web da empresa em que presta serviços. Os sistemas operacionais dos servidores são Windows Server 2012 R2 e Windows Server 2012.

Analise as afirmativas a seguir.

I. Microsoft Security Assessment Tool 4.0 é uma ferramenta de avaliação de riscos que fornece informações e recomendações sobre as práticas recomendadas de segurança em uma infraestrutura de TI.

II. Microsoft Baseline Security Analyzer 2.2 é uma ferramenta que identifica as atualizações de segurança ausentes e erros de configuração de segurança comuns.

III. Microsoft Security Compliance Manager 3.5 é a ferramenta que verifica a compatibilidade do sistema de arquivos com as políticas de segurança da informação baseadas na ISO/IEC 27001 e 27002.

Está correto somente o que se afirma em:

**A** I; **B** II; **C** III; **D** I e II; **E** II e III.

Sidnei Almeida

07 de Abril de 2018 às 12:42

**GABARITO: D**

**I) CERTO**

**II) CERTO**

**III) ERRADO - *O Microsoft Security Compliance Manager***(SCM) fornece políticas prontas para implementar com base nas recomendações do Guia de Segurança da Microsoft e nas melhores práticas do setor, permitindo que você gerencie facilmente o drift de configuração e os requisitos de conformidade de endereços para sistemas operacionais Windows e aplicativos Microsoft. Além dos principais recursos da versão anterior, o SCM 4.0 oferece suporte para linhas de base do Windows 10 e Server 2016 e correções de bugs. O SCM permite que você configure e gerencie rapidamente computadores e sua nuvem privada usando a Diretiva de Grupo e o Gerenciador de Configuração do Microsoft System Center.

*Fonte:*[*https://social.technet.microsoft.com/wiki/pt-br/contents/articles/37701.security-compliance-manager-scm-4-0-e-o-windows-server-2016-mcse.aspx*](https://social.technet.microsoft.com/wiki/pt-br/contents/articles/37701.security-compliance-manager-scm-4-0-e-o-windows-server-2016-mcse.aspx)

# 7 [**Q873286**](https://www.qconcursos.com/questoes-de-concursos/questoes/8ce55014-26)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2018 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[Câmara de Salvador - BA](https://www.qconcursos.com/questoes-de-concursos/institutos/camara-de-salvador-ba) **Prova:**[FGV - 2018 - Câmara de Salvador - BA - Analista de Tecnologia da Informação](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2018-camara-de-salvador-ba-analista-de-tecnologia-da-informacao)

Os sistemas operacionais modernos do tipo Unix-like tais como o Debian 9 oferecem aos administradores e analistas de suporte os mecanismos PAM (Pluggable Authentication Modules) e NSS (Name Service Switch).

Analise as afirmativas a seguir.

I. O PAM oferece um mecanismo de autenticação flexível, que é utilizado por aplicações e assim envolve trocas de permissões de acesso aos arquivos.

II. O NSS oferece um mecanismo de serviço de nomes flexível, que é utilizado frequentemente pela biblioteca C padrão para obter o nome do usuário e grupo para comandos, tais como o ls e o id.

III. O serviço LDAP utiliza os mecanismos PAM e NSS com os pacotes ldap-libpam e ldap-libnss para oferecer informações sobre as contas dos usuários do sistema.

Está correto somente o que se afirma em:

**A** I; **B** II; **C** III; **D** I e II; **E** I e III.

Ellen C.

04 de Outubro de 2018 às 14:05

**I. O PAM oferece um mecanismo de autenticação flexível, que é utilizado por aplicações e assim envolve trocas de permissões de acesso aos arquivos. (Errada)**- O propósito do do projeto PAM é separar a concessão de privilégios nos aplicativos do desenvolvimento de esquemas de autenticação apropriados e seguros. Isto é realizado fornecendo-se uma biblioteca de funções utilizada pelas aplicações para solicitar a autenticação de usuários.

**II. O NSS oferece um mecanismo de serviço de nomes flexível, que é utilizado frequentemente pela biblioteca C padrão para obter o nome do usuário e grupo para comandos, tais como o ls e o id. (Correta)**

**III. O serviço LDAP utiliza os mecanismos PAM e NSS com os pacotes ldap-libpam e ldap-libnss para oferecer informações sobre as contas dos usuários do sistema. (errada) -**O correto seria *libpam-ldap e libnss-ldap*

**GABARITO ITEM B**

[*https://www.vivaolinux.com.br/artigo/Uma-introducao-ao-LinuxPAM*](https://www.vivaolinux.com.br/artigo/Uma-introducao-ao-LinuxPAM)

[*https://wiki.debian.org/LDAP/NSS#NSS\_Setup\_with\_libnss-ldapd*](https://wiki.debian.org/LDAP/NSS#NSS_Setup_with_libnss-ldapd)

Leandro Henrique

13 de Outubro de 2020 às 15:28

Questão boa para avaliar a sorte dos candidatos

Leandro

12 de Outubro de 2020 às 14:04

tá de zueira cobrar nesse nível né? só tinha Linux e especificamente PAM no edital né? o google foi disponibilizado também para fazer a prova? pqp viu

# 8 [**Q827338**](https://www.qconcursos.com/questoes-de-concursos/questoes/402048d9-66)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2017 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[IBGE](https://www.qconcursos.com/questoes-de-concursos/institutos/ibge) **Prova:**[FGV - 2017 - IBGE - Analista Censitário - Análise de Sistemas - Desenvolvimento de Aplicações - Web Mobile](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2017-ibge-analista-censitario-analise-de-sistemas-desenvolvimento-de-aplicacoes-web-mobile)

Um dos fundamentos da arquitetura de segurança do Android é que, por padrão, cada aplicativo opera em uma sandbox de processo. Esse mecanismo de segurança isola a execução do aplicativo que precisa declarar no arquivo AndroidManifest.xml as permissões necessárias para acessar recursos que não são fornecidos pela sandbox básica.

A permissão que deve ser declarada para permitir que aplicativos abram soquetes de rede é:

**A** android.permission.ACCESS\_NETWORK\_STATE;

**B** android.permission.ACCESS\_WIFI\_STATE;

**C** android.permission.ACCESS\_INTERNET;

**D** android.permission.TRANSMIT\_IR;

**E** android.permission.INTERNET.

Francisco Borges

28 de Agosto de 2017 às 20:08

**a) android.permission.ACCESS\_NETWORK\_STATE;**

**Errado**. ACCESS\_NETWORK\_STATE permite que aplicativos acessem informações sobre as redes.

**b) android.permission.ACCESS\_WIFI\_STATE;**

**Errado.** ACCESS\_WIFI\_STATE  permite que aplicativos acessem informações sobre as redes WIFI.

**c) android.permission.ACCESS\_INTERNET;**

**Errado**. Não existe essa permissão no manifesto Android.

**d) android.permission.TRANSMIT\_IR;**

**Errado**. TRANSMIT\_IR  permite que aplicativos utilizem o transmissor IR (infravermelho) do dispositivo, se o mesmo estiver disponível.

**e) android.permission.INTERNET.**

**Certo**. INTERNET permite que aplicativos abram soquetes de redes.

Fonte: <https://developer.android.com/reference/android/Manifest.permission.html>

# 9 [**Q632538**](https://www.qconcursos.com/questoes-de-concursos/questoes/de9599b4-0e)[Apache ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/apache)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2016 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[IBGE](https://www.qconcursos.com/questoes-de-concursos/institutos/ibge) **Prova:**[FGV - 2016 - IBGE - Analista - Análise de Sistemas - Suporte Operacional](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2016-ibge-analista-analise-de-sistemas-suporte-operacional)

Os servidores HTTP podem estar sujeitos a ataques do tipo DoS. No entanto, os analistas de suporte operacional utilizam diversas medidas para mitigar tais ataques. São exemplos de diretivas dos servidores HTTP Server Apache (versão 2.4) que auxiliam a mitigar esses problemas:

**A** TimeOut e ProxyBlock; **B** KeepAlive e ProxySet; **C** LimitRequestLine e SessionMaxAge;

**D** MaxRequestWorkers e SSLVerifyClient; **E** RequestReadTimeout e KeepAliveTimeout.

Andrew S. Tanenbaum

10 de Julho de 2016 às 13:30

GABARITO E.

A grosso modo **RequestReadTimeout**é uma diretiva que permite limitar o tempo que um cliente pode levar para enviar um pedido.

Já a diretiva **KeepAliveTimeout** pode ser usada, apesar da baixa performance em alguns contextos, em sites que estão sujeitas a ataques DoS (Denial of Service), e preconiza que os valores das várias directivas relacionadas ao tempo limite fornecidos por outros módulos devem ser verificados.

Traduzido e adaptado de: <https://httpd.apache.org/docs/2.4/mod/core.htmlv>

Jonathan Clemente

21 de Maio de 2016 às 11:38

Denial of Service (DoS) attacks

All network servers can be subject to denial of service attacks that attempt to prevent responses to clients by tying up the resources of the server. It is not possible to prevent such attacks entirely, but you can do certain things to mitigate the problems that they create.

Often the most effective anti-DoS tool will be a firewall or other operating-system configurations. For example, most firewalls can be configured to restrict the number of simultaneous connections from any individual IP address or network, thus preventing a range of simple attacks. Of course this is no help against Distributed Denial of Service attacks (DDoS).

There are also certain Apache HTTP Server configuration settings that can help mitigate problems:

The **RequestReadTimeout** directive allows to limit the time a client may take to send the request.

The **TimeOut** directive should be lowered on sites that are subject to DoS attacks. Setting this to as low as a few seconds may be appropriate. As TimeOut is currently used for several different operations, setting it to a low value introduces problems with long running CGI scripts.

The **KeepAliveTimeout** directive may be also lowered on sites that are subject to DoS attacks. Some sites even turn off the keepalives completely via **KeepAlive**, which has of course other drawbacks on performance.

The values of various timeout-related directives provided by other modules should be checked.

The directives **LimitRequestBody**,**LimitRequestFields**, **LimitRequestFieldSize**,**LimitRequestLine**, and **LimitXMLRequestBody** should be carefully configured to limit resource consumption triggered by client input.

On operating systems that support it, make sure that you use the **AcceptFilter** directive to offload part of the request processing to the operating system. This is active by default in Apache httpd, but may require reconfiguration of your kernel.

Tune the **MaxRequestWorkers** directive to allow the server to handle the maximum number of simultaneous connections without running out of resources. See also the performance tuning documentation.

The use of a threaded mpm may allow you to handle more simultaneous connections, thereby mitigating DoS attacks. Further, the event mpm uses asynchronous processing to avoid devoting a thread to each connection. Due to the nature of the OpenSSL library the event mpm is currently incompatible with mod\_ssl and other input filters. In these cases it falls back to the behaviour of theworker mpm.

There are a number of third-party modules available through http://modules.apache.org/ that can restrict certain client behaviors and thereby mitigate DoS problems.

Fonte: <https://httpd.apache.org/docs/trunk/misc/security_tips.html>

Bonfim Martins da Silva

24 de Abril de 2022 às 20:02

Todos os servidores de rede podem estar sujeitos a ataques de negação de serviço que tentam impedir respostas aos clientes, limitando os recursos do servidor. Não é possível evitar totalmente esses ataques, mas você pode fazer algumas coisas para mitigar os problemas que eles criam.

Muitas vezes, a ferramenta **anti-DoS** mais eficaz será um firewall ou outras configurações do sistema operacional. Por exemplo, a maioria dos firewalls pode ser configurada para restringir o número de conexões simultâneas de qualquer endereço IP individual ou rede, evitando assim uma série de ataques simples. Claro que isso não ajuda contra ataques de negação de serviço distribuído (DDoS).

Há também algumas configurações do Apache HTTP Server que podem ajudar a mitigar os problemas:

A diretiva **RequestReadTimeout** permite limitar o tempo que um cliente pode levar para enviar a solicitação.

A diretiva **TimeOut** deve ser reduzida em sites sujeitos a ataques DoS. Definir isso para tão baixo quanto alguns segundos pode ser apropriado. Como o TimeOut é usado atualmente para várias operações diferentes, configurá-lo para um valor baixo apresenta problemas com scripts CGI de execução longa.

A diretiva **KeepAliveTimeout** também pode ser reduzida em sites sujeitos a ataques DoS. Alguns sites até desativam completamente os keepalives via KeepAlive, o que obviamente tem outras desvantagens no desempenho.

Os valores de várias diretivas relacionadas a tempo limite fornecidos por outros módulos devem ser verificados.

As diretivas **LimitRequestBody, LimitRequestFields, LimitRequestFieldSize, LimitRequestLine e LimitXMLRequestBody** devem ser cuidadosamente configuradas para limitar o consumo de recursos acionado pela entrada do cliente.

Nos sistemas operacionais que o suportam, certifique-se de usar a diretiva **AcceptFilter** para descarregar parte do processamento da solicitação para o sistema operacional. Isso está ativo por padrão no Apache httpd, mas pode exigir a reconfiguração do seu kernel.

Ajuste a diretiva **MaxRequestWorkers** para permitir que o servidor lide com o número máximo de conexões simultâneas sem ficar sem recursos. Consulte também a documentação de ajuste de desempenho.

O uso de um **mpm** encadeado pode permitir que você lide com mais conexões simultâneas, mitigando assim os ataques DoS. Além disso, o evento mpm usa processamento assíncrono para evitar dedicar um thread a cada conexão. Devido à natureza da biblioteca OpenSSL, o evento mpm é atualmente incompatível com mod\_ssl e outros filtros de entrada. Nestes casos, volta-se para o comportamento do trabalhador mpm.

Há vários módulos de terceiros disponíveis em http://modules.apache.org/ que podem restringir determinados comportamentos do cliente e, assim, mitigar problemas de DoS.

Fonte: <https://httpd.apache.org/docs/trunk/misc/security_tips.html>

# 10 [**Q608975**](https://www.qconcursos.com/questoes-de-concursos/questoes/bd411de5-d4)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2015 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[TJ-PI](https://www.qconcursos.com/questoes-de-concursos/institutos/tj-pi) **Prova:**[FGV - 2015 - TJ-PI - Analista Judiciário - Analista de Sistemas / Banco de Dados](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2015-tj-pi-analista-judiciario-analista-de-sistemas-banco-de-dados)

Em um ambiente com sistema operacional Windows, para criar um recurso compartilhado oculto, que não seja visível no Windows Explorer, deve-se:

**A** digitar $ como último caractere do recurso compartilhado;

**B** digitar # como primeiro caractere do recurso compartilhado;

**C** digitar & como último caractere do recurso compartilhado;

**D** digitar @ como primeiro caractere do recurso compartilhado;

**E** não é possível criar um recurso compartilhado oculto no sistema Windows.

Ibsen Maciel vulgo "Perito"

27 de Junho de 2017 às 08:46

Gabarito A

Ao criar o compartilhamento, digite $ após o nome... Por exemplo, pasta$. Não precisa renomear a pasta com o sifrão no final, nomeie ou renomeie apenas o nome do compartilhamento, que é um “apelido”, um “alias” para a pasta na rede.

Dessa forma ela não será exibida no Windows Explorer, isso inclui o Ambiente de rede (“Meus locais de rede”, nas versões mais recentes de Windows) e as janelas comuns “Abrir” e “Salvar”, “Procurar pasta”, etc.

Para acessá-la, você deverá digitar o caminho completo dela na barra de endereços ou no “Iniciar > Executar”.

O caminho completo é formado assim: “*\\nomedoservidor\pasta$*”. Ou seja, duas barras invertidas, o nome do computador onde a pasta ou recurso foi compartilhado, seguido do caminho dela. O “$” fará parte do nome da pasta, sempre ao referenciá-la, use esse caractere.

Veja que o nome da pasta compartilhada pode não coincidir com o nome da pasta real, ele é como um "apelido", um "alias" para a pasta na rede, como comentei mais acima.

Pollyana Villela

09 de Fevereiro de 2022 às 09:50

Para criar um recurso compartilhado oculto, que não seja visível no Windows Explorer, deve-se digitar um nome para a pasta ou unidade e coloque um sinal de cifrão ( $ ) no final do nome. Por exemplo, uma pasta com o nome " Myfiles " quando mudou para torná-lo escondido ficará " Myfiles $ . " O nome pode ter até 12 caracteres. Agora , a pasta está oculto e outros usuários da rede não será capaz de notá-lo , e ele não vai aparecer em Meus Locais de Rede . O único método qualquer um será capaz de ver a pasta é se eles sabem o nome da pasta.

Disponível em/:

<http://ptcomputador.com/Networking/other-computer-networking/78695.html>

# 11 [**Q576325**](https://www.qconcursos.com/questoes-de-concursos/questoes/3b19b07f-8b)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2015 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[DPE-RO](https://www.qconcursos.com/questoes-de-concursos/institutos/dpe-ro) **Prova:**[FGV - 2015 - DPE-RO - Analista da Defensoria Pública - Analista de Redes e Comunicação de Dados](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2015-dpe-ro-analista-da-defensoria-publica-analista-de-redes-e-comunicacao-de-dados)

Considere um sistema operacional que utiliza um mecanismo para gerenciamento de permissões de arquivos, como medida de segurança, que define a possibilidade de usuários acessarem e alterarem arquivos. Cada arquivo possui uma permissão representada por três partes que indicam as ações permitidas para o dono do arquivo, o grupo do arquivo e demais usuários, respectivamente. Cada uma destas partes é rotulada usando as letras rwx que descrevem permissões para leitura (r=read), escrita (w=write) e execução (x=execute). Um traço no lugar da letra proíbe a respectiva ação. Com base nessa informação, a opção que permite que um arquivo seja executado apenas pelo dono e pelo grupo do arquivo, possa ser lido e alterado apenas pelo dono, e não dê qualquer permissão aos demais usuários, é:

**A** - w x - - x - - - **B** r w - r w - r w - **C** r w x r - x - - - **D** r w x - - x - - - **E** r w x - - - - - x

Sávio Carneiro

02 de Abril de 2016 às 11:09

Depois da aula particular que a excelentíssima banca examinadora deu para o candidato no enunciado, era necessário muito esforço para errar essa questão.

WENDELL LOPES

14 de Dezembro de 2015 às 23:39

-rw-rw-r-- 1 aluno curso 1024 Fev 13 10:55 teste

A primeira coluna mostra as permissões de acesso dos subdiretórios e arquivos.

O primeiro caractere diz qual é o tipo do objeto:

**-** para arquivo comum;**b** para dispositivos de bloco (oferecem grandes quantidades de dados de cada vez).**c** para dispositivo de caracteres (oferecem dados de um caractere de cada vez);**d** para diretório;**l** para link simbólico;**p** para FIFO ou Named Pipe;**s** para socket mapeado em arquivo;

Os três caracteres seguintes mostram as permissões do dono (permissão de leitura e escrita).

O quinto, o sexto e o sétimo caracteres dizem quais as permissões do grupo (permissão de leitura e escrita).

Os três últimos caracteres especificam as permissões dos outros (permissão de leitura).

Como não há qualquer permissão especial definida no exemplo, é possível dizer que o arquivo teste tem permissão 0664.

Eduardo Santos

02 de Maio de 2022 às 10:12

A ordem é seguinte: Dono; Grupo; Outros

**r** ( Read ou Leitura);**w**(Write ou Escrita);**r** (Execute ou Execução do verbo executar)

O "**-** "(traço) significa que nenhum permissão foi concedida.

# 12 [**Q486915**](https://www.qconcursos.com/questoes-de-concursos/questoes/58412bd5-cf)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2015 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[DPE-MT](https://www.qconcursos.com/questoes-de-concursos/institutos/dpe-mt) **Prova:**[FGV - 2015 - DPE-MT - Analista de Sistemas](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2015-dpe-mt-analista-de-sistemas)

O *User Access Control*(UAC), recurso disponível nos sistemas operacionais Windows, a partir da versão “Vista”, é, algumas vezes, visto como um fator indesejado por solicitar confirmação do usuário para ações entendidas como corriqueiras. Entretanto, o UAC pode ser explorado de outras formas. Sobre o UAC, analise as afirmativas a seguir.

I. Ações de acesso podem ser registradas no log de eventos do Windows.

II. Aplicações específicas podem ser bloqueadas pelo administrador.

III. Aplicações assinadas digitalmente por uma autoridade de certificação reconhecida podem ser excluídas das solicitações de confirmação.

Assinale:

**A** se somente a afirmativa I estiver correta.

**B** se somente a afirmativa II estiver correta.

**C** se somente a afirmativa III estiver correta.

**D** se as somente as afirmativas I e II estiverem corretas.

**E** se todas as afirmativas estiverem corretas.

Sávio Carneiro

22 de Março de 2016 às 19:50

Nas provas da FGV isso não é raro.

É lógico que não na mesma prova, mas fazendo vários exercícios de provas diferentes dá para perceber que eles gostam desse tipo de questão em que todas as alternativas estão corretas.

Rodrigo G. Marcelo

05 de Setembro de 2015 às 13:29

Todas estão certas . mas da um nó quando todas estão certa raro isso

# 13 [**Q465296**](https://www.qconcursos.com/questoes-de-concursos/questoes/c0007b60-a7)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2014 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[PROCEMPA](https://www.qconcursos.com/questoes-de-concursos/institutos/procempa) **Prova:**[FGV - 2014 - PROCEMPA - Analista em TI e Comunicação - Analista em Infraestrutura e Redes Computacionais](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2014-procempa-analista-em-ti-e-comunicacao-analista-em-infraestrutura-e-redes-computacionais)

Um computador utilizando Windows Server passou a ter um comportamento estranho, o que levou à suspeita de contaminação por um vírus. Verificou-se que alguns processos “desconhecidos” estavam sendo carregados na inicialização do sistema.

Para desabilitar o carregamento desses processos, os nomes dos programas foram verificados e removidos

**A** no arquivo c:\autoexec.bat. **B** usando o programa msc.exe. **C** através do gerenciador de tarefas.

**D** no registro do sistema (*registry).* **E** usando o comando “net use”.

Paulo Sizino

06 de Maio de 2015 às 11:30

Questão pode ser anulada, pois, a partir do windows server 2012 é possível desabilitar a inicialização de processos pelo gerenciador de tarefas e também pelo registry, como não informa qual o Windows Server é usado, poderia dar entrada em recurso.

# 14 [**Q465286**](https://www.qconcursos.com/questoes-de-concursos/questoes/b2614896-a7)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2014 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[PROCEMPA](https://www.qconcursos.com/questoes-de-concursos/institutos/procempa) **Prova:**[FGV - 2014 - PROCEMPA - Analista em TI e Comunicação - Analista em Infraestrutura e Redes Computacionais](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2014-procempa-analista-em-ti-e-comunicacao-analista-em-infraestrutura-e-redes-computacionais)

Leia o fragmento a seguir.

Recentemente foi divulgada uma vulnerabilidade de segurança chamada *Shellshock*, que afeta um dos mais populares interpretadores de comandos usados no Linux, conhecido como *Bash*. Essa vulnerabilidade afeta o recurso do interpretador que é usado para o armazenamento e compartilhamento de parâmetros por diversos programas.

Assinale a opção que apresenta o nome correto do recurso citado no fragmento acima.

**A** Variáveis de sistema. **B** Parâmetros *Bash.* **C** Registro do sistema.

**D** Parâmetros do ambiente. **E** Variáveis de ambiente.

Sidnei Almeida

12 de Outubro de 2015 às 12:02

**GABARITO: E**

Outra forma usada por esses scripts para gerar conteúdo são as *variáveis de ambiente*. Elas são responsáveis por informar valores como o sistema operacional do usuário, sua versão, hora ou data. É através dessas informações que uma página sabe, por exemplo, se o usuário está acessando de um desktop ou dispositivo móvel. Embora essas variáveis sejam definidas pelo sistema, é possível modificá-las manualmente e enganar o servidor, fazendo com que ele acredite que você está usando um sistema operacional ou navegador diferente.

# 15 [**Q444754**](https://www.qconcursos.com/questoes-de-concursos/questoes/1d33eeee-65)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2014 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[TJ-GO](https://www.qconcursos.com/questoes-de-concursos/institutos/tj-go) **Prova:**[FGV - 2014 - TJ-GO - Analista Judiciário - Análise de Sistemas - Suporte Técnico](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2014-tj-go-analista-judiciario-analise-de-sistemas)

As permissões de acesso servem para proteger o sistema de arquivos Linux do acesso indevido de pessoas ou programas não autorizados.

Observe abaixo um exemplo de uso das permissões de acesso a um arquivo no GNU/Linux (obtido com o comando ls –la):

-rwxr-xr-- 1 jose user 8192 nov 4 16:00 teste

Com essas permissões de acesso, é possível:

I - ao usuário dono do arquivo ler e alterar seu conteúdo e executar o arquivo;

II - aos usuários que pertencem ao grupo do dono do arquivo ler seu conteúdo e executar o arquivo;

III - ao usuário dono do arquivo somente ler o conteúdo do arquivo;

IV - a todos os usuários, menos o dono e os que pertencem ao grupo do dono, ler, alterar seu conteúdo e executar o arquivo.

É correto apenas o que se afirma em:

**A** I e II; **B** II e III; **C** I e IV; **D** III e IV; **E** II e IV.

Luis

10 de Janeiro de 2015 às 15:27

-rwxr-xr-- 1 jose user 8192 nov 4 16:00 teste

-  rwx   r-x   r--

-       indica que é um arquivo

rwx   indica as permissões do proprietário do arquivo.

        Permissão para leitura, gravação e execução do arquivo respectivamente.

r-x    indica as permissões do grupo ao qual o usuário pertence.

        Permissão de leitura e execução apenas.

r--    indica as permissões dos demais usuários. Apenas leitura.

# 16 [**Q373178**](https://www.qconcursos.com/questoes-de-concursos/questoes/e1e3e2b0-ce)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2014 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[DPE-RJ](https://www.qconcursos.com/questoes-de-concursos/institutos/dpe-rj) **Prova:**[FGV - 2014 - DPE-RJ - Técnico Superior Especializado - Suporte](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2014-dpe-rj-tecnico-superior-especializado-suporte)

Em um ambiente Linux, para poder atribuir permissões avançadas de acesso a arquivos usando ACL, é requisito indispensável

**A** usar a distribuição SuSe. **B** usar o sistema de arquivos ext4.

**C** usar a versão 2.2 do kernel. **D** ter a partição onde esses arquivos residem montada com a opção ACL.

**E** ativar o modo de compatibilidade com BSD.

Eduardo Carianha

15 de Abril de 2015 às 09:33

a) usar a distribuição SuSe. - **Falso**, pois pode usar ACL em outras distribuições.

b) usar o sistema de arquivos ext4 - **Falso**, pois também é suportado por partições ReiserFS, Ext2, Ext3, JFS e XFS.

c) usar a versão 2.2 do kernel -**Falso**, pois o Linux só suporta nativamente desde o **Kernel 2.6.**

d) Ter a partição onde esses arquivos residem montada com a opção ACL. - ***Correto*** é necessário baixar o ACL e fazer as devidas montagem com a opção ACL  por ex: /dev/sda1 / reiserfs noatime,notail,acl 0 1e # mount / -o remount,acl.

e) ativar o modo de compatibilidade com BSD - **Falso**. Não tem nada haver.

Ibsen Maciel vulgo "Perito"

07 de Novembro de 2017 às 12:40

Gabarito D

Na tecnologia da informação, uma **lista de controle de acesso** (**ACL**, do inglês *Access Control List*) é uma lista que define as permissões de acesso de um usuário à um determinado componente ou serviço de um sistema, como um arquivo ou diretório[1][2].

Para que um servidor forneça acesso a um recurso, ele antes consulta a lista para verificar se o dispositivo que o está requisitando possui permissão para utilizá-lo. As listas de controle de acesso normalmente definem suas permissões com base em atributos do requisitante e do recurso solicitado, como a identificação do usuário, local de acesso, horário, nome do arquivo e endereço de rede.

Existem firewalls que fazem uso de listas de controle de acesso para a filtragem de pacotes de entrada e de saída.

# 17 [**Q609292**](https://www.qconcursos.com/questoes-de-concursos/questoes/e84deb35-d5)[Linux ,](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/linux)[Segurança de sistemas operacionais](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-sistemas-operacionais/seguranca-de-sistemas-operacionais) **Ano:**2013 **Banca:**[FGV](https://www.qconcursos.com/questoes-de-concursos/bancas/fgv) **Órgão:**[INEA-RJ](https://www.qconcursos.com/questoes-de-concursos/institutos/inea-rj) **Prova:**[FGV - 2013 - INEA-RJ - Analista de Sistemas](https://www.qconcursos.com/questoes-de-concursos/provas/fgv-2013-inea-rj-analista-de-sistemas)

No sistema operacional Linux o usuário *root* é o único que possui permissão de escrita no arquivo /etc/passwd. Entretanto, o comando *passwd*permite aos usuários comuns alterar algumas informações contidas no arquivo /etc/passwd.

Assinale a alternativa que explica corretamente como isso   é possível.

**A** O comando *passwd*possui o usuário *root*como proprietário e tem o *bit setuid* ativado. Ele é então executado com o EUID do usuário *root*e não do usuário comum, permitindo que o arquivo /etc/passwd seja modificado.

**B** O comando *passwd*possui o usuário *root*como proprietário e tem o *bit sticky* ativado. Ele é então executado com o EUID do usuário *root*e não do usuário comum, permitindo que o arquivo /etc/passwd seja modificado.

**C** O comando *passwd*possui o usuário *root*como proprietário e tem o *bit sticky* ativado. Ele é então executado com o UID do usuário *root*e não do usuário comum, permitindo que o arquivo /etc/passwd seja modificado.

**D** O comando *passwd*possui o usuário *sys*como proprietário e tem o *bit setuid* ativado Ele é então executado com o EUID do usuário *sys*e não do usuário comum, permitindo que o arquivo /etc/passwd seja modificado.

**E** O comando *passwd*possui o usuário *sys*como proprietário e possui o *bit sticky* setado. Ele é então executado com o UID do usuário *sys*e não do usuário comum, permitindo que o arquivo /etc/passwd seja modificado.

Nixon

20 de Maio de 2022 às 04:57

B e C = Se tem o STICKY BIT ATIVADO APENAS O DONO VAI PODER MEXER

D e E = USUÁRIO SYS É LHUFAS

GABARITO A

COMO O SET UID ESTÁ ATIVADO QUALQUER UM USUÁRIO TEM O MESMO PODER QUE O ROOT EM ARQUIVOS EXECUTÁVEIS.

TG

25 de Março de 2023 às 23:01

**Sticky Bit** - só permite modificação do usuário **root** ou o **dono**, mesmo que um grupo ou outros tenham permissão de modificação.

Se os usuários **comuns** podem modificar o arquivo **etc/passwd** não cabe o uso do **sticky bit**