



Descrição:

A aquisição de servidor dedicado com administração GCTEC Sistemas é Linux com cPanel e nós faremos toda a instalação, configuração e testes de todos os componentes do serviço. Não usamos scripts para este serviço, personalizamos todos os componentes manualmente para obter a instalação e configuração correta requerida pelo servidor.

Este serviço é para ajudá-lo:

- A assegurar seu servidor contra ataques
- Otimizar o servidor para o melhor uso da CPU
- Fornecer relevantes informações de seu servidor para identificar todas as rupturas da segurança e comportamento anômalo (monitoração contínua)
- Checar a existência de exploits instalados ou em execução no servidor
- Monitoração, intervenção e atualização de aplicativos sempre que necessário

Todo o serviço será executado em até 72 horas, compreendendo-se a entrega do servidor, configuração básica do cPanel, zonas de DNS, planos e contas. Após os testes preliminares do servidor, dos planos e testes de envio e recepção de e-mail, serão executados todos os outros serviços relacionados na tabela abaixo e estes passarão a ser à base de segurança do servidor, bem como a nossa monitoração e intervenção sempre que for necessário:

Pacotes de serviço cPanel	Descrição
iptables SPI firewall (csf) **	csf é um completo e caracterizado SPI (Pacote de Inspeção de Estabilidade) aplicação da configuração do firewall, iptables escrita por nós
Detecção de falha de login (lfd)	O lfd é integrado com o csf para bloquear tentativas de ataque via login, usuários inválidos
Desativar processos desnecessários	Análise de configuração de serviço ativo padrão do OS que não é usado por um servidor web com cPanel e pode ser um risco de segurança se continuar em uso
Logcheck	Logcheck é configurado para enviar arquivos de log por e-mail a cada hora usando expressão regular combinando os principais arquivos de log do servidor
Logwatch	Logwatch é um relatório diário que resume informações contidas nos principais arquivos de log do servidor
Checagem da configuração do WHM	Analisa as opções de configuração do WHM verifica segurança, performance e altera o que julga apropriado
Checagem da configuração do OpenSSH	OpenSSH é checado para garantir que somente o protocolo SSHv2 esteja ativo
Aterar de proftpd para pure-ftpd	Pure-ftpd é considerado mais leve e com maior segurança nas comparações de servidores com cPanel e proftpd
Rootkit Hunter	Rootkit Hunter é uma ferramenta essencial para detectar possíveis instalações de rootkit
Chkrootkit	Chkrootkit é outra essencial ferramenta para detectar possíveis rootkit's, em complemento ao rkhunter com diferentes regras de detecção
mod_security	O módulo apache mod_security é uma camada de segurança no apache que previne o servidor contra exploits de scripts web vulneráveis. Instalamos e configuramos estas linhas do apache para serem usadas com o módulo WHM que limitando a versão e configuração do mod_security
mod_evasive	O modulo apache mod_evasive é uma camada de segurança que previne tipos de ataques Denial of Services no apache. Porém, quando o implementamos podem causar efeitos colaterais nas extensões do FrontPage, portanto você não deve habilitar as extensões do FrontPage para seus clientes..
Host spoof protection	Previne contra IP spoofing e DNS cache poisoning
Operating System check	Checa o OS do servidor quanto a atualizações, se não estiver atualizado, executa a atualização
Name server configuration check	Se o nome servidor (name server (bind)) estiver

	ativo, checa se está funcionando corretamente e ativa DNS lookups
Disk check	Assegura que os discos estão montados corretamente e limpa qualquer arquivo antigo para liberar o maior espaço possível
Kernel check	Checa se é o Kernel correto que está instalado e atualiza para o mais atualizado se necessário e implementa ferramentas para prevenir contra possíveis ameaças (e.g. disabling core file creation)
Apache tune and check	Checa se o apache foi configurado corretamente para sua necessidade com a última versão estável
MySQL tune and check	Checa se o MySql foi configurado corretamente para sua necessidade com a última versão estável
Enhanced log rotation	Nem todos os servidores tem os arquivos de logs corretamente atualizados com o sistema padrão do cPanel, portanto instalamos (logrotate) que garante que estão corretamente configurados para uma melhor performance e estabilidade do sistema
Additional backup rotations	Se você tem discos de backups separados e tem suficiente espaço para adicionais atualizações, adicionamos um backup rotativo configurado "em um dia da semana" onde o sistema cPanel é configurado diária, semanal e mensalmente com os ciclos de backup
Secure /tmp /var/tmp /dev/shm	Estes diretórios são remontados com noexec e nosuid com uma adicional camada de proteção contra web script hackers
Libsafe for 2.4 kernels	OS's antigos (e.g. FC1, RH9 e RH7.3) podem ser beneficiados pelo libsafe que ajuda a proteger contra hacker stack smashing techniques que possam obter acesso root
Exploit check	Uma checagem dos scripts web instalados de conhecidos scripts hacking onde destacamos os (exploited web applications). Também checa o abuso de espaço dos diretórios /tmp e /dev/shm de qualquer exploits ativos além de escanear os processos ativos. Também desabilita qualquer versão de phpBB insegura.
Explorer (cse)	cse permite que você navegue por sua estrutura de diretórios e modifique tarefas shell diretamente pelo WHM o que é bastante prático se o SSH falhar por alguma razão
Mail Queues (cmq)	cmq permite que você cheque diretamente pelo WHM e administre as filas (queues) exim do servidor os e-mails individuais na espera para serem entregues
Mail Manage (cmm)	cmm permite que você veja e edite contas de e-mail e quotas de seus clientes diretamente pelo WHM

	sem a necessidade de logar no cPanel
Perl installation check	Checa se o apache está corretamente instalado e configurado e se é a última versão e atualiza se necessário
Delete unnecessary OS users	Na instalação padrão do OS, muitas contas de usuários são criadas desnecessariamente causando riscos de segurança
Disable open DNS recursion	Protege contra abuso e envenenamento do cache do DNS local se o DNS server (bind) estiver ativo
Enhanced path protection	Protege contra clientes e hackers de navegar e acessar arquivos fora do diretório de suas contas
Remove SUID/GUID from binaries	Na instalação padrão do OS muitas aplicações binárias tem bits SUID e GUID que não são necessárias e podem expor a riscos de segurança
PHP hardening	Dynamic Library loading são desabilitadas e abusos comuns de funções de php também são desabilitadas para prevenir vulnerabilidade de scripts php contra hackers
Exploit cleanup if required	Se forem encontrado exploits no servidor, estes serão limpos – isto não inclui a restauração de arquivos web comprometidos
Initial cPanel configuration	O cPanel será entregue completamente configurado e pronto para ser usado
MailMan performance	Ferramentas para ajudá-lo a otimizar o MailMan quando o servidor estiver ocupado
Munin Service monitor	Munin, os gráficos reportam o desempenho do servidor
MailScanner Server service	<i>O serviço MailScanner está incluído no cPanel Service Package + MailScanner package</i>
Monitoração, atualização e intervenção	<i>Monitoração contínua dos serviços, atualização de pacotes quando necessários e intervenção para recuperação ou resgate do servidor, não inclui reinstalação de OS, pacotes ou aplicativos</i>