**Proteção de Acesso Remoto**

**1. TCP Wrapper**

O TCP Wrapper é um sistema de rede baseado em ACL (Access Control List) de hots, usado para filtrar o acesso a serviços de rede compatível. Não é recomendado o uso do TCP Wrapper em sistemas que existem no Netfilter (IPTables), porém em sistemas embarcados onde memória e espaço de armazenamento é limitado só temos como opção o uso do TCP Wrapper.

Ele é utilizado para filtrar serviços que utilizam o protocolo de internet TCP tais como: SSH, FTP, TELNET, etc.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 026: Política de controle de acesso.

9.1.1 - Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios. (ABNT, NBR 27002, 2013, p.23)

. Controle 027: Acesso às redes e aos serviços de rede.

9.1.2 - Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados para utilizar. (ABNT, NBR 27002, 2013, p.25)

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27)

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33)

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54)

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67)

**2. Proteção do acesso remoto via SSH**

O SSH (Secure Shell) é o um dos serviços de acesso remoto para o gerenciamento da máquina de forma segura. Sua comunicação entre o cliente e o servidor se da de forma criptografada, sendo um protocolo para substituir o acesso através do TELNET, RLogin, RSH e REXEC que trafegam seus dados de forma insegura (texto puro), e por isso, altamente recomendado o uso do SSH.

E mesmo assim, ainda é necessário configuramos ele de forma que o acesso seja controlado e com a possibilidade de rastreabilidade, além de auditável.

Para isso devemos:

* Configurar o arquivo de configuração (/etc/ssh/sshd\_config) de forma que garanta a segurança do serviço 🡪 Vamos editar o arquivo de configuração do ssh em */etc/ssh/sshd\_config*. Podemos deixá-lo mais seguro fazendo algumas modificações básicas.
* Limitar o acesso por tempo através do PAM 🡪 Podemos utilizar o PAM para limitar o horário de acesso ao serviço de ssh, para garantir que os usuários terão acesso ao serviço apenas em horário permitido.
* Restringindo o acesso ao SSH via grupo de e usuários ou ACL em arquivos 🡪 Aqui iremos garantir o controle de acesso aos usuários que tem permissão explicitamente.
* Limite de logins consecutivos 🡪 Para evitar que um único usuário seja usado por diversas pessoas podemos restringir o número de logins consecutivos que este usuário pode fazer.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27)

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31)

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31)

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33)

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54)

. Controle 065: Registro de eventos (log) de administrador e operador

12.4.3 - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.56)

. Controle 071: Controles de redes

13.1.1 - Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações. (ABNT, NBR 27002, 2013, p.61)

. Controle 072: Segurança dos serviços de rede.

13.1.2 - Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados. (ABNT, NBR 27002, 2013, p.61)

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67)

. Controle 111: Regulamentação de controles de criptografia

18.1.5 - Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentação pertinentes (ABNT, NBR 27002, 2013, p.94)

**3. Segurança nos terminais**

Quando falamos em segurança, a primeira coisa que vem à mente é um possível ataque remoto. Então, os nossos servidores que não estão conectados à Internet não estão correndo nenhum perigo, certo? Errado, aliás, dois fatores estão errados. Não está conectado diretamente à Internet, não quer dizer que está totalmente seguro, pois, se um cracker conseguir passar pelo nosso firewall, ele vai conseguir acesso às outras máquinas que estão conectadas à rede interna e não necessariamente conectada diretamente à Internet.

Outro fator é funcionários mal-intencionados, com acesso local (físico) aos servidores. Muitas vezes quem entende de tecnologia costuma subestimar as pessoas com cargos mais braçais. Ledo engano, pois esse pessoal tem computadores em suas casas e mesmo sem intenções maliciosas podem causar problemas ao ver um terminal em sua frente. Além disso, se por um descuido da equipe de TI, um funcionário mal-intencionado conseguir acesso ao Datacenter, se passando por não entender nada de informática, pode na verdade ser um espião industrial com conhecimentos superior aos seus!

**3.1 - Remoções dos Shell desnecessárias**

Vamos remover os Shell válidas de todos os usuários que não vão executar oficialmente login no sistema, por meio de um terminal local (tty) ou via SSH. Isso garante que se uma aplicação for executada por um usuário como www-data, que é usado para subir o serviço de WEB, e for comprometido, esse usuário não poderá efetuar login.

Observação: crie um usuário que utilizaremos para administrar o servidor (sem permissões privilegiadas) e atribua uma senha para esse usuário.

**3.2 - Acessos aos Terminais da Console**

Por questões de segurança não é interessante deixarmos o login habilitado em todos os terminais de texto. Por isso, vamos desabilitar alguns terminais, deixando somente dois disponíveis. Você poderá escolher quais terminais você deseja bloquear.

**3.3 - Reboot**

Caso seu sistema tenha teclado conectado, por default, qualquer um poderá reinicializar o sistema sem efetuar login. Por medidas de segurança é bom ter o controle dos acessos, inclusive de quem reinicia a máquina. Para desativar o uso do Ctrl+Alt+Del, como forma de reiniciar o sistema sem a necessidade de login, devemos editar o arquivo/etc/inittab.

**Observação:** Isso também evitará que um servidor Linux em um mesmo rack que outro servidor com sistema operacional Windows® possa ser reiniciado por engano, pois o CTRL+ALT+DEL no Windows® tem outro contexto, o de apresentar a tela de login e não de reiniciar o sistema operacional.

Enquanto alguns promovem o CTRL+ALT+DEL, outros não gostam de usá-lo tanto assim.

O Linux é um sistema muito estável, porém como qualquer outro software, poderá falhar em algum momento, onde nem CTRL+ALD+DEL poderá te ajudar. Neste momento você poderá usar um recurso de Kernel chamado “Magic SysRq key”. Com ele você poderá desligar o sistema sem comprometer o seu filesystem (coisa que um desligamento forçado, pressionando o botão de liga/desliga faz).

Suas principais funções são:

• ALT+SysRq+r 🡪 Tira o teclado e o mouse do controle do Servidor X. Isso pode ser útil quando o seu Servidor X estiver travado, você pode mudar para um terminal e matar o X ou verificar o log.

• ALT+SysRq+k 🡪 Mata todos os processos que estão rodando no momento. Não faça isso no console onde está rodando o X, pois ele poderá travar.

• ALT+SysRq+b 🡪Um reboot sem desmontar o sistema (Esse é o perigo).

• ALT+SysRq+o 🡪 Desliga via APM.

• ALT+SysRq+s 🡪 Executa um sync em todos os sistemas de arquivos montados.

• ALT+SysRq+u 🡪 Remonta todo o sistema de arquivos montado como read-only.

• ALT+SysRq+m 🡪 Joga todas as informações da memória para o terminal.

• ALT+SysRq+e 🡪Envia um SIGTERM para todos os processos exceto o init.

• ALT+SysRq+i 🡪 Envia um SIGKILL para todos os processos exceto o init.

• ALT+SysRq+l 🡪 Envia um SIGKILL para todos os processos inclusive o init (O sistema não funcionará mais após esta sequência ser pressionada).

Aqui entre uma questão do que é mais importante, gerenciamento, facilidades ou segurança? Pois com este recurso habilitado não adianta nada termos desabilitado o CTRL+ALT+DEL se este recurso pode ser usado para reiniciar a máquina com o pressionamento das teclas ALT+SysRq+b.

**3.4 - Bloqueios do terminal por inatividade**

Quando abandonamos a console de um sistema em que estamos trabalhando é importante que ele tenha algum recurso que desconecte automaticamente após um período inativo ou ainda uma forma de bloqueamos a console na necessidade de nos ausentamos. Para isso podemos usar a variável global TMOUT e o programa vlock respectivamente.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27)

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31)

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31)

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33)

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34)

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67)