Sessão 10: Configuração segura de servidores Linux

As atividades desta sessão serão realizadas na máquina virtual *LinServer-G*.

Nesta seção iremos fazer uma série de configurações de segurança básica em um servidor Linux, especificamente a máquina *LinServer-G*. O estabelecimento de um *baseline* de segurança, como o que faremos aqui, é um passo importante na definição de uma fundação segura para a implantação de diferentes serviços de rede e, no caso da virtualização, de *templates* de máquinas virtuais.

1) Análise de *rootkits*

1. As ferramentas `chkrootkit` e `rkhunter` podem ser utilizadas para buscar por *rootkits* em um sistema Linux. *Rootkits*, como vimos na teoria, são conjuntos de programas de computador desenhados para permitir acesso continuado a área não-autorizadas de um sistema, usualmente com permissões elevadas.

   Instale os pacotes `chkrootkit` e `rkhunter` na máquina *LinServer-G*, e verifique se existem *rootkits* instalados.

2) Inserção de senha no *bootloader*

O cuidado com a segurança física das máquinas deve ser amplo, indo desde o acesso à sala dos servidores até a adição de senha na BIOS dos sistemas (impedindo, por exemplo, alteração do dispositivo de *boot*).

Um aspecto que não pode ser esquecido é o *bootloader*, que faz a carga inicial do kernel — se desprotegido, um atacante com acesso físico à máquina pode utilizá-lo para alterar a senha do usuário `root` e ter acesso irrestrito ao sistema, dentre outras possibilidades.

O *bootloader* em uso pela grande maioria das distribuições Linux atualmente é o GRUB (*GRand Unified Bootloader*), e o Debian não é exceção. Vamos configurar uma senha de acesso ao GRUB para impedir que um atacante consiga ter acesso indevido ao sistema.

1. Usando o comando `grub-mkpasswd-pbkdf2`, gere um hash para a senha `rnpesr123`.
2. Edite o arquivo `/etc/grub.d/40_custom` e insira o superusuário `admin`, com senha idêntica ao hash gerado no passo anterior.
3. Reconfigure o GRUB com a nova combinação usuário/senha e reinicie a máquina. Verifique o funcionamento da sua configuração.
4. Edite a configuração do GRUB para que ele solicite senha **apenas** em caso de edição de entradas do menu, e que o *boot* normal do sistema prossiga sem que haja necessidade de interação.

3) Remoção de serviços desnecessários

A remoção de serviços que não estão sendo utilizados em um servidor é premissa básica de segurança, pois reduz a superfície de ataque disponível para um agente malicioso. Deve-se fazer esse trabalho de forma diligente e constante, de forma a manter apenas aqueles serviços absolutamente necessários em operação.

1. Descubra quais serviços estão escutando por conexões TCP na máquina *LinServer-G*. Em seguida, faça o mesmo para o protocolo UDP.
2. Usando o comando `lsof`, descubra mais detalhes sobre o processo escutando na porta 25/TCP.
3. Descubra o nome do pacote escutando na porta 25/TCP. Em seguida, remova-o juntamente com seus arquivos de configuração.
4. Verifique que a porta 25/TCP não está mais na lista de *sockets* em estado LISTEN.

4) Controle granular de acesso a comandos

O `sudo` é uma importante ferramenta no controle de permissionamento em sistemas Linux. Ele permite que um usuário execute comandos como outro usuário do sistema, mas apenas aqueles previamente autorizados pelo usuário `root`. Dessa forma, pode-se permitir controle parcial do sistema a um colaborador, sem que ele tenha que ter acesso irrestrito à conta de superusuário.

1. Instale o pacote `sudo`, e verifique sua configuração padrão.
2. Adicione o usuário `aluno` ao grupo `sudo`, e verifique quais comandos ele pode utilizar a partir de então. Adicionalmente, faça com que não seja necessário digitar senha para executar comandos privilegiados.
3. Suponha que um novo colaborador, `mcfly`, acaba de entrar em seu setor e ficou responsável pela edição das regras de firewall dos servidores.
    a. Crie um novo usuário para esse colaborador, e configure sua senha como `rnpesr`.
    b. Edite as regras de `sudo` para que ele possa editar as regras de firewall da máquina *LinServer-G* como o usuário `root`, e apenas isso.
    c. Teste sua configuração.

5) Controle de uso do binário *su*

Por padrão, através do comando `su` o Linux permite que qualquer usuário possa se tornar o superusuário `root`, se a senha correta for digitada. Para evitar esse comportamento, temos duas opções básicas:

a. Desabilitar a conta do usuário `root`, e controlar o acesso a comandos através do `sudo`, como fizemos na atividade (4), ou
b. Implementar um grupo especial, `wheel`, e permitir que apenas membros desse grupo possam utilizar o binário `su`.

Vamos testar esse segundo controle.

1. Crie um novo usuário, `docbrown` com senha `rnpesr`, e também um novo grupo de sistema, `wheel`. Adicione o novo usuário a esse grupo e edite o arquivo `/etc/pam.d/su` e implemente o controle de acesso ao binário `su`. Teste sua configuração.

6) Controle de acesso à console do sistema

Agora vamos restringir a quantidade de usuários que podem autenticar no console da máquina. Para tal, vamos configurar o módulo `pam_access` nos principais sistemas de autenticação: `ssh`, console texto, console gráfico (se instalado) e, opcionalmente, para os demais subsistemas.

1. Habilite o módulo `pam_access` para logins `ssh`, editando o arquivo `/etc/pam.d/sshd`.
2. Habilite o módulo `pam_access` para logins em console texto, editando o arquivo `/etc/pam.d/login`.
3. Edite o arquivo `/etc/security/access.conf` e restrinja o acesso à console local e logins `ssh` apenas para membros do grupo `wheel` que efetuem login local ou logins remotos oriundos da rede 172.16.G.0/24, especificamente. Teste sua configuração.
4. Reverta as configurações realizadas nesta atividade.

7) Exigência de parâmetros mínimos de senha

O uso de senhas fortes é um requisito de segurança básico em sistemas computacionais; em servidores, especialmente, o descuido com senhas pode ocasionar falhas de segurança graves. As bibliotecas `pwquality` e `pwhistory` possibilitam a checagem da qualidade das senhas dos usuários, impondo requisitos mínimos em termos de tamanho e complexidade, bem como a manutenção de histórico de senhas

1. Instale os pacotes `libpam-modules` e `libpam-pwquality`, e configure o sistema para que novas senhas tenham os seguintes requisitos mínimos:
    - Tamanho mínimo de 10 caracteres.
    - Ao menos uma letra maiúscula.
    - Ao menos um caractere numérico.
    - Ao menos um caractere especial.
    - As últimas seis senhas não possam ser repetidas.
2. Teste suas configurações. Tente alterar a senha de um usuário não-privilegiado sem respeitar os requisitos mínimos de qualidade estabelecidos. Depois, tente reutilizar senhas e verifique o comportamento do sistema.

8) Controle de logoff automático

A opção de logoff automático evita o uso indevido da sessão de um administrador quando este, inadvertidamente, não faz o logoff manual. A variável `$TMOUT` do *shell* controla, em segundos, o tempo máximo aceito pelo sistema sem que o usuário execute um comando ou aperte uma tecla. Decorrido esse tempo, a máquina vai, automaticamente, efetuar o logoff do usuário.

1. Edite o arquivo `/etc/profile` e ative o logoff automático de usuários para dez segundos. Teste sua configuração.

9) Desabilitando a combinação de teclas CTRL + ALT + DEL

1. Para evitar que o servidor Linux seja reiniciado quando o seu teclado for confundido com o de um servidor Windows, desabilite a combinação de teclas CTRL + ALT + DEL.