Sessão 11: Configuração segura de servidores

1) Controle de acesso ao sistema operacional

O objetivo dessa atividade é realizar a instalação de um software chamado SuRun. A ideia por trás do SuRun é semelhante ao que acontece no Linux com o sudo, ou seja, não permitir que um usuário administrador possa se autenticar remotamente e, a partir de uma lista de usuários válidos, permitir que eles possam executar binários como administrador. Nesta atividade o aluno deverá inserir o usuário em algum grupo com permissão para logon local, ou essa diretiva deverá ser alterada para que seja incluso o grupo SuRun nessa police, além de ativar a diretiva de logon pelo serviço de terminal no snap-in Local security > Local Polices > Users rights assignment

1. Utilizando o snap-in “Users and Groups” em “Administrative Tools”, crie o usuário “suporteloc” com a senha “rnpesr”. Baixe a ferramenta SuRun (semelhante ao sudo do Unix) do endereço: http://kay-bruns.de/wp/software/surun e instale como Administrador. Abra a janela de configuração do SuRun, na aba “Common Settings”. Habilite a opção “Users must enter their password”, com dois minutos (min grace period before asking again). Habilite a opção “Show SuRun settings for experienced users”. Na aba Advanced, habilite “Hide SuRun from users that are not members of the ‘SuRunners’ group”. Clique em “Apply” e, em seguida, em “Save”.

Utilizando o snap-in “Computer Management”, adicione ao grupo SunRunners o usuário suporteloc. Faça um logon/logoff e autentique utilizando o usuário suporteloc. Para utilizar o SuRun, basta clicar com o botão direito em cima de um snap-in qualquer ou um executável e selecionar a opção Start as Administrator.

1. Agora, vamos configurar o acesso remoto ao servidor Windows 2008 utilizando o serviço de Terminal. Para isso, acesse o painel de controle e clique em System. Selecione “Advanced System Settings” e clique na aba “Remote”. Habilite a opção “Allow connections from computers running any version of Remote Desktop (less secure)”.

Utilizando o snap-in “Computer Management”, acrescente o usuário suporteloc dentro do grupo “Remote Desktop Users”.

1. Agora vamos bloquear o acesso remoto de usuários membros do grupo Administradores. Acesse a ferramenta Terminal Services Configuration em Administrative Tools > Terminal Service. Clique com o botão direito na conexão RDP-Tcp e edite suas propriedades. Na aba Security, acesse a opção Advanced. Escolha o grupo Administrators. Selecione a opção Edit. Na permissão Logon, marque a opção Deny. Para testar, tente autenticar utilizando o usuário Administrator. Agora tente utilizando o usuário suporteloc.

2) Configuração segura de servidor Linux

Utilizando as técnicas estudadas, vamos modificar algumas configurações do servidor Linux de modo a torná-lo mais seguro.

1. Acesse o servidor LinServer-G e configure uma senha para evitar que um usuário reinicie e o

servidor e consiga inicializá-lo em modo single, ou seja, como root sem precisar inserir a senha de root. Essa configuração deve ser encarada como obrigatória sempre que o servidor estiver localizado em uma sala insegura.

```
#/sbin/grub
GRUB version 0.92 (640K lower / 3072K upper memory)
Minimal BASH-like line editing is supported. For the first word, TAB lists possible
command completions. Anywhere else TAB lists the possible completions of a
device/filename.

grub> md5crypt
Password: ********(Comentário: foi digitado rnpesr no prompt)
Encrypted: $1$T7/dgdIJ$dJM.n2wZ8RG.oEiIOwJUs.
grub> quit
```

Agora, insira a linha abaixo no final do arquivo /boot/grub/menu.lst não esquecendo de colar a senha gerada no passo anterior:

```
password --md5 $1$T7/dgdIJ$dJM.n2wZ8RG.oEiIOwJUs.
```

2. Verifique todos os serviços que estão sendo inicializados junto com o servidor. Pesquise na internet o papel de todos os serviços. Atenção aos que você não conheça. Verifique se é vital para o funcionamento do sistema. Para essa verificação pode ser utilizado o comando:

```
# apt-get install rcconf
# rcconf
```

Isso removerá da inicialização conjunta com o sistema operacional quando este for iniciado. Para verificar os serviços que estão ativos, podemos utilizar os comandos:

```
# netstat –nap
```

Para mais detalhes sobre uma determinada porta que esteja aguardando por conexão na rede, podemos utilizar o comando:

```
# lsof –i PROTOCOLO:PORTA -n
```

3. Para pacotes que você pesquisou e sabe que não serão necessários ao seu sistema, a recomendação é remover. Para remover os pacotes desnecessários sem remover as configurações personalizadas, vamos utilizar o comando:

```
# apt-get remove nome_do_pacote
```

Para remover todos os históricos de um pacote, vamos utilizar o comando:

```
# apt-get purge nome_do_pacote
```

Para listar todos os pacotes instalados no sistema, podemos utilizar o comando:

```
# dpkg –l
```

4. Para modificar o acesso administrativo no servidor, vamos utilizar a ferramenta sudo para nos auxiliar. Instale o pacote sudo com o comando:

```
# apt-get install sudo
```

Edite o arquivo de configuração do sudo (/etc/sudoers) e adicione a linha:

```
aluno ALL=(ALL) ALL
```

Essa linha vai permitir ao usuário aluno todos os níveis de acessos do usuário root.

5. Verifique o funcionamento do sudo. Conecte remotamente com o protocolo SSH e como usuário aluno, mude para modo privilegiado com sudo:

```
aluno@LinServer-A:~$ sudo su -
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
[sudo] password for aluno:
```

6. Por padrão, através do comando su o Linux permite que qualquer usuário possa se tornar o root do sistema. Para evitar esse comportamento o Linux implementa um grupo especial chamado wheel e podemos configurar o arquivo /etc/pam.d/su de forma a permitir que apenas os membros desse grupo possam se tornar root do sistema. Crie um usuário chamado “suporteloc”:

```
[root@localhost ~]# adduser suporteloc
```

Crie um grupo chamado “wheel”:

```
[root@localhost ~]# addgroup wheel
```

Faça com que o usuário “suporteloc” seja membro do grupo “wheel”:

```
[root@localhost ~]# usermod –G wheel suporteloc
```

Edite o arquivo /etc/pam.d/su e descomente a linha abaixo.

```
auth required pam_wheel.so
```

7. Para testar o funcionamento do grupo wheel, autentique-se na máquina LinServer-G com o usuário aluno e tente executar o comando $ su -. Observe que não vai funcionar. Agora, realize o login utilizando o mesmo usuário e tente, novamente, executar o comando $ su -
8. 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 Login, Graphical Gnome Login (se estiver instalada) e, opcionalmente, para todos os outros sistemas. Para o SSH adicione o pam_access no arquivo /etc/pam.d/sshd após a linha pam_nologin.so:

   ```
   account required pam_access.so
   ```

   Para o console adicione o pam_access no arquivo /etc/pam.d/login após a linha pam_nologin.so:

   ```
   account required pam_access.so
   ```

   Adicionar ao final do arquivo /etc/security/access.conf que é lido pelo módulo pam_access as seguintes linhas Cuidado: se essa configuração for realizada de forma errada, ninguém poderá mais autenticar na máquina.

   ```
   + : wheel : LOCAL 172.16.
   - : ALL : ALL
   ```

   A primeira linha permite aos usuários do grupo wheel autenticar na máquina local cuja a origem seja a rede 172.16.0.0/16, enquanto a segunda linha bloqueia o acesso para qualquer outro usuário.

9. Para verificar o funcionamento do pam_access, monitore o arquivo /var/log/ auth.log e tente realizar a autenticação via SSH a partir da estação de trabalho física.. Observe que mesmo que acerte a senha você não conseguirá acesso ao servidor e que, no arquivo auth.log, será gerada a linha

   ```
   pam_access(sshd:account): access denied for user `suporteloc` from `10.1.1.10`
   ```

   Tente autenticar via SSH a partir do servidor FWGW1-G. Observe que funcionará normalmente.

10. Agora vamos obrigar os usuários locais a utilizar senhas fortes. Para isso vamos instalar e configurar a biblioteca craklib. Para instalar, execute:

```
# apt-get install libpam-cracklib
```

Edite o arquivo /etc/pam.d/common-password, remova o comentário e modifique a linha pam_cracklib conforme abaixo:

```
password required pam_cracklib.so retry=3 minlen=14 difok=3 lcredit=-1 ucredit=-1
dcredit=-1 ocredit=-1
password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok
remember=12
```

Isso adicionará o cracklib, que vai obrigar todas as novas senhas de usuário a ter:

Você deve criar o arquivo /etc/security/opasswd caso ele não exista.

```
[root@localhost ~]# touch /etc/security/opasswd
[root@localhost ~]# chown root:root /etc/security/opasswd
[root@localhost ~]# chmod 600 /etc/security/opasswd
```

O usuário root não obedece as restrições impostas pela cracklib.

11. Para testar essa configuração, autentique utilizando o usuário suporteloc e tente modificar sua senha para algo bem simples. Agora tente alterar para um senha que atenda a política acima configurada.

12. Vamos ativar um mecanismo interessante para fortalecer a política de senhas locais implementando o processo de expiração para senhas antigas. Em geral, não é recomendado que o sistema imponha a expiração da senha para contas de serviço. Isso pode levar a interrupções de um serviço se a conta de um aplicativo expirar. Uma política corporativa deve reger as alterações de senha para contas de usuários individuais do sistema e deve expirar as senhas automaticamente. Os seguintes arquivos e parâmetros da tabela devem ser usados quando uma nova conta é criada com o comando useradd. Essas configurações são registradas para cada conta de usuário no arquivo /etc/shadow. Portanto, certifique-se de configurar os seguintes parâmetros antes de criar qualquer usuário contas utilizando o comando useradd:

Certifique-se de que os parâmetros acima foram alterados nos arquivos /etc/login.defs e /etc/default/useradd. As configurações acima passam a ser utilizadas apenas por usuários criados a partir desse momento. Usuários antigos não vão receber esses atributos. Observe que, quando uma conta de usuário é criada usando o comando useradd, os parâmetros listados na tabela acima são inseridos no arquivo /etc/shadow, no seguinte formato:

```
<nome-de-usuário>: <senha>: <data>: PASS_MIN_DAYS: PASS_ MAX_DAYS: PASS_WARN_AGE:
INACTIVE: EXPIRE:
```

Você pode alterar a data de envelhecimento a qualquer momento. Para desabilitar a data do envelhecimento para contas de sistema e contas compartilhadas, você pode executar o comando chage:

```
# chage -M 99999 <account>
```

Para adicionar uma data de expiração da conta, execute:

```
#useradd -e mm/dd/yy <login_name>
```

Para obter informações sobre a expiração da senha:

```
# chage -l <account>
```

Na instalação padrão, as contas de serviço já possuem data de expiração igual a 99999.

13. 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 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. Edite o arquivo /etc/profile e adicione a seguinte linha:

```
TMOUT=900
```

O valor da variável “TMOUT=” é em segundos, ou seja, 15 minutos (15*60 = 900 segundo).

14. As configurações abaixo são recomendadas para o serviço de terminal SSH. Para alterá-las, vamos editar o arquivo de configuração do servidor Open SSH /etc/ssh/sshd_config. Observe os comentários para decidir que parâmetros você vai utilizar. Em nosso treinamento, configure todos os parâmetros abaixo:

```
#Não permitir o login do usuario root
PermitRootLogin no
#Prevenir que o SSH seja configurado para realizar forwarding do serviço do X11
AllowTcpForwarding no
X11Forwarding no
# Configurar o Banner padrão
Banner /etc/issue
```

Reinicie o servidor SSH para aplicar as novas configurações:

```
# /etc/init.d/ssh restart
```

Verifique o funcionamento e tente acessar remotamente utilizando o usuário “root”. A partir desse momento, você está convidado a utilizar sempre o usuário aluno e/ou suporteloc com permissões básicas. Quando necessitar realizar alguma atividade administrativa, utilize sudo ou su para obter os privilégios necessários. Dessa forma, teremos registros do usuário que realizou determinada atividade com privilégios administrativos.

15. Desabilite a permissão para que o usuário root acesse o sistema pelo console físico. Para isso, edite o arquivo de configuração /etc/securetty. Vamos apagar todo o conteúdo desse arquivo de configuração:

```
# cp /etc/securetty /etc/securetty.old
# echo “ “ > /etc/securetty
```

Para testar a configuração, acesse o console via Virtual Box e acesse o servidor com o usuário root. Se não for possível, acesse com o usuário aluno.

16. Para evitar que o servidor Linux seja reiniciado quando o seu teclado for confundido com o de um servidor Windows, desabilite a combinação Ctrl+Alt+Del editando o arquivo de configuração /etc/inittab e comente ou apague a seguinte linha:

```
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
```

Ficando assim:

```
# ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
```

17. O comando umask serve como uma máscara para ajustar a permissão de arquivos e diretórios, assim, um umask mal configurado vai atribuir para novos arquivos criados pelo root permissão de acesso para qualquer usuário. Recomenda-se alterar o umask de todos os usuários para 177, ajustando o arquivo /etc/profile. Caso existam problemas na instalação de novos binários no servidor, modifique o umask para a opção padrão utilizando o comando umask 022.
18. Personalizar o kernel do Linux com o intuito de torná-lo mais eficaz não é uma tarefa simples, pois depende muito do cenário e das aplicações que serão utilizadas. De forma geral, os parâmetros abaixo podem ser inseridos no final do arquivo /etc/sysctl.conf em diversos cenários sem comprometer o funcionamento do servidor.

```
#TCP SYN Cookie Protection
net.ipv4.tcp_max_syn_backlog=1280
net.ipv4.tcp_syncookies = 1
#Disable IP Source Routing
net.ipv4.conf.all.accept_source_route = 0
#Disable ICMP Redirect Acceptance
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects=0
# Habilita proteção contra IP spoofing
net.ipv4.conf.all.rp_filter = 1
#Ignoring Broadcasts Request
net.ipv4.icmp_echo_ignore_broadcasts=1
#Bad Error Message Protection
net.ipv4.icmp_ignore_bogus_error_responses = 1
#Desativa o forward de pacotes. Não deve ser configurado em servidores que assumam
serviço de gateway/roteador
net.ipv4.ip_forward = 0
# Habilita log de pacotes spoof. Obs. Esse recurso gera muitas entradas no log e
deve ser avaliado com cuidado.
net.ipv4.conf.all.log_martians = 0
# Desativar o proxy_arp
net.ipv4.conf.all.proxy_arp=0
# Habilita o execshield
kernel.core_uses_pid = 1
```

Reinicie o sistema para que as configurações sejam aplicadas.