Sessão 6: Serviços básicos de segurança

1) Configuração do servidor de log remoto

Esta atividade será realizada nas máquinas virtuais *FWGW1-G*, *LinServer-G* e *WinServer-G*.

Nesta atividade iremos configurar um repositório de logs em um servidor da DMZ (*LinServer-G*), e enviar os logs dos demais servidores para esse concentrador. O objetivo desta atividade é fazer o aluno aplicar os conceitos de repositório de logs de uma rede e preparar o ambiente para os serviços seguintes, que serão configurados durante o curso.

1. Primeiro, vamos configurar o concentrador de logs. Acesse a máquina *LinServer-G* e instale o pacote `syslog-ng`.

   ```
   # hostname
   LinServer-A

   # apt-get install --no-install-recommends syslog-ng
   ```

2. Observe que na última linha do arquivo `/etc/syslog-ng/syslog-ng.conf` são incluídos arquivos com a extensão `.conf` localizados no diretório `/etc/syslog-ng/conf.d`:

   ```
   # tail -n1 /etc/syslog-ng/syslog-ng.conf
   @include "/etc/syslog-ng/conf.d/*.conf"
   ```

   Aproveitando-se desse fato, crie um novo arquivo com a extensão apropriada nesse diretório e configure o recebimento de logs remotos. Faça com que o `syslog-ng` escute por conexões na porta 514/UDP, e envie os arquivos de log de uma dado *host* para o arquivo `/var/log/$HOST.log`. Finalmente, reinicie o `syslog-ng`.

   Abaixo, mostramos o conteúdo do arquivo `/etc/syslog-ng/conf.d/rserver.conf`, que cumpre os objetivos especificados:

   ```
   source s_net { udp(); };
   destination d_rhost { file("/var/log/$HOST.log"); };
   log { source(s_net); destination(d_rhost); };
   ```

   Depois, basta reiniciar o serviço:

   ```
   # systemctl restart syslog-ng.service
   ```

3. Agora, na máquina *FWGW1-G*, instale o `syslog-ng` e configure-o como um cliente Syslog. Crie um arquivo de configuração na pasta `/etc/syslog-ng/conf.d` que envie todos os eventos de log locais

para a máquina *LinServer-G* na porta 514/UDP.

```
# hostname
FWGW1-A

# apt-get install --no-install-recommends syslog-ng
```

A seguir, temos o arquivo `/etc/syslog-ng/conf.d/rclient.conf`, que envia os logs locais para o servidor remoto:

```
destination d_rserver { udp("172.16.1.10" port(514)); };
log { source(s_src); destination(d_rserver); };
```

Finalmente, basta reiniciar o `syslog-ng`:

```
# systemctl restart syslog-ng.service
```

4. Usando o comando `logger`, teste seu ambiente.

   Na máquina *FWGW1-G*, crie um evento de log qualquer usando o comando `logger`:

   ```
   # hostname
   FWGW1-A

   # logger -p error Teste
   ```

   Observando a máquina *LinServer-G*, perceba que foi criado um novo arquivo `/var/log/172.16.G.1.log`. Verificando seu conteúdo, é possível constatar que, de fato, os logs remotos do *host FWGW1-G* estão sendo enviados para cá.

   ```
   # hostname
   LinServer-A

   # tail -n1 /var/log/172.16.1.1.log
   Aug 26 06:49:30 172.16.1.1 aluno: Teste
   ```

5. Agora, vamos configurar a máquina *WinServer-G* para enviar registros de eventos para o concentrador Syslog. Faça login como usuário `Administrator` e abra o *Group Policy Editor* digitando `gpedit.msc` no menu *Start* > *Run...*.

   Na ferramenta, acesse a seção *Computer Configuration* > *Windows Settings* > *Security Settings* > *Local Policies* > *Audit Policy* e habilite os seguintes eventos como "Sucesso" e "Falha":

   Tabela 1. Políticas de auditoria para o WinServer-G

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure

A tela ficaria, portanto, desta forma:

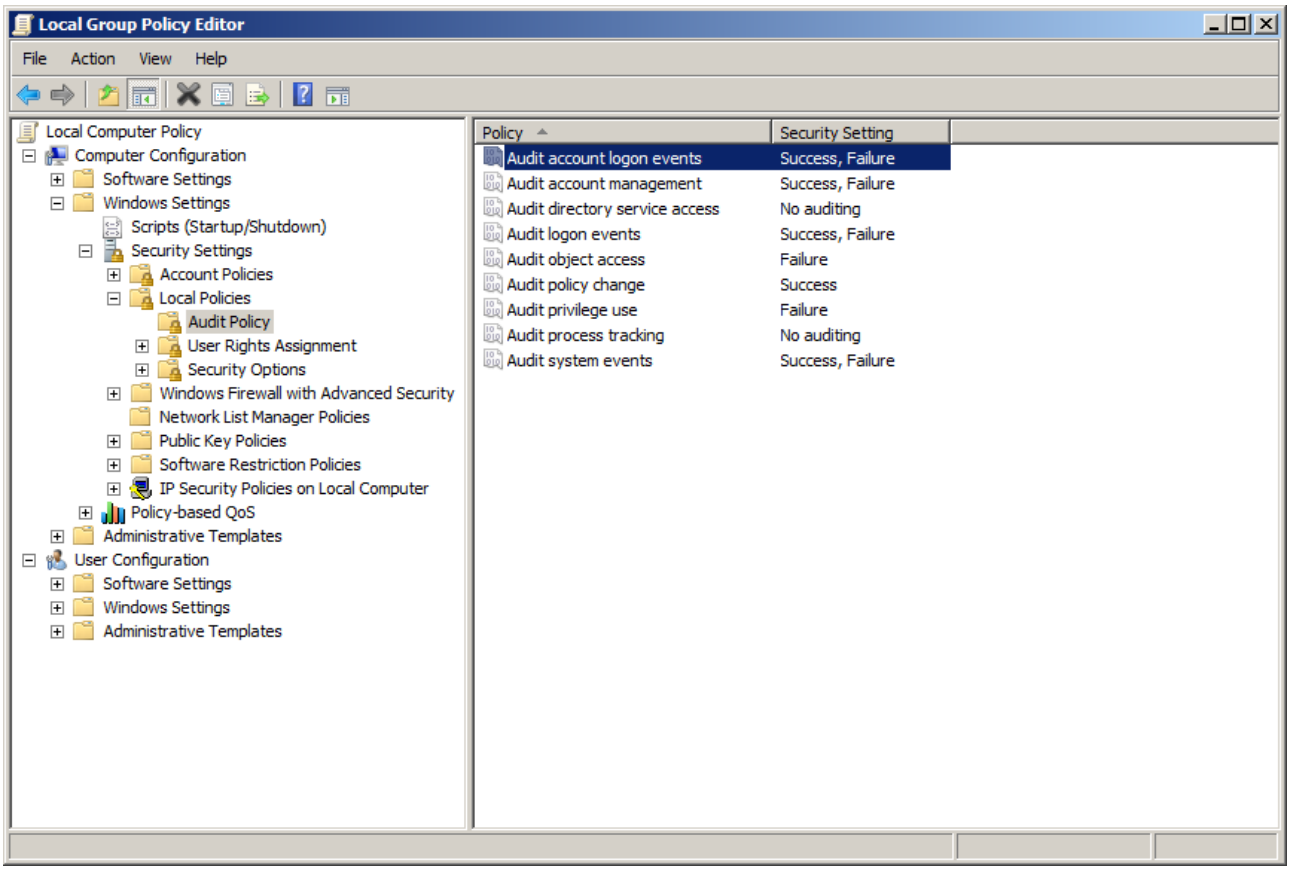

Figura 29: Tela de políticas de auditoria para o WinServer-G

6. O próximo passo é instalar o Snare, que permitirá envio dos registros de eventos do Windows para um servidor Syslog remoto. Faça o download em https://www.snaresolutions.com/products/snare-agents/open-source-agents/ ; será necessário cadastrar seu nome/email para receber o link de download. Alternativamente, solicite o instalador ao instrutor.

   Durante a instalação, responda todas as perguntas com as opções padrão, exceto:

   Tabela 2. Opções de instalação do Snare

Opção	Escolha
Snare Auditing	Yes
Service Account	Use System Account
Remote Control Interface	Enable Web Access (Password: rnpesr)

7. Após a instalação, abra o Snare. Clique em *Start* e digite "snare", escolhendo a opção `Snare for Windows (Open Source)`, como se segue:

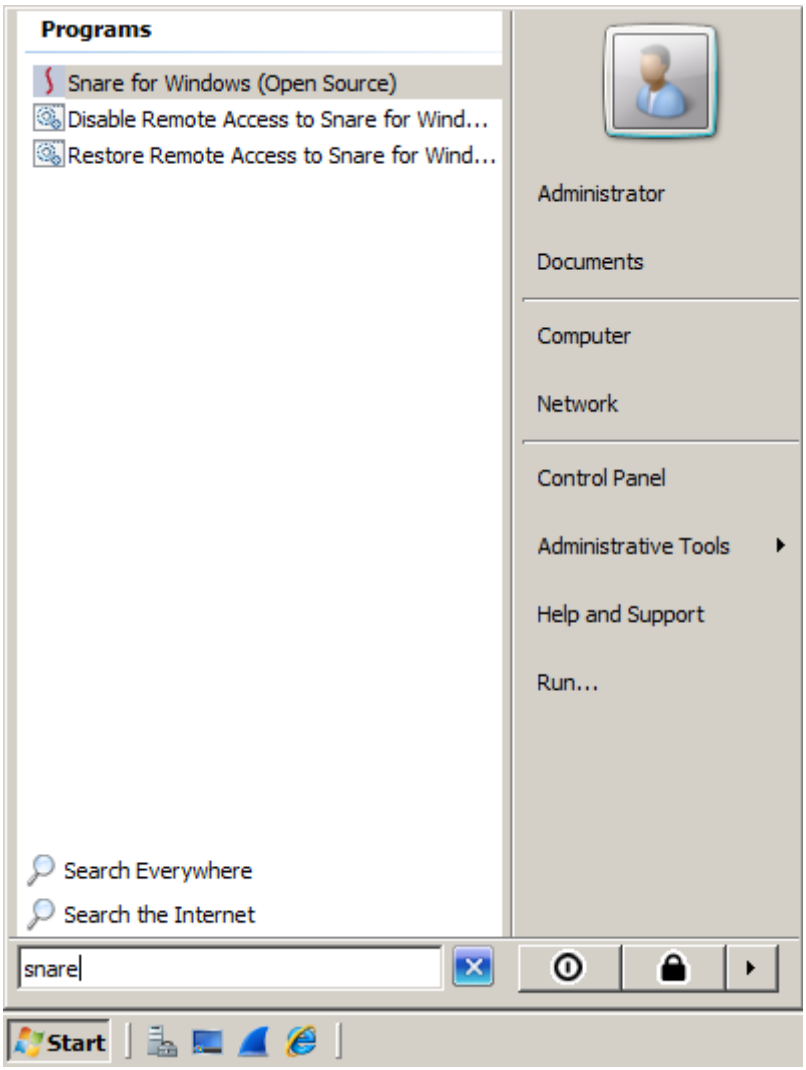

Figura 30: Inicialização do Snare

Irá ser lançada uma janela do navegador. Informe o usuário `snare`, e senha `rnpesr`, como se segue:

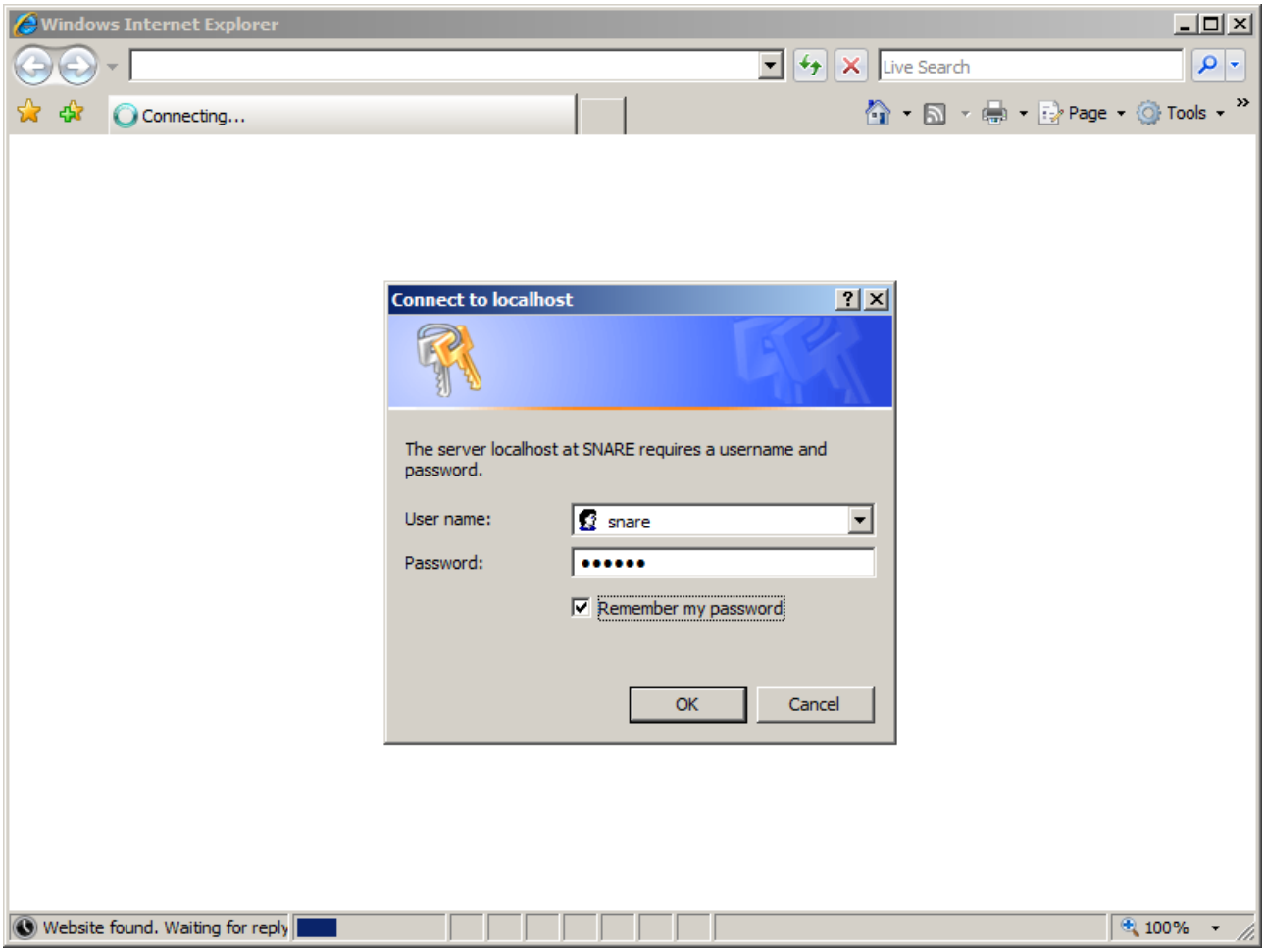

Figura 31: Login no Snare

Clique em *Network Configuration* — informe o IP da máquina *LinServer-G* no campo *Destination Snare Server address*, e a porta 514 no campo *Destination Port*, como se segue. Em seguida, clique em *Change Configuration*.

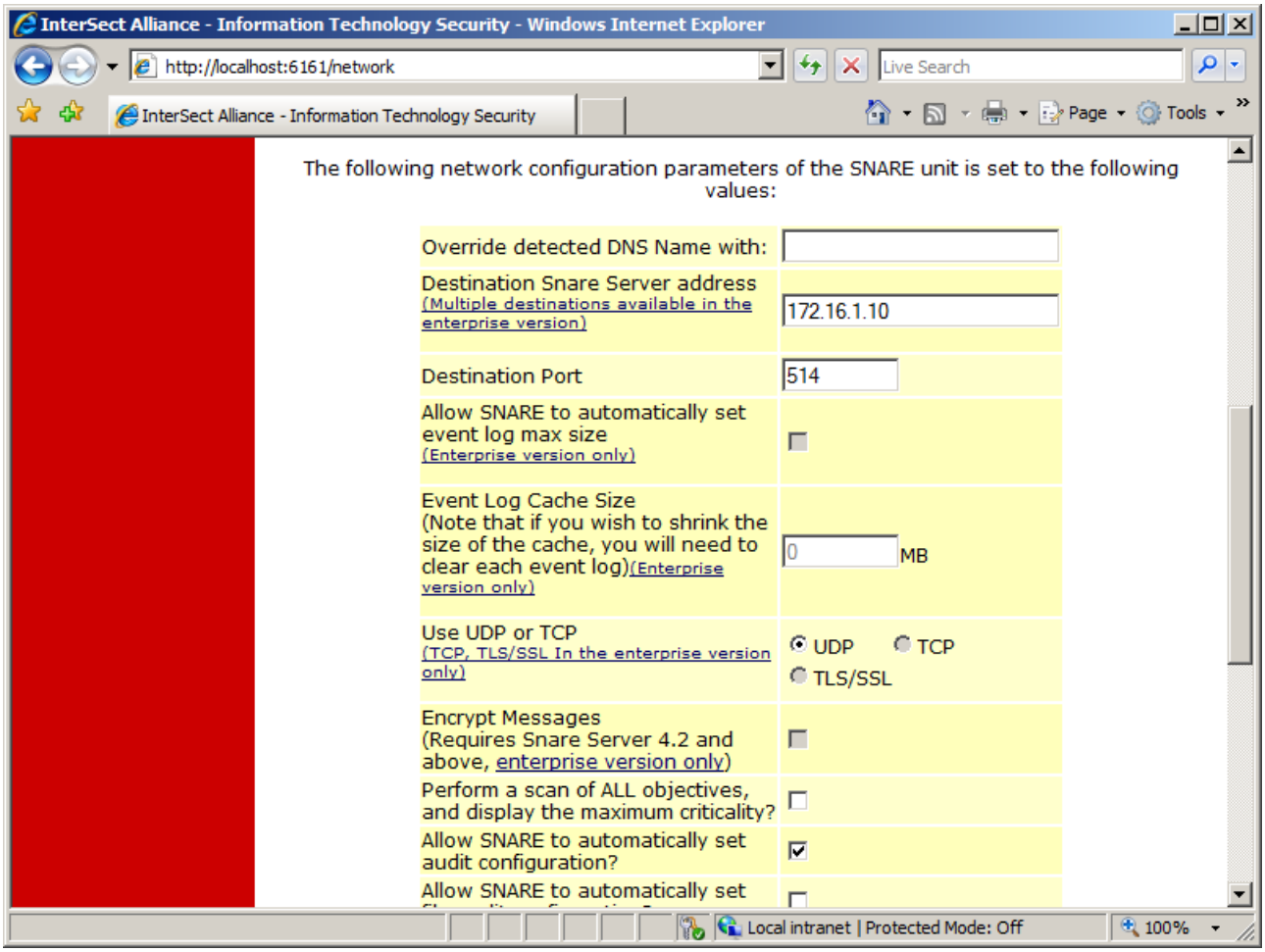

Figura 32: Configurações do Snare

Em seguida, clique em *Apply the Latest Audit Configuration* e depois em *Reload Settings*.

8. Faça logoff/logon no *WinServer-G* para gerar registros de eventos. Em seguida, volte à máquina *LinServer-G* e verifique que os logs estão de fato sendo enviados.

```
# hostname
LinServer-A

# grep Logoff /var/log/172.16.1.20.log
Aug 26 07:10:25 172.16.1.20 WinServer-A MSWinEventLog   1       Security        50
dom ago 26 08:10:23 2018  4647    Microsoft-Windows-Security-Auditing
WINSERVER-A\Administrator       N/A     Success Audit     WinServer-A     Logoff
User initiated logoff:    Subject:   Security ID:  S-1-5-21-1959434341-4039883546-
812769935-500   Account Name:  Administrator   Account Domain:  WINSERVER-A   Logon
ID:  0x16898    This event is generated when a logoff is initiated but the token
reference count is not zero and the logon session cannot be destroyed.  No further
user-initiated activity can occur.  This event can be interpreted as a logoff
event.  41
```