

AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

Carlos Almeida (1181132) André
Teixeira (1190384)

SEGS – Segurança de Sistemas e
Informação

Índice

Introdução.....	3
Parte Prática	4
FreeRadius	4
1) Criação de utilizadores.....	4
2) Criação de grupos	5
3) Atribuição dos grupos aos utilizadores	5
4) Demonstração	7
5) Considerações adicionais	7
Federated Radius	8
1) Criação de utilizadores.....	8
2) Associação da máquina Linux ao Windows server	9
3) Confirmação dos acessos	10
Conclusão	11

Índice Figuras

Figura 1: Demonstração dos grupos, utilizadores e designação dos mesmo a cada grupo	5
Figura 2: Configuração dos grupos existentes	6
Figura 3: Demonstração para evidenciar o acesso permitido/restrito/negado dos utilizadores	7
Figura 4: Criação Users no FreeRadius.....	8
Figura 5: Criação Users no Active Directory	9
Figura 6: Adicionar o endereço IP do AD à máquina Linux	9
Figura 7 ntlm_auth.....	10
Figura 8 Ficheiro smb.conf	10

Introdução

Neste trabalho, abordamos a implementação de mecanismos de segurança baseados no modelo AAA (Authentication, Authorization, and Accounting) em sistemas de informação. O modelo AAA é amplamente utilizado em redes, onde se torna essencial para garantir a segurança e o controle de acesso. Cada um dos três pilares—Autenticação, Autorização e Contabilidade—desempenha um papel crítico:

- Autenticação assegura que o utilizador é realmente quem afirma ser.
- Autorização define os níveis de acesso e as ações permitidas para cada utilizador.
- Contabilidade regista e monitoriza as atividades para auditoria e análise de segurança.

O objetivo deste trabalho é desenvolver competências na implementação de sistemas de AAA por meio de ferramentas específicas como FreeRadius e Active Directory. Essas tecnologias permitem configurar e gerir acessos em ambientes complexos, onde a integração entre sistemas e a interoperabilidade entre plataformas são fundamentais.

O FreeRadius é uma ferramenta amplamente utilizada para autenticação em redes e sistemas Linux, enquanto o Active Directory, da Microsoft é solução popular para a gestão de identidades e diretórios em ambientes Windows e Linux, respetivamente.

Assim, este relatório apresentará as configurações realizadas para a concretização das tarefas feitas, a evidência de acessos e as limitações de acesso de acordo com o perfil dos utilizadores. Essa prática visa não apenas o desenvolvimento técnico, mas também a compreensão de como o AAA contribui para uma infraestrutura de segurança robusta.

Parte Prática

FreeRadius

O FreeRADIUS é um servidor de RADIUS (Remote Authentication Dial-In User Service) de código aberto, amplamente utilizado para autenticação, autorização e contabilidade (AAA) em redes de comunicações. Um servidor de autenticação permite autenticar utilizadores, máquinas, serviços, etc. Numa rede de dados é muito comum existirem servidores de autenticação de forma que, por exemplo, só os utilizadores autorizados possam aceder aos mais diversos serviços da rede.

No segmento dos servidores de autenticação, o FreeRadius destaca-se como sendo uma ótima opção, já que é bastante completo e disponibiliza variadíssimas funcionalidades

Para este exercício foi-nos pedido que, alteremos o FreeRadius configurado na PL2 realizando as seguintes modificações:

1. Adicione os utilizadores Isaac, Moses, Sara e Abraham;
2. Adicione os grupos PU (Utilizadores Privilegiados) e NPU (Utilizadores Não-Privilegiados). O grupo PU tem todas as permissões, enquanto o grupo NPU apenas pode realizar tarefas não-administrativas;
3. Atribua dois dos utilizadores criados ao grupo PU e os outros dois ao grupo NPU. Os utilizadores criados em PL2 devem ser mantidos sem qualquer alteração nas suas especificações;
4. Além das principais partes da configuração, o relatório deve apresentar evidências dos papéis atribuídos a todos os utilizadores.

1) Criação de utilizadores

Para isso, começamos por adicionar os utilizadores, usando o comando “sudo adduser” e o nome do utilizador a adicionar, como por exemplo “sudo adduser isaac”

2) Criação de grupos

Posto isto, fizemos a criação dos grupos necessários com o comando “sudo groupadd” e o nome do grupo a adicionar.

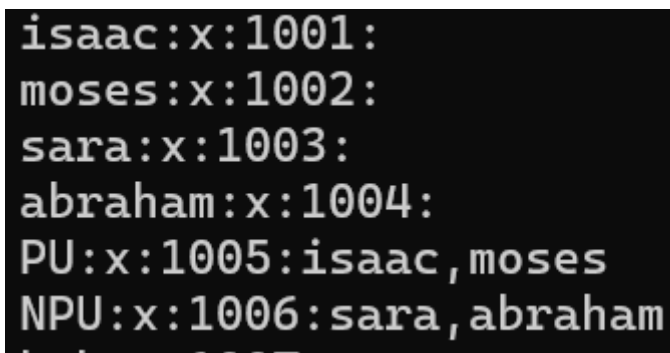
```
sudo groupadd PU
```

```
sudo groupadd NPU
```

3) Atribuição dos grupos aos utilizadores

Posteriormente para designar os utilizadores aos respetivos grupos com as devidas permissões que cada grupo possuía, usamos o comando “sudo usermod -aG” seguido de mais dois parâmetros, sendo eles o nome do grupo e o nome do utilizador adicionar.

Segundo o exercício, adicionamos 2 utilizadores ao grupo PU, sendo eles o Isaac e o Moses, e os outros utilizadores, Sara e Abraham ao grupo NPU, como se vê na imagem abaixo.



```
isaac:x:1001:  
moses:x:1002:  
sara:x:1003:  
abraham:x:1004:  
PU:x:1005:isaac,moses  
NPU:x:1006:sara,abraham  
1007:
```

Figura 1: Demonstração dos grupos, utilizadores e designação dos mesmo a cada grupo

Os utilizadores do grupo PU e NPU tem restrições diferentes, sendo que os utilizadores no grupo PU não tem restrições nenhuma e os utilizadores do grupo NPU têm restrições, conforme os grupos criados abaixo.

```
DEFAULT Group == "standard_users"
    Reply-Message := "Bem vindo, utilizador padrao!"

DEFAULT Group == "admin"
    Reply-Message := "Bem vindo, administrador!"

DEFAULT Group == "PU"
    Service-Type := Administrative-User,
    Reply-Message := "Acesso privilegiado!"

DEFAULT Group == "NPU"
    Service-Type := Framed-User,
    User-Profile := Non-Admin,
    Reply-Message := "Acesso não privilegiado!"

DEFAULT Auth-Type := Reject
    Reply-Message := "Acesso negado!"
```

Figura 2: Configuração dos grupos existentes

Grupo PU (Privileged Users):

- Acesso Completo: Utilizadores do grupo PU têm permissões administrativas, o que significa que podem realizar todas as tarefas.
- Service-Type: Na configuração do FreeRADIUS, esses utilizadores recebem o atributo Service-Type = Administrative-User. Esse atributo geralmente indica que tem acesso a recursos e comandos administrativos.
- Mensagem de Resposta: Uma Reply-Message para informar ao utilizador que tem "Acesso privilegiado".

Grupo NPU (Non-Privileged Users):

- Acesso Restrito: Utilizadores no grupo NPU possuem permissões limitadas e podem realizar apenas tarefas não administrativas. Isso significa que não têm autorização para executar ações que possam modificar configurações críticas ou aceder a informações sensíveis.

- Service-Type: Na configuração do FreeRADIUS, esses utilizadores recebem o atributo Service-Type = Framed-User. Esse tipo de atributo é frequentemente usado para indicar um acesso regular (não administrativo) em serviços de rede.
- Mensagem de Resposta: A Reply-Message desses utilizadores indica "Acesso restrito", refletindo que são "Non-Privileged Users" e, portanto, têm limitações no uso dos recursos.

4) Demonstração

Para demonstrar o funcionamento deste sistema, podemos utilizar o seguinte comando:

radtest <username> <password> <server_ip> <nas_port> <shared_secret>

```
miguel@LAPTOP-4DB1ER32:~$ radtest moises moises123 127.0.0.1 0 testing123
Sent Access-Request Id 217 from 0.0.0.0:35759 to 127.0.0.1:1812 length 75
  User-Name = "moises"
  User-Password = "moises123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Cleartext-Password = "moises123"
Received Access-Accept Id 217 from 127.0.0.1:1812 to 127.0.0.1:35759 length 66
  Message-Authenticator = 0x4b8eaf0e365b6a080a9109217fa3eef2
  Service-Type = Administrative-User
  Reply-Message = "Acesso privilegiado!"
miguel@LAPTOP-4DB1ER32:~$ radtest isaac isaac123 127.0.0.1 0 testing123
Sent Access-Request Id 48 from 0.0.0.0:46099 to 127.0.0.1:1812 length 75
  User-Name = "isaac"
  User-Password = "isaac123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Cleartext-Password = "isaac123"
Received Access-Accept Id 48 from 127.0.0.1:1812 to 127.0.0.1:46099 length 66
  Message-Authenticator = 0x6a53e335a9923d41e82bed4d46bcbdb3e
  Service-Type = Administrative-User
  Reply-Message = "Acesso privilegiado!"
miguel@LAPTOP-4DB1ER32:~$ radtest sara saral23 127.0.0.1 0 testing123
Sent Access-Request Id 91 from 0.0.0.0:46282 to 127.0.0.1:1812 length 74
  User-Name = "sara"
  User-Password = "saral23"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Cleartext-Password = "saral23"
Received Access-Accept Id 91 from 127.0.0.1:1812 to 127.0.0.1:46282 length 71
  Message-Authenticator = 0x34d236fe98ec9995069c9cd8dac216b0
  Service-Type = Framed-User
  Reply-Message = "Acesso não privilegiado!"

miguel@LAPTOP-4DB1ER32:~$ radtest abraham abraham123 127.0.0.1 0 testing123
Sent Access-Request Id 126 from 0.0.0.0:50605 to 127.0.0.1:1812 length 77
  User-Name = "abraham"
  User-Password = "abraham123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Cleartext-Password = "abraham123"
Received Access-Accept Id 126 from 127.0.0.1:1812 to 127.0.0.1:50605 length 71
  Message-Authenticator = 0x1e48da660fc88c2e7c04ae69dc913fa6
  Service-Type = Framed-User
  Reply-Message = "Acesso não privilegiado!"
miguel@LAPTOP-4DB1ER32:~$ radtest alice alice123 127.0.0.1 0 testing123
Sent Access-Request Id 8 from 0.0.0.0:44266 to 127.0.0.1:1812 length 75
  User-Name = "alice"
  User-Password = "alice123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Cleartext-Password = "alice123"
Received Access-Accept Id 8 from 127.0.0.1:1812 to 127.0.0.1:44266 length 69
  Message-Authenticator = 0x111efb6ecb1f2dc00d411c146da3fd13
  Reply-Message = "Bem vindo, utilizador padrao!"
miguel@LAPTOP-4DB1ER32:~$ radtest john john123 127.0.0.1 0 testing123
Sent Access-Request Id 78 from 0.0.0.0:48037 to 127.0.0.1:1812 length 74
  User-Name = "john"
  User-Password = "john123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Cleartext-Password = "john123"
Received Access-Reject Id 78 from 127.0.0.1:1812 to 127.0.0.1:48037 length 54
  Message-Authenticator = 0x3e3af5c6e28e9e344196b23a3726af07
  Reply-Message = "Acesso negado!"
(0) -: Expected Access-Accept got Access-Reject
```

Figura 3: Demonstração para evidenciar o acesso permitido/restrito/negado dos utilizadores

5) Considerações adicionais

Apesar de ter sido realizada para fins académicos, é possível identificar algumas considerações relevantes sobre segurança a partir da instalação do servidor FreeRADIUS.

Em primeiro lugar, é importante destacar o tipo de password que foi usada. Neste trabalho, todos os utilizadores foram definidos com a palavra-passe "nomedouser123", o que torna os ataques de força bruta mais fáceis. A decisão de utilizar uma senha fraca foi propositada, tendo em conta a natureza académica da tarefa e a utilização num ambiente controlado. Em cenários reais, uma estratégia de passwords robustas seria implementada para reforçar a segurança.

Federated Radius

O propósito deste exercício, seria configurar um FreeRADIUS para autenticar utilizadores que estão armazenados tanto no Active Directory (AD) quanto no FreeRADIUS.

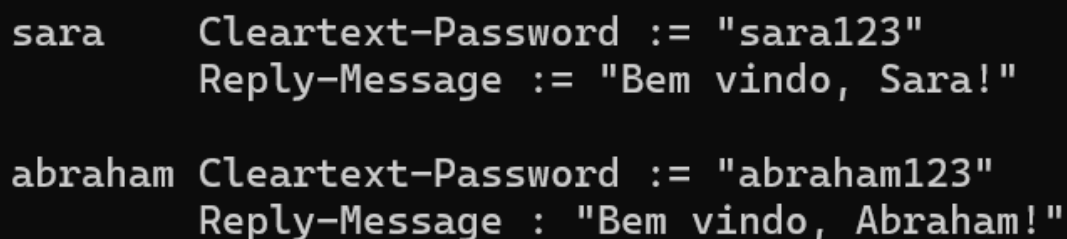
O Active Directory é um serviço de diretório desenvolvido pela Microsoft para sistemas operacionais Windows Server. Desempenha um papel crucial na gestão de identidades, oferece uma abordagem centralizada para a autenticação de utilizadores, controlo de acesso a recursos e aplicação de políticas de segurança, tornando-se essencial para a administração eficaz de redes corporativas.

A integração do AD com serviços como o FreeRADIUS, exemplifica como diferentes sistemas podem trabalhar juntos para fornecer autenticação e autorização robustas em ambientes heterogêneos.

1) Criação de utilizadores

Na realização deste exercício tínhamos de adicionar dois utilizadores Sara e Abraham ao FreeRADIUS e o Isaac e Moses ao Active Directory.

Para a adição dos utilizadores ao FreeRadius, editamos o ficheiro de configuração em “etc/freeradius/3.0/users/” e foram adicionados os utilizadores.



```
sara      Cleartext-Password := "sara123"  
          Reply-Message := "Bem vindo, Sara!"  
  
abraham  Cleartext-Password := "abraham123"  
          Reply-Message : "Bem vindo, Abraham!"
```

Figura 4: Criação Users no FreeRadius

Já no Windows Server, adicionamos o Isaac e Moses acedendo ao sistema administrativo do Active Directory “Active Directory Users and Computers”.

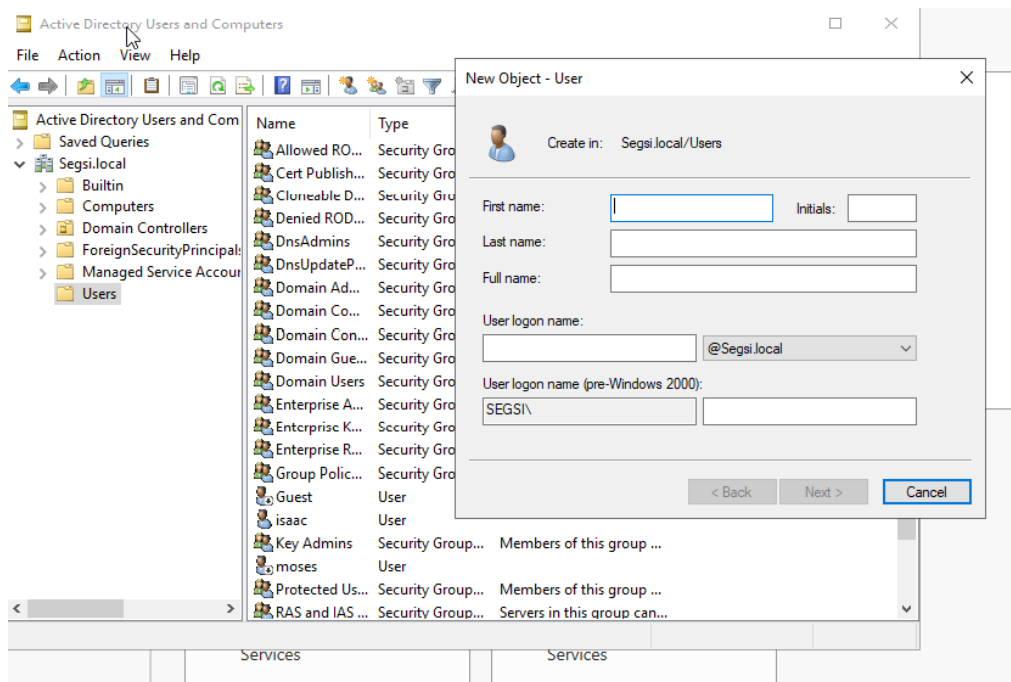


Figura 5: Criação Users no Active Diretory

2) Associação da máquina Linux ao Windows server

De forma a associar a máquina Linux ao Windows Server é necessário realizar a instalação dos seguintes packages: Samba e Winbind, sendo Samba utilizado para integrar o sistema Linux com o Active directory, e Winbind para realizar o sistema de autenticação para esse AD. Utilizamos o seguinte comando para instalar os packages necessários.

```
sudo apt-get install winbind samba
```

É depois necessário também adicionar o endereço IP do Active Directory como servidor DNS da máquina Linux, alterando o ficheiro “etc/resolv.conf”

```
nameserver 172.18.48.1

search Segsi.local
nameserver 10.0.2.15
```

Figura 6: Adicionar o endereço IP do AD à máquina Linux

Para incluir o campo `ntlm_auth` que define o sistema de autenticação da Microsoft (NTLM) no ficheiro de configuração do FreeRADIUS, adicionamos uma linha que chama o comando `ntlm_auth` na seção de autenticação apropriada do ficheiro `/etc/freeradius/3.0/sites-enabled/default`

```
ntlm_auth = "/usr/bin/ntlm_auth --username=%{mschap:User-Name} --domain=SEGSi --password=%{User-Password}"  
#
```

Figura 7 `ntlm_auth`

Alteramos o ficheiro de configuração do Samba, `/etc/samba/smb.conf`, com a informação do Active Directory configurado, SEGSi, no realm `segsi.local`.

```
#===== Global Settings =====  
  
[global]  
#### Kali configuration (use kali-tweaks to change it) ####  
  
# By default a Kali system should be configured for wide compatibility,  
# to easily interact with servers using old vulnerable protocols.  
client min protocol = LANMAN1  
  
## Browsing/Identification ##  
  
# Change this to the workgroup/NT-domain name your Samba server will part of  
workgroup = SEGSi  
security = ads  
realm = Segsi.local  
encrypt passwords = yes
```

Figura 8 Ficheiro `smb.conf`

Finalmente, é adicionado a máquina linux como administradora do Active Directory, utilizando o comando “`sudo net ads join -U Administrator`”.

3) Confirmação dos acessos

Durante a execução deste projeto, não conseguimos confirmar o acesso dos utilizadores após a configuração da Máquina Virtual Linux para integrar com o Active Directory, possivelmente devido a questões de configuração. No entanto, com os dados disponíveis, é viável deduzir a situação de acesso de cada máquina.

Na máquina Linux, todos os utilizadores configurados têm permissão de acesso. Isso ocorre porque a máquina Linux está configurada para permitir acessos via FreeRadius, onde os utilizadores Sara e Abraham estão inscritos, além de aceitar acessos dos utilizadores do Active Directory configurado na VM Windows, onde Isaac e Moses estão

registados. Por outro lado, apenas Isaac e Moses têm permissão de acesso à máquina Windows, configurada especificamente para esses dois utilizadores e não possui integração com a configuração do FreeRadius realizada na máquina Linux.

Devido às vulnerabilidades conhecidas do protocolo RADIUS, a conexão do Active Directory através do FreeRadius pode representar um ponto único de falha (SPOF). Isso ocorre porque esse tipo de acesso é menos seguro do que o acesso direto ao Active Directory.

Conclusão

Este estudo evidenciou a importância e as vantagens de implementar um sistema de controlo de acessos, destacando a habilidade de acelerar o procedimento de autenticação e autorização para múltiplos utilizadores. Neste cenário, a configuração e administração de serviços como FreeRadius e Active Directory demonstraram ser eficientes na definição de permissões.

Além disso, a experiência obtida possibilitou um entendimento mais profundo dos desafios de segurança associados a estes sistemas. Cada um deles pode apresentar as suas próprias fragilidades e vulnerabilidades, exigindo uma análise crítica das suas vantagens e desvantagens.