Hackers do Bem – Fundamental
Prof. Fábio Carneiro de Castro
24/02/2026

Atividade Prática – Módulo 5

Aulas 1 e 2

Gabriel dos Santos Schmitz

Este documento foi criado usando LaTeX
https://github.com/gabrielzschmitz/uni/tree/main/hackers-do-bem/fundamental/modulo5/aulas1-2.

1 Introdução

Este documento apresenta as evidências práticas das atividades do Módulo 5 (Aulas 1 e 2) do Programa Hackers do Bem – Nível Fundamental, por meio dos prints solicitados, demonstrando a correta execução das tarefas propostas.

Conforme as orientações do curso, este documento reúne, em um único arquivo PDF, os seguintes registros obrigatórios: Atividade 5.1 (passo 9), Atividade 5.2 (passo 9), Atividade 5.3 (passo 11), Atividade 5.4 (passo 10) e Atividade 5.5 (passo 12), todos acompanhados de breve descrição explicativa, com o objetivo de facilitar a análise e avaliação por parte do instrutor.

2 Atividades

Atividade 5.1. Criando o Active Directory no Windows Server 2022

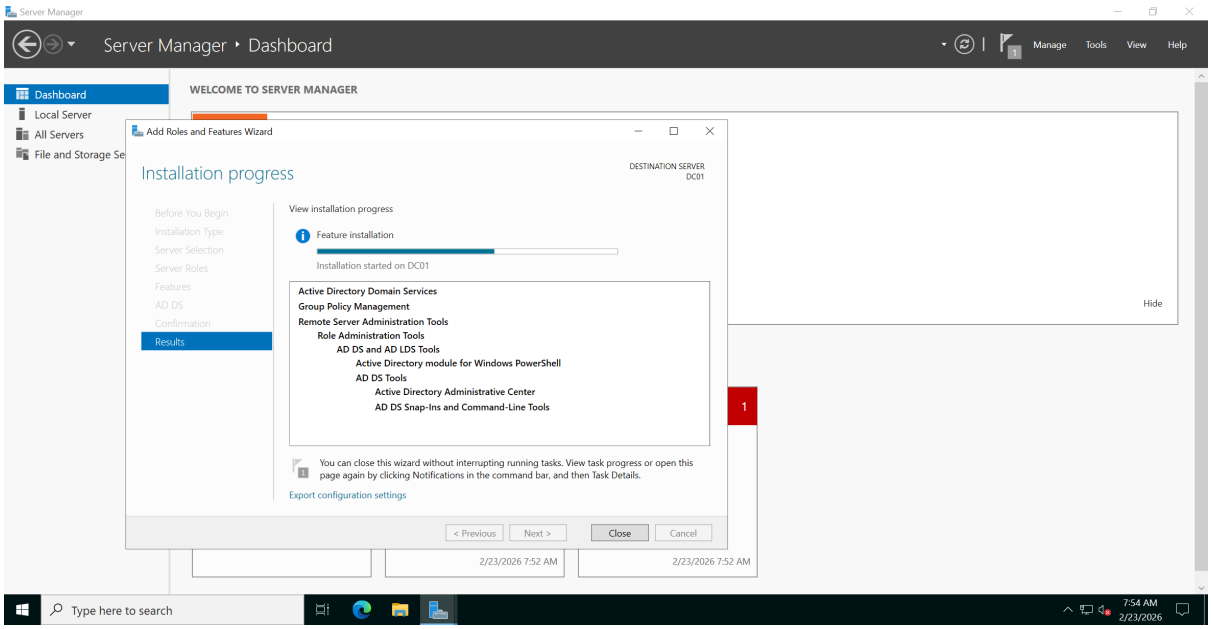

Fig. 1: Instalação da função Active Directory Domain Services no Windows Server 2022

Sobre:

Nesta atividade, foi realizado o processo de criação de um Active Directory no Windows Server 2022, evidenciando a configuração inicial de um controlador de domínio em um ambiente corporativo.

Inicialmente, foi estabelecida a conexão remota ao servidor por meio do RDP, utilizando as credenciais administrativas. Em seguida, foi acessado o utilitário *Server Manager*, responsável pelo gerenciamento centralizado das funções e recursos do sistema.

Posteriormente, foi realizada a alteração do nome do servidor para `DC01`, com o objetivo de padronizar a nomenclatura do controlador de domínio. Após a modificação, o sistema foi reiniciado para aplicar as alterações, sendo validada a mudança ao acessar novamente o *Server Manager*.

Na sequência, foi iniciado o assistente de instalação de funções e recursos por meio da opção *Add Roles and Features*. Durante esse processo, foram selecionadas as funções *Active Directory Domain Services* e *DNS Server*, essenciais para a implementação de um domínio e resolução de nomes na rede.

Também foram incluídos automaticamente recursos complementares, como *Group Policy Management* e *Remote Server Administration Tools*, necessários para o gerenciamento do ambiente.

Por fim, a instalação foi confirmada e executada, sendo possível acompanhar o progresso até sua conclusão. Este procedimento demonstrou a configuração inicial de um serviço de diretório, fundamental para o gerenciamento centralizado de usuários, grupos e políticas de segurança em redes corporativas.

Atividade 5.2. Criando o Domain Controller no Active Directory

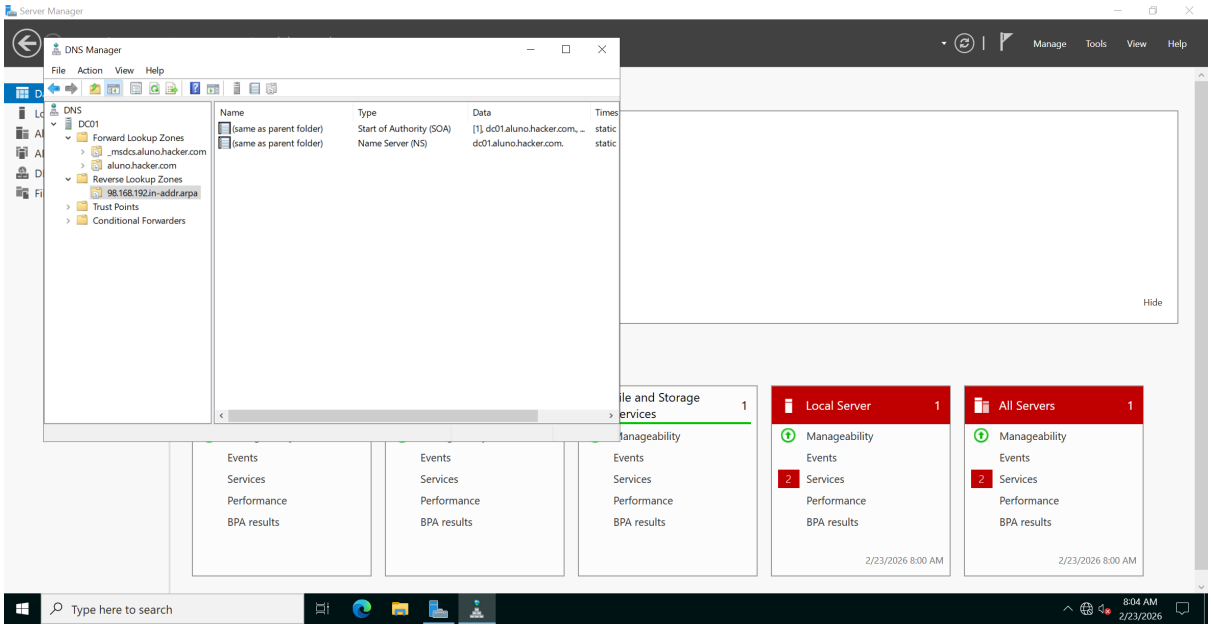

Fig. 2: Configuração do Domain Controller e verificação do DNS no Windows Server 2022

Sobre:

Nesta atividade, foi realizada a promoção do servidor previamente configurado a um Controlador de Domínio (*Domain Controller*), consolidando a implantação do Active Directory no ambiente.

Inicialmente, por meio do *Server Manager*, foi acessado o alerta de configuração pendente, representado por uma bandeira com indicação de atenção. A partir dessa notificação, foi iniciada a promoção do servidor utilizando a opção *Promote this server to a domain controller*.

Durante o assistente de configuração, foi selecionada a opção de criação de uma nova floresta (*Add a new forest*), sendo definido o domínio raiz como `aluno.hacker.com`. Em seguida, foram configuradas as credenciais de segurança do modo de restauração de serviços de diretório (DSRM), garantindo a proteção administrativa do ambiente.

Na etapa de validação, foi confirmado que o nome NetBIOS foi automaticamente definido como `ALUNO`. Após a verificação dos pré-requisitos, que foram atendidos com sucesso, a instalação foi iniciada, culminando na reinicialização automática do servidor para aplicação das configurações.

Após o reinício, foi estabelecida uma nova conexão remota via RDP, sendo realizado o acesso com a conta administrativa do domínio. Caso solicitado pelo sistema, a senha foi atualizada conforme as políticas de segurança.

Posteriormente, foi verificado no *Server Manager* que os serviços *Active Directory Domain Services (AD DS)*, *DNS* e *File and Storage Services* estavam devidamente instalados e ativos.

Na sequência, foi acessado o gerenciador de DNS, onde foram analisadas as zonas de pesquisa direta (*Forward Lookup Zones*), confirmando a criação do domínio `aluno.hacker.com`.

Em seguida, foi criada uma zona de pesquisa reversa (*Reverse Lookup Zone*), associada à rede `192.168.98.0/24`, permitindo a resolução de nomes a partir de endereços IP. Foi verificada a autoridade da zona (SOA) e a correta resolução de nomes, evidenciada por indicadores positivos no sistema.

Além disso, foi habilitada a atualização automática do registro PTR para o servidor, garantindo a correspondência entre nome e endereço IP. Após a atualização, foi confirmada a presença do registro na zona reversa, validando o funcionamento do DNS bidirecional.

Ao final, observou-se que o ambiente de domínio estava plenamente funcional, com serviços de diretório e resolução de nomes corretamente configurados, caracterizando a conclusão bem-sucedida da promoção do servidor a Domain Controller.

Atividade 5.3. Inserindo um usuário no Domínio do Active Directory

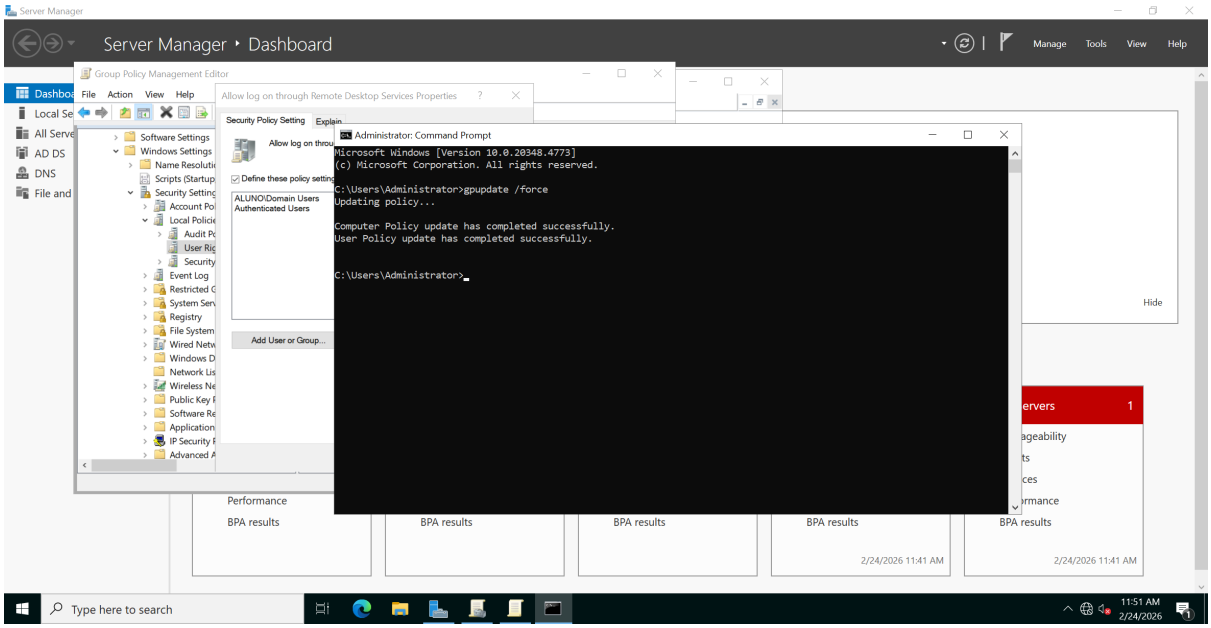

Fig. 3: Criação de usuário no Active Directory e aplicação de políticas de grupo

Sobre:

Nesta atividade, foi realizada a criação de um novo usuário no domínio do Active Directory, bem como a configuração de permissões e políticas de acesso por meio de Group Policy, garantindo a autenticação e o acesso remoto ao ambiente.

Inicialmente, por meio do *Server Manager*, foi acessada a ferramenta *Active Directory Users and Computers*. Dentro do domínio `aluno.hacker.com`, na pasta *Users*, foi criado um novo usuário com os seguintes dados: nome `Nome1 Sobrenome1` e login `nome1`. Durante a criação, foi definida uma senha segura e ajustadas as configurações para que a senha não expirasse, além de desabilitar a exigência de alteração no primeiro acesso.

Após a criação, foram configuradas permissões adicionais para o usuário, incluindo sua inserção no grupo *Remote Desktop Users*, permitindo o acesso remoto ao servidor via protocolo RDP.

Em seguida, foi realizada a configuração de políticas de grupo utilizando a ferramenta *Group Policy Management*. Foi criada uma nova Unidade Organizacional (OU) denominada `Rede1`, com o objetivo de organizar os objetos do domínio e aplicar políticas específicas.

Dentro dessa OU, foi criado um novo Objeto de Política de Grupo (GPO) chamado `Alunos`, que foi posteriormente editado para definir permissões de acesso remoto. No editor de políticas, foi configurada a diretiva *Allow log on through Remote Desktop Services*, adicionando os grupos *Domain Users* e *Authenticated Users*, garantindo que usuários do domínio possam realizar login remoto.

Por fim, foi executado o comando `gpupdate /force` no prompt de comando, forçando a atualização das políticas de grupo no sistema. A mensagem de sucesso confirmou que tanto as políticas de computador quanto as de usuário foram aplicadas corretamente.

Com isso, o ambiente passou a permitir a autenticação de usuários do domínio e o acesso remoto controlado, evidenciando a correta configuração do Active Directory e das políticas de segurança associadas.

Atividade 5.4. Configurando um cliente para ingressar no domínio do Active Directory

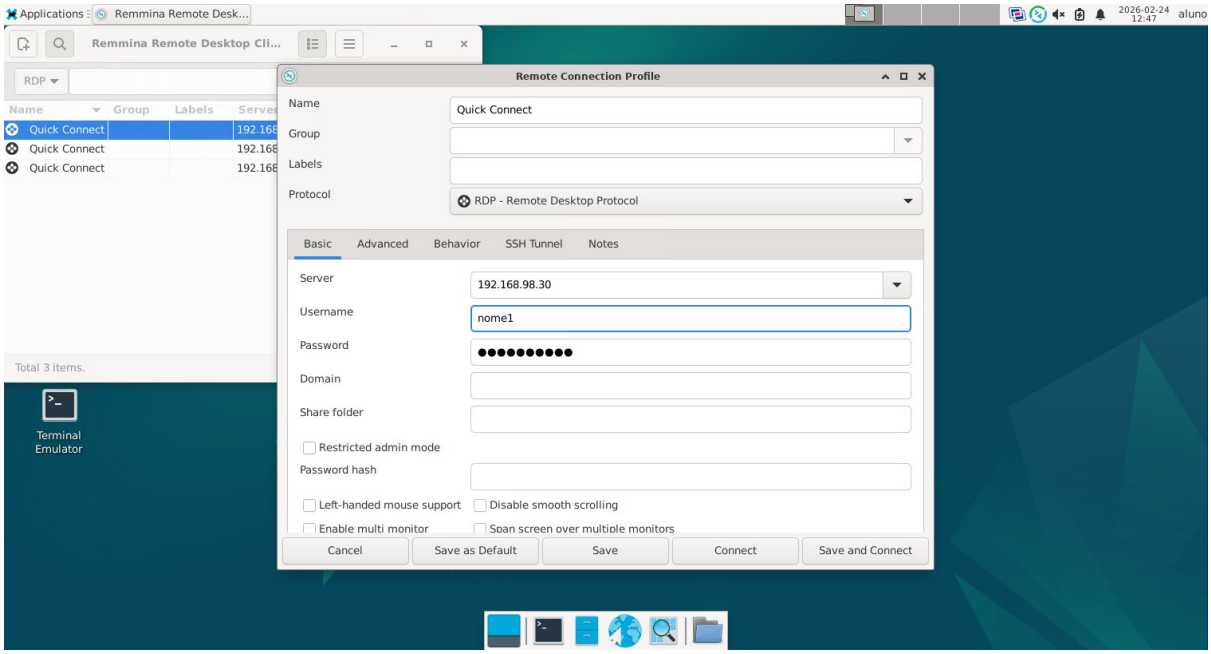

Fig. 4: Configuração do cliente no domínio e autenticação via Active Directory

Sobre:

Nesta atividade, foi realizada a configuração de um cliente Windows Server 2022 para ingressar no domínio do Active Directory previamente criado, permitindo a autenticação centralizada de usuários.

Inicialmente, no servidor, foi utilizado o comando `ipconfig` para identificar o endereço IP da máquina, sendo este `192.168.98.20`, que será utilizado como servidor DNS para os demais dispositivos da rede.

Em seguida, foi estabelecida uma conexão RDP com a máquina cliente (`192.168.98.30`), onde foram realizadas as configurações necessárias. Primeiramente, foi verificada a conectividade com o servidor por meio do comando `ping 192.168.98.20`, confirmando a comunicação entre as máquinas.

Posteriormente, foi configurado manualmente o servidor DNS do cliente, definindo o endereço `192.168.98.20` como servidor DNS preferencial. Essa etapa é essencial para que o cliente consiga localizar o controlador de domínio na rede.

Na sequência, foi acessado o *Server Manager* para instalar o recurso *Remote Assistance*, garantindo suporte remoto ao sistema. Em seguida, nas configurações avançadas do sistema, o cliente foi associado ao domínio `aluno.hacker.com`, utilizando as credenciais do usuário previamente criado no Active Directory.

Após a autenticação, o sistema confirmou a inclusão no domínio e foi realizada a reinicialização da máquina para aplicar as alterações.

Após o reinício, foram configuradas as permissões de acesso remoto, habilitando conexões RDP e adicionando o usuário do domínio `nome1` à lista de usuários autorizados para acesso remoto.

Por fim, foi realizada a autenticação no cliente utilizando as credenciais do domínio (`ALUNO\nome1`), validando que o computador foi corretamente integrado ao Active Directory e que o usuário possui permissão de acesso ao sistema.

Este procedimento demonstra o processo de integração de um cliente a um domínio Active Directory, evidenciando a centralização da autenticação e o controle de acesso em ambientes corporativos.

Atividade 5.5. Configurando política de senhas no GPO do Windows Server 2022

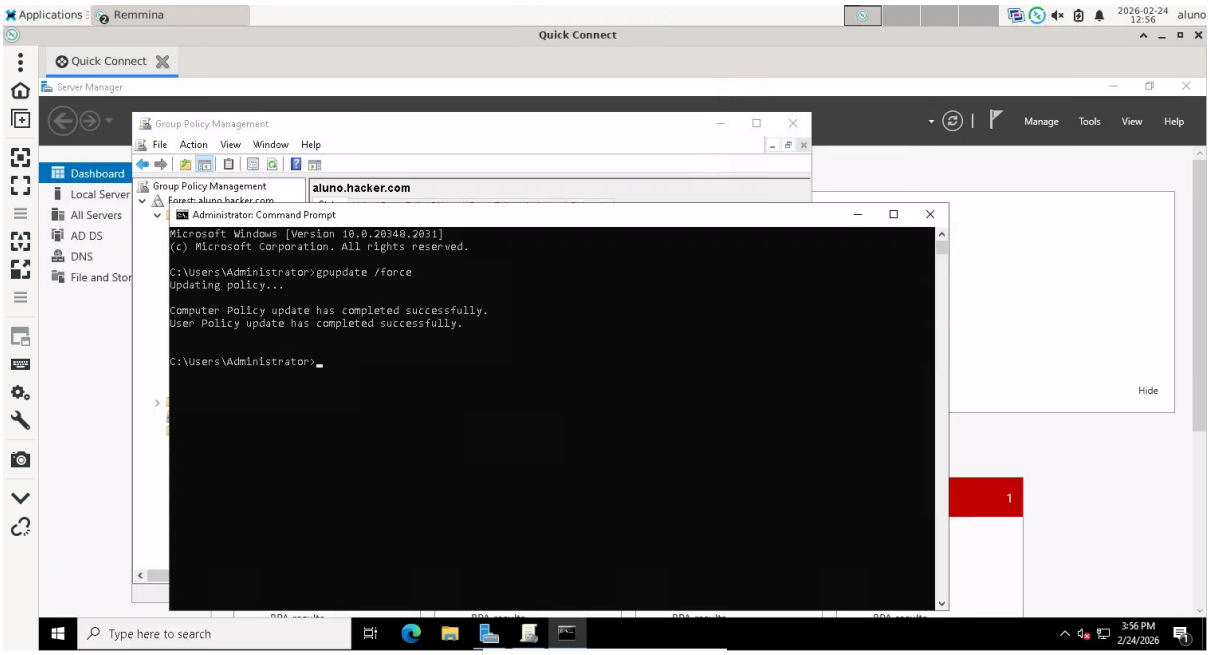

Fig. 5: Aplicação da política de senhas via Group Policy no domínio

Sobre:

Nesta atividade, foi realizada a configuração de uma política de senhas no Active Directory por meio do Group Policy Object (GPO), com o objetivo de reforçar a segurança das credenciais utilizadas no domínio.

Inicialmente, foi acessado o *Server Manager* no Windows Server 2022 e, por meio da opção *Tools*, foi aberta a ferramenta *Group Policy Management*. Em seguida, navegou-se até o domínio `aluno.hacker.com`, onde foi criada uma nova política denominada `Politica de senhas` dentro da pasta *Group Policy Objects*.

Após a criação, a política foi editada utilizando o *Group Policy Management Editor*, onde foram configuradas as diretrizes de senha localizadas em *Computer Configuration ¿ Policies ¿ Windows Settings ¿ Security Settings ¿ Account Policies ¿ Password Policy*.

Foram definidos os seguintes parâmetros de segurança:

- Idade mínima da senha configurada para 120 dias, garantindo a expiração periódica das credenciais;
- Comprimento mínimo da senha definido em 9 caracteres, aumentando a resistência contra ataques de força bruta;
- Habilitação da complexidade de senha, exigindo a combinação de diferentes tipos de caracteres;
- Histórico de senhas configurado para armazenar as últimas 3 senhas, prevenindo a reutilização imediata.

Após a configuração, a política foi vinculada ao domínio `aluno.hacker.com`, garantindo que todos os computadores e usuários do domínio estejam sujeitos às regras estabelecidas.

Por fim, foi utilizado o comando `gpupdate /force` no *Command Prompt* para forçar a atualização das políticas no sistema, confirmando a aplicação das configurações definidas.

Este procedimento evidencia a utilização de políticas de grupo para o fortalecimento da segurança em ambientes corporativos, promovendo boas práticas de gerenciamento de credenciais e mitigando riscos relacionados a senhas fracas ou reutilizadas.