2025

Relatório de Vulnerabilidade dos servidores

CIBERSEGURANÇA

JOSÉ COUTO, 2024026
RAFAEL BAPTISTA,2024134
RODRIGO BALTAZAR, 2024142
SAMUEL ROCHA, 2024127

Índice

Introdução

Este relatório tem como objetivo alertar a instituição acerca de uma vulnerabilidade crítica que encontramos no domínio do ISTEC. Através dos computadores da sala de aula podemos aceder e tomar controle total do servidor da instituição, podendo colocar em causa todo o funcionamento de seus serviços e o vazamento de toda a informação sigilosa.

Por meio do servidor, notamos ser possível aceder aos computadores da secretaria, e seus respetivos conteúdos, assim como os do administrador de rede e de toda a instituição, o que permite o controle total do sistema.

O nosso intuito em relatar aqui esta vulnerabilidade é para que seja mitigada o mais rápido possível e assegurar a segurança da informação de todos. Realçamos o nosso zelo e compromisso ético perante a instituição de que nenhuma informação sigilosa foi comprometida e nenhum dano ao servidor e demais serviços foi realizado durante a análise desta vulnerabilidade.

Vulnerabilidade

O servidor do ISTEC presta um importante serviço a instituição. Através dele, diferentes utilizadores, com cargos e funções variados, podem aceder aos seus postos de trabalho, compartilhar pastas e arquivos, utilizar programas e muito mais, o que facilita muito a administração do sistema. Todo esse serviço é gerido por um administrador de sistema, que é o responsável por criar as regras para os utilizadores, instalar os programas e fazer a sua manutenção, o que lhe dá controle total de todo o servidor.

A vulnerabilidade está justamente na existência de um utilizador chamado de ***teste*** com credenciais de administrador. Notamos a existência deste utilizador ao usarmos os computadores da sala de aula e acedermos a pasta utilizadores, lá ao habilitarmos as pastas ocultas o encontramos.

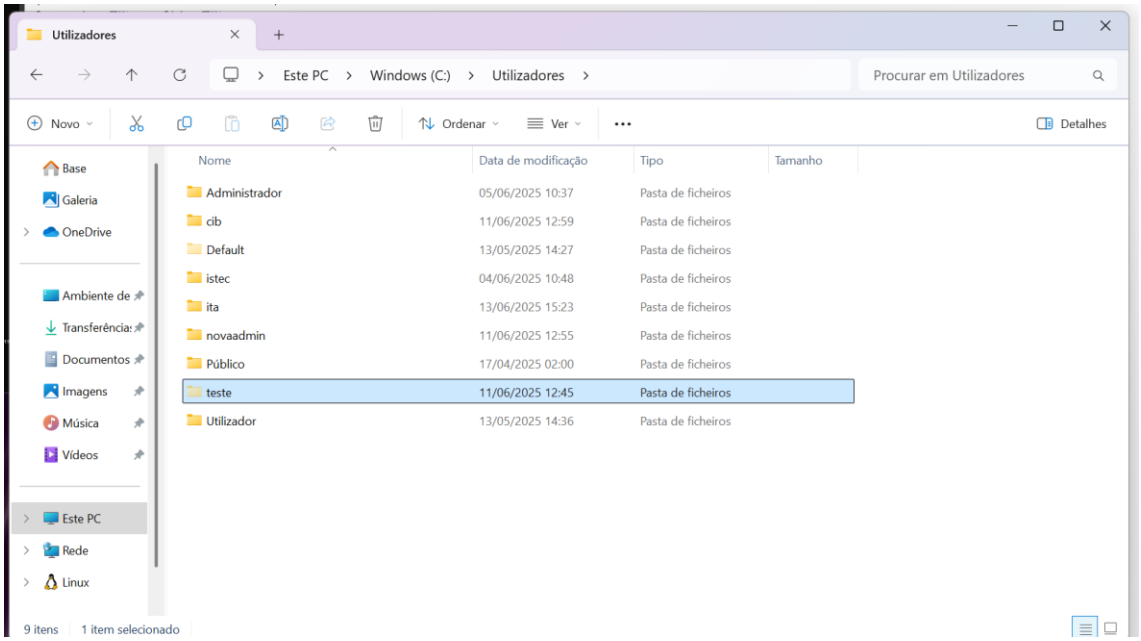

Figura 1 Imagem retirada dos computadores da sala de Cibersegurança.

A existência do utilizador não é a vulnerabilidade, e sim a sua palavra-passe muito frágil: “teste”. Isso nos permitiu aceder aos computadores da sala de aula com privilégio de administrador.

Escalada para o servidor

Agora com este utilizador somos administradores locais, apenas no computador da sala de aula, o próximo passo para explorar a vulnerabilidade é escalar para administrador de domínio, o responsável pelo servidor. Para isso nós precisávamos do endereço do servidor, o seu ip.

Para obtermos o ip bastou aceder até o prompt de comando do Windows, e utilizar o comando: *ipconfig /all*.

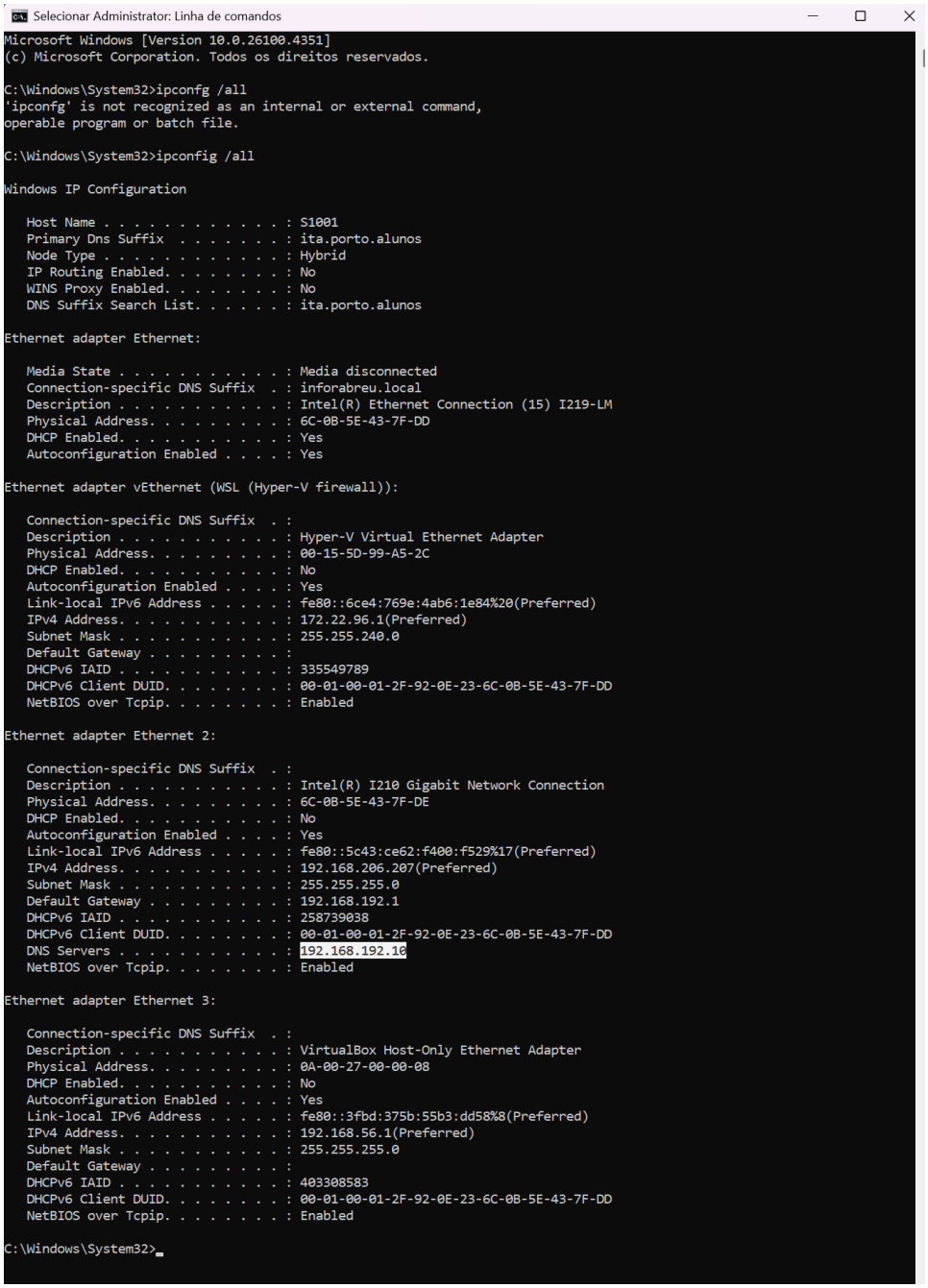

Figura 2 Imagem retirada do terminal de comando apos o comando ipconfig /all

O comando exibe todas as configurações de ip do Windows, onde o computador está conectado e muitas outras informações. Obtivemos 2 números de ips importantes, o ip do roteador, que logo foi descartado com uma das possibilidades de ser o servidor, e o ip do servidor DNS.

Para confirmarmos se o ip do servidor era realmente o mesmo do DNS rodamos um pequeno script chamado **nmap**, com ele é possível verificar todas as portas abertas do firewall.

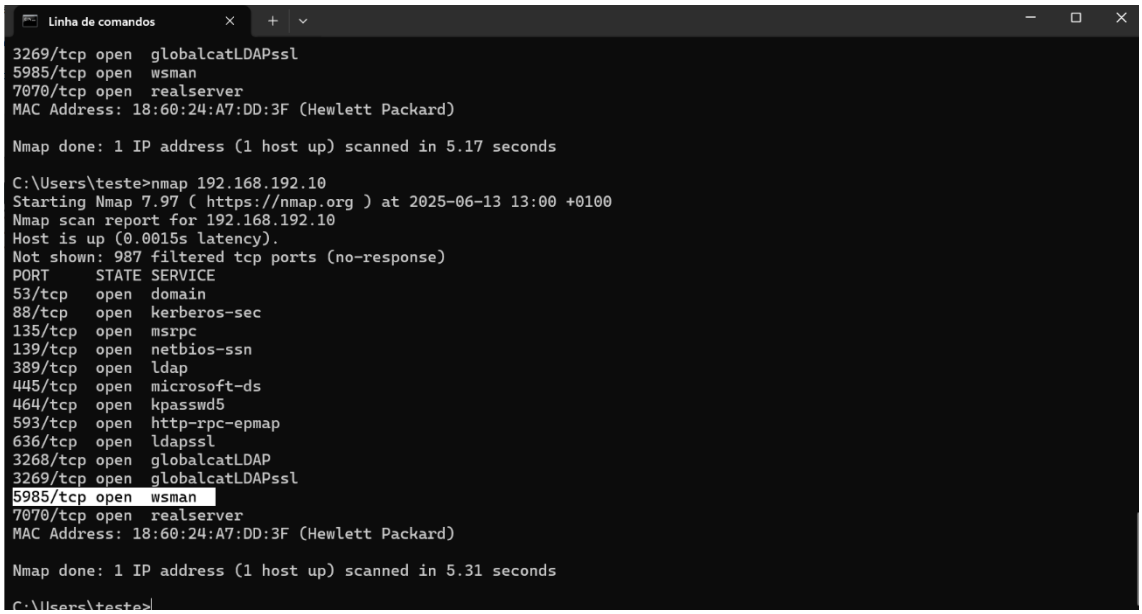

Figura 3 Imagem retirada do terminal após o comando nmap.

Duas portas chamaram a nossa atenção, a primeira a porta 88, do protocolo de autenticação Kerberos, utilizada principalmente em servidores de ambiente corporativo que utilizam o Active Directory da Microsoft, forte indício de que encontramos o ip do servidor.

A segunda porta trata-se da 5985 wsman, porta para aceder remotamente ao servidor e que não possuí nenhum tipo de criptografia.

O próximo passo era testar se nossas credenciais de administradores locais também estavam configuradas como administradores de domínio, e assim acedermos ao controle do servidor. Para isso, utilizamos o PowerShell do Windows e tentamos aceder remotamente através da porta 5985 o terminal de controle do servidor com o seguinte comando.

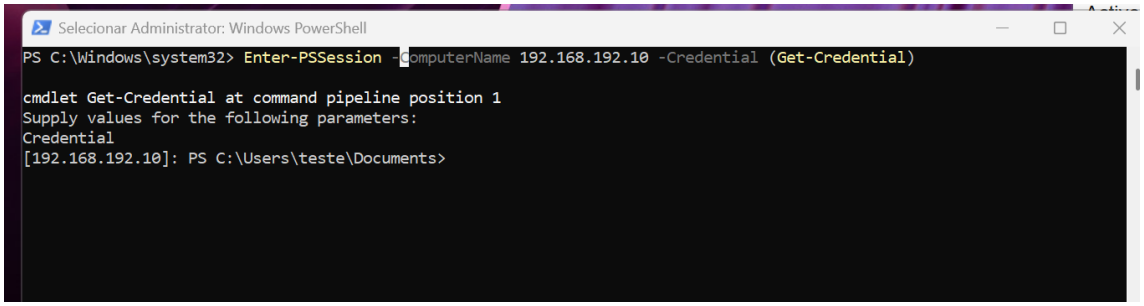

Figura 4 Comando realizado no PowerShell para aceder remotamente.

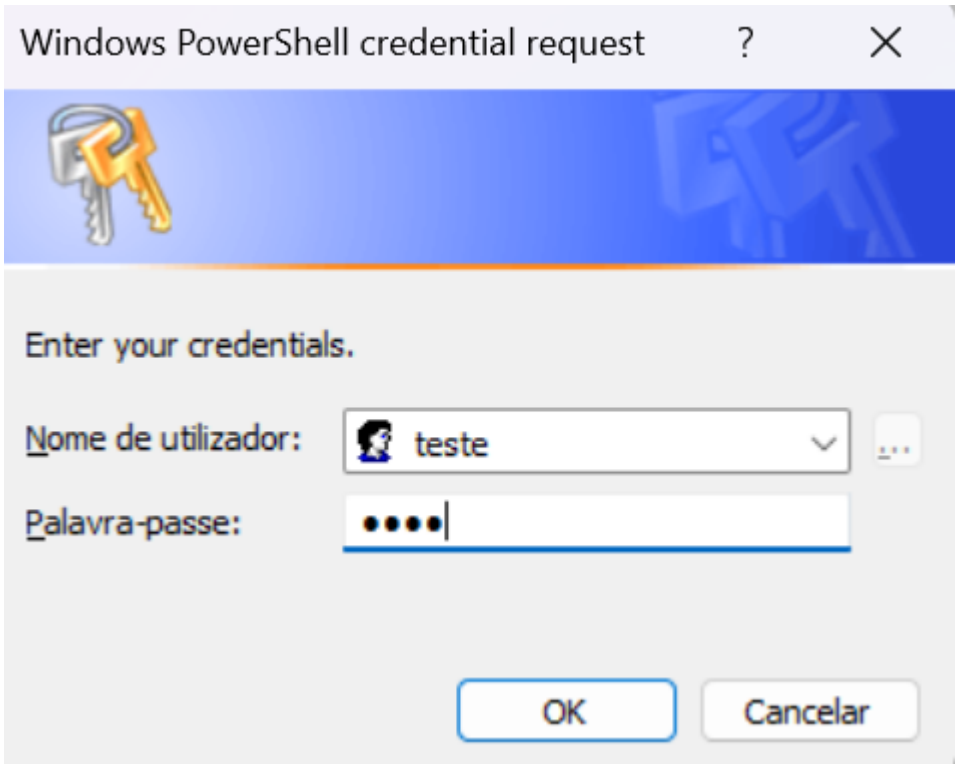

Figura 5 Credenciais do utilizador teste.

Assim descobrimos que o utilizador teste possuía o privilégio de administrador de domínio e entramos no terminal do servidor.

No terminal utilizamos dois comandos no terminal do servidor para podermos aceder remotamente:

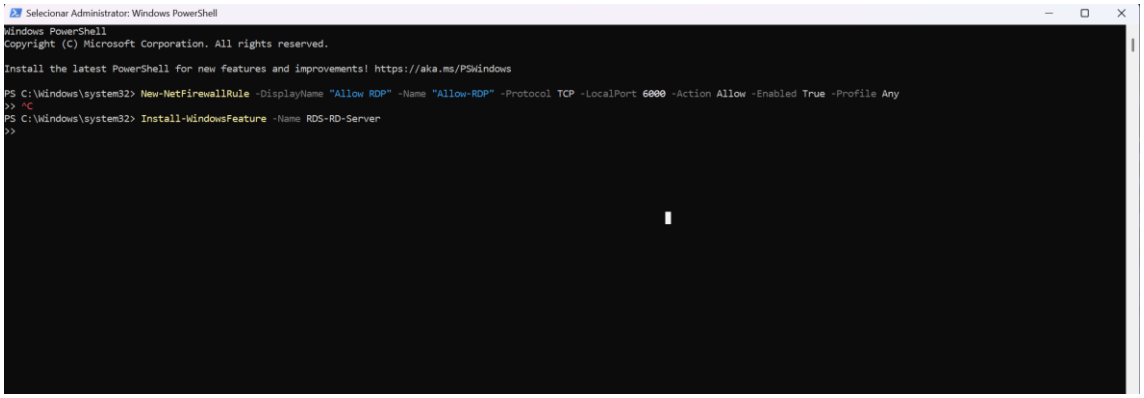

Figura 6 Comandos utilizados no PowerShell

O primeiro adicionou uma nova regra na firewall do servidor que permitiu a conexão remota. O segundo instalou no servidor o acesso remoto do Windows, ferramenta amplamente utilizada criada pela própria Microsoft para aceder remotamente.

Bastava agora aceder remotamente através do ip do servidor com o seguinte comando:

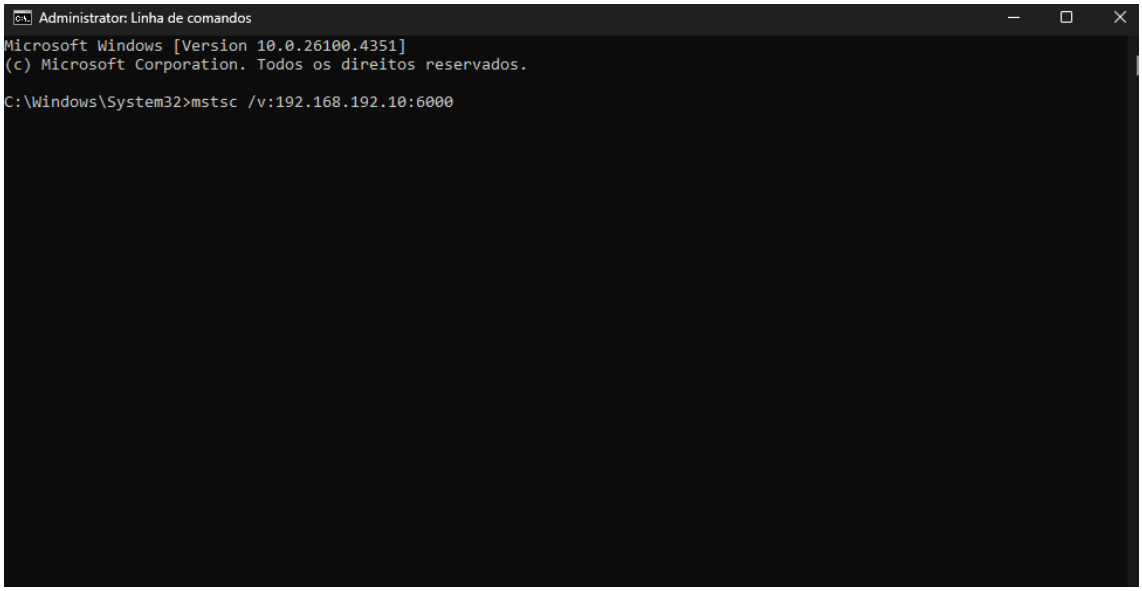

Figura 7 Comandos utilizado no prompt de comando do Windows.

O que nos permitiu aceder e tomar controle total do servidor:

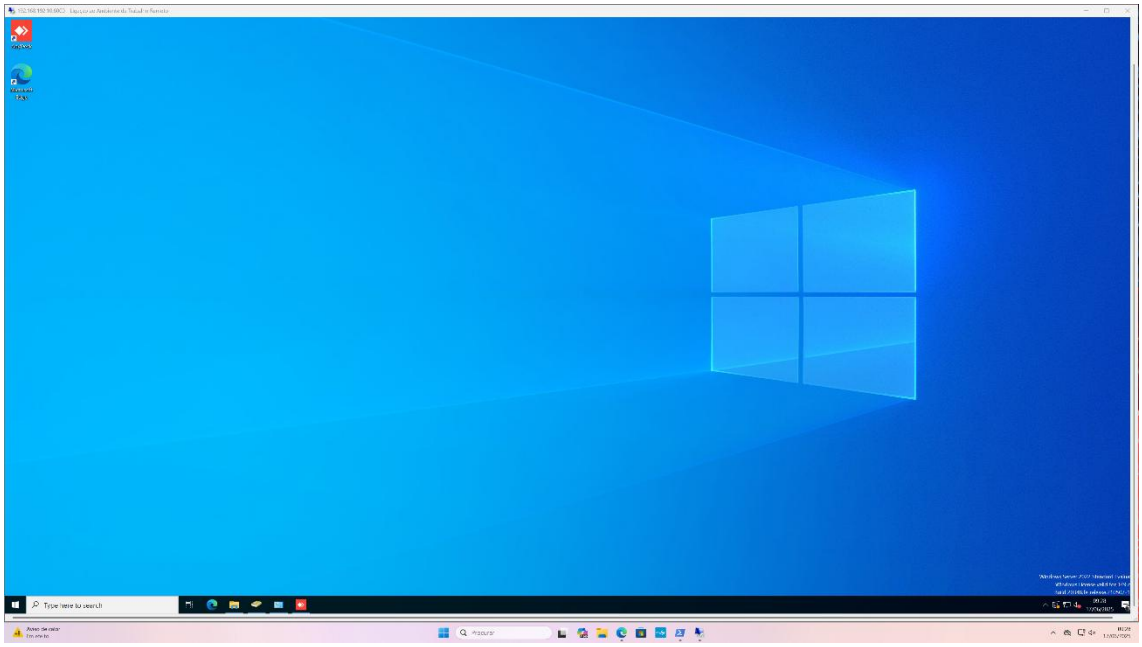

Figura 8 Imagem retirada do Desktop do servidor.

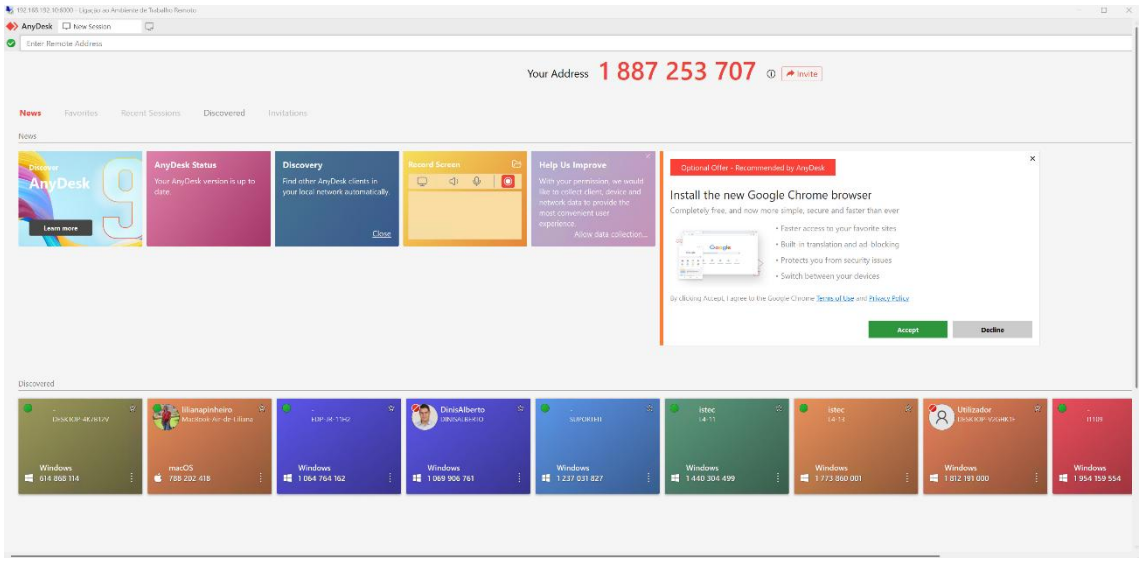

Figura 9 Imagem do AnyDesk retirada do servidor durante a tomada de controle.

Aqui, é possível aceder remotamente a qualquer computador e utilizador do ISTEC, assim como suas pastas e conteúdos. Apesar de totalmente possível, não acedemos a nenhum outro computador ou pasta para respeitar a privacidade e informação de todos, demonstrar essa capacidade violaria a lei de proteção de dados, RGPD.

Solução para a vulnerabilidade

A principal causa desta vulnerabilidade está na existência de um utilizador com privilégios de administrador com credencias muitos simples. Para maior segurança, somente a utilizador do administrador deve ter estes privilégios e sua palavra-passe deve ser a mais segura possível. Por isso recomendamos a exclusão imediata do utilizador teste e a mudança da palavra passe do administrador, que também foi descoberta por estar em uma pasta compartilhada no domínio:

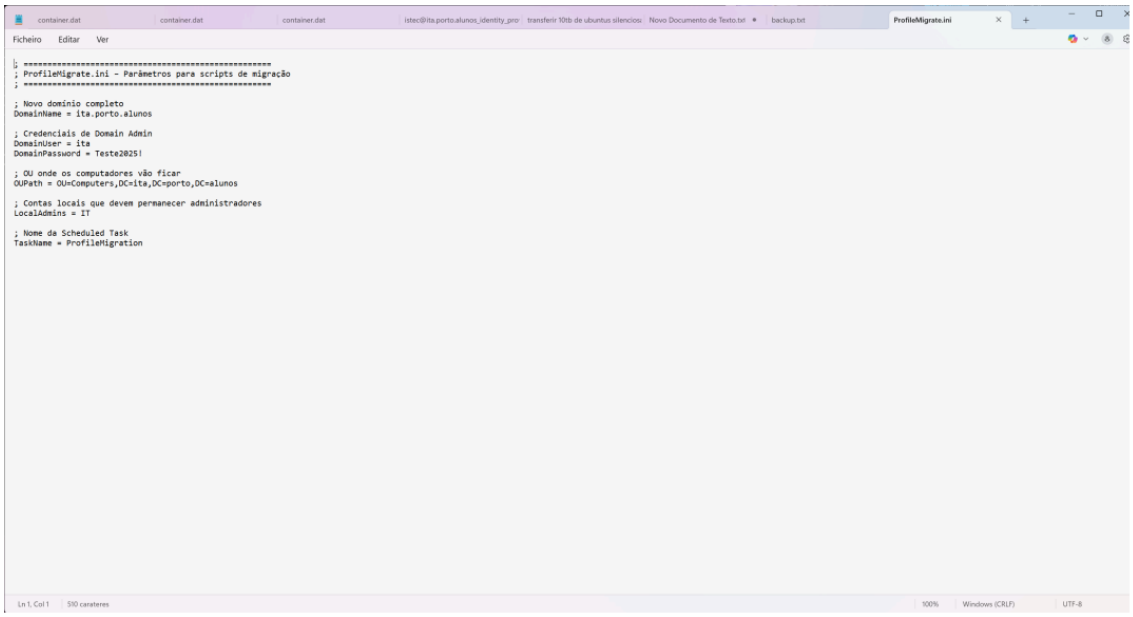

Figura 10 Arquivo de texto com as credenciais do administrador.

Além da vulnerabilidade principal, outra vulnerabilidade encontrada foi o uso da porta da, 5985 wsman. Está porta utiliza o protocolo HTTP sem nenhum tipo de criptografia, o que a torna insegura. Se o acesso remoto for necessário, deve-se utilizar a porta 5986 com o protocolo HTTS, criptografando o tráfego WinRM. Caso o acesso remoto for desnecessário, esta porta deve ser fechada.

Conclusão

O controle do servidor por pessoas não autorizadas é uma das falhas mais graves que podem ocorrer, pois poem em causa a segurança de toda a informação ali armazenada. Nós como alunos do ISTEC, zelamos pela segurança, privacidade e integridade da instituição, e por isso escrevemos esse relatório tendo em vista exclusivamente a proteção de todos. Em nenhum momento tivemos a intenção de prejudicar o trabalho dos profissionais envolvidos na administração, secretaria, professores e alunos. Esperamos que este pequeno relatório ajude a instituição a se tornar cada vez melhor e que demonstre o sucesso técnico e ético do curso de Cibersegurança que começou a tão pouco tempo. Estamos a inteira disponibilidade para esclarecer qualquer dúvida que surja sobre o tema abordado e dispostos a contribuir mais para a segurança da instituição caso seja requisitado.