

Instituto Superior de Engenharia

Politécnico de Coimbra

Projeto B

SERVIÇOS DE REDE 2

Diogo Valente

a2020144110@isec.pt

Alexandre Moreira

a2020144214@isec.pt

Licenciatura em Engenharia Informática
Ramo de Redes e Administração de Sistemas
ISEC

Coimbra, 25 de janeiro 2024

Índice

1	Introdução	1
2	iSCSI	3
2.1	Introdução ao iSCSI	3
2.2	Arquitetura iSCSI	4
2.3	Porquê TCP/IP?	4
2.4	iSCSI Protocol Data Unit	5
2.4.1	Operation codes for iSCSI initiators:	6
2.4.2	Operation codes for iSCSI targets:	6
2.5	Funcionamento iSCSI	7
2.5.1	Sessão iSCSI	7
2.5.2	iSCSI Login	8
2.5.3	Exemplo de Operação de Escrita	10
2.5.4	Exemplo de Operação de Leitura	10
3	Implementação do iSCSI	11
3.1	Ambiente de Configuração	11
3.2	Topologia do Switch	12
3.3	Configurar o iSCSI Target	12
3.4	Configurar o iSCSI Initiator	15
4	Análise Prática	23
4.1	Fase de login	23
4.1.1	Normal Login	25
4.1.2	Discovery	27

4.2	NOP-IN e NOP-OUT	28
4.3	Operação de Escrita	29
4.4	Operação de Escrita	31
4.5	Conclusão	33
Referências		35

Lista de Figuras

2.1	TCP	5
2.2	iSCSI PDU	6
2.3	Fases iSCSI	8
2.4	Write Operation	10
2.5	Read Operation	10
3.1	ESXi Web Interface	11
3.2	Switch	12
3.3	Role Target Server	13
3.4	Diretório do disco Virtual no Target	13
3.5	CHAP	14
3.6	Initiators Permitidos	14
3.7	Tools	15
3.8	Iniciar o serviço	15
3.9	Quick Connect	16
3.10	Connect	17
3.11	Advanced	18
3.12	Autenticação CHAP	19
3.13	Conectado com sucesso	20
3.14	Disco Virtual iSCSI	21
3.15	Colocar disco online	21
3.16	Disco iSCSI	22
4.1	iSCSI Login	24
4.2	Primeiro Pacote iSCSI Login	25

4.3	ESXi VMs	26
4.4	Segundo Pacote iSCSI Login	26
4.5	Value: Discovery	28
4.6	Retorno	28
4.7	NOP-IN e NOP-OUT	29
4.8	Pacotes Operação Write	29
4.9	1º pacote Write	30
4.10	2º pacote Write	30
4.11	3º pacote Write	30
4.12	4º pacote Write	31
4.13	Pacotes Operação Read	31
4.14	1º Pacote da Operação Read	32
4.15	2º Pacote da Operação Read	32
4.16	3º Pacote da Operação Read	33

Acrónimos e Siglas

iSCSI *Internet Small Computer System Interface.*

IP *Internet Protocol.*

LUN *Logical Unit Number.*

OSI *Open System Interconnection*

SCSI *Small Computer System Interface*

iSCSI PDU *iSCSI protocol data unit*

VPN *Virtual Private Network*

CHAP *Challenge-Handshake Authentication Protocol*

PDU *Protocol Data Unit*

Capítulo 1

Introdução

No âmbito do projeto B da disciplina de Serviços de Rede 2, fomos desafiados pelo docente, a explorar um serviço de rede. A escolha recaiu sobre o *Internet Small Computer System Interface* (iSCSI), um protocolo que permite o acesso a blocos de dados de armazenamento remoto por meio de uma infraestrutura *Internet Protocol* (IP) existente. Este protocolo é uma das principais tecnologias de armazenamento em rede e é utilizado por uma vasta gama de empresas para aumentar a sua estrutura de armazenamento.

Capítulo 2

iSCSI

2.1 Introdução ao iSCSI

O *Internet Small Computer System Interface* (iSCSI) é um protocolo de transporte de nível 2 que permite a transferência de dados pela Internet e a gestão de armazenamento em redes de longa distância, utilizando o protocolo TCP/IP. Desenvolvido no final dos anos 90 e início dos anos 2000 como uma alternativa de baixo custo aos canais de fibra tradicionais, o iSCSI é agora amplamente utilizado em muitas aplicações de armazenamento de dados, incluindo armazenamento em *cloud* e virtualização. Como é um protocolo de transporte de nível 2, o iSCSI opera na camada de transporte do modelo *Open System Interconnection* (OSI), responsável pela entrega confiável e sequencial de pacotes de uma origem para um destino, com controle de fluxo, detecção e correção de erros.

Comparativamente, o *Small Computer System Interface* (SCSI) é um protocolo de nível 1 que opera na camada física e permite que múltiplos dispositivos sejam conectados numa única cadeia. A principal diferença entre SCSI e iSCSI reside no fato de que o SCSI é um protocolo de conexão direta que requer um cabo físico, enquanto o iSCSI é um protocolo de rede que permite que os comandos SCSI sejam enviados através de uma rede *Internet Protocol* (IP).

2.2 Arquitetura iSCSI

A arquitetura do iSCSI é composta por initiators e um target, que comunicam entre si através do protocolo iSCSI.

- **Initiator:** São dispositivos que estão localizados do lado do cliente. Estabelecem uma ligação TCP/IP para se conectar aos targets e enviam comandos SCSI para pedir serviços de componentes, as *Logical Unit Number* (LUN), de um servidor, chamado de target.
- **Target:** O target é um dispositivo de armazenamento remoto que recebe, processa os comandos SCSI enviados pelo initiator e retorna as respostas ao initiator, permitindo o acesso aos dados armazenados.

O que o target partilha é uma área de armazenamento conhecida como LUN que é essencialmente uma área num disco rígido que o initiator procura depois de ter estabelecido a conectividade. O resultado é uma ligação direta entre um cliente a um disco rígido / sistema de armazenamento, como se os mesmos estivessem fisicamente conectados.

2.3 Porquê TCP/IP?

[1]Não ocorre perda de pacotes durante a transferência de dados, se houver alguma perda, é tratada pelo protocolo TCP/IP no sistema operativo. O protocolo iSCSI é uma representação do modelo de invocação de procedimentos remotos SCSI sobre o protocolo TCP. Comandos SCSI são transportados por iSCSI requests, e SCSI responses e os estados são transportados por respostas iSCSI. O iSCSI utiliza o mecanismo de pedido e resposta.

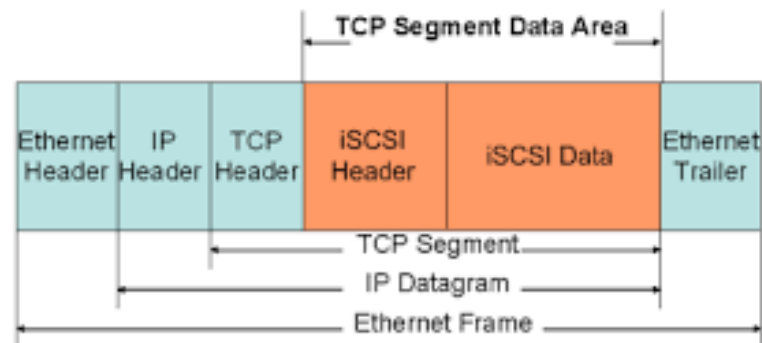


Figura 2.1: TCP

O *initiator* e o *target* dividem as suas comunicações em mensagens. As mensagens são transferidas em termos de *iSCSI protocol data unit* (iSCSI PDU). A comunicação entre o *initiator* e o *target* ocorre através de uma ou várias conexões TCP. A conexão TCP transporta mensagens de controlo, comandos SCSI, dados e parâmetros através de Unidades de Dados de Protocolo iSCSI (iSCSI PDUs). O conjunto de conexões TCP que ligam um *initiator* a um *target* forma uma sessão.

Um ID de sessão define uma sessão e consiste numa parte do *initiator* e numa parte do *target*. As conexões TCP podem ser adicionadas e removidas de uma sessão. Todas as conexões numa sessão são identificadas através de um ID de conexão.

2.4 iSCSI Protocol Data Unit

A PDU iSCSI é a unidade de informação do iSCSI. A PDU é utilizada para a comunicação entre o *initiator* e o *target*. Esta comunicação inclui a deteção do nó, a ligação e o estabelecimento de sessões, o transporte de comandos iSCSI e a transferência de dados. O segmento tem um comprimento fixo de 48 bytes.

A figura 2.2 representa a estrutura básica do iSCSI PDU.

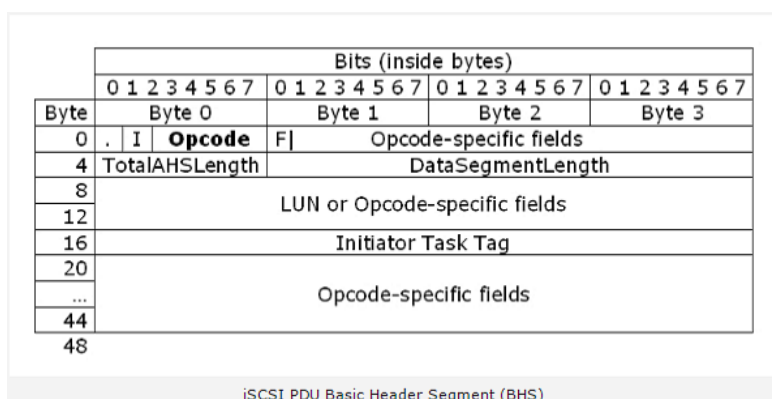


Figura 2.2: iSCSI PDU

2.4.1 Operation codes for iSCSI initiators:

- 0×00 – NOP-Out
- 0×01 – SCSI Command
- 0×02 – SCSI Task Management Function Request
- 0×03 – Login Request
- 0×04 – Text Request
- 0×05 – SCSI Data-Out
- 0×06 – Logout Request
- 0×10 – SNACK Request
- 0×1C-0×1E – Vendor specific codes

2.4.2 Operation codes for iSCSI targets:

- 0×20 – NOP-In
- 0×21 – SCSI Response
- 0×22 – SCSI Task Management function response

- 0×23 – Login Response
- 0×24 – Text Response
- 0×25 – SCSI Data-In
- 0×26 – Logout Response
- 0×31 – Ready To Transfer (R2T)
- 0×32 – Asynchronous Message
- 0×3C-0×3E – Vendor specific codes
- 0×3F – Reject

2.5 Funcionamento iSCSI

Para o restante deste documento, os termos "initiator" e "target" referem-se, respetivamente, ao nó "iSCSI initiator" e ao nó "iSCSI target".

Por razões de desempenho, o iSCSI permite uma "phase-collapse". Um comando e os dados associados podem ser enviados em conjunto do *initiator* para o *target*, e dados e respostas podem ser enviados em conjunto dos *targets*.

A direção de transferência iSCSI é definida em relação ao *initiator*. Transferências de saída ou de envio são transferências do *initiator* para um *target*, enquanto transferências de entrada ou de receção são do *target* para um *initiator*.

2.5.1 Sessão iSCSI

- **Sessão Operacional Normal** - [2] uma sessão na qual comandos SCSI, dados e respostas podem ser transferidos entre um *initiator* iSCSI e um *target* iSCSI
- **Sessão de Discovery** - uma sessão aberta apenas para a descoberta de *targets*.

2.5.2 iSCSI Login

Uma sessão iSCSI tem duas fases:

- Fase de Login
- Fase completa com recursos

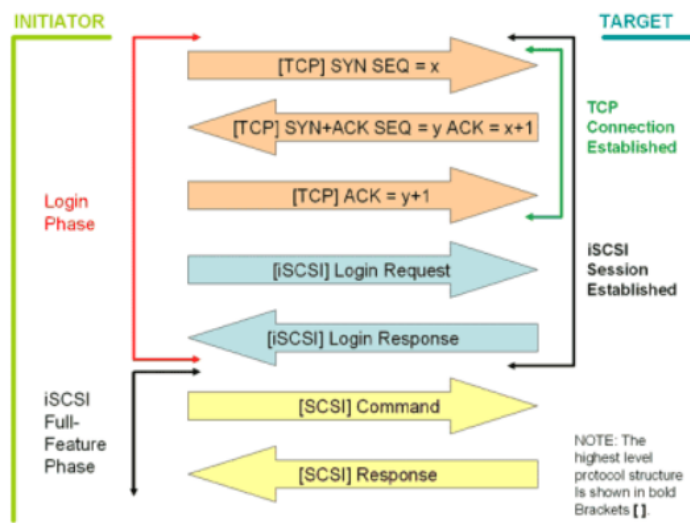


Figura 2.3: Fases iSCSI

Fase de Login

A Fase de Início de Sessão iSCSI consiste em *request e responses* de início de sessão. Uma vez concluída a autenticação e definidos os parâmetros operacionais, a sessão transita para a Fase Completa com Recursos, e o *initiator* começa a realizar operações.

Os parâmetros iSCSI são negociados através de pedidos e respostas de início de sessão durante o estabelecimento da sessão. Durante a Fase Completa com Recursos, os parâmetros iSCSI são negociados através de pedidos e respostas de texto. Em ambos os casos, o mecanismo consiste numa troca de pares chaves=valor de texto iSCSI (também referidos como pares key=value pairs).

A Fase de Login ocorre em duas etapas:

- Etapa de Segurança/Autenticação

Esta etapa consiste em trocas de texto utilizando IDs e Certificados, através de pares chave=valor.

Uma das chaves negociadas nesta etapa da Fase de Login é o AuthMethod. Por exemplo:

- key=value AuthMethod=CHAP
- AuthMethod define o método de autenticação.

- Etapa de Negociação de Parâmetros Operacionais

Esta etapa consiste na negociação de strings de texto para os parâmetros operacionais utilizando pares chave=valor em troca de parâmetros de *login*.

Dois dos muitos parâmetros de início de sessão negociados nesta etapa de Negociação de Parâmetros Operacionais da Fase de Início de Sessão são o *MaxRecvDataSegmentLength* e o *FirstBurstLength*. Por exemplo:

- key=value MaxRecvDataSegmentLength=<valor-numérico>
- MaxRecvDataSegmentLength define o comprimento máximo do segmento de dados que um iniciador ou destino pode receber num PDU iSCSI (em bytes).
- key=value key=value FirstBurstLength=<valor-numérico>
- FirstBurstLength define a quantidade máxima de dados não solicitados que o iniciador pode enviar ao destino durante a execução de um único comando SCSI (em bytes).
- *FirstBurstLength* define a quantidade máxima de dados não solicitados que o iniciador pode enviar ao destino durante a execução de um único comando SCSI (em bytes).

Fase completa com recursos

Após concluir com sucesso a Fase de Login na primeira ligação da sessão, a sessão entra na Fase Completa com Recursos.

Na Fase Completa com Recursos, o *initiator* envia comandos e dados SCSI para o *target* encapsulando-os em PDUs iSCSI que percorrem a sessão iSCSI (transporte). O *initiator* recebe respostas SCSI incorporadas em PDUs iSCSI do *target*. As operações só ocorrem após o início da Fase Completa com Recursos.

2.5.3 Exemplo de Operação de Escrita

Na imagem 2.4 podemos ver a ordem dos pacotes de escrita.

Initiator Function	PDU Type	Target Function
Command request (write)	SCSI Command (Write)>>>	Receive command and queue it
		Process old Commands
	<<< R2T	Ready to process WRITE command
Send Data	SCSI Data-Out >>>	Receive Data
	<<< R2T	Ready for data
	<<< R2T	Ready for data
Send Data	SCSI Data-Out >>>	Receive Data
Send Data	SCSI Data-Out >>>	Receive Data
	<<< SCSI Response	Send Status and Sense
Command Complete		

Figura 2.4: Write Operation

2.5.4 Exemplo de Operação de Leitura

Na imagem 2.5 podemos ver a ordem dos pacotes de Leitura.

Initiator Function	PDU Type	Target Function
Command request (read)	SCSI Command (READ)>>>	
		Prepare Data Transfer
Receive Data	<<< SCSI Data-In	Send Data
Receive Data	<<< SCSI Data-In	Send Data
Receive Data	<<< SCSI Data-In	Send Data
	<<< SCSI Response	Send Status and Sense
Command Complete		

Figura 2.5: Read Operation

Capítulo 3

Implementação do iSCSI

3.1 Ambiente de Configuração

A implementação do *Internet Small Computer System Interface* (iSCSI) envolve várias considerações e etapas. Inicialmente estabelece-se uma *Virtual Private Network* (VPN) para a rede do ISEC. Após a primeira VPN estar ativa, uma segunda VPN é estabelecida para garantir o acesso ao servidor no ISEC onde irão ser feitas todas as experiências deste projeto. Desta forma, os dois membros do grupo são capazes de participar na experiência e não ter o impacto de estar a gastar recursos das próprias máquinas.

Com as VPNs ativas, coloca-se o endereço IP privado do servidor e é inserido no browser para aceder ao VMware ESXi Host Client. O VMware ESXi Host Client é uma interface em Web(figura 3.1) que permite gerir o host ESXi e as máquinas virtuais que está a executar.

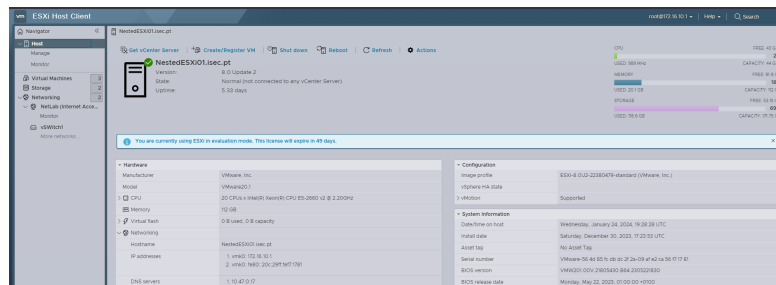


Figura 3.1: ESXi Web Interface

3.2 Topologia do Switch

O switch(figura3.2) utilizado em todas as maquinas virtuais, nele foi configurado a network NetLab e servia para comunicação entre elas e para comunicação com o exterior.

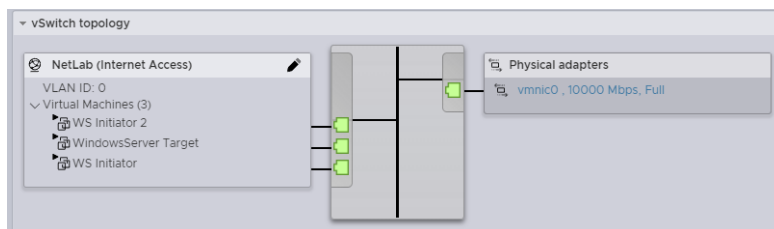


Figura 3.2: Switch

3.3 Configurar o iSCSI Target

Este servidor utiliza o sistema operativo Windows Server 2022 - Desktop Experience, e foi atribuído o IP 172.16.0.12 na interface ligada a network NetLab.

Para começar foi instalada a Role *iSCSI Target Server*(fig 3.3), o intuito de criar um disco virtual que viria a ser partilhado e acessível nos *initiators*.

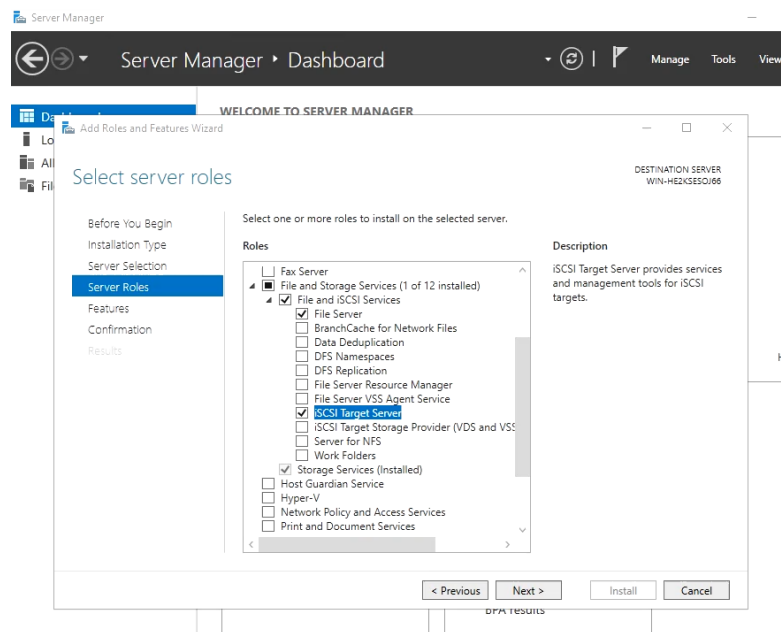


Figura 3.3: Role Target Server

De seguida, foi escolhido o diretório para localização dos ficheiros do disco Virtual (3.4).

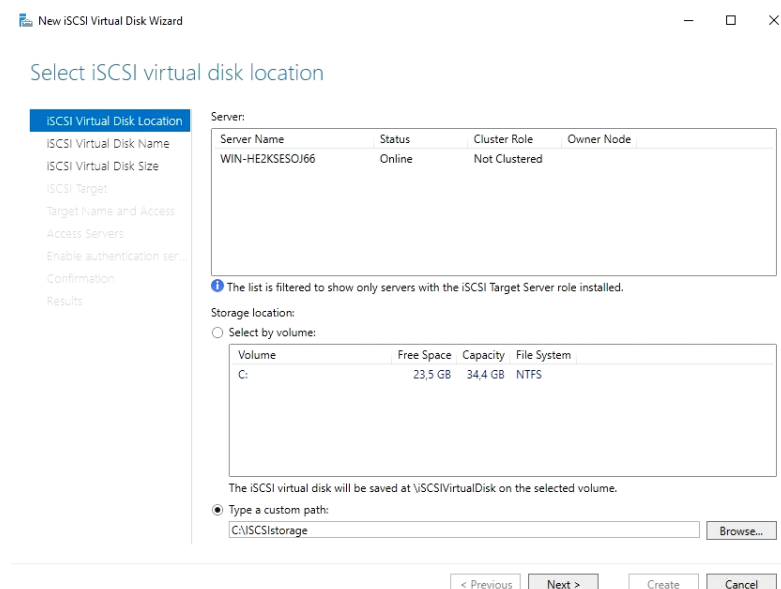


Figura 3.4: Diretório do disco Virtual no Target

Após a configuração do disco virtual, foi configurada a autenticação, neste caso foi utilizado *Challenge-Handshake Authentication Protocol* (CHAP)(fig 3.5).

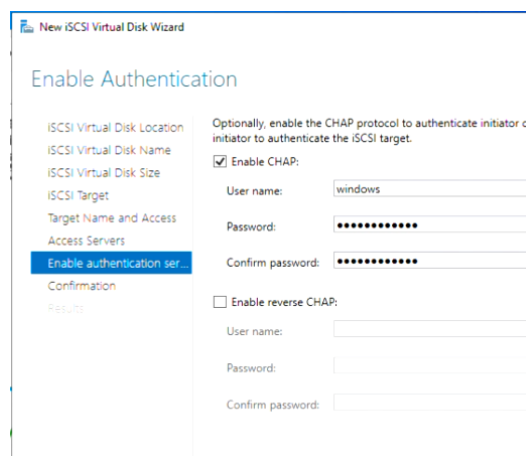


Figura 3.5: CHAP

Neste momento foi configurado os *initiator* com permissões para se conectarem ao *target*(fig 3.6).

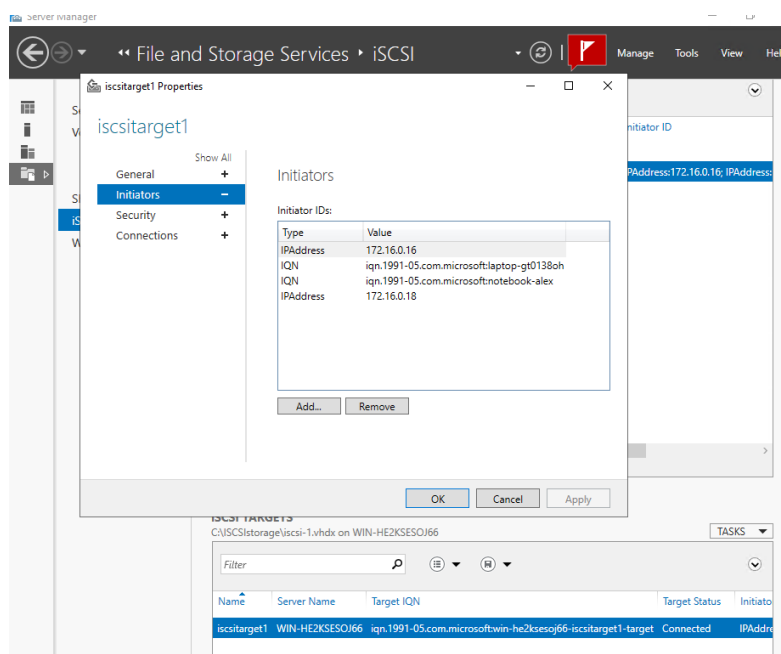


Figura 3.6: Initiators Permitidos

3.4 Configurar o iSCSI Initiator

Apesar de todas as versões de Windows, a partir do Windows 2008, o serviço iSCSI initiator estar disponível, o grupo decidiu inicialmente configurar o iSCSI initiator no Windows Server 2022. Para isso foi adicionada mais uma máquina virtual com o Sistema Operativo Windows Server 2022 - Desktop Experience.

Para configurar o iSCSI initiator tem de se no server manager abrir as tools e seleccionar o *iSCSI initiator*.

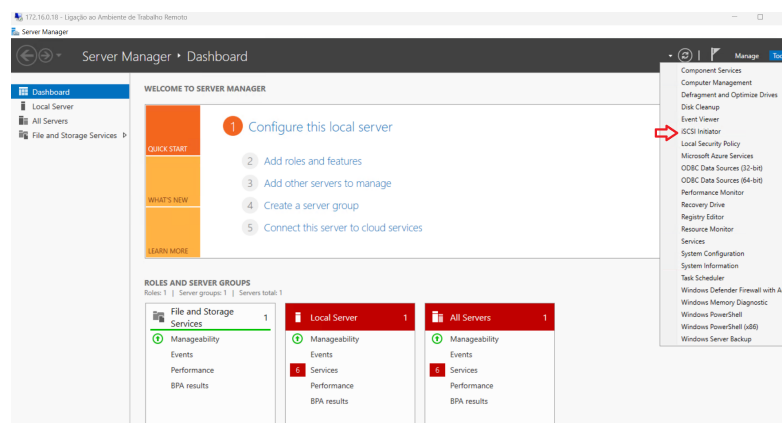


Figura 3.7: Tools

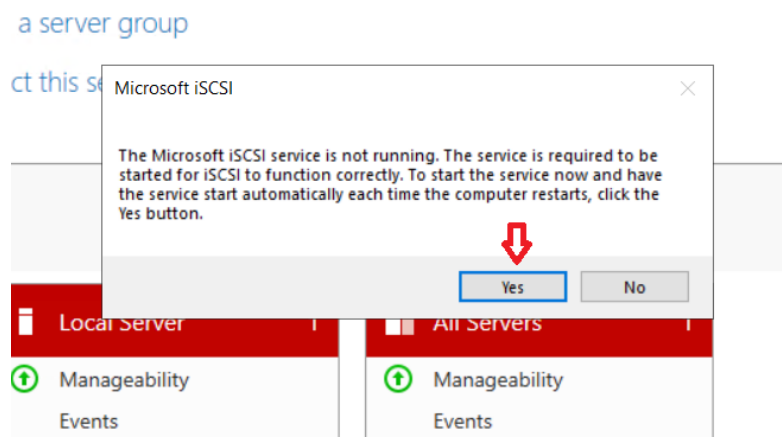


Figura 3.8: Iniciar o serviço

Colocar o IP do iSCSI target e depois clicar em Quick Connect.

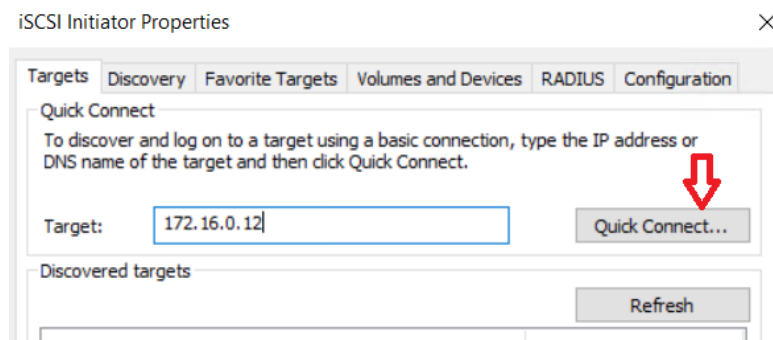


Figura 3.9: Quick Connect

Agora o target já aparece mas ainda não foi possível efetuar o login, para isso, clica-se no *connect* da figura 4.9 e em *advanced* da figura 4.10.

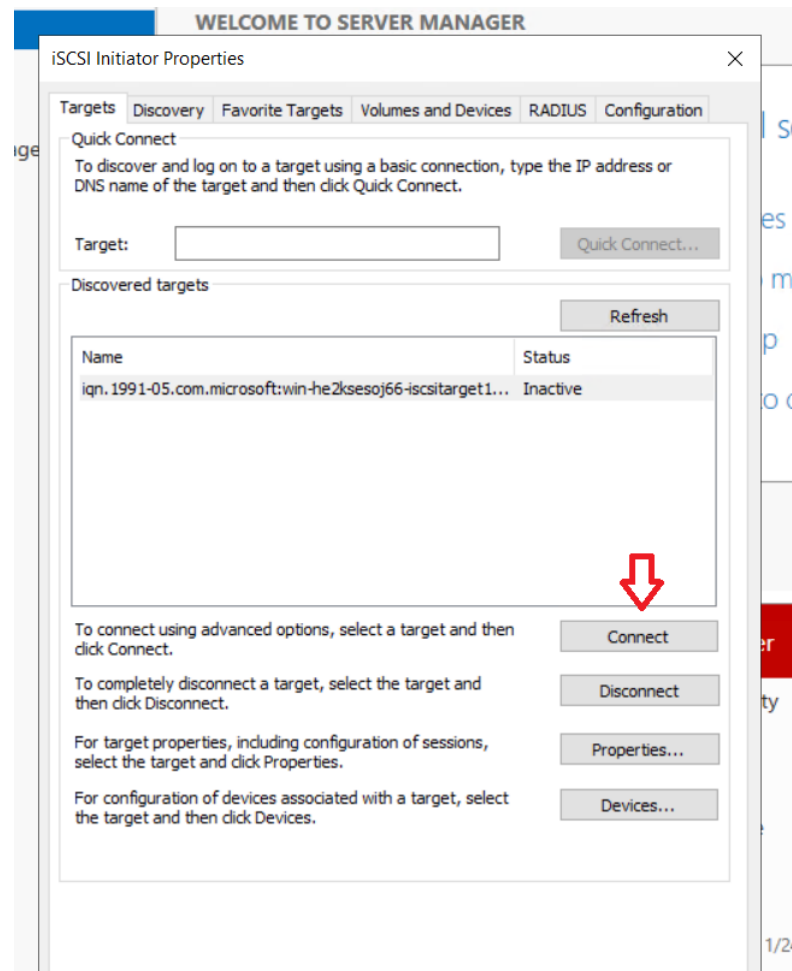


Figura 3.10: Connect

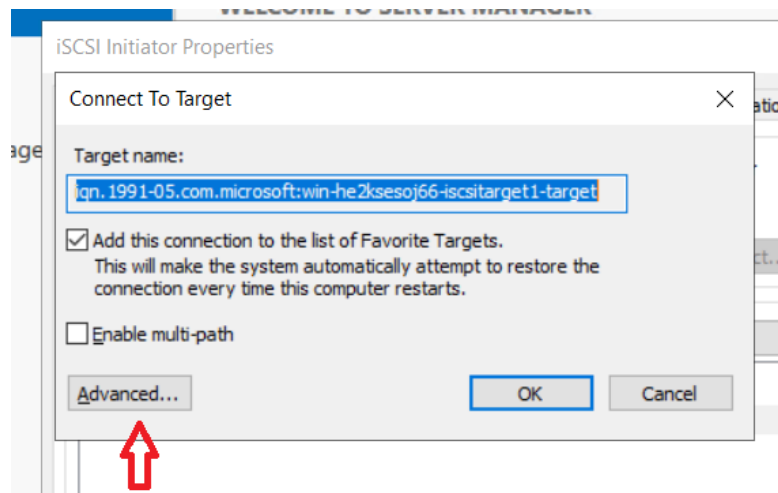


Figura 3.11: Advanced

Nesta página, ativa-se o CHAP e coloca-se o username e password que foram configurados no *target*.

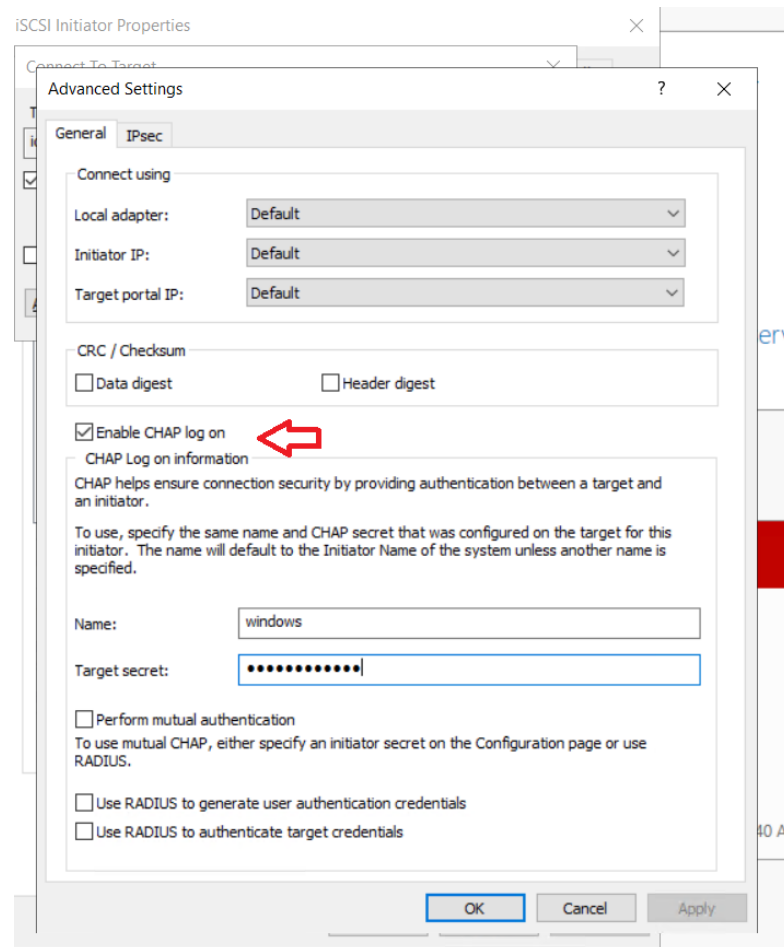


Figura 3.12: Autenticação CHAP

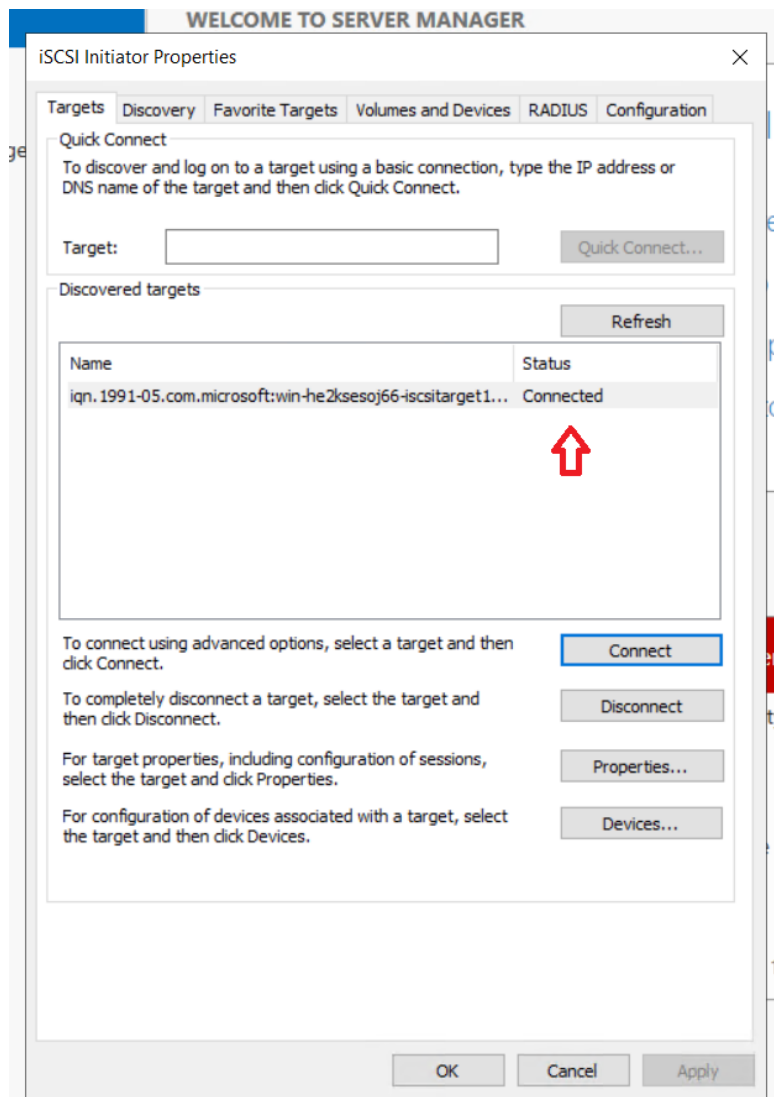


Figura 3.13: Conectado com sucesso

No server manager já é possível ver o novo disco virtual iSCSI, sendo apenas necessário colocá-lo online.

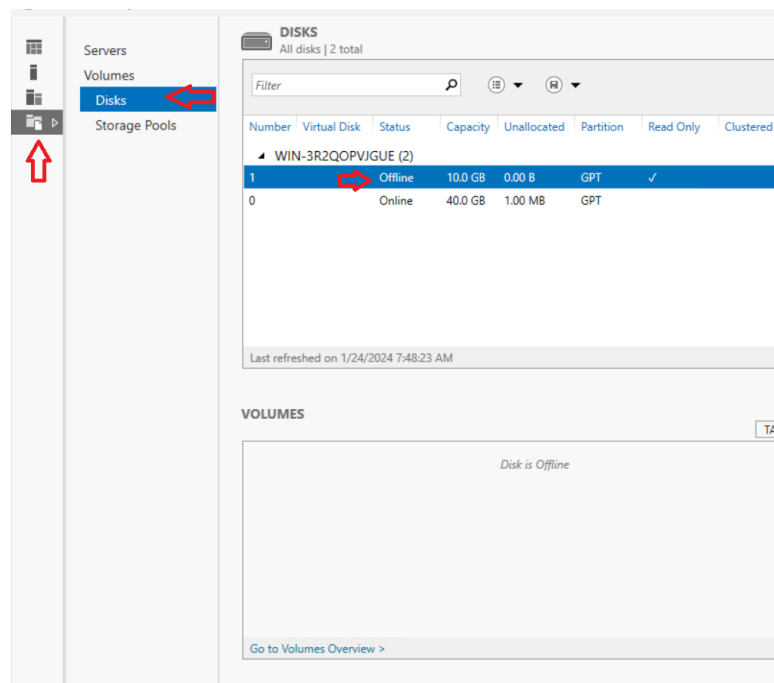


Figura 3.14: Disco Virtual iSCSI

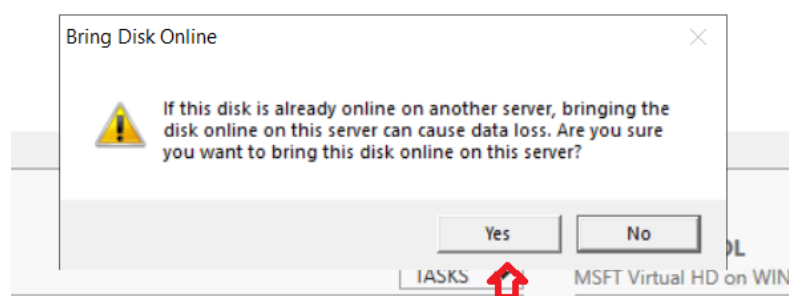


Figura 3.15: Colocar disco online

Agora já é possível ver o disco iSCSI.

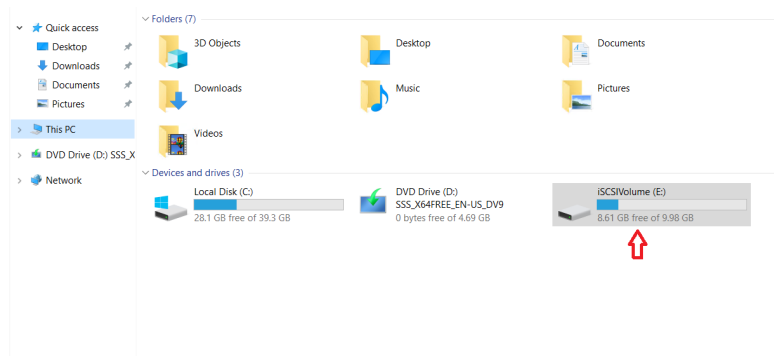


Figura 3.16: Disco iSCSI

Como referido anteriormente é possível também usar as nossas próprias máquinas para serem um iSCSI initiator. Para isso basta barra de pesquisas, pesquisar *iniciador iSCSI* e seguir exatamente os mesmos passos. No entanto não é necessário colocar um disco online, uma vez que o Sistema Operativo faz isso automaticamente.

Capítulo 4

Análise Prática

Para este capítulo e após o *Internet Small Computer System Interface* (iSCSI) estar devidamente implementado o grupo decidiu fazer uma série de experiências de forma a perceber como o protocolo funciona através de capturas Wireshark.

4.1 Fase de login

Segundo a RFC 3720 ([3]) o iSCSI a fase de login do iSCSI é quando um initiator estabelece uma ligação com o target. Nesta fase também são definidos os parâmetros do protocolo iSCSI, os parâmetros de segurança e autentica o iniciador e o alvo entre si

Para melhor compreensão destas sessões reiniciamos o initiator que já estava previamente conectado ao target e fizemos uma captura Wireshark no target. Nesta experiência é feita uma ligação do *initiator*(172.16.0.16) para o *target* (172.16.0.12). Esta análise é efetuada através dos pacotes presentes na imagem 4.1 e utilizando um filtro "tcp.port == 3260" e não o filtro "iscsi" para ser possível observar todo o tráfego que está a passar pela porta 3260, que é a porta usada pelo iSCSI

No.	Time	Source	Destination	Protocol	Length	Info
118345	111.967148	172.16.0.16	172.16.8.12	TCP	66	49669 → 3268 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
118346	111.967492	172.16.0.12	172.16.0.16	TCP	66	3268 → 49669 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
118347	111.967798	172.16.0.16	172.16.0.12	TCP	60	49669 → 3268 [ACK] Seq=1 Ack=1 Win=262656 Len=0
118348	111.968730	172.16.0.16	172.16.0.12	ISCSI	266	Login Command
118349	111.972291	172.16.0.12	172.16.0.16	ISCSI	174	Login Response (Success)
118350	111.972715	172.16.0.16	172.16.0.12	ISCSI	114	Login Command
118351	111.973373	172.16.0.12	172.16.0.16	ISCSI	258	Login Response (Success)
118352	111.973677	172.16.0.16	172.16.0.12	ISCSI	162	Login Command
118353	111.973957	172.16.0.12	172.16.0.16	ISCSI	102	Login Response (Success)
118354	111.974176	172.16.0.16	172.16.0.12	ISCSI	402	Login Command
118355	111.974527	172.16.0.12	172.16.0.16	ISCSI	306	Login Response (Success)
118356	111.984813	172.16.0.16	172.16.0.12	TCP	60	49669 → 3268 [ACK] Seq=729 Ack=705 Win=261888 Len=0
118357	111.985056	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Report LUNs LUN: 0x00
118358	111.985335	172.16.0.12	172.16.0.16	ISCSI	118	SCSI: Data In LUN: 0x00 (Report LUNs Response Data) SCSI: Response LUN: 0x00 (Report LUNs) (Good)
118359	111.985719	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00
118360	111.985999	172.16.0.12	172.16.0.16	ISCSI	138	SCSI: Data In LUN: 0x00 (Inquiry Response Data) [SCSI transfer limited due to allocation_length too small]
118361	111.986445	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00 Supported Vital Product Data Pages
118362	111.986714	172.16.0.12	172.16.0.16	ISCSI	110	SCSI: Data In LUN: 0x00 (Inquiry Response Data) SCSI: Response LUN: 0x00 (Inquiry) (Good)
118363	111.987019	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00 Device Identification Page
118364	111.987289	172.16.0.12	172.16.0.16	ISCSI	358	SCSI: Data In LUN: 0x00 (Inquiry Response Data) SCSI: Response LUN: 0x00 (Inquiry) (Good)
118365	111.987673	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00 Device Identification Page
118366	111.987970	172.16.0.12	172.16.0.16	ISCSI	526	SCSI: Data In LUN: 0x00 (Inquiry Response Data) SCSI: Response LUN: 0x00 (Inquiry) (Good)
118367	111.988921	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00 Unit Serial Number Page
118368	111.989154	172.16.0.12	172.16.0.16	ISCSI	142	SCSI: Data In LUN: 0x00 (Inquiry Response Data) SCSI: Response LUN: 0x00 (Inquiry) (Good)
118369	111.989419	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00
118370	111.989700	172.16.0.12	172.16.0.16	ISCSI	198	SCSI: Data In LUN: 0x00 (Inquiry Response Data) SCSI: Response LUN: 0x00 (Inquiry) (Good)
118371	112.000706	172.16.0.16	172.16.0.12	TCP	60	49669 → 3268 [ACK] Seq=1065 Ack=1917 Win=262400 Len=0
118372	112.002229	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Read Capacity(10) LUN: 0x00
118373	112.002448	172.16.0.12	172.16.0.16	ISCSI	110	SCSI: Data In LUN: 0x00 (Read Capacity(10) Response Data) SCSI: Response LUN: 0x00 (Read Capacity(10)) (Good)
118374	112.003036	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Mode Sense(6) LUN: 0x00
118375	112.003240	172.16.0.12	172.16.0.16	ISCSI	106	SCSI: Data In LUN: 0x00 (Mode Sense(6) Response Data) SCSI: Response LUN: 0x00 (Mode Sense(6)) (Good)
118376	112.003469	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Inquiry LUN: 0x00 Supported Vital Product Data Pages
118377	112.003673	172.16.0.12	172.16.0.16	ISCSI	110	SCSI: Data In LUN: 0x00 (Inquiry Response Data) SCSI: Response LUN: 0x00 (Inquiry) (Good)
118378	112.003916	172.16.0.16	172.16.0.12	TCP	60	49669 → 3268 [ACK] Seq=1209 Ack=2081 Win=262400 Len=0
118379	112.004668	172.16.0.16	172.16.0.12	ISCSI	102	SCSI: Mode Sense(6) LUN: 0x00

Figura 4.1: iSCSI Login

Graças a este filtro é possível observar o 3-Way Handshake que inicia a fase de login do iSCSI entre os pacotes 118345 ao 118347.

1. Pacote 118345: Este pacote é um pacote TCP SYN (sincronização) enviado pelo *initiator* (172.16.0.16) para o *target* (172.16.8.12). Este pacote indica ao *target* que estão a fazer um pedido de sincronização por parte do *initiator*.
2. Pacote 118346: Este pacote é um pacote TCP SYN/ACK enviado pelo *target* (172.16.8.12) para o *initiator* (172.16.0.16). O *target* envia também um pedido de sincronização ao *initiator* e confirma o pedido de sincronização enviado pelo *initiator* foi aceite
3. Pacote 118347: Este pacote é um pacote TCP ACK enviado pelo *initiator* (172.16.0.16) para o *target* (172.16.8.12). Este pacote confirma o pedido de sincronização do *target*.

Desta forma a ligação tcp é estabelecida entre o *initiator* e começa a fase de login para ganhar mais acesso ao target. Basicamente há dois tipos de sessões de login. A normal e a discovery. Nesta captura vamos ver o normal que é uma sessão estabelecida entre o initior realiza o login para ligar-se ao target.

4.1.1 Normal Login

Antes de analisarmos os pacotes vamos var decode aos pacotes para permitir que possamos analisar com mais detalhe o protocolo iSCSI e mais fácil de o entender.

4. Pacote 118348: Este pacote é um pacote iSCSI login enviado pelo *initiator* (172.16.0.16) para o *target* (172.16.8.12). Este pacote contém informações sobre o *initiator*, como o seu endereço IP, o seu nome de utilizador e o tipo de sessão que se pretende fazer, que neste caso é **Normal**. Podemos ver isso nas figuras 4.2 e 4.3.

iscsi.keyvalue == "SessionType=Normal"						
No.	Time	Source	Destination	Protocol	Length	Info
118348	111.968730	172.16.0.16	172.16.0.12	iSCSI	266	Login Command

Ethernet II, Src: VMware_14:15:46 (00:0c:29:14:15:46), Dst: VMware_6e:49:26 (00:0c:29:6e:49:26)						
Internet Protocol Version 4, Src: 172.16.0.16, Dst: 172.16.0.12						
Transmission Control Protocol, Src Port: 49669, Dst Port: 3260, Seq: 1, Ack: 1, Len: 212						
iSCSI (Login Command)						
..00 0011 = Opcode: Login Command (0x03)						
0... = T: Stay in current login stage						
.0.. = C: Text is complete						
.... 00.. = CSG: Security negotiation (0x0)						
VersionMax: 0x00						
VersionMin: 0x00						
TotalAHSLength: 0 (0x00)						
DataSegmentLength: 164 (0x000000a4)						
> ISID: 400001370001						
TSIH: 0x0000						
InitiatorTaskTag: 0x00000001						
CID: 0x0001						
CmdSN: 1 (0x00000001)						
ExpStatSN: 1 (0x00000001)						
v Key/Value Pairs						
KeyValue: InitiatorName=iqn.1991-05.com.microsoft:win-vr7o9ifrgn8						
KeyValue: SessionType=Normal						
KeyValue: TargetName=iqn.1991-05.com.microsoft:win-he2ksesoj66-iscsitarget1-target						
KeyValue: AuthMethod=CHAP						

Figura 4.2: Primeiro Pacote iSCSI Login

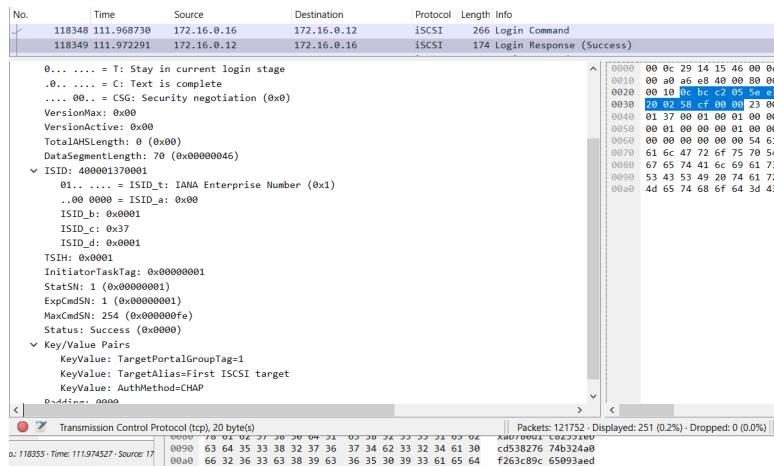


Figura 4.3: ESXi VMs

5. Pacote 118349: Este pacote é um pacote iSCSI login response enviado pelo *target* (172.16.8.12) para o *initiator* (172.16.0.16). Este pacote contém informações sobre o estado do login. Como podemos ver na figura 4.4 o CSG, *current stage*, informa o *initiator* que é a negociação de segurança e método de autenticação.

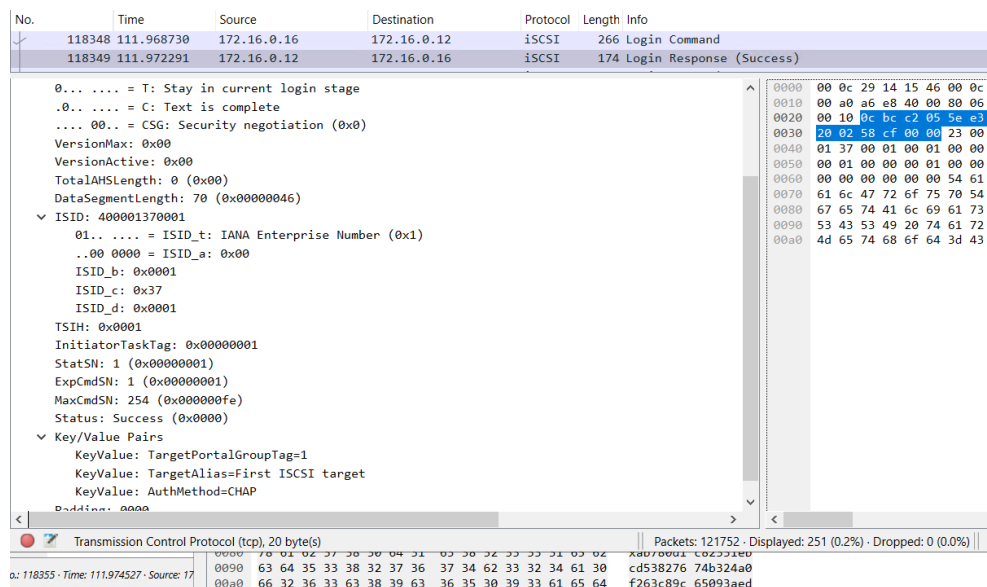


Figura 4.4: Segundo Pacote iSCSI Login

Após o sucesso do login, o *initiator* e o *target* podem trocar dados usando pacotes iSCSI. Estes pacotes iSCSI são utilizados para enviar comandos SCSI entre o *initiator* e o *target*.

Na imagem 4.1, os seguintes pacotes SCSI são enviados:

6. Pacote 118357: Este pacote é um pacote iSCSI SCSI Report LUNs enviado pelo *initiator* (172.16.0.16) para o *target* (172.16.8.12). Este pacote é utilizado para solicitar uma lista de LUNs disponíveis no *target*.
7. Pacote 118358: Este pacote é um pacote iSCSI SCSI Report LUNs response enviado pelo *target* (172.16.8.12) para o *initiator* (172.16.0.16). Este pacote contém uma lista de LUNs disponíveis no *target*.
8. Pacote 118359: Este pacote é um pacote iSCSI SCSI Inquiry enviado pelo *initiator* (172.16.0.16) para o *target* (172.16.8.12). Este pacote é utilizado para solicitar informações sobre uma LUN específica.
9. Pacote 118360: Este pacote é um pacote iSCSI SCSI Inquiry response enviado pelo *target* (172.16.8.12) para o *initiator* (172.16.0.16). Este pacote contém informações sobre a LUN específica.

Os pacotes 118357 e 118358 são utilizados para obter uma lista de LUNs disponíveis no *target*. O pacote 118359 é utilizado para obter informações sobre uma LUN específica.

Após receber o pacote SCSI response, o *initiator* pode usar as informações obtidas para realizar operações de leitura, gravação ou outro tipo de operação no armazenamento.

4.1.2 Discovery

Como já anteriormente mencionado, existem dois tipos de sessões, o *Normal* e o *discovery* sendo este apenas usado para a descoberta dos *target* disponíveis. Fomos capazes de verificar o sucedido quando, ao fazer a configuração do *initiator* estamos no passo 3.9 e na captura que estávamos a realizar no *target*

após a ligação TCP estar concluída, o *initiator*(172.16.10.18) enviar como Discovery e o target lhe responder com as informações.

No.	Time	Source	Destination	Protocol	Length	Info
583	6.771370	172.16.0.5	172.16.0.12	iSCSI	102	NOP Out
588	6.822104	172.16.0.12	172.16.0.5	TCP	54	3260 → 50075 [ACK] Seq=49 Ack=49 Win=8191
1452	26.744292	172.16.0.12	172.16.0.16	iSCSI	102	NOP In
1454	26.744983	172.16.0.16	172.16.0.12	iSCSI	102	NOP Out
1456	26.759562	172.16.0.12	172.16.0.16	TCP	54	3260 → 49803 [ACK] Seq=161 Ack=145 Win=8195
1681	31.744307	172.16.0.12	172.16.0.5	iSCSI	102	NOP In
1683	31.750610	172.16.0.5	172.16.0.12	iSCSI	102	NOP Out
1687	31.806387	172.16.0.12	172.16.0.5	TCP	54	3260 → 50075 [ACK] Seq=97 Ack=97 Win=8190
2074	38.953685	172.16.0.18	172.16.0.12	TCP	66	49792 → 3260 [SYN, ECE, CWR] Seq=0 Win=6424
2075	38.953983	172.16.0.12	172.16.0.18	TCP	66	3260 → 49792 [SYN, ACK, ECE] Seq=0 Ack=1 Win=262656
2076	38.954577	172.16.0.18	172.16.0.12	TCP	60	49792 → 3260 [ACK] Seq=1 Ack=1 Win=262656
2077	38.954862	172.16.0.18	172.16.0.12	iSCSI	198	Login Command
2078	38.962229	172.16.0.12	172.16.0.18	iSCSI	118	Login Response (Success)
2079	38.963373	172.16.0.18	172.16.0.12	iSCSI	222	Login Command
2080	38.964082	172.16.0.12	172.16.0.18	iSCSI	210	Login Response (Success)
2081	38.965889	172.16.0.18	172.16.0.12	iSCSI	118	Text Command
2082	38.966910	172.16.0.12	172.16.0.18	iSCSI	210	Text Response
2083	38.968298	172.16.0.18	172.16.0.12	iSCSI	102	Logout Command (Close session)
2084	38.968488	172.16.0.12	172.16.0.18	iSCSI	102	Logout Response
2085	38.969320	172.16.0.18	172.16.0.12	TCP	60	49792 → 3260 [FIN, ACK] Seq=425 Ack=425 Win=
2086	38.969434	172.16.0.12	172.16.0.18	TCP	54	3260 → 49792 [ACK] Seq=425 Ack=426 Win=20974

Packet 2085 details:

- DataSegmentLength: 94 (0x0000005e)
- ISID: 400001370000
- TSIH: 0x0000
- InitiatorTaskTag: 0x00000001
- CID: 0x0001
- CmdSN: 1 (0x00000001)
- ExpStatSN: 1 (0x00000001)
- Key/Value Pairs:
 - KeyValue: InitiatorName=iqn.1991-05.com.microsoft:win-3r2qopvjgue
 - KeyValue: SessionType=Discovery
 - KeyValue: AuthMethod=None
 - Padding: 0000

Figura 4.5: Value: Discovery

No.	Time	Source	Destination	Protocol	Length	Info
2074	38.953685	172.16.0.18	172.16.0.12	TCP	66	49792 → 3260 [SYN, ECE, CWR] Seq=0 Win=6424
2075	38.953983	172.16.0.12	172.16.0.18	TCP	66	3260 → 49792 [SYN, ACK, ECE] Seq=0 Ack=1 Win=262656
2076	38.954577	172.16.0.18	172.16.0.12	TCP	60	49792 → 3260 [ACK] Seq=1 Ack=1 Win=262656
2077	38.954862	172.16.0.18	172.16.0.12	iSCSI	198	Login Command
2078	38.962229	172.16.0.12	172.16.0.18	iSCSI	118	Login Response (Success)
2079	38.963373	172.16.0.18	172.16.0.12	iSCSI	222	Login Command
2080	38.964082	172.16.0.12	172.16.0.18	iSCSI	210	Login Response (Success)
2081	38.965889	172.16.0.18	172.16.0.12	iSCSI	118	Text Command
2082	38.966910	172.16.0.12	172.16.0.18	iSCSI	210	Text Response
2083	38.968298	172.16.0.18	172.16.0.12	iSCSI	102	Logout Command (Close session)
2084	38.968488	172.16.0.12	172.16.0.18	iSCSI	102	Logout Response
2085	38.969320	172.16.0.18	172.16.0.12	TCP	60	49792 → 3260 [FIN, ACK] Seq=425 Ack=425 Win=
2086	38.969434	172.16.0.12	172.16.0.18	TCP	54	3260 → 49792 [ACK] Seq=425 Ack=426 Win=20974

Packet 2085 details:

- TotalAHSLength: 0 (0x00)
- DataSegmentLength: 106 (0x0000006a)
- LUN
- InitiatorTaskTag: 0x00000001
- TargetTransferTag: 0xffffffff
- StatSN: 3 (0x00000003)
- ExpCmdSN: 2 (0x00000002)
- MaxCmdSN: 255 (0x000000ff)
- Key/Value Pairs:
 - KeyValue: TargetName=iqn.1991-05.com.microsoft:win-he2ksoj66-iscsitarget1-target
 - KeyValue: TargetAddress=172.16.0.12:3260,1
 - Padding: 0000

Figura 4.6: Retorno

4.2 NOP-IN e NOP-OUT

O NOP-IN e NOP-OUT, pedido e resposta, é usado como se fosse um mecanismo de ping entre o *target* e o *initiator* para verificarem se a sessão/conexão

ainda estão ativos. Segundo a RFC, tanto pode ser desencadeado pelo *target* ou *initiator*, porém no nosso caso observamos apenas ao processo ser desencadeado pelo *target* como podemos observar nos pacotes 1129 e 1130 e os pacotes 2919 e 2920 de uma captura feita posterior à fase e login.

1129	13.699099	172.16.0.12	172.16.0.16	iSCSI	102 NOP In
1130	13.700188	172.16.0.16	172.16.0.12	iSCSI	102 NOP Out
2919	38.699205	172.16.0.12	172.16.0.16	iSCSI	102 NOP In
2920	38.699873	172.16.0.16	172.16.0.12	iSCSI	102 NOP Out

Figura 4.7: NOP-IN e NOP-OUT

4.3 Operação de Escrita

Na imagem 4.8 podemos ver marcados a vermelho os pacotes utilizados para a escrita de um bloco de dados. Como descrito no capítulo 3, neste processo, o *initiator* faz um *request write* para o *target* em comandos *Small Computer System Interface* (SCSI) (fig: 4.9) e depois espera receber do *target* o pacote "*Ready to Transfer*" (fig:4.10). De seguida existe a operação *SCSI Data-Out* (fig: 4.11), do *initiator* para o *target*. No final é obtida uma resposta de transferência concluída (fig:4.12).

3312	109.990101	172.16.0.12	172.16.0.5	iSCSI	102 Ready to Transfer
3432	110.004329	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Write(10) LUN: 0x00 (LBA: 0x000114b0, Len: 512) SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
3433	110.004598	172.16.0.12	172.16.0.5	iSCSI	102 Ready To Transfer
3555	110.012683	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
3677	110.028411	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
3800	110.037036	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
3829	110.039941	172.16.0.12	172.16.0.5	iSCSI	102 SCSI: Response LUN: 0x00 (Write(10)) (Good)
3923	110.052264	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4048	110.063869	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4168	110.078797	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4194	110.081223	172.16.0.12	172.16.0.5	iSCSI	102 SCSI: Response LUN: 0x00 (Write(10)) (Good)
4291	110.088634	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4413	110.108367	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4536	110.114408	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4574	110.116696	172.16.0.12	172.16.0.5	iSCSI	102 SCSI: Response LUN: 0x00 (Write(10)) (Good)
4659	110.134418	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4782	110.191424	172.16.0.5	172.16.0.12	iSCSI	590 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4904	110.201453	172.16.0.5	172.16.0.12	iSCSI	254 SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
4985	110.204271	172.16.0.12	172.16.0.5	iSCSI	102 SCSI: Response LUN: 0x00 (Write(10)) (Good)

Figura 4.8: Pacotes Operação Write

```

> Frame 3432: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
> Ethernet II, Src: da:60:b3:bd:2f:29 (da:60:b3:bd:2f:29), Dst: 02:00:00:00:00:00
> Internet Protocol Version 4, Src: 172.31.0.5, Dst: 172.16.0.12
> Transmission Control Protocol, Src Port: 50384, Dst Port: 3260, Seq: 1723105000, Win: 65536, Len: 0
> [124 Reassembled TCP Segments (65584 bytes): #4352-4475]
✓ iSCSI (SCSI Command)
  ..00 0001 = Opcode: SCSI Command (0x01)
  - - - - -

```

Figura 4.9: 1º pacote Write

```

> Frame 3433: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: VMware_6e:49:26 (00:0c:29:6e:49:26), Dst: 02:00:00:00:00:00
> Internet Protocol Version 4, Src: 172.16.0.12, Dst: 172.31.0.5
> Transmission Control Protocol, Src Port: 3260, Dst Port: 50384, Seq: 1721601200, Win: 65536, Len: 0
✓ iSCSI (Ready To Transfer)
  ..11 0001 = Opcode: Ready To Transfer (0x31)

```

Figura 4.10: 2º pacote Write

```

> Frame 4904: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
> Ethernet II, Src: da:60:b3:bd:2f:29 (da:60:b3:bd:2f:29), Dst: 02:00:00:00:00:00
> Internet Protocol Version 4, Src: 172.31.0.5, Dst: 172.16.0.12
> Transmission Control Protocol, Src Port: 50384, Dst Port: 3260, Seq: 1723105000, Win: 65536, Len: 65536
> [123 Reassembled TCP Segments (65584 bytes): #4352-4474]
✓ iSCSI (SCSI Data Out)
  ..00 0101 = Opcode: SCSI Data Out (0x05)
  TotalAHSLength: 0 (0x00)
  DataSegmentLength: 65536 (0x00010000)

```

Figura 4.11: 3º pacote Write

```

> Frame 4905: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: VMware_6e:49:26 (00:0c:29:6e:49:26), Dst: 02:00:0c:00:00:00
> Internet Protocol Version 4, Src: 172.16.0.12, Dst: 172.16.0.16
> Transmission Control Protocol, Src Port: 3260, Dst Port: 3260
  ✓ iSCSI (SCSI Response)
    ..10 0001 = Opcode: SCSI Response (0x21)
    Response: Command completed at target (0x00)
    Status: Good (0x00)

```

Figura 4.12: 4º pacote Write

4.4 Operação de Escrita

Na imagem 4.13 podemos ver marcados a verde os pacotes utilizados para a operação de escrita de um bloco de dados. Como descrito no capítulo 3, neste processo, o *initiator* faz um *request read* para o *target* em comandos SCSI (fig: 4.14). De seguida existe a operação *SCSI Data-In* (fig: 4.15), do *target* para o *initiator*. No final, a flag de ultima *Protocol Data Unit* (PDU) desta operação esta ativa e flag de estado também esta ativada e é obtida uma resposta de transferência concluída (fig:4.16).

118451	112.073886	172.16.0.12	172.16.0.16	TCP	60 49669 → 3260 [ACK] Seq=19465 Ack=207373 Win=262656 Len=0
118452	112.073902	172.16.0.12	172.16.0.16	iSCSI	11502 SCSI: Data In LUN: 0x00 (Read(10) Response Data) SCSI: Response LUN: 0x00 (Read(10)) (Good)

Figura 4.13: Pacotes Operação Read

```

> Frame 118479: 102 bytes on wire (816 bits), 102 bytes
> Ethernet II, Src: VMware_14:15:46 (00:0c:29:14:15:46),
> Internet Protocol Version 4, Src: 172.16.0.16, Dst: 17
> Transmission Control Protocol, Src Port: 49669, Dst Po
✓ iSCSI (SCSI Command)
  ..00 0001 = Opcode: SCSI Command (0x01)
  .0.. .... = I: Queued delivery
  TotalAHSLength: 0 (0x00)
  DataSegmentLength: 0 (0x00000000)
  > LUN
    InitiatorTaskTag: 0x00000031
    ExpectedDataTransferLength: 131072 (0x00020000)
    CmdSN: 49 (0x00000031)
    ExpStatSN: 53 (0x00000035)
    Data In in: 118480
    Response in: 118482
  ✓ Flags: 0xc1, F, R, Attr: Simple
    1... .... = F: Final PDU in sequence
    .1.. .... = R: Data will be read from target
    ..0. .... = W: No data will be written to target
    .... .001 = Attr: Simple (0x1)

```

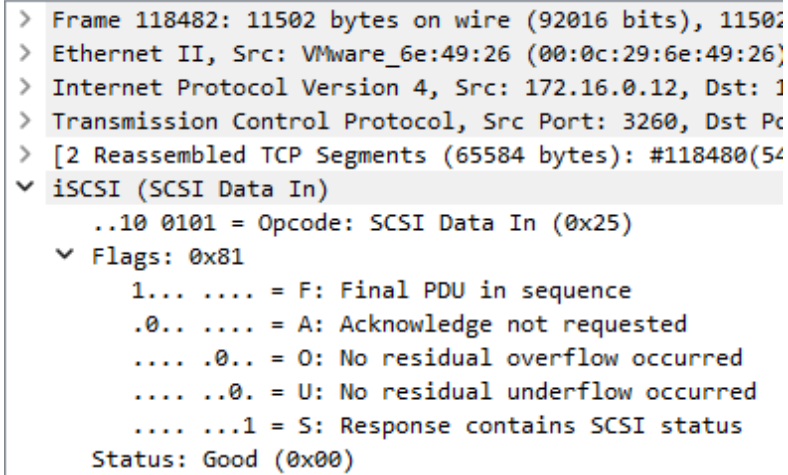
Figura 4.14: 1º Pacote da Operação Read

```

> Frame 118480: 119774 bytes on wire (958192 bits), 119774 bytes
> Ethernet II, Src: VMware_6e:49:26 (00:0c:29:6e:49:26), Dst: VMw
> Internet Protocol Version 4, Src: 172.16.0.12, Dst: 172.16.0.16
> Transmission Control Protocol, Src Port: 3260, Dst Port: 49669,
✓ iSCSI (SCSI Data In)
  ..10 0101 = Opcode: SCSI Data In (0x25)
  ✓ Flags: 0x00
    0... .... = F: Not final PDU in sequence
    .0.. .... = A: Acknowledge not requested
    .... .0.. = O: No residual overflow occurred
    .... ..0. = U: No residual underflow occurred
    .... ...0 = S: Response does not contain SCSI status
  TotalAHSLength: 0 (0x00)
  DataSegmentLength: 65536 (0x00010000)
  InitiatorTaskTag: 0x00000031
  StatSN: 0 (0x00000000)
  ExpCmdSN: 50 (0x00000032)
  MaxCmdSN: 303 (0x0000012f)
  DataSN: 0 (0x00000000)
  BufferOffset: 0 (0x00000000)
  ResidualCount: 0 (0x00000000)

```

Figura 4.15: 2º Pacote da Operação Read



```
> Frame 118482: 11502 bytes on wire (92016 bits), 11502 captured (92016 bits) on interface 0  
> Ethernet II, Src: VMware_6e:49:26 (00:0c:29:6e:49:26), Dst: 08:00:27:00:00:00  
> Internet Protocol Version 4, Src: 172.16.0.12, Dst: 172.16.0.1  
> Transmission Control Protocol, Src Port: 3260, Dst Port: 3260  
> [2 Reassembled TCP Segments (65584 bytes): #118480(5440) - #118481(61144)]  
▼ iSCSI (SCSI Data In)  
  ..10 0101 = Opcode: SCSI Data In (0x25)  
  ▼ Flags: 0x81  
    1... .... = F: Final PDU in sequence  
    .0.. .... = A: Acknowledge not requested  
    .... .0.. = O: No residual overflow occurred  
    .... ..0. = U: No residual underflow occurred  
    .... ...1 = S: Response contains SCSI status  
  Status: Good (0x00)
```

Figura 4.16: 3º Pacote da Operação Read

4.5 Conclusão

A realização do projeto foi concluído com êxito, apesar de algumas dificuldades encontradas no início devido a problemas de configuração com Windows Server 2022 CLI.

Através da ferramenta Wireshark foram capturados os pacotes essenciais para entender a sequência e a troca de mensagens entre o *initiator* e o *target*, e estes foram detalhados no decorrer do relatório.

Este projeto permitiu expandir os nossos conhecimentos e aprimorar as nossas técnicas de pesquisa.

Referências

- [1] *Introdução iSCSI*. URL: <https://calsoftinc.com/blogs/2017/03/iscsi-introduction-steps-configure-iscsi-initiator-target.html> (acedido em 21/01/2024).
- [2] *iSCSI*. URL: <http://www.3kranger.com/HP3000/mpeix/en-hpux/T1452-90011/ch01s05.html?btnNext=next%A0%BB> (acedido em 21/01/2024).
- [3] *iSCSI*. URL: <https://datatracker.ietf.org/doc/html/rfc3720.html#section-1> (acedido em 21/01/2024).