Report di Progetto - Compagnia Theta

1. INQUADRAMENTO GENERALE

Nel corso dell'ultima settimana è stata progettata e documentata un'infrastruttura di rete completa per la **Compagnia Theta**, una realtà organizzata su sei piani con circa **120 postazioni di lavoro**, suddivise tra aree operative e creative.

L'obiettivo del progetto è stato fornire un **preventivo tecnico-economico** dettagliato, accompagnato da una proposta di rete **scalabile, sicura ed efficiente**, in grado di supportare le attività quotidiane e le esigenze del team creativo.

2. ARCHITETTURA DI RETE

Per rispondere alle esigenze di distribuzione, sicurezza e prestazioni elevate, è stata progettata un'**architettura di rete ben segmentata**, basata su una topologia a livelli e dispositivi professionali.

La rete è strutturata su **sei piani**, ciascuno dotato di uno switch dedicato per le postazioni locali. I servizi critici, tra cui routing, firewall, archiviazione e sicurezza, sono concentrati nella **stanza server al piano terra**.

2.1 Componenti principali della rete

Switch di secondo livello (L2) – 7 unità

- Installati su ogni piano per il collegamento diretto delle postazioni PC (20 per piano).
- Gestione del traffico locale e possibilità di futura espansione.

Switch di terzo livello (L3) – 1 unità

- Posizionato al piano terra, con funzione di **core switch**.
- Gestisce il **routing tra le subnet** (se implementate) e le zone funzionali (es. DMZ, NAS).

Router aziendale – 1 unità

- Gestisce il traffico Internet, il NAT e la comunicazione con il firewall.
- Punto di ingresso/uscita della rete aziendale.

Firewall perimetrale – 1 unità

- Installato tra il router e la rete interna.
- Protegge da accessi non autorizzati e consente la creazione della Zona Demilitarizzata (**DMZ**).

2.2 DMZ – Web Server (DVWA - Metasploitable)

La **DMZ** è una rete isolata che ospita servizi accessibili da Internet. È posizionata tra il **firewall** e il **router**, per garantire sicurezza anche in caso di compromissione.

Motivazioni per la creazione della DMZ:

- **Protezione della rete interna:** anche in caso di compromissione del web server, l'attaccante non può accedere direttamente alla LAN aziendale.
- **Isolamento dei servizi pubblici:** riduce i rischi legati all'esposizione su Internet.
- **Controllo granulare:** il firewall gestisce e limita il traffico tra DMZ, Internet e rete interna.
- **Sicurezza multilivello:** migliora la resilienza generale della rete.

Servizi ospitati nella DMZ:

- Web Server (DVWA – Metasploitable)
- IDS dedicato
- WAF (Web Application Firewall)
- Switch dedicato

2.3 Sistemi di Sicurezza – IDS/IPS (3 unità)

- Sono stati installati **3 sistemi di sicurezza** per il monitoraggio e la prevenzione delle minacce:

Posizione	Tipo	Funzione
DMZ	IDS	Monitoraggio delle richieste al web server DVWA
Tra LAN e NAS	IPS	Protezione del server NAS contro attacchi e traffico sospetto
Tra Internet e FW	IPS	Primo livello di filtraggio per il traffico in entrata

2.4 Server DHCP

Un server DHCP dedicato gestisce **l'assegnazione dinamica degli IP**, garantendo:

- Ordine e continuità
- Minore configurazione manuale
- Supporto alla scalabilità

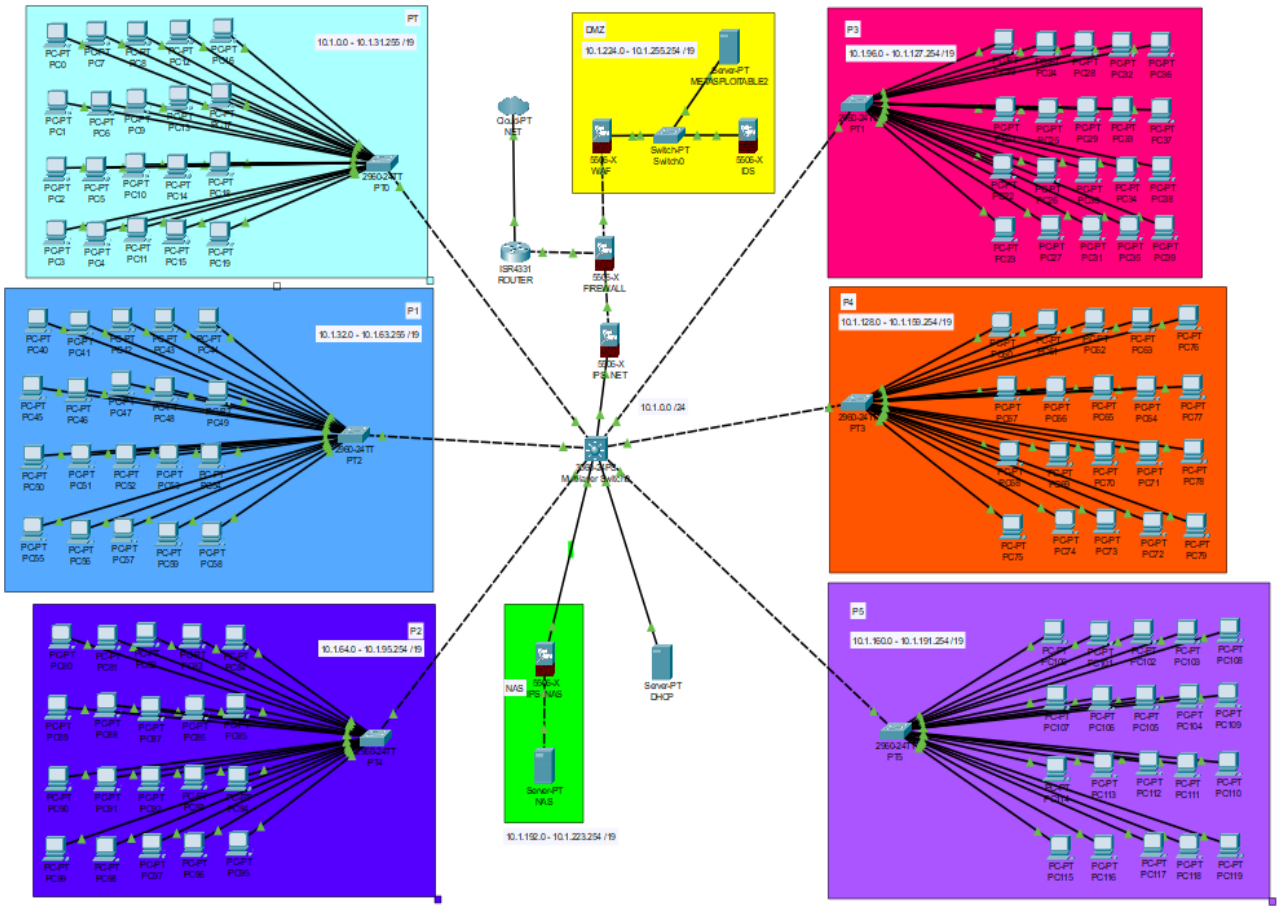
2.5 NAS Aziendale

Il **NAS** è utilizzato per l'**archiviazione centralizzata dei dati** e la **condivisione sicura** tra i reparti. È posizionato in un segmento protetto della rete e monitorato da un IPS.

2.6 Cablaggio strutturato

La rete è stata cablata con:

- **137 cavi Cat.6**
- Patch panel, canaline e armadi rack
- Cablaggio realizzato secondo **best practice**, con separazione tra dati e alimentazione.



3. DISTRIBUZIONE DEI DISPOSITIVI PER PIANO

3.1 Piano Terra:

- 20 postazioni PC

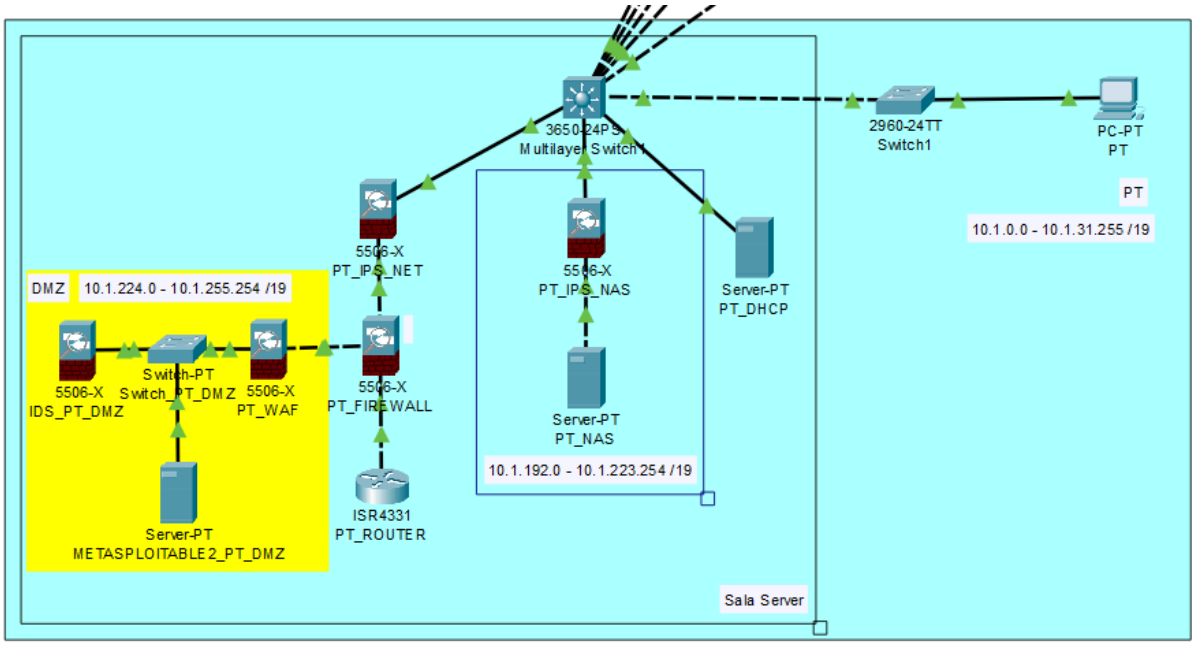
cd /Stanza_Server:

All'interno del piano terra è stata predisposta una stanza server dedicata, progettata per ospitare l'infrastruttura centrale di rete. L'accesso a quest'area è controllato e riservato al personale autorizzato tramite badge o chiave dedicata, per garantire la sicurezza fisica dei dispositivi critici.

- Switch L2
- Switch Multilayer L3
- Router aziendale
- Firewall perimetrale
- NAS
- IPS x2

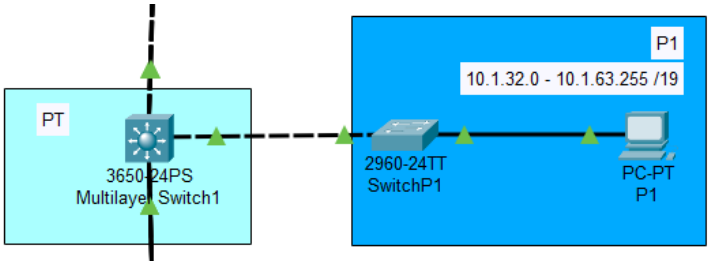
cd /DMZ:

- WAF
- Switch
- IDS
- Web Server



3.2 Piani 1–5:

- 20 postazioni PC per piano
- 1 switch L2 per piano
- Topologia: ogni PC è collegato allo switch del piano



4. PREVENTIVO DI SPESA

Al termine della fase di progettazione, è stato **realizzato un preventivo di spesa dettagliato**, basato sui **componenti hardware e software individuati** nel corso dell'analisi.

4.1. Dispositivi Informatici

Totale computer: 120, suddivisi in:

- **80 postazioni standard per uso ufficio**
  Prezzo unitario stimato: **€850**
  Totale: 80 × €850 = **€68.000**

- **40 postazioni grafiche avanzate per reparto Marketing e Comunicazione**
  Prezzo unitario stimato: **€1.300**
  Totale: 40 × €1.300 = **€52.000**

Totale dispositivi informatici: €120.000

4.2. Infrastruttura di Rete

Componente	Quantità	Prezzo unitario (€)	Totale (€)
Switch di secondo livello	7	500	3.500
Switch di terzo livello	1	1.800	1.800
Router aziendale	1	1.200	1.200
Firewall perimetrale	5	3.500	17.500
Server (3 unità)	3	1.800	5.400
Server DHCP dedicato	1	1.200	1.200
NAS aziendale	1	1.000	1.000
IDS/IPS (2 IPS, 1 IDS)	3	2.500	7.500
Cavi di rete (Cat 6)	137	10 (stima media)	1.370
Patch panel, rack, canaline	—	—	685

Totale infrastruttura di rete: €31.985

4.3. Servizi Tecnici

- **Sopralluogo iniziale:** €350
- **Installazione e configurazione:**
  5 tecnici × 3 giorni × 8 ore × €40/h = **€4.800**

Totale manodopera e sopralluogo: €5.150

4.4 Progettazione e Simulazione

Attività	Dettagli	Totale (€)
Progettazione iniziale	Analisi e schema logico preliminare (10 ore a €70/h)	700
Simulazione rete	Simulazione apparati e connessioni (Cisco Packet Tracer)	250

Totale progettazione e simulazione: €950

4.5 Trasporto e Nolo Attrezzature

- Trasporto materiali (3% valore materiali): **~€4.559**
- Nolo attrezzature (5% su materiale + manodopera): **~€7.856**

Totale trasporto e nolo: €12.416

4.7 Totale Generale Stimato

Voce	Totale (€)
Dispositivi informatici	120.000
Infrastruttura di rete	31.985
Manodopera e sopralluogo	5.150
Progettazione e simulazione	950
Trasporto e nolo attrezzature	12.416

Totale generale stimato: €170.501

5. TOOL DI SUPPORTO PER TESTING DELLA RETE

Per verificare il corretto funzionamento e la sicurezza della rete creata, sono stati sviluppati e utilizzati tre strumenti (tool/script) fondamentali per effettuare attività di monitoraggio, test e analisi. :

5.1 Rilevatore di verbi HTTP

Questo tool consente di identificare e analizzare i **verbi HTTP** (come **GET**, **POST**, **PUT**, **DELETE**, ecc.) utilizzati nelle richieste verso i server web. Questi metodi definiscono le azioni che il client intende compiere sul server.

- **Analisi delle vulnerabilità:** alcuni verbi HTTP possono essere usati per attaccare applicazioni web. Identificarli permette di rilevare possibili configurazioni non sicure.
- **Controllo delle operazioni web:** utile per testare come il server risponde a diversi metodi HTTP e individuare potenziali punti deboli.
- **Supporto al penetration testing:** monitora le azioni effettuate dai client per garantire che non vengano eseguite operazioni non autorizzate.

Di seguito vediamo un esempio indicativo del tool:

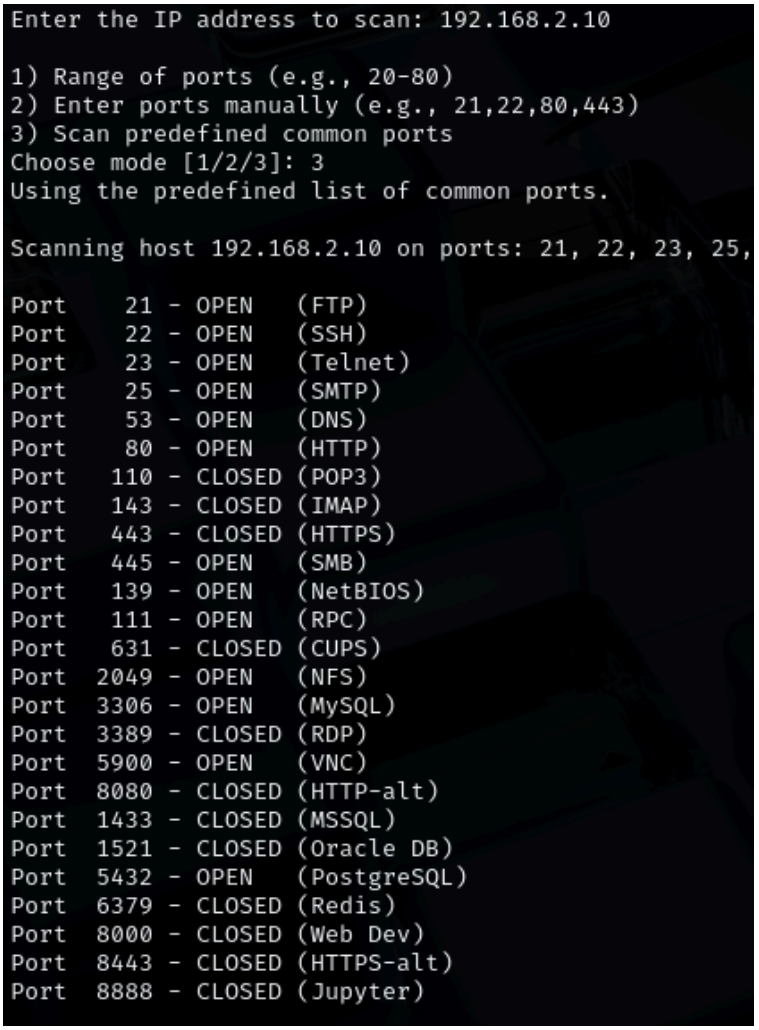
```
┌──(kali㉿kali)-[~/Desktop/Socket]
└─$ python3 http_request_script.py
Enter host/IP of target system: 192.168.2.10
Enter the port of target system (default: 80):
Enter the path to test (default: /phpMyAdmin/):

Testing HTTP methods on 192.168.2.10:80/phpMyAdmin/

GET      → 200 OK
POST     → 200 OK
PUT      → 200 OK
DELETE   → 200 OK
PATCH    → 200 OK
OPTIONS  → 200 OK
HEAD     → 200 OK
TRACE    → 200 OK
CONNECT  → 400 Bad Request
```

5.2 Port Scanner

Il port scanner è stato impiegato per identificare le **porte di rete aperte** sugli host e i **servizi attivi** associati. La scansione delle porte è un'operazione chiave per valutare lo stato di esposizione di un sistema.

- **Rilevamento di porte vulnerabili o non necessarie**: consente di chiudere porte aperte inutilizzate, riducendo la superficie di attacco.
- **Supporto al troubleshooting**: utile per verificare la corretta configurazione di firewall e servizi di rete.

- **Mappatura dei servizi di rete**: permette di ottenere una visione chiara di quali servizi siano attivi e raggiungibili.



Come possiamo osservare, ci sono numerose porte rischiose da tenere aperte, soprattutto se non strettamente necessarie:

- 21 (FTP) – Protocollo non cifrato. Se non strettamente necessario, chiudila o sostituiscila con SFTP (via SSH).
- 23 (Telnet) – Assolutamente da chiudere: è insicuro, trasmette tutto in chiaro.
- 25 (SMTP) – Se il server non invia mail direttamente, non è necessaria.
- 111 (RPC) – Raramente necessario, ed è una porta sfruttata in molti exploit.
- 5432 (PostgreSQL) – Aperta sulla rete. Se il DB non deve essere raggiunto da altri host, andrebbe limitato l'accesso o chiuso direttamente.

6. IMPLEMENTAZIONI POSSIBILI

6.1 Subnet di Rete

Un'implementazione possibile è la suddivisione della rete aziendale in 8 subnet, ognuna di dimensioni sufficientemente grandi da garantire **ampia scalabilità futura**, anche in presenza di un numero attuale ridotto di dispositivi.

L'azienda è strutturata su **6 piani**, ognuno dei quali ospita diversi dispositivi di rete. Oltre a questi, sono presenti due sezioni dedicate: una per la **DMZ** e una per il **NAS**.

È stato deciso di creare **8 subnet con prefisso /19**, in modo da assegnare:

- una subnet per ciascun piano,
- una per la DMZ,
- una per il NAS.

Ogni subnet con prefisso **/19** ha:

- 8192 indirizzi totali
- 8190 host validi (poiché si escludono l'indirizzo di rete e il broadcast)
- Una subnet mask di 255.255.224.0

Le subnet sono ricavate a partire dalla rete **10.1.0.0**, incrementando di **8192 indirizzi** a ogni nuova subnet. Questo approccio garantisce la semplicità nella configurazione, chiarezza nell'assegnazione degli indirizzi IP e possibilità di espansione.

Di seguito, **le subnet** assegnate:

Subnet	Utilizzo
10.1.0.0/19	Piano Terra (PT)
10.1.32.0/19	Primo Piano (P1)
10.1.64.0/19	Secondo Piano (P2)
10.1.96.0/19	Terzo Piano (P3)
10.1.128.0/19	Quarto Piano (P4)
10.1.160.0/19	Quinto Piano (P5)
10.1.192.0/19	NAS
10.1.224.0/19	DMZ

Per permettere il routing tra le otto subnet sfruttando la configurazione Router on a stick, che utilizza un'unica interfaccia fisica del router, andremo a creare un VLAN per ognuna di esse:

VLAN	Nome	Subnet	Gateway
10	PT	10.1.0.0/19	10.1.0.1
20	P1	10.1.32.0/19	10.1.32.1
30	P2	10.1.64.0/19	10.1.64.1
40	P3	10.1.96.0/19	10.1.96.1
50	P4	10.1.128.0/19	10.1.128.1
60	P5	10.1.160.0/19	10.1.160.1
70	NAS	10.1.192.0/19	10.1.192.1
80	DMZ	10.1.224.0/19	10.1.224.1

Il funzionamento si basa sulla configurazione di sub-interfacce logiche sul router, ciascuna associata a una VLAN specifica. A ogni sub-interfaccia viene assegnato un indirizzo IP con funzione di gateway per la relativa subnet, oltre al tag VLAN corrispondente. La comunicazione tra le VLAN avviene tramite una porta trunk configurata sullo switch centrale collegato al router.

6.2 Sniffer di pacchetti

Un Packet Sniffer è un software che intercetta e cattura i pacchetti di dati che transitano in una rete. Il nostro permette inoltre di scegliere due modalità distinte di sniffing:

1. **Sniffing continuo:** il programma lavora finché l'utente non decide di interrompere l'intercettazione.
2. **Sniffing controllato:** con questa modalità viene richiesto all'utente di inserire il numero di pacchetti da intercettare.

Abbiamo inoltre integrato un menù per filtrare il tipo di pacchetti da intercettare, offrendo cinque opzioni:

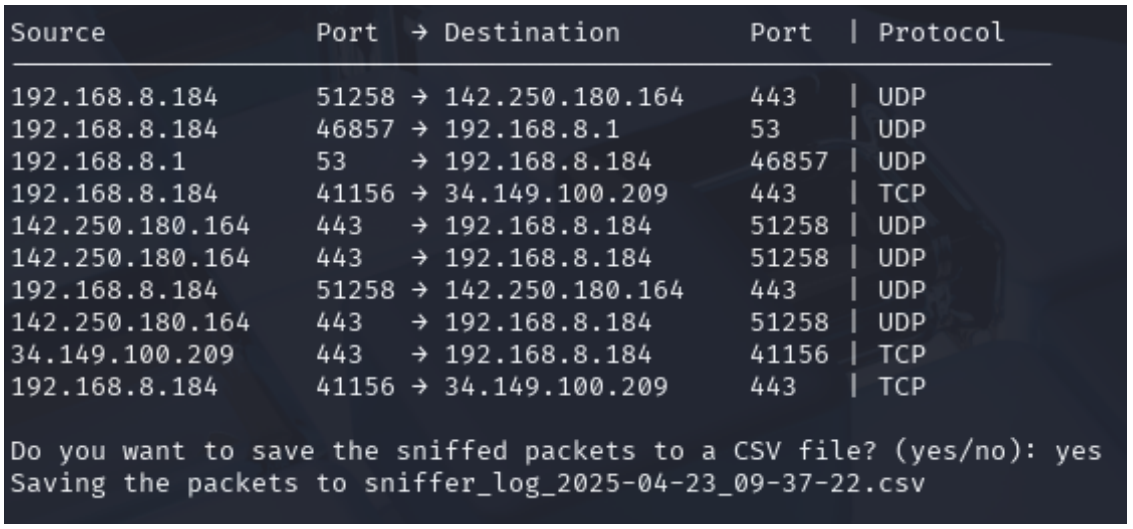
1. Only TCP
2. Only UDP
3. Only ICMP
4. Only DNS
5. All IP packets

Utilizzandolo abbiamo svolto le seguenti operazioni:

- **Monitoraggio del traffico di rete:** analisi del traffico in tempo reale per identificare problemi di performance, anomalie o attacchi DoS.

- **Analisi della sicurezza:** Permette di identificare potenziali attacchi in corso, come attacchi di Man-in-the-Middle, sniffing di dati in chiaro, o traffico sospetto.

Di seguito troviamo due immagini. La prima è un esempio di output su terminale, la seconda invece raffigura il file CSV derivato dalla precedente scansione. La creazione di un Log permette l'analisi approfondita e curata di tutto il traffico sulla rete, permettendo di tenere traccia di eventuali irregolarità.



```
Source              Port  → Destination         Port   | Protocol
-------------------------------------------------------------------
192.168.8.184       51258 → 142.250.180.164     443    | UDP
192.168.8.184       46857 → 192.168.8.1         53     | UDP
192.168.8.1         53    → 192.168.8.184       46857  | UDP
192.168.8.184       41156 → 34.149.100.209      443    | TCP
142.250.180.164     443   → 192.168.8.184       51258  | UDP
142.250.180.164     443   → 192.168.8.184       51258  | UDP
192.168.8.184       51258 → 142.250.180.164     443    | UDP
142.250.180.164     443   → 192.168.8.184       51258  | UDP
34.149.100.209      443   → 192.168.8.184       41156  | TCP
192.168.8.184       41156 → 34.149.100.209      443    | TCP

Do you want to save the sniffed packets to a CSV file? (yes/no): yes
Saving the packets to sniffer_log_2025-04-23_09-37-22.csv
```

Source	Source Port	Destination	Destination Port	Protocol
192.168.8.184	51258	142.250.180.164	443	UDP
192.168.8.184	46857	192.168.8.1	53	UDP
192.168.8.1	53	192.168.8.184	46857	UDP
192.168.8.184	41156	34.149.100.209	443	TCP
142.250.180.164	443	192.168.8.184	51258	UDP
142.250.180.164	443	192.168.8.184	51258	UDP
192.168.8.184	51258	142.250.180.164	443	UDP
142.250.180.164	443	192.168.8.184	51258	UDP
34.149.100.209	443	192.168.8.184	41156	TCP
192.168.8.184	41156	34.149.100.209	443	TCP

7. CONCLUSIONI

Il progetto di rete realizzato per la Compagnia Theta rappresenta un passo importante verso una gestione più moderna, sicura ed efficiente delle attività aziendali. La rete è stata pensata per adattarsi alle esigenze attuali ma anche per crescere nel tempo, mantenendo alti standard di sicurezza e affidabilità.

Grazie a una struttura ben organizzata, la rete distribuisce in modo intelligente le connessioni tra i vari piani dell'edificio, protegge i dati con sistemi di sicurezza avanzati e permette il controllo centralizzato tramite una sala server dedicata. Inoltre, l'introduzione di strumenti per il monitoraggio e il test della rete rende più semplice individuare problemi e intervenire rapidamente in caso di necessità.

Dal punto di vista dei **costi**, l'investimento iniziale è stato pianificato per garantire un buon equilibrio tra qualità e sostenibilità economica, scegliendo componenti professionali e soluzioni flessibili. Questo significa meno interventi futuri e meno spese impreviste per il futuro della Compagnia Theta.