

# Relazione configurazione tecnica

## INDICE

1. Introduzione.....	Pag. 1
2. Architettura di rete.....	Pag. 1
● 2.1 Rete interna (LAN)	
● 2.2 NAS	
● 2.3 Firewall	
● 2.4 Web Server	
3. Test di funzionamento.....	Pag. 3
● Scansione delle Porte (Port Scanner)	
● Verifica Verbi HTTP	
● Cattura del traffico (packet sniffing)	

---

## 1. Introduzione

La presente relazione certifica il completamento delle fasi di installazione, configurazione e testing dell'infrastruttura IT progettata per la Compagnia Theta. Si attesta la piena rispondenza del sistema ai requisiti funzionali e di sicurezza concordati.

## 2. Architettura di rete

Questa sezione mostra nel dettaglio la configurazione di rete per ciascun apparato.

### ROUTER CENTRALE

Poiché l'edificio ha 6 piani con 20 computer ciascuno e ogni piano ha uno switch dedicato abbiamo optato per una configurazione "Router-on-a-Stick", dove un'unica interfaccia fisica è suddivisa in sotto-interfacce logiche, una per ogni piano, creando una VLAN). Ogni piano avrà pertanto un indirizzo IP specifico sull'interfaccia del router che fungerà da gateway per i 20 host di quel piano.

Se decidi di affrontare il Bonus sul subnetting, la relazione dovrebbe dettagliare come hai diviso lo spazio di indirizzamento.

**DMZ e Internet:** Il router non comunica solo internamente, ma deve gestire i flussi verso il perimetro di sicurezza:

- **Default Route:** Configurazione di una default static route che punta verso l'indirizzo IP del Firewall perimetrale per tutto il traffico destinato a Internet.
- **Routing verso la DMZ:** Definizione delle rotte per permettere agli host interni di raggiungere il Web Server (DVWA) posizionato nella DMZ, passando attraverso il firewall.
- **Integrazione IDS/IPS:** Descrizione di come il traffico viene convogliato attraverso i **3 sistemi IDS/IPS** implementati nel perimetro interno per il monitoraggio.

## **SWITCH E WORKSTATION**

Dovendo gestire un totale di 120 host più i dispositivi di rete, la scelta più appropriata ricade su una maschera di sottorete /24 che garantisce ampio spazio per l'aggiunta di altri dispositivi quali stampanti, telefoni VoIP e future postazioni di lavoro senza dover riconfigurare l'intera rete.

**Subnetting:** al fine di elevare gli standard di sicurezza e ridurre traffico di rete non necessario, abbiamo scelto di implementare una soluzione di Subnetting, senza alcun costo aggiuntivo a Vostro carico. Questa ottimizzazione permetterà una gestione più granulare degli indirizzi IP e preparerà la rete a future espansioni in modo ordinato.

**DHCP:** Per ottimizzare la gestione del traffico ogni piano è stato segmentato in una sottorete specifica. Sul router è stato configurato, inoltre, il servizio DHCP (Dynamic Host Configuration Protocol) che assegna automaticamente gli indirizzi IP alle 120 workstation secondo il seguente schema logico:

**P1 Gateway:** 192.168.1.1 | **IP da 192.168.1.1 a 192.168.1.254, subnet 255.255.255.0;**

**P2 Gateway:** 192.168.2.1 | **IP da 192.168.2.2. a 192.168.2.254, subnet 255.255.255.0;**

**P3 Gateway:** 192.168.3.1 | **IP da 192.168.3.3 a 192.168.3.254, subnet 255.255.255.0;**

**P4 Gateway:** 192.168.4.1 | **IP da 192.168.4.4 a 192.168.4.254, subnet 255.255.255.0;**

**P5 Gateway:** 192.168.5.1 | **IP da 192.168.5.5 a 192.168.5.254, subnet 255.255.255.0;**

**P6 Gateway:** 192.168.6.1 | **IP da 192.168.6.6 a 192.168.6.254, subnet 255.255.255.0;**

## **SISTEMI IDS/IPS**

Il servizio di IDS agisce come un "sistema di allarme". Monitora passivamente il traffico di rete alla ricerca di attività sospette o firme di attacchi noti. L'IPS, oltre a rilevare la minaccia, interviene in tempo reale per fermarla.

Questi servizi sono stati implementati in 3 punti del perimetro interno (piano 1, piano 2 e piano 3) per il monitoraggio costante del traffico e la prevenzione delle intrusioni.

## **FIREWALL PERIMETRALE**

Il firewall perimetrale è un dispositivo di sicurezza che funge da "barriera" tra la rete interna aziendale e Internet.

Posizionato strategicamente tra il router interno e la connessione Internet per filtrare il traffico in entrata e in uscita ed è stato configurato con un indirizzo ip statico.

**Indirizzo IP:** 10.0.0.1

**Gateway:** 10.0.0.2

## **WEB SERVER (DMZ)**

La macchina DVWA è stata isolata in una Zona Demilitarizzata (DMZ) tra il firewall e Internet, garantendo l'accessibilità esterna senza esporre la rete interna con un indirizzo IP statico.

**Indirizzo IP:** 192.168.50.10

**Gateway:** 192.168.50.1

## NAS

Il NAS (Network Attached Storage) è un hard disk di rete di elevata capacità di storage e prestazioni che garantisce la condivisione di files all'interno del perimetro aziendale. È stato collegato al router con un indirizzo IP statico.

**Indirizzo IP:** 192.168.7.2

**Gateway:** 192.168.7.1

## 3. Test di funzionamento e sicurezza

Sono stati sviluppati tool ad hoc personalizzati in Python per verificare la sicurezza dell'infrastruttura, senza l'ausilio di tool preesistenti.

### 3.1 Scansione delle Porte (Port Scanner)

**Obiettivo:** Verificare le porte aperte sul target “Metasploitable”.

Il programma sviluppato accetta in input un IP target e un range di porte. Tenta una connessione socket per ogni porta e restituisce l'elenco delle porte aperte con l'indice di rischio.

#### Risultato scansione:

```
kali@kali: ~/Desktop/Python
Session Actions Edit View Help
Inserisci l'IP target (es. 192.168.1.1): 192.168.0.181
Inserisci porta di partenza: 10
Inserisci porta di fine: 500

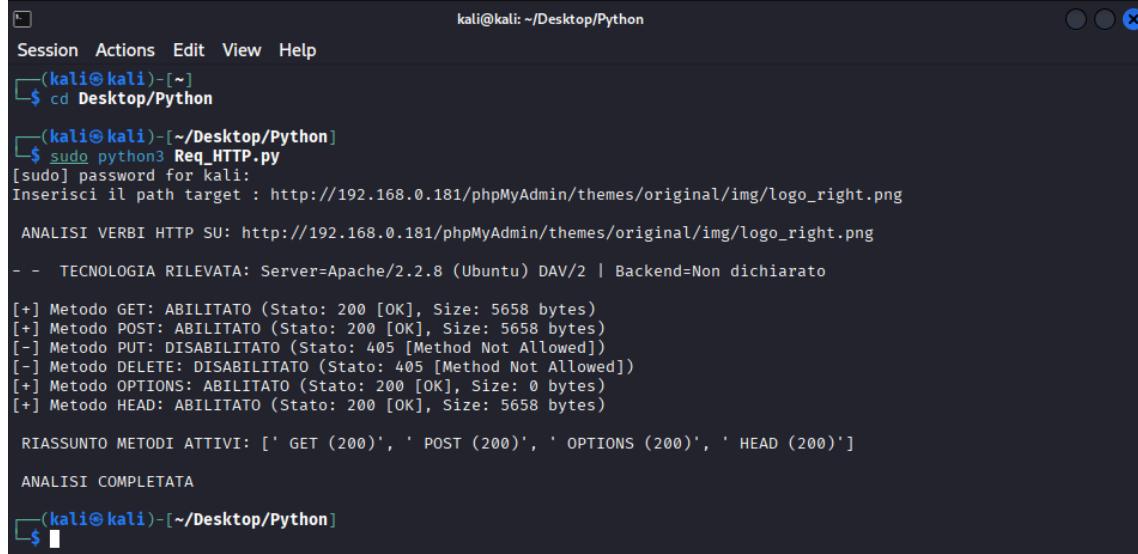
[*] Verifica raggiungibilità di 192.168.0.181 in corso ...
[*] Host 192.168.0.181 è ONLINE. Inizio scansione ...

AVVIO SCANSIONE ...
+---+ +---+ +---+
| PORTA | SERVIZIO | RISCHIO RILEVATO |
+---+ +---+ +---+
| 21 | ftp | ALTO: FTP (Non criptato, sniffabile) |
| 22 | ssh | MEDIO: SSH (Rischio Brute Force) |
| 23 | telnet | CRITICO: Telnet (Non criptato, obsoleto) |
| 25 | smtp | MEDIO: SMTP (Possibile Open Relay) |
| 53 | domain | MEDIO: DNS (Rischio DDoS Amplification) |
| 80 | http | BASSO: HTTP (Non criptato) |
| 111 | sunrpc | GENERICO (Superficie di attacco) |
| 139 | netbios-ssn | ALTO: NetBIOS (Info Leak) |
| 445 | microsoft-ds | CRITICO: SMB (Rischio Ransomware/Worm) |
+---+ +---+ +---+
— SCANSIONE COMPLETATA —
```

### 3.2 Verifica Verbi HTTP

**Obiettivo:** mappare i metodi HTTP abilitati sul percorso phpMyAdmin26 utilizzando un programma che invia richieste con diversi verbi (GET, POST, PUT, DELETE, HEAD) e analizza le risposte del server.

#### Risultato verifica:



```
kali㉿kali: ~/Desktop/Python
Session Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop/Python

(kali㉿kali)-[~/Desktop/Python]
$ sudo python3 Req_HTTP.py
[sudo] password for kali:
Inserisci il path target : http://192.168.0.181/phpMyAdmin/themes/original/img/logo_right.png

ANALISI VERBI HTTP SU: http://192.168.0.181/phpMyAdmin/themes/original/img/logo_right.png
- - TECNOLOGIA RILEVATA: Server=Apache/2.2.8 (Ubuntu) DAV/2 | Backend=Non dichiarato

[+] Metodo GET: ABILITATO (Stato: 200 [OK], Size: 5658 bytes)
[+] Metodo POST: ABILITATO (Stato: 200 [OK], Size: 5658 bytes)
[-] Metodo PUT: DISABILITATO (Stato: 405 [Method Not Allowed])
[-] Metodo DELETE: DISABILITATO (Stato: 405 [Method Not Allowed])
[+] Metodo OPTIONS: ABILITATO (Stato: 200 [OK], Size: 0 bytes)
[+] Metodo HEAD: ABILITATO (Stato: 200 [OK], Size: 5658 bytes)

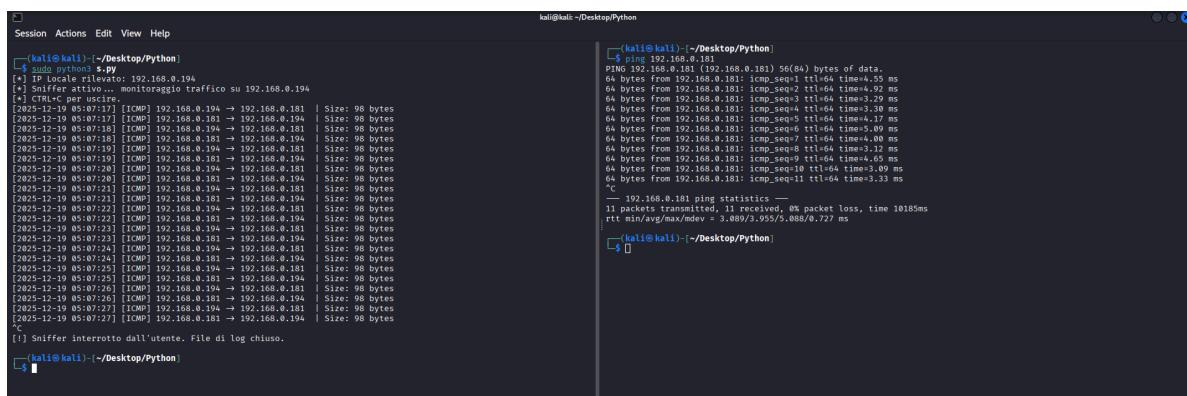
RIASSUNTO METODI ATTIVI: [' GET (200)', ' POST (200)', ' OPTIONS (200)', ' HEAD (200)']

ANALISI COMPLETATA
(kali㉿kali)-[~/Desktop/Python]
$
```

### 3.3 Cattura del traffico (packet sniffing)

**Obiettivo:** Monitorare e analizzare in tempo reale il traffico di pacchetti che attraversa l'infrastruttura di rete

#### Risultato verifica:



```
kali㉿kali: ~/Desktop/Python
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ./Req_HTTP.py
[*] IP locale rilevato: 192.168.0.194
[*] Sniffer attivo... monitoraggio traffico su 192.168.0.194
[*] ^CRLc per uscire
[2025-12-19 05:07:17] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:17] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:18] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:18] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:19] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:19] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:20] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:20] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:21] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:21] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:22] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:22] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:23] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:23] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:24] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:24] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:25] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:25] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:26] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:26] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[2025-12-19 05:07:27] [ICMP] 192.168.0.194 -> 192.168.0.181 | Size: 98 bytes
[2025-12-19 05:07:27] [ICMP] 192.168.0.181 -> 192.168.0.194 | Size: 98 bytes
[*] Sniffer interrotto dall'utente. File di log chiuso.
(kali㉿kali)-[~]
$
```