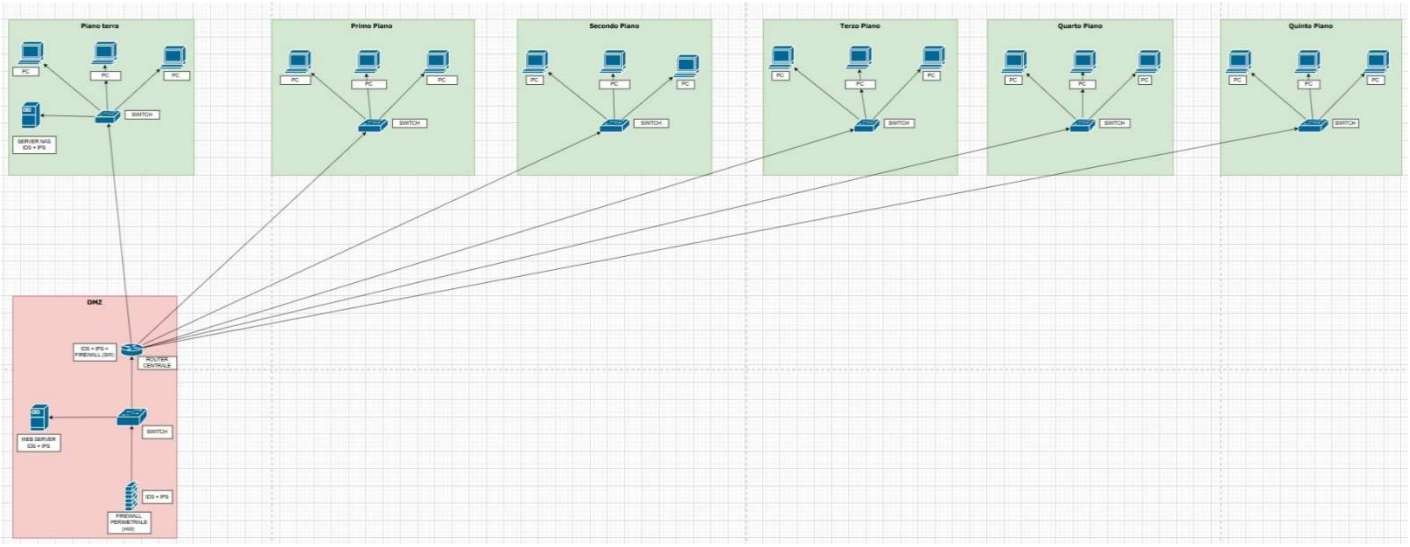
PROGETTO DI RETE

AZIENDA COMMITTENTE: THETA SPA

SOMMARIO

STRUTTURA DELLA RETE

LAYOUT

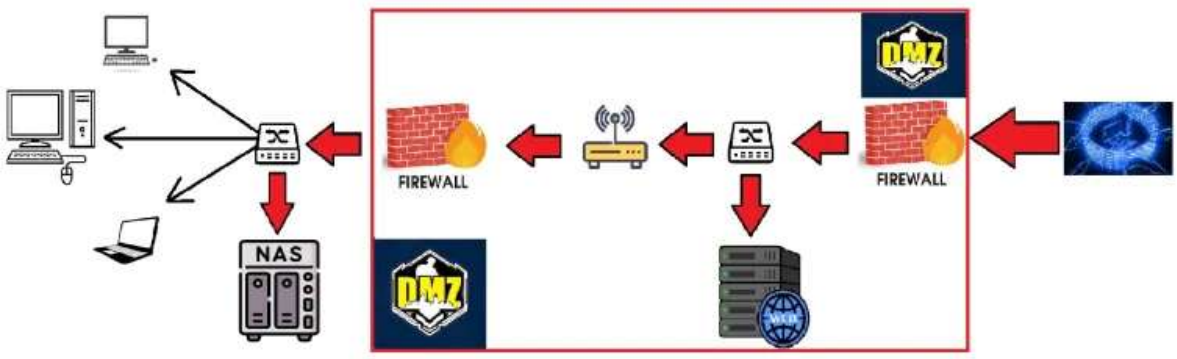


DESCRIZIONE

Il layout sopra rappresenta una configurazione base in cui non sono rappresentati i 20 PC previsti nella richiesta del committente risultando pertanto uno spaccato esemplificativo. E' inoltre possibile visualizzare la suddivisione della rete nei vari piani.

La rete, suddivisa in **subnet**, è configurata per utilizzare il protocollo **DHCP (Dynamic Host Configuration Protocol)** che consente di assegnare automaticamente gli indirizzi IP ai dispositivi, semplificando la gestione e riducendo il rischio di errori.

PIANO TERRA



Il piano terra ospiterà la **DMZ (zona demilitarizzata)**, che funge da punto di ingresso per il traffico proveniente da Internet. La DMZ è progettata per essere completamente protetta, con l'implementazione di un **firewall perimetrale (HW)** e sistemi **IDS/IPS (Intrusion Detection/Prevention System)**, che monitorano e bloccano eventuali attacchi provenienti dall'esterno. Accanto alla DMZ, sarà posizionata un'area sicura per il **NAS (Network Attached Storage)**, dove saranno conservati i backup aziendali.

Componenti principali della DMZ:

- **Firewall Perimetrale (HW) con IDS/IPS**: protegge la rete aziendale da accessi non autorizzati e attacchi esterni.
- **Switch a 6 Porte con IDS/IPS**: gestisce il traffico all'interno della DMZ, monitorando e proteggendo i dispositivi collegati.
- **Web Server con IDS/IPS**: gestisce i servizi web aziendali e viene monitorato in tempo reale per prevenire attacchi.

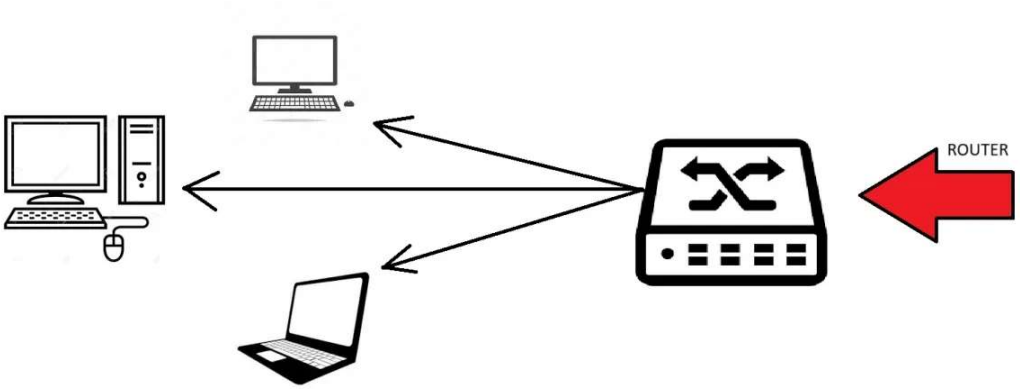
Flusso del Traffico e Sicurezza Aggiuntiva

Il traffico dalla DMZ si propaga nel resto della struttura fornendo la connessione a tutti i piani della stessa.

Nello stesso piano troviamo inoltre:

- **NAS**: gestisce il backup dei dati ed è protetto da un sistema IDS/IPS per monitorare il traffico in accesso;
- **Switch**: dotato di IDS per garantire prestazioni ottimali e gestire al meglio il traffico.

PIANI SUPERIORI



I piani superiori sono configurati per essere coerenti con il piano terra, al fine di mantenere un'infrastruttura di rete omogenea e facilmente gestibile. Ogni piano è dotato di uno switch a 24 porte con IDS per poter offrire un margine di espansione, consentendo di aggiungere nuovi dispositivi senza dover modificare l'infrastruttura esistente.

TESTING

Test di connettività tra due PC in rete

```
C:\> ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.6.2: bytes=32 time<1ms TTL=127
Reply from 192.168.6.2: bytes=32 time<1ms TTL=127
Reply from 192.168.6.2: bytes=32 time<1ms TTL=127
Reply from 192.168.6.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

L'immagine mostra un test di connessione tramite ping tra PC situati in reti differenti.

Test di connettività tra PC e Web Server

```
C:\> ping 169.254.137.10

Pinging 169.254.137.10 with 32 bytes of data:

Reply from 169.254.137.10: bytes=32 time<1ms TTL=127
Reply from 169.254.137.10: bytes=32 time<1ms TTL=127
Reply from 169.254.137.10: bytes=32 time=16ms TTL=127
Reply from 169.254.137.10: bytes=32 time<1ms TTL=127

Ping statistics for 169.254.137.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms
```

L'immagine mostra un ping tra un PC e il Web Server nella zona DMZ.

Test di connettività tra PC e Nas

```
C:\> ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=127
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

L’immagine mostra un ping tra un PC e il NAS.

Si è optato inoltre di configurare il Web Server su una rete completamente distinta da quella della intera struttura per prevenire eventuali scalate esterne.

TESTING DELLA RETE

VERIFICA DEI VERBI HTTP E SCANSIONE DELLE PORTE

L'azienda Theta ci ha incaricato di sviluppare un software in grado di verificare quali verbi HTTP sono abilitati sul loro server.

Codice:

Usando il linguaggio Python, abbiamo ideato questo script.

```python
import requests

def check_all_http_methods():
    print("\n--- Verifica di tutti i metodi HTTP abilitati e non abilitati ---")
    url = input("Inserisci l'URL (es. https://example.com): ").strip()

    # Lista di metodi HTTP comuni
    methods = ['GET', 'POST', 'PUT', 'DELETE', 'OPTIONS', 'PATCH', 'HEAD']
    results = {}

    for method in methods:
        try:
            # Invia una richiesta con il metodo specifico
            response = requests.request(method, url)

            # Se il metodo è supportato, aggiungi il codice di stato
            if response.status_code != 405:  # 405 significa "Method Not Allowed"
                results[method] = f"Abilitato (Status Code: {response.status_code})"
            else:
                results[method] = "Non abilitato (405 Method Not Allowed)"
        except requests.exceptions.RequestException as e:
            results[method] = f"Errore durante la richiesta: {e}"

    # Stampa i risultati
    print("\n--- Risultati ---")
    for method, status in results.items():
        print(f"{method}: {status}")

    # Dettagli aggiuntivi: prova a ottenere metodi supportati tramite OPTIONS
    try:
        print("\n--- Tentativo con OPTIONS per recuperare i metodi supportati ---")
        response_options = requests.options(url)
        if "Allow" in response_options.headers:
            allowed_methods = response_options.headers["Allow"]
            print("Metodi dichiarati dal server nell'header 'Allow':")
            for method in allowed_methods.split(","):
                print(f"- {method.strip()}")
        else:
            print("Il server non ha restituito l'header 'Allow'.")
    except requests.exceptions.RequestException as e:
        print(f"Errore durante la richiesta OPTIONS: {e}")

if __name__ == "__main__":
    while True:
        check_all_http_methods()
        another = input("\nVuoi verificare un altro URL? (s/n): ").strip().lower()
        if another != 's':
            print("Programma terminato.")
            break
```

Funzionamento del codice:

1. **Input dell'utente**: viene richiesto all'utente di inserire l'URL che desidera verificare.
2. **Test metodi HTTP**: invia una richiesta per ciascun metodo nella lista e salva il risultato (abilitato/non abilitato).
3. **Verifica con OPTIONS**: se il server fornisce l'header *Allow*, mostra tutti i metodi dichiarati abilitati.
4. **Output dei risultati**: mostra i metodi abilitati, non abilitati, e i codici di stato.
5. **Ripetizione opzionale**: richiesta di eventuale verifica di un ulteriore URL.

Risultato ed esempio pratico:

```
--- Risultati ---
GET: Abilitato (Status Code: 200)
POST: Abilitato (Status Code: 200)
PUT: Non abilitato (405 Method Not Allowed)
DELETE: Non abilitato (405 Method Not Allowed)
OPTIONS: Abilitato (Status Code: 200)
PATCH: Non abilitato (405 Method Not Allowed)
HEAD: Abilitato (Status Code: 200)

--- Tentativo con OPTIONS per recuperare i metodi supportati ---
Metodi dichiarati dal server nell'header 'Allow':
- GET
- HEAD
```

Si può fare un piccolo accenno al fatto che è stato necessario bypassare il sistema *php* e utilizzare l'immagine del logo per comunicare direttamente con il server di Apache, dunque come URL di indagine, è stato utilizzato quello del logo.

Report Port Scanner

Il presente documento descrive l'implementazione e il testing di un port scanner sviluppato in Python. Il port scanner è uno strumento di rete che permette di analizzare lo stato delle porte TCP su un host specificato, identificando quali porte sono aperte, chiuse o presentano errori di connessione. Questo strumento è particolarmente utile per l'analisi della sicurezza di rete e la diagnostica dei servizi di rete.

SCRIPT DI PROGRAMMAZIONE

Lo script è strutturato in tre fasi:

1. Richiesta indirizzo IP:

Il programma chiede all'utente di inserire l'indirizzo IP da verificare.

Qualora l'indirizzo IP non fosse valido, il programma risponderà con:

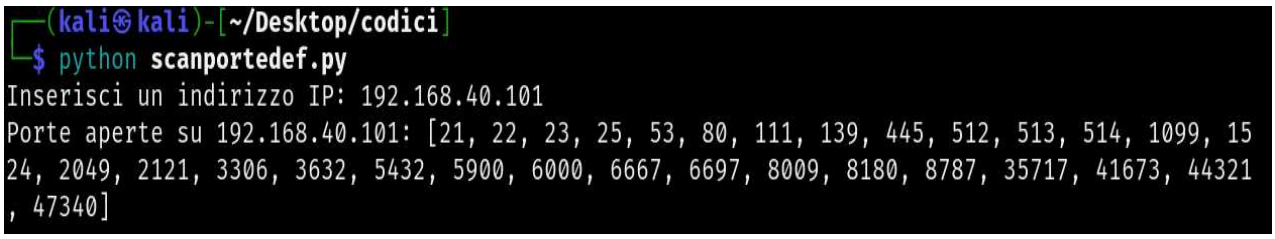
2. Raggiungibilità IP:

Dopo aver inserito l'indirizzo IP il programma verifica tramite Ping che questo sia raggiungibile.Qualora l'indirizzo IP non fosse raggiungibile, Il programma rispondera con:

3. Scansione singola di ogni porta:

Se l'indirizzo IP è raggiungibile il programma inizia la scansione delle porte mostrando lo stato di avanzamento. Terminata la scansione, potremmo ricevere due tipi di risultati:

- Se vengono trovate porte aperte:



- Se non viene trovata nessuna porta aperta:

REPORT

Sulla base dei test effettuati, si riportano le seguenti osservazioni:

1. Funzionalità:

- Lo script esegue correttamente la sua funzione principale
- La rilevazione dello stato delle porte è accurata
- L'interfaccia utente è funzionale anche se basica

2. Affidabilità:

- Gestione robusta degli errori
- Nessun crash durante i test
- Chiusura appropriata delle risorse di sistema

3. Limitazioni:

- Scansione sequenziale (non parallela)
- Timeout fisso non configurabile
- Mancanza di supporto per scansioni UDP

4. Raccomandazioni:

Attraverso i test effettuati in precedenza, abbiamo rilevato che le seguenti porte erano aperte:

- 21
- 23
- 139
- 445

Si raccomanda pertanto al cliente di limitare l'accesso ai servizi FTP, Telnet, SMB, considerati insicuri.

5. Conclusioni:

Lo script rappresenta una solida implementazione base di un port scanner. È funzionale e affidabile per l'uso su reti locali e può essere utilizzato come base per sviluppi futuri. Si raccomanda l'implementazione delle migliorie suggerite per un utilizzo in ambiente di produzione.

ANALISI DEL CODICE MALEVOLO

Nel corso dell'attività di analisi, il team ha ricevuto un file compresso in formato *.zip* proveniente dall'azienda Theta. Il file conteneva diverse immagini e documenti, apparentemente innocui, ma che dopo un'approfondita indagine, hanno rivelato contenuti nascosti e informazioni crittografate utilizzando tecniche avanzate di steganografia.

L'obiettivo principale della nostra analisi è stato quello di decifrare i dati nascosti all'interno dei file forniti, identificando eventuali messaggi e/o codici segreti.

Il file **photo.zip** che l'azienda Theta ci ha mandato contiene i seguenti elementi:

- varie immagini in formato .jpg
- file html
- cartelle contenenti codici riguardanti pagine internet.

Il team ha iniziato con l'estrazione del file .zip in una macchina virtuale (Kali Linux), così da rendere il processo più sicuro.

Abbiamo subito notato che le immagini contenute dal file avevano un aspetto insolito, infatti utilizzando lo strumento **steghide** ci siamo accorti che c'erano file nascosti all'interno delle foto.

Il processo non è stato semplice, il primo indizio che abbiamo trovato è stato un commento (***mistero risolto***) non inerente al codice all'interno del file *main.js*.

Utilizzando **steghide**, è stato possibile estrarre questi file, che risultavano essere frammenti di codice scritti in due linguaggi esoterici:

- **Brainfuck**, un linguaggio di programmazione noto per la sua sintassi complessa e difficile da interpretare (i frammenti di codice **Brainfuck** estratti sono stati tradotti in testo leggibile, rivelando una passphrase).
- **Cow Code**, un linguaggio basato sulla parola "moo", è simile al Brainfuck ed è stato creato per divertimento, con comandi limitati e una sintassi volutamente assurda. Anche in questo caso abbiamo tradotto il codice in testo leggibile, rilevando ulteriori indizi.

Il team ha analizzato con successo numerose immagini presenti nel file *.zip*, utilizzando strumenti avanzati per rilevare eventuali dati nascosti. Tra i vari file estratti, uno in particolare si è rivelato di fondamentale importanza: una delle immagini, infatti, conteneva un file HTML nascosto denominato ***thankyou.html***; una volta aperto il file è emerso un messaggio chiaro e inquietante visualizzato direttamente sulla pagina web:

"Abbiamo svuotato i vostri conti! Grazie azienda Theta."

Dopo aver comunicato il messaggio alla vostra azienda è stato per voi possibile recuperare il capitale presente nei vostri conti.

PREVENTIVO FINALE DEI COSTI

Il preventivo prevede l'acquisto della migliore strumentazione possibile avvalendosi dei principali brand sul mercato *(CISCO, HP, Schneider, ect)* per garantire una maggiore affidabilità e robustezza della rete.

PREVENTIVO THETA				
MATERIALE	**Q.TA'**	**PREZZO UNITARIO**	**IVA**	**IMPORTO**
Cavo di rete cat.8 (bobine da 100mt per coprire 2km di cablaggi)	20	191,76 €	22%	4.678,94 €
Cavo di rete cat.8 per patching	150	3,26 €	22%	596,58 €
Presa di rete da incasso a parete	150	12,21 €	22%	2.234,43 €
Rack (ai piani)	6	179,66 €	22%	1.315,11 €
Rack (DMZ)	1	2.958,97 €	22%	3.609,94 €
Patch panel 24 porte (ai piani)	6	114,35 €	22%	837,04 €
Switch 24 porte (ai piani)	6	2.747,00 €	22%	20.108,04 €
UPS (40kVA)	2	11.281,23 €	22%	27.526,20 €
Switch 8 porte (in DMZ)	1	1.039,23 €	22%	1.267,86 €
Router 8 porte	1	1.718,07 €	22%	2.096,05 €
NAS	1	39.225,63 €	22%	47.855,27 €
WEB Server	1	6.378,50 €	22%	7.781,77 €
IDS	10	2.565,71 €	22%	31.301,66 €
IPS	4	4.525,00 €	22%	22.082,00 €
Firewall SW su Router Centrale	1	2.080,50 €	22%	2.538,21 €
Firewall perimetrale [HW]	1	16.766,91 €	22%	20.455,63 €
Licenze varie + aggiornamenti + assistenza on-site **(costo annuo)**	1	51.236,22 €	22%	62.508,19 €
SUBTOTALE				**258.792,93 €**
MANODOPERA	**Q.TA'**	**PREZZO UNITARIO**	**IVA**	**IMPORTO**
Elettricisti (14 persone) - 5gg	560	46,70 €	10%	28.767,20 €
Sistemisti di rete (4 persone) - 3gg	96	52,55 €	10%	5.549,28 €
Progetto (8 persone) - 5gg	320	65,98 €	10%	23.224,96 €
Team Cyber Security (4 persone)	96	80,36 €	10%	8.486,02 €
SUBTOTALE				**66.027,46 €**
TOTALE				**324.820,38 €**

Nel preventivo in questione sono stati tenuti in considerazione, non solo la strumentazione di rete e la manodopera, ma anche l'assistenza post vendita in quanto riteniamo che il nostro lavoro non si concluda con la semplice installazione e configurazione del tutto, ma offra al cliente un supporto costante nel tempo: sono previsti pertanto dei costi ricorsivi annui in cui forniamo gli aggiornamenti della strumentazione di sicurezza e tempestivi remote/on-site supports da parte del team WOLFGUARD che garantiscono interventi nell' arco delle 12 ore, il tutto per permettere la continuità di servizio da parte del cliente.

E' stata prevista inoltre l'installazione di n.2 gruppi di continuità (UPS) onde evitare la perdita di lavoro causata da impreviste interruzioni di elettricità.

Nel preventivo si tiene inoltre conto del servizio di assistenza messo a disposizione dalla nostra società tramite i tecnici di Cyber Security che si son occupati, in tempi davvero ristretti, di analizzare e fornire quanti più dettagli possibili per far fronte alla minaccia che ha coinvolto la vostra società, permettendovi di rientrare in possesso dei vostri capitali.

Considerando l'intera spesa del cliente, abbiamo ritenuto cosa gradita non effettuare alcun ricarico sulla materiale acquistato, girando tale importo come scontistica sul totale poiché il contratto in questione garantisce tra le parti un rapporto costante nel tempo.