REPORT S4

BUILD WEEK

Il team Sniffing Sockets: Elena - Giuseppe - Manfredi - Cristiano - Gianluca - Giacomo - Kevin

Presenta:

Spiegazione della traccia del progetto

Siamo stati ingaggiati dalla compagnia Theta per sviluppare un preventivo di spesa e un progetto di rete per la loro infrastruttura IT.
Di seguito un riepilogo dei componenti richiesti e necessari per la creazione dell'infrastruttura.

1. Analisi della Struttura e Utenti

L'edificio si sviluppa su **6 livelli.** La rete deve garantire connettività **stabile e sicura** per un totale di **120 postazioni di lavoro**.

2. Architettura di Rete e Sicurezza

Il cuore dell'infrastruttura si basa su una **separazione logica** tra i servizi interni e quelli esposti all'esterno (***DMZ***), protetti da un sistema di difesa multilivello.

- ***Firewall Perimetrale (router-firewall), chiamato ASA in PT o PFSense nel laboratorio*:** dispositivo di frontiera con funzioni *L3* (routing) e di sicurezza (*stateful filtering/NAT*). Rappresenta il punto di controllo del traffico tra *Internet*, *DMZ* e *rete interna*, applicando policy di accesso e registrando gli eventi;
- ***Segmentazione e posizionamento IDS/IPS*:** Saranno implementati **3 sistemi di rilevamento e prevenzione intrusioni** posizionati strategicamente per monitorare:
    1. **Traffico Perimetro** ↔ **DMZ**: accessi ai servizi esposti in *DMZ* e tentativi di exploit/scansione verso il web server;
    2. **Traffico Perimetro** ↔ **LAN** (verso router centrale): controllo del traffico diretto alla rete interna e prevenzione di attività anomale o tentativi di attraversamento verso le *VLAN* aziendali;
    3. **Monitoraggio Area Server** (*VLAN 100 / NAS*): rilevamento di accessi anomali e possibili pattern di esfiltrazione dati verso lo storage aziendale
- ***Web Server (DMZ)*:** Implementazione di un server web (simulato dalla *DVWA*) isolato in una zona demilitarizzata per scopi applicativi/test;
- ***Storage (NAS)*:** Unità di archiviazione centrale per il *backup* dei dati e la condivisione di file aziendali, protetta da ***policy di accesso restrittive***.

3. Elenco Componenti Hardware Necessari

Per soddisfare i requisiti, la lista di materiali da acquistare (*Bill of Materials*) dovrà includere:

1. ***Networking*:**
    - 1 *Router centrale* (*inter-VLAN routing* in modalità *router-on-a-stick*) con *DHCP* configurato via *CLI*.
    - 1 *Firewall perimetrale* (*router-firewall*) (unico punto di accesso/uscita verso *Internet*).
      La separazione tra routing interno (*router centrale*) e routing di frontiera

(*router-firewall*) consente di mantenere policy perimetrali e policy interne distinte.
    - 6 *Switch* di accesso (uno per piano, minimo 24 porte ciascuno) per connettere le 20 postazioni di lavoro di ogni livello;
2. ***Server & Storage*:**
    - 1 *Server* fisico per l'istanza Web (Rappresentato dalla *DVWA*);
    - 1 Unità *NAS* con storage in ***RAID*** per garantire la tolleranza ai guasti e la continuità operativa: in caso di malfunzionamento di un singolo disco, i dati rimangono integri e accessibili, riducendo drasticamente i tempi di inattività (***downtime***).
3. **Sicurezza:**
    - 3 *Security Appliance* per la gestione delle intrusioni (1 *IDS*/2 *IPS*).
4. **Infrastruttura Passiva:**
    - Cablaggio strutturato in *Cat 6a* o superiore;
    - *Armadio Rack* principale (*CED*) e piccoli rack di piano.

Progetto di Rete per la Compagnia Theta

Rete Interna Aziendale

Traccia e requisiti :

- ***Switch* per ogni piano**: Collegare i 20 computer di ciascun piano a uno *switch* dedicato;
- ***Router***: Collegare tutti gli *switch* dei vari piani a un *router* centrale;
- ***Firewall***: Posizionare il *firewall perimetrale* tra il *router* interno e la connessione a *Internet*;
- ***NAS***: Collegare il *NAS* allo *switch* del piano terra (vicino al *router*) per garantire l'accesso ai dati da parte di tutti i computer aziendali;
- ***IDS/IPS*** Implementare 3 *IDS/IPS* nel perimetro interno per monitorare il traffico di rete e prevenire intrusioni;
- **Connessione a *Internet***: Collegare il *firewall perimetrale* a *Internet*;
- **Web Server**: Posizionare il *web server* (*DVWA* di Metasploitable) nella zona demilitarizzata (*DMZ*) tra il *firewall* e la connessione a *Internet*, garantendo così un accesso sicuro dall'esterno;
- Se avete bisogno di un altro *firewall* potete comprarlo e montarlo.

Testing della Rete:

Traccia :

Per concludere il progetto, effettueremo una serie di test sulla rete implementata
I test includeranno:

1. **Verifica dei *Verbi HTTP*:** Scriveremo un programma in *Python* per inviare richieste HTTP (*GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE*) al *web server* e verificare le risposte;

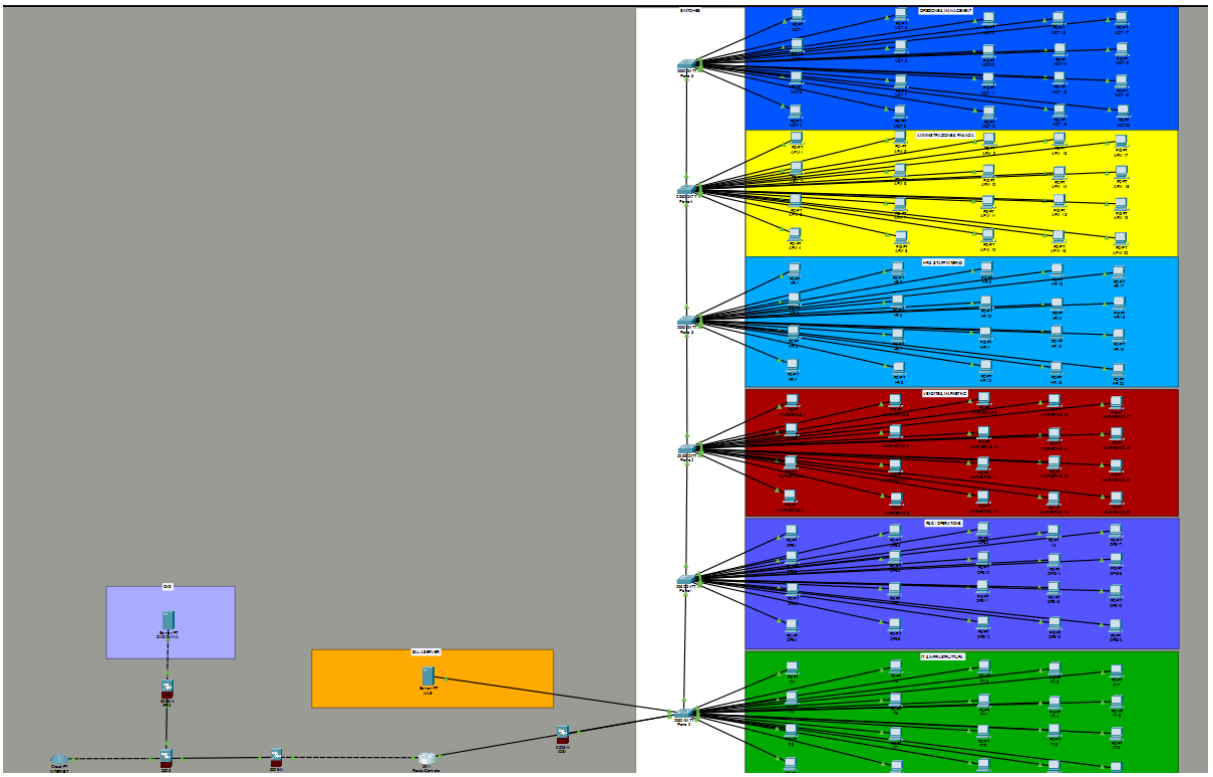
2. **Scansione delle *Porte***: Utilizzeremo un programma in *Python* per eseguire una scansione delle porte sui dispositivi di rete, verificando lo stato delle varie porte di comunicazione.

Report Finale :

Alla conclusione dei test, redigeremo un report dettagliato che include:

- **Risultati dei *Test HTTP:*** Documentazione delle risposte ricevute dal *web server* per ogni *verbo HTTP* testato;
- **Risultati della *Scansione delle Porte*:** Elenco delle porte aperte, chiuse e filtrate sui vari dispositivi, con **raccomandazioni di sicurezza**. Questo approccio garantirà che l'infrastruttura di rete della compagnia ***Theta*** sia ben progettata, sicura e pronta per operare in modo efficiente.

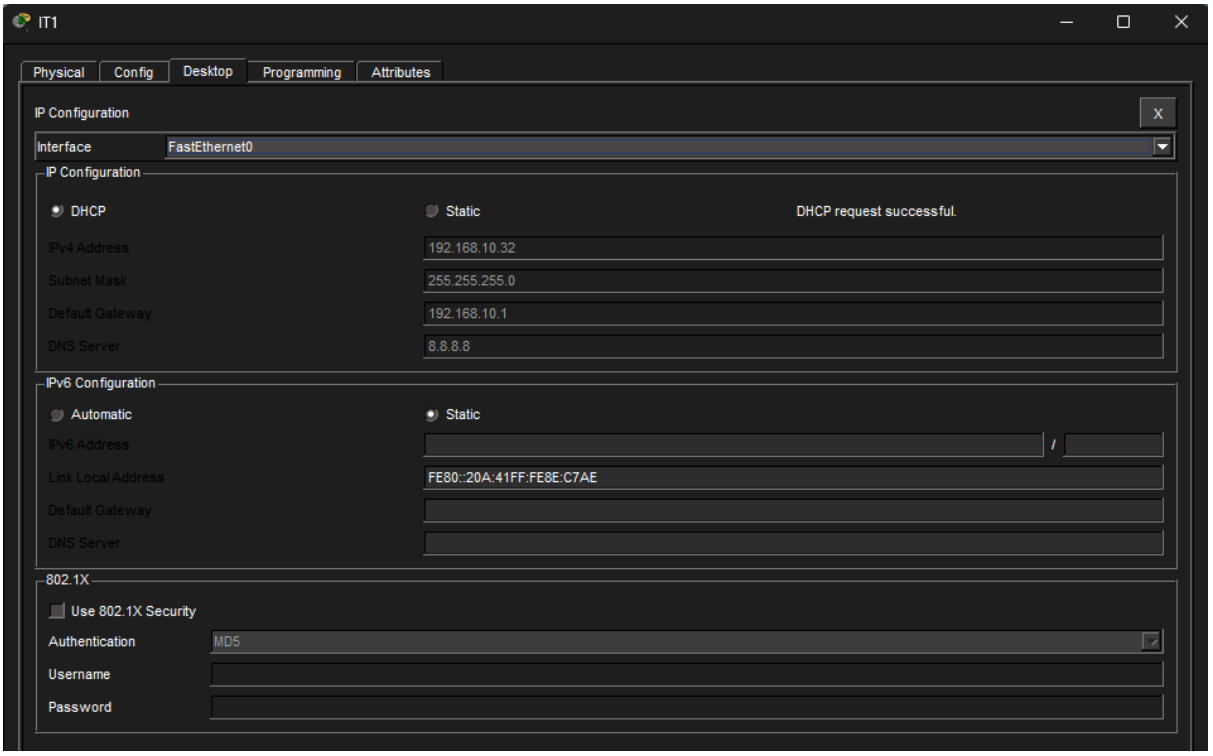
Configurazione rete Cisco Packet Tracer



(Disposizione finale su Cisco Packet Tracer)

Dopo aver disposto uno *switch* per ciascuno dei 6 piani e aver collegato 20 *computer* a ciascuno di essi, abbiamo configurato il servizio ***DHCP*** *(Dynamic Host Configuration*

Protocol) direttamente sul *router centrale* tramite *CLI (Command Line Interface)*, creando un *pool* dedicato (indirizzi IP disponibili per l'assegnazione) per ciascuna *VLAN*.



(Configurazione DHCP del dispositivo IT1 impostato su VLAN10)

In questo modo i *client* ricevono automaticamente *indirizzo IP, subnet mask e default gateway* coerenti con la *VLAN* di appartenenza.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
50   VLAN0050                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
60   VLAN0060                          active
100  VLAN100                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

(Esempio di struttura VLAN sullo Switch Piano 4)

Nella simulazione su *Packet Tracer*, il *router centrale* è stato configurato con un'interfaccia verso la rete interna (*trunk* per il *router-on-a-stick*) e un'*interfaccia* di *uplink* verso il *router-firewall*, che funge da *gateway perimetrale* verso *Internet* e *DMZ*.

Abbiamo configurato le ***VLAN*** (*Virtual Local Area Network*) nei vari switch, andando a collegare ad essi i dispositivi di ciascun piano.
L*'inter-VLAN routing* è stato implementato con architettura *router-on-a-stick*: il collegamento tra *switch* e *router centrale* è configurato come *trunk 802.1Q* e sul *router* sono state create *sub-interfacce* (una per VLAN) con *incapsulamento dot1Q.*

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      10,20,30,40,50,60,100
Gig0/2      10,20,30,40,50,60,100

Port        Vlans allowed and active in management domain
Gig0/1      10,20,30,40,50,60,100
Gig0/2      10,20,30,40,50,60,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30,40,50,60,100
Gig0/2      10,20,30,40,50,60,100

Switch#
```

(Esempio di settaggio porte dello Switch Piano 4)

Ogni *sub-interfaccia* rappresenta il *gateway* della rispettiva subnet (es. 192.168.10.1 per VLAN 10), consentendo la comunicazione controllata tra le VLAN secondo le policy di sicurezza definite.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/0.40  192.168.40.1    YES manual up                    up
GigabitEthernet0/0.50  192.168.50.1    YES manual up                    up
GigabitEthernet0/0.60  192.168.60.1    YES manual up                    up
GigabitEthernet0/0.100 192.168.100.1   YES manual up                    up
GigabitEthernet0/1     10.0.0.1        YES manual down                  down
GigabitEthernet0/2     unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

(Divisione per VLAN all'interno del Router)

Per semplificare la gestione e rendere immediata l'identificazione del *segmento di rete*, è stato adottato lo schema di indirizzamento 192.168.<*VLAN*>.0/24 per le *VLAN* interne e 192.168.100.0/24 per l'area server (*NAS)* e 192.168.200.0/24 per la *DMZ* (DVWA).

Di seguito il prospetto:

VLAN	**Subnet**	**Gateway**	**Reparto/Funzione**	**DHCP Range**
10	192.168.10.0/24	192.168.10.1	IT / Infrastruttura	192.168.10.20 - 192.168.10.254

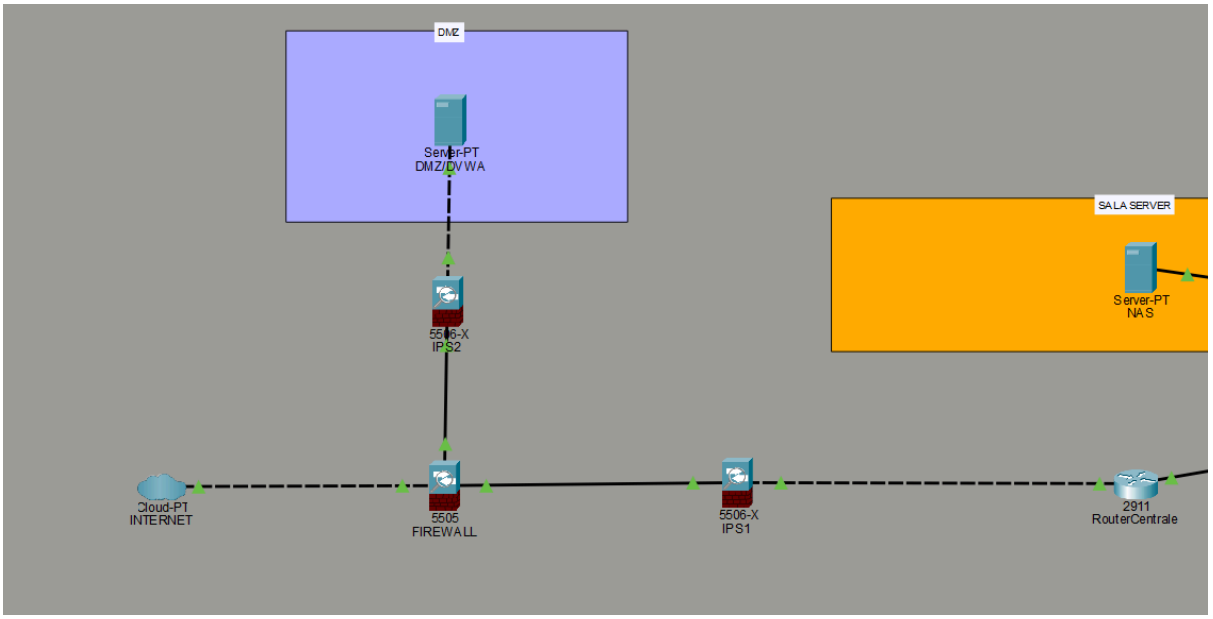
20	192.168.20.0/24	192.168.20.1	R&D / Operations	192.168.20.20 - 192.168.20.254
30	192.168.30.0/24	192.168.30.1	Vendite / Marketing	192.168.30.20 - 192.168.30.254
40	192.168.40.0/24	192.168.40.1	HR / Staff Interno	192.168.40.20 - 192.168.40.254
50	192.168.50.0/24	192.168.50.1	Amministrazione / Finanza	192.168.50.20 - 192.168.50.254
60	192.168.60.0/24	192.168.60.1	Direzione / Management	192.168.60.20 - 192.168.60.254
100	192.168.100.0/24	192.168.100.1	Server / NAS	Statico (192.168.100.10)
200	192.168.200.0/24	192.168.200.1	DMZ / DVWA	Statico (192.168.200.20)

Le *sub-interfacce* del *router* ospitano ciascuna il *gateway* della propria *VLAN* e le regole di routing sono configurate per controllare il traffico *inter-VLAN* in base alle policy di sicurezza.

Le ***VLAN*** ci permettono di suddividere una ***rete fisica*** in più ***reti logiche*** separate e indipendenti. Le *VLAN* offrono una moltitudine di vantaggi cruciali per la gestione e le prestazioni delle reti aziendali:

- ➔ **Isolamento del traffico**;
- ➔ **Riduzione del rischio**;
- ➔ **Migliori Prestazioni** tra cui la riduzione del dominio di broadcast, infatti segmentando la rete in *VLAN* più piccole si riduce notevolmente la dimensione dei domini di broadcast;
- ➔ **Organizzazione logica**;
- ➔ **Risparmio dei costi,** in quanto consente di utilizzare un **numero inferiore** di *switch* e *router* fisici per ottenere la separazione logica desiderata;
- ➔ **Gestione prioritaria del Traffico**.

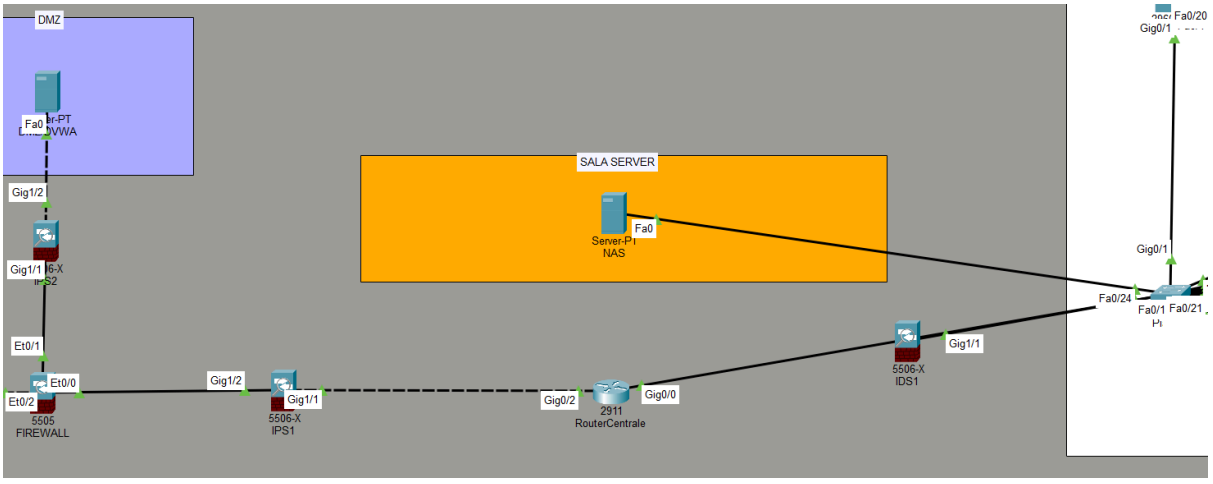
Come da traccia è richiesto il posizionamento strategico del *firewall perimetrale*, il cui compito è di **proteggere** la *connessione interna* dell'azienda monitorando tutto il *traffico dati* in entrata e in uscita, decidendo cosa può passare e cosa deve essere bloccato.



(Posizionamento del Firewall)

Come da immagine, il *router-firewall* perimetrale è posizionato tra il *router centrale* (routing interno) e la *connettività Internet (WAN)*. In aggiunta, ospita un'interfaccia dedicata alla *DMZ* per filtrare il traffico diretto al *web server* esposto.

Il *NAS* (*Network Attached Storage*) è stato inserito nella **VLAN 100** (subnet 192.168.100.0/24), dedicata ai server aziendali, e collegato all'infrastruttura di rete del **piano terra,** in prossimità del *router centrale*. In questo modo è raggiungibile dalle *VLAN* autorizzate secondo le *policy* di *inter-VLAN routing*, ma il suo ***accesso rimane controllato e segmentato***. Tutte le postazioni aziendali autorizzate possono accedere al NAS tramite il gateway della propria VLAN, garantendo ***archiviazione centralizzata, backup RAID e condivisione di file aziendali*** in modo sicuro e ordinato. Per configurare il *NAS* abbiamo bisogno sempre del *CLI* del dispositivo che ci consente di configurare tramite terminale quello che desideriamo implementare.
Senza questo collegamento il ***NAS*** sarebbe **isolato** e **non accessibile** dalla rete.



(Posizionamento del NAS)

Altra fondamentale richiesta è la posizione strategica degli ***IDS/IPS.***
Questi ci permettono di applicare una **seconda barriera difensiva** alla rete dell'azienda.
Prima di mostrare la loro posizione, è meglio specificare cosa fanno singolarmente:

- ***IDS (Intrusion Detection System):*** Rileva e segnala un'attività anomala nella rete attraverso un ***alert*** agli amministratori, è posizionato **in parallelo** e non crea rallentamenti alla rete, ma analizza il traffico con i suoi tempi;
- ***IPS(Intrusion Prevent System):*** Rileva e agisce direttamente **bloccando** un'attività anomala, è posizionato **in linea** e deve essere potente abbastanza da evitare rallentamenti al traffico di rete.

Quindi:

- ***IDS* rileva e segnala**;
- ***IPS* rileva e agisce**.

Nel progetto sono stati implementati **3 sistemi *IDS/IPS*** in posizioni strategiche per fornire **copertura multilivello**:

- **IPS1** (Perimetro ↔ *LAN* / verso router centrale): posizionato sul collegamento tra firewall e router centrale, controlla e previene attività anomale **dirette alla rete interna** e/o tentativi di attraversamento verso le VLAN aziendali;
- **IPS2** (Perimetro ↔ *DMZ*): posizionato tra firewall e rete DMZ (*DVWA*), analizza e blocca traffico potenzialmente malevolo diretto ai servizi esposti in DMZ (es. *scansioni, exploit, richieste anomale*);
- **IDS1** (Monitoraggio *LAN*/*Server VLAN*): posizionato per monitorare il traffico relativo all'area servizi/server (inclusa *VLAN 100* dove risiede il *NAS*), generando **alert** su accessi anomali ed eventuali pattern di esfiltrazione.

Come da traccia, il servizio web dell'azienda Theta è stato simulato tramite la macchina *Metasploitable*, utilizzando *DVWA* come applicazione target per le attività di test.
Il web server è stato posizionato in una zona demilitarizzata (DMZ), realizzata come VLAN dedicata (VLAN 200 - subnet 192.168.200.0/24), separata logicamente dalla LAN interna e dalla VLAN dei server (NAS) riducendo drasticamente l'esposizione della rete interna in caso di compromissione.
Il traffico verso la DMZ viene gestito dal firewall perimetrale: l'accesso alla DVWA è consentito solo per i servizi necessari ai test, mentre ogni comunicazione dalla DMZ verso la LAN e verso la VLAN 100 (NAS) è bloccata per impostazione predefinita, limitando il movimento laterale.

Configurazione Firewall

Regole Firewall:

Router-Firewall centrale:

Collegato a *LAN* (*VLAN* 10–60) e *NAS* (*VLAN* 100). Gestisce soprattutto l'accesso al *NAS* e *l'egress* **controllato** verso *l'uplink*

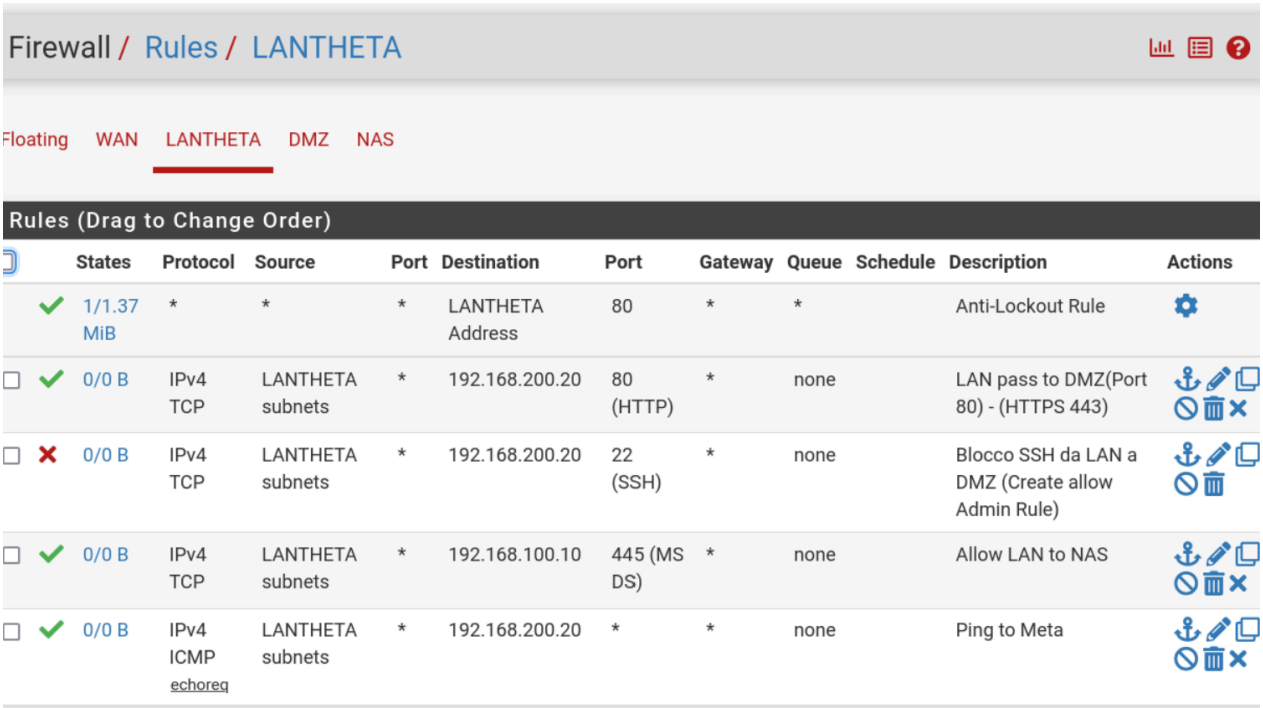
ID	Interface	Source	Destination	Protocollo/ Porta	Azione	Scopo/Note
C-01	LAN (VLAN 10-60)	INSIDE_NET (VLAN 10-60)	192.168.100.10	TCP/445 (SMB)	ALLOW	Accesso al NAS solo dai segmenti autorizzati.
C-02	LAN (VLAN 10-60)	INSIDE_NET (VLAN 10-60)	192.168.100.10	ICMP	ALLOW (opz.)	Ping verso NAS per troubleshooting (lab).
C-03	LAN (VLAN 10-60)	INSIDE_NET (VLAN 10-60)	UPLINK_NET (verso firewall perimetrale)	TCP/80,443 + DNS	ALLOW (hardening)	Uscita Internet controllata: permettere solo servizi necessari.
C-04	NAS (VLAN 100)	192.168.100.0/24	INSIDE_NET (VLAN 10-60)	ANY	BLOCK (default)	NAS non deve iniziare connessioni verso VLAN utenti.
C-05	NAS (VLAN 100)	192.168.100.0/24	IP admin all'interno di VLAN	TCP/22	ALLOW (opz.)	Gestione NAS solo da IP admin (se serve amministrarlo via SSH).
C-06	LAN (VLAN 10-60)	INSIDE_NET (VLAN 10-60)	192.168.100.0/24	ANY	BLOCK (default)	Blocco di tutto ciò che non è esplicitamente permesso verso NAS.

C-99	ANY	ANY	ANY	ANY	BLOCK	Regola finale/implicita: tutto il resto negato.

Router-firewall perimetrale:
Filtra traffico tra DMZ e rete interna (uplink verso router-firewall centrale) e tra Internet e DMZ

ID	Interface	Source	Destination	Protocollo /Porta	Azione	Scopo/Note
P-01	WAN	ANY	192.168.200.20	TCP/80	ALLOW (opz.)	Pubblicazione server esposto su Internet; opzionale.
P-02	WAN	ANY	INSIDE_NET (LAN+NAS: VLAN 10-60+100)	ANY	BLOCK	Blocco inbound verso reti interne **LAN e NAS**.
P-03	INSIDE/ uplink	INSIDE_NET (VLAN 10-60)	192.168.200.20	TCP/80	ALLOW	Accesso dalla LAN al server esposto per test HTTP.
P-04	INSIDE/ uplink	INSIDE_NET (VLAN 10-60) meglio: IP admin	192.168.200.20	TCP/22	ALLOW	**SSH LAN → DMZ** (per hardening: meglio restringere a IP admin).
P-05	INSIDE	INSIDE_NET (VLAN 10-60)	192.168.200.20	ICMP	ALLOW	Ping/diagnostica **LAN → DMZ** per troubleshooting (come da test di connettività).
P-06	DMZ	192.168.200.0 /24	INSIDE_NET (VLAN 10-60)	ANY	BLOCK	Isolamento **DMZ → rete interna** (anti lateral movement).

P-07	DMZ	192.168.200.0 /24	192.168.100.0/ 24	ANY	BLOCK	Isolamento **DMZ → NAS** (protezione dati).
P-08	DMZ	192.168.200.0 /24	WAN	ANY	ALLOW (opz.)	Egress DMZ verso Internet **solo se necessario** (per update mirati); altrimenti BLOCK.
P-99	ANY	ANY	ANY	ANY	BLOCK	Regola finale/implicita: tutto il resto negato.



Nel laboratorio virtualizzato, pfSense implementa sia il ruolo di router-firewall perimetrale sia quello di router-firewall centrale, tramite interfacce dedicate e rule-set separati (tabelle C-xx e P-xx)

(Ipv4 TCP) Pass LANTHETA subnets to DMZ 192.168.200.20 (Port 80) (Consigliato utilizzare HTTPS 443):
Abbiamo configurato una regola che permette alla *LAN* (dispositivo in LAN rappresentato dalla Kali) di raggiungere il web server DVWA ospitato sul server Theta (rappresentato dalla *Metasploitable)* in *DMZ* tramite HTTP (TCP/80). Nella regola la destinazione corrisponde all'IP dell'host Metasploitable/DVWA in DMZ (impostato come 'Address or Alias'), così da abilitare i test sui metodi HTTP richiesti dal progetto.

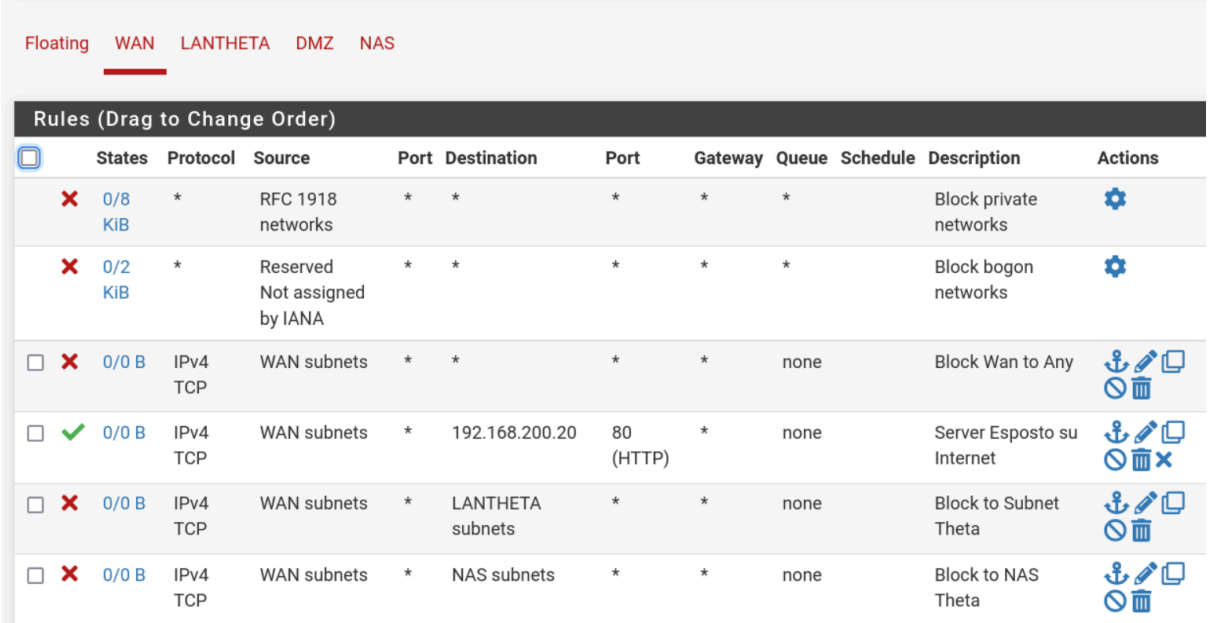
(IPv4 TCP) Blocco SSH (Port 22) to DMZ:
È stata implementata una regola di blocco specifica per il traffico **TCP sulla porta 22 (SSH Secure Shell)** verso l'indirizzo IP del server in DMZ (**192.168.20.20**). Questa misura di sicurezza impedisce ai dipendenti della LAN di tentare l'accesso amministrativo al terminale del server, riducendo drasticamente la superficie di attacco interna.

(IPv4 TCP) Pass Lantheta subnets to NAS (Port 445):
Abbiamo implementato questa regola per consentire agli *Host* di raggiungere il **NAS** potendo condividere file direttamente mediante la **porta 445 SMB (Server Message Block) (MS DS Microsoft Directory Services)**

IPV4 ICMP Ping to Meta (echorequest):
Abbiamo creato una regola sulla *LAN* che consente alla macchina *Kali* (client in LAN) di inviare richieste *ICMP Echo Request* verso la macchina *Metasploitable* (host in DMZ/OPT1). Questa regola permette di verificare la connettività di rete (routing e raggiungibilità) tra i due segmenti prima di eseguire i test applicativi richiesti dal progetto.

Echo Request:
è un messaggio ***ICMP*** usato per verificare se un *host* è raggiungibile. È il pacchetto 'di andata' del comando *ping*; la risposta dell'host è l'*Echo Reply*, gestita automaticamente perché il *firewall* lavora in modalità *stateful*.
La modalità Stateful indica che il firewall mantiene una tabella di tutte le connessioni attive ricordandosi così di tutte le "Conversazioni" avvenute e così facendo abbiamo una maggiore sicurezza qualora ci siano dei tentativi di accesso non desiderati

IPV4 TCP:
abbiamo inserito una regola temporanea che consente il traffico *TCP* in uscita dalla rete *LAN* verso altre destinazioni, per garantire operatività e facilità di troubleshooting durante la fase di laboratorio.
In ottica di hardening, questa regola verrà sostituita da permessi più specifici (ad esempio LAN → WAN solo per i servizi necessari all'uscita Internet e LAN → DMZ limitato solo alle porte richieste).



Floating | WAN | LANTHETA | DMZ | NAS

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/8 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0/2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
0/0 B	IPv4 TCP	WAN subnets	*	*	*	*	none		Block Wan to Any	
0/0 B	IPv4 TCP	WAN subnets	*	192.168.200.20	80 (HTTP)	*	none		Server Esposto su Internet	
0/0 B	IPv4 TCP	WAN subnets	*	LANTHETA subnets	*	*	none		Block to Subnet Theta	
0/0 B	IPv4 TCP	WAN subnets	*	NAS subnets	*	*	none		Block to NAS Theta	

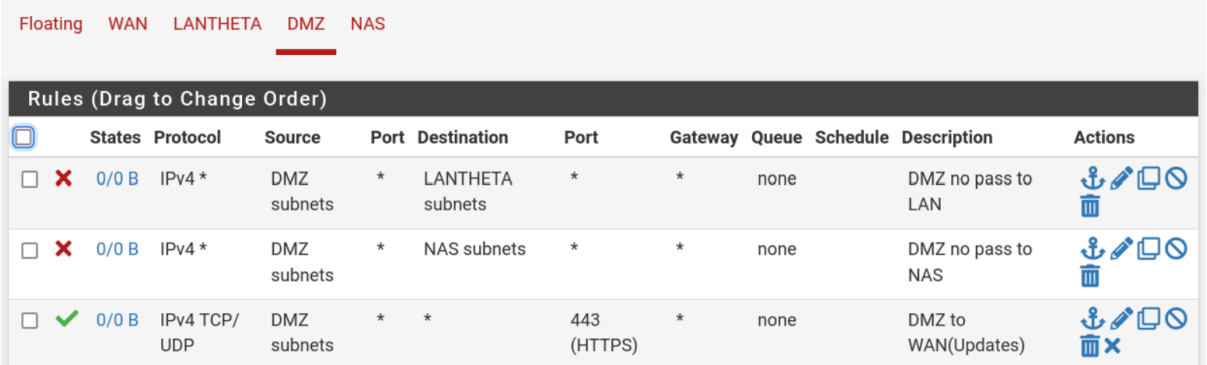
Nella sezione WAN (simulando la WAN della nostra configurazione su Cisco Packet Tracer) del firewall abbiamo introdotto le seguenti regole:

(IPv4 TCP) - Block WAN to Any (Default Deny):
è una regola di sicurezza che impedisce al traffico originato sulla WAN di accedere a qualsiasi altra risorsa interna o esterna non specificamente autorizzata

(IPv4 TCP) - Server Esposto su Internet (Port Forwarding):
Regola di sicurezza che permette agli utenti esterni su Internet di raggiungere un server web interno (es. un sito web o un'interfaccia di gestione) situato all'indirizzo `192.168.200.20`.

(IPv4 TCP) - Block to Subnet Theta (Sottorete):
Impedisce specificamente al traffico proveniente dalla WAN di raggiungere la sottorete denominata "LAN THETA". È una misura di **segmentazione della rete** per proteggere un'area specifica del sistema.

(IPv4 TCP) - Block to NAS Theta:
questa regola isola il **NAS** (Network Attached Storage) dalle connessioni esterne. Assicura che i dati archiviati nel server di storage non siano accessibili direttamente da Internet.



Floating WAN LANTHETA DMZ NAS

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/0 B	IPv4 *	DMZ subnets	*	LANTHETA subnets	*	*	none		DMZ no pass to LAN	
✗	0/0 B	IPv4 *	DMZ subnets	*	NAS subnets	*	*	none		DMZ no pass to NAS	
✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	*	443 (HTTPS)	*	none		DMZ to WAN(Updates)	

Sezione **DMZ**: Isolamento del Server e Contenimento delle Minacce *(Nella DMZ è riposto il nostro server WEB che nella nostra simulazione è la Metasploitable)*

La zona **DMZ** (***Demilitarized Zone***) rappresenta il punto più critico della nostra infrastruttura Theta che ospita in questo il server web “Meta”(192.168.200.20) che è direttamente esposto alla rete pubblica (**WAN**)

Analisi delle Regole di Sicurezza che abbiamo introdotto per rendere più sicura la nostra rete:

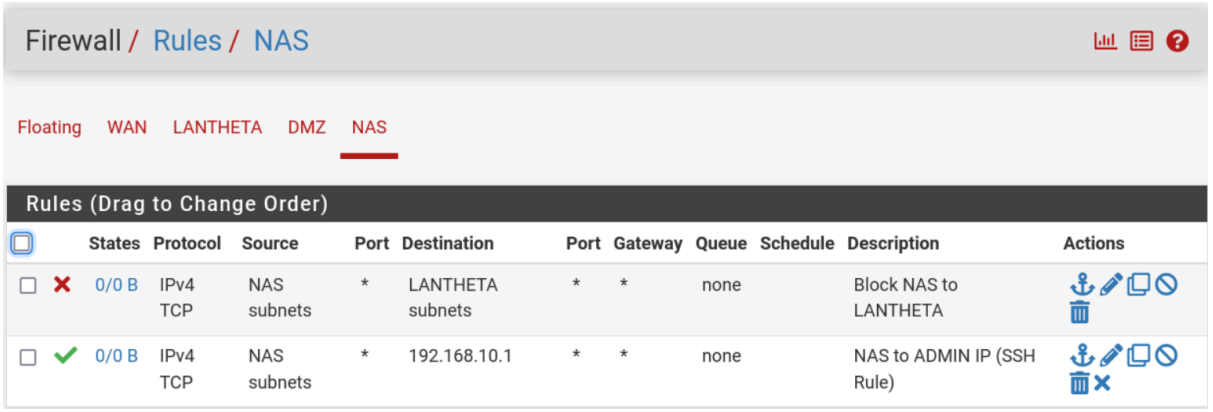
(IPv4) - DMZ no pass to LAN: Questa regola di blocco (X rossa) è la colonna portante della sicurezza aziendale. Impedisce al server, nel caso venisse compromesso, di avviare qualsiasi tipo di connessione verso la rete dei dipendenti (**LANTHETA**), proteggendo i 120 host interni.

(IPv4) - DMZ no pass to NAS: Analogamente, viene bloccato ogni traffico originato dal server verso lo storage aziendale (**NAS subnets**). Questa configurazione assicura che i database e i documenti sensibili contenuti nel NAS rimangano inaccessibili anche a seguito di un'intrusione riuscita sul sito web.

(IPv4 TCP/UDP) - DMZ to WAN (Updates): È stata inserita una regola di **Pass** specifica per il traffico sulla porta **443 (HTTPS)** verso l'esterno. Questo permette al server di connettersi ai repository ufficiali esclusivamente per scaricare gli aggiornamenti di sicurezza necessari alla manutenzione del sistema.

Nella sezione (**DMZ/DVWA**) abbiamo configurato regole dedicate a mantenere la **DMZ** isolata dalla rete interna. In particolare, abbiamo bloccato il traffico dalla **DMZ** verso la **LAN** (e verso la VLAN del NAS) per ridurre il rischio di movimento laterale in caso di compromissione del server esposto. L’eventuale traffico in uscita dalla DMZ verso Internet viene consentito solo se necessario e in modo mirato.

UDP(user Datagram Protocol): Protocollo “Senza Connessione"
A differenza del protocollo TCP prima citato, quest’ultimo è un protocollo ***connectionless***: non stabilisce una connessione e non garantisce consegna/ordine dei pacchetti come fa TCP. Per questo è spesso più leggero e veloce, ma meno affidabile in termini di controllo della trasmissione.

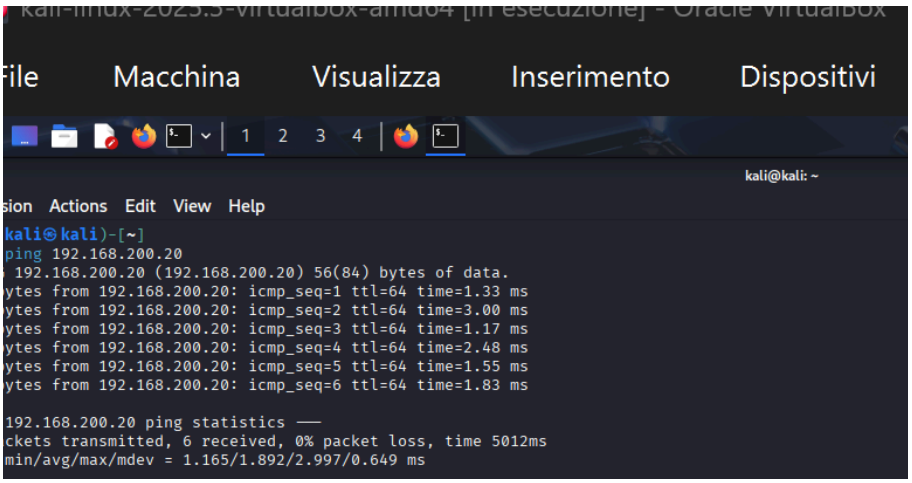


Nell’interfaccia del NAS abbiamo invece introdotto:

(IPv4 TCP) - Blocco dalla NAS SUBNETS to LANTHETA:

Questa regola impedisce a qualsiasi dispositivo situato nella rete NAS di iniziare una comunicazione verso la rete LAN THETA.
Serve a isolare i dispositivi. Se il NAS dovesse essere compromesso, un eventuale attaccante non potrebbe usare il NAS come "ponte" per attaccare i computer nella rete LANTHETA.

(IPv4 TCP) - NAS to ADMIN IP (SSH Rule):
Questa è un'eccezione specifica che permette al traffico proveniente dal NAS di raggiungere l'indirizzo IP dell'amministratore (192.168.10.1).



Abbiamo effettuato un test di connettività tramite ping dalla Kali (LAN THETA) verso Metasploitable (DMZ/OPT1). Il test è risultato positivo perché, sulla LAN, è stata configurata una regola ICMP (Echo Request) che consente esplicitamente questo traffico; il firewall, essendo stateful, permette automaticamente anche il traffico di risposta (Echo Reply).
Le configurazioni delle regole e i testi pervenuti sono ovviamente simulati dalle nostre macchine virtuali in possesso.
Poiché Cisco Packet Tracer non consente di eseguire verifiche reali su pfSense e sulle VM, la fase di testing è stata riprodotta in un ambiente virtualizzato separato utilizzando pfSense, Kali e Metasploitable, in modo da validare concretamente regole firewall, raggiungibilità e accesso al servizio DVWA.

Testing della Rete

Programmi Python

Come seconda parte del progetto,viene richiesta l'implementazione di:

- Programma in python per inviare richieste verbi HTTP(GET, POST, PUT, DELETE) al web server e verificarne le risposte, si è deciso di includere anche verbi extra.
  Lo scopo dello script è testare l'interazione tra un client (il nostro tool su *python*) e un *server*.
- Programma in python per la scansione delle porte su un host target, individuando porte aperte e chiuse, si è deciso di aggiungere anche l'opzione filtered.
- Programma in python per l'intercettazione dei pacchetti in transito.

Tool 1: HTTP Methods Verifier

È stato sviluppato uno *script Python* che utilizza la libreria *requests* per inviare richieste con tutti i metodi *HTTP* supportati (*GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE*) verso il server DVWA in DMZ. Lo script accetta in *input* un *URL* con un path specifico (es. /phpmyadmin), quindi restituisce l'*elenco dei metodi consentiti* sulla risorsa, con i relativi *codici di risposta HTTP*. Questo permette di identificare quali metodi potrebbero esporre la superficie di attacco.

Tool 2: Port Scanner

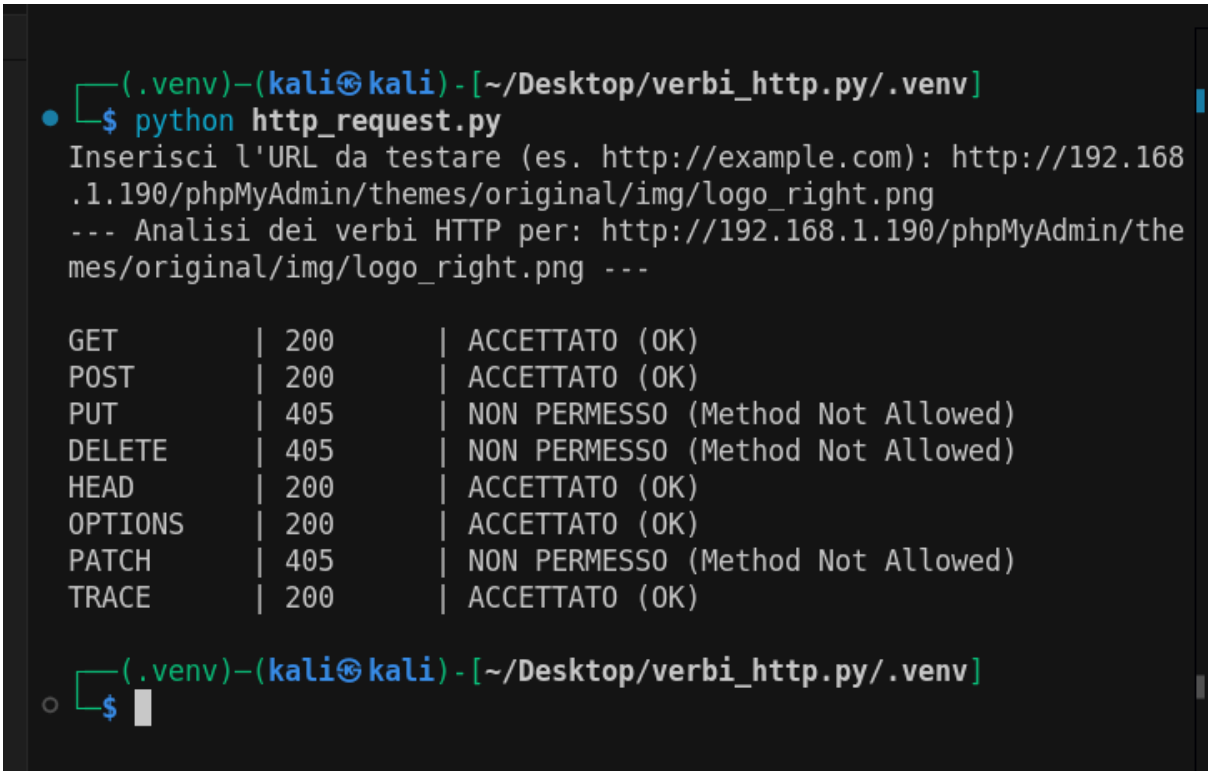
È stato realizzato un port scanner in *Python* che utilizza *socket e threading* per scansionare un determinato range di porte su un host target (indirizzo IP e intervallo porte in input). Lo script ritorna un elenco dettagliato delle porte in stato open/closed e dei servizi identificati.

Tool 3: Socket Network Capture (Extra)

Come richiesta bonus, è stato sviluppato un programma che cattura il socket di rete e analizza i pacchetti in transito per scopi di monitoraggio e troubleshooting.

Conclusione dei Test:

Risultati dei test HTTP:



Durante i test applicativi sul web server in DMZ (simulato dalla DVWA), lo script per la verifica dei verbi HTTP ha evidenziato la presenza di metodi HTTP che, in un contesto di produzione, è generalmente opportuno disabilitare o limitare perché possono aumentare la superficie d'attacco o fornire informazioni utili a un attaccante. Nel nostro caso si tratta di un ambiente didattico e di test, tuttavia i risultati vengono riportati come raccomandazioni di hardening per un'eventuale messa in esercizio reale del servizio.

Vulnerabilità Critica: Metodo HTTP TRACE
In ambiente di test, il web server dell'infrastruttura espone il metodo diagnostico *TRACE*, aumentando significativamente il rischio di attacchi di *Cross-Site Tracing (XST)* in combinazione con il *Cross-Site Scripting (XSS)*. Normalmente, il flag "*HttpOnly*" impedisce a *JavaScript* di leggere i cookie di sessione tramite *document.cookie*.
Tuttavia, se ***TRACE*** è abilitato, un attaccante può aggirare questa protezione tramite alcuni step:

- **Iniezione XSS**: L'attaccante inietta uno *script* maligno che sfrutta la vulnerabilità *Cross Site Scripting* presente nell'applicazione.
- **Loop-back diagnostico**: Lo script invia una richiesta ***TRACE*** al server; questo metodo effettua un "echo" dei dati ricevuti, riflettendo nel corpo della risposta l'intera richiesta, *header* inclusi.

- **Esfiltrazione dati**: Poiché la risposta del *server* contiene ora i *cookie* (anche quelli *HttpOnly*) come semplice testo nel *body*, lo *script* può leggerli in chiaro, permettendo il *session hijacking*.
- **Aggiramento dei blocchi**: *TRACE* trasforma gli *header* di trasporto in dati leggibili dallo *script* malevolo, annullando l'efficacia delle restrizioni di sicurezza del *browser*.

Soluzione e Mitigazione:
- Disabilitare **sempre** i metodi *TRACE* (e *TRACK,* se presente) sul web server/reverse proxy. È fondamentale consentire solo i metodi *HTTP* strettamente necessari e applicare un rigoroso *hardening XSS* lato applicativo (con validazione/encoding dell'input/output).

Rischio Informativo: Esposizione HTTP OPTIONS

La seconda vulnerabilità riguarda l'uso del metodo *HTTP OPTIONS*, che può causare una *Information Disclosure* dei *metodi/verbs* consentiti dal *server*.

- **Mappatura dell'attacco**: Il server risponde indicando i metodi abilitati, facilitando la ricognizione e permettendo all'attaccante di individuare subito endpoint sensibili.
- **Esposizione di metodi critici**: Se metodi come *PUT* o *DELETE* fossero attivi per errore, *OPTIONS* ne rivelerebbe immediatamente la disponibilità, guidando l'attaccante verso azioni distruttive.
- **Gestione CORS**: Sebbene necessario per le richieste di "*preflight*" in scenari *Cross-Origin*, se non configurato correttamente il metodo *OPTIONS* rischia di esporre configurazioni troppo permissive.

Soluzione: Gestire *OPTIONS* in modo intenzionale, abilitandolo solo sugli endpoint che ne hanno strettamente bisogno (es. *API cross-origin*) e limitando i metodi ammessi a una whitelist minima e necessaria.

Risultati della Scansione Porte:

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/verbi_http.py/.venv]
└─$ python port_scanner.py
IP da scansionare: 192.168.1.190
Range porte (es. 20-100) o porta singola (es 80): 0-1023
Scannerizzo 192.168.1.190 da 0 a 1023 (timeout 1s)...
Output salvato in: scan_results.json
Porte aperte trovate: [21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514]
```

La scansione delle porte sul target in DMZ (Metasploitable/DVWA) evidenzia numerosi servizi esposti; trattandosi di una VM volutamente vulnerabile, l'elevata superficie d'attacco è preventivata e viene sfruttata per validare il funzionamento dello scanner.

Nel contesto di una rete reale, quale quella della Theta, l'obiettivo è quello di ridurre i servizi esposti al minimo necessario e filtrare/segmentare i restanti tramite regole firewall e hardening dei servizi.
Di seguito una lista delle possibili vulnerabilità e come mitigarle:

1. Berkeley r-commands / Legacy Unix

Porte: TCP/512 (exec/rexec),TCP/513 (login/rlogin), TCP/514 (shell/rsh)
Livello di Rischio: ALTO/CRITICO (servizi legacy, insicuri)

Questi servizi si basano,storicamente, su meccanismi di "trust" host-based (es. configurazioni tipo .rhosts) e non garantiscono la riservatezza del traffico. In caso di configurazioni errate del file .rhosts, possono essere facilitati accessi non autorizzati e attività di sniffing e spoofing/impersonificazione (falsificazione del proprio IP per sembrare un dispositivo fidato).

Mitigazione:

- disabilitare i remote services legacy e sostituirli con SSH,
- bloccare le porte a livello firewall

---

2. Protocolli in Chiaro (FTP/Telnet/HTTP)

Porte: TCP/21 (FTP), TCP/23 (Telnet), TCP/80 (HTTP)
Livello di Rischio: MEDIO/ALTO (assenza di cifratura e possibile furto di credenziali/sessione)

FTP e Telnet non cifrano credenziali e contenuto della sessione, quindi su reti non completamente fidate un attaccante può intercettare il traffico (sniffing) e recuperare username/password.

FTP può essere esposto a rischi aggiuntivi in caso di configurazioni deboli (es. login anonimi - senza password - o abuso FTP bounce - usare il server per scansionare altre macchine).

HTTP (porta 80) non cifra i dati applicativi, se su HTTP vengono gestite credenziali o sessioni, aumenta il rischio di intercettazione o manomissione del traffico, inoltre espone la superficie d'attacco applicativa (es. possibili tentativi di XSS/SQLi su applicazioni vulnerabili).

Mitigazione:

- Disabilitare Telnet e sostituirlo con SSH;
- Disabilitare FTP o sostituirlo con protocolli cifrati (SFTP/FTPS) e limitare l'accesso tramite segmentazione e firewall;
- Preferire HTTPS (TLS) per autenticazioni e pannelli di login, esporre HTTP solo se necessario e comunque protetto da policy hardening;

- Applicare regole firewall “least privilege” consentendo solo i servizi necessari e solo dalle reti autorizzate.

---

3. SMB/NetBIOS

Porte: TCP/139 (NetBIOS Session Service), TCP/445 (SMB)
Livello di Rischio: ALTO (esposizione servizi di file-sharing e possibili vettori di enumerazione/exploit)

Queste porte sono legate a servizi di condivisione file e stampanti (Samba su Linux o SMB su Windows): se esposte a segmenti non autorizzati, possono facilitare attività di enumerazione (utenti, share, risorse) che forniscono informazioni utili per attacchi successivi e aumentando significativamente la superficie d’attacco.
In scenari reali, componenti SMB obsoleti o non patchati (in particolare implementazioni legacy come SMBv1) possono risultare vulnerabili ad attacchi noti, per questo motivo SMB va limitato e segmentato, soprattutto in presenza di asset critici come un NAS.
In particolare la porta 445 può essere associata a vulnerabilità sfruttabili da remoto in presenza di implementazioni vulnerabili (es. casi storici come EternalBlue, citato in relazione a campagne come WannaCry).

Mitigazione:

- Consentire SMB solo dai segmenti autorizzati (es. VLAN utenti verso VLAN NAS) e bloccarlo da/verso DMZ e WAN;
- Disabilitare componenti legacy e mantenere patching e hardening del servizio;
- Applicare il principio del minimo privilegio su share e permessi (no anonymous/guest, ACL coerenti);
- Monitorare accessi e tentativi anomali (log + IDS/IPS dove previsto).

---

4. Porte di Infrastruttura (SMTP/DNS/RCPbind)

Porte: TCP/25 (SMTP), TCP/53 (DNS), TCP/111 (RPCbind/portmapper)
Livello di Rischio: MEDIO/ALTO (servizi infrastrutturali; se osposti o mal configurati aumentano abuso di servizio e information disclosure)

Queste porte sono associate a servizi di infrastruttura(posta, risoluzione nomi/DNS e servizi RPC). Se esposte a segmenti non autorizzati possono fornire informazioni utili per la ricognizione e facilitare attacchi successivi (enumerazione, abuso di servizio, ampliamento della superficie d’attacco).

TCP/25 (SMTP): configurazioni errate possono trasformare il server di posta in un *Open Relay* permettendo a terzi di inviare grandi volumi di email tramite l’infrastruttura (spam/abuso reputazionale). Inoltre, l’abilitazione di comandi come VRFY/EXPN può facilitare l’enumerazione di utenti/indirizzi validi.

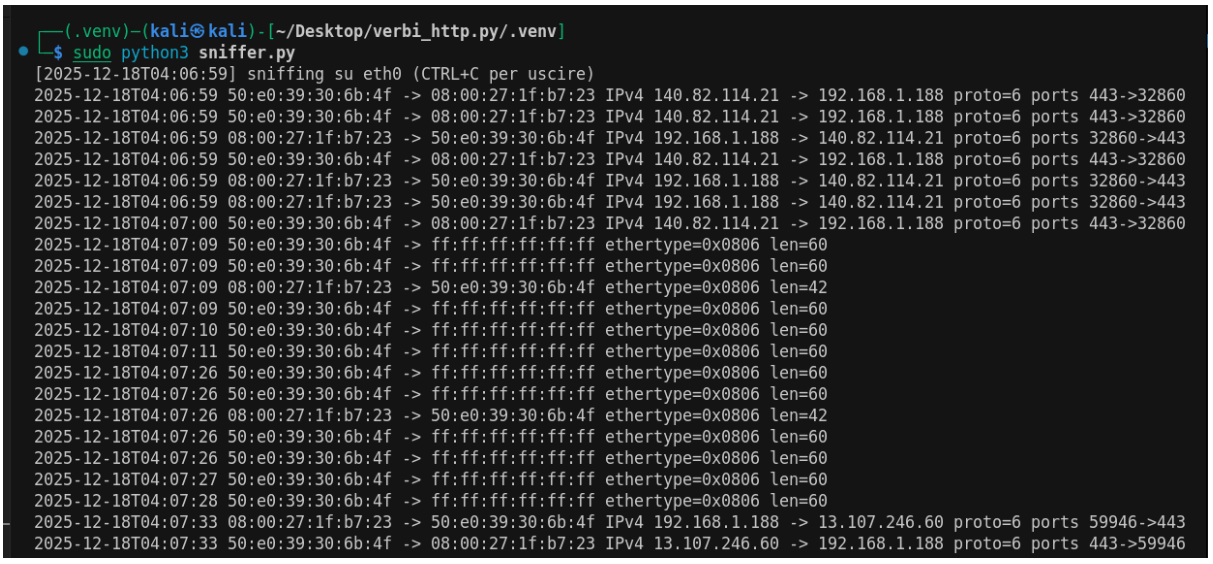
TCP/53 (DNS): se il DNS consente trasferimenti di zona non autorizzati (AXFR/zone transfer), un attaccante può ottenere un elenco di host e sottodomini, migliorando la mappatura dell'infrastruttura e la precisione degli attacchi;.

TCP/111 (RPCbind/Portmapper): espone informazioni sui servizi RPC attivi e sulle relative porte (es. servizi legati a NFS), facilitando l'identificazione di ulteriori servizi e bersagli.

Mitigazione:

- Esporre SMTP/DNS/RCPbind solo dove necessario e solo verso sorgenti autorizzate (segmentazione + firewall)
- SMTP: prevenire open relay e disabilitare/limitare VRFY/EXPN se non necessari, applicare controlli anti abuso (rate-limit, policy di autenticazione dove prevista)
- DNS: consentire trasferimenti di zona (AXFR) solo tra nameserver autorizzati (whitelist IP/policy dedicate)
- RPCbind: disabilitare servizi RPC non necessari e bloccare la porta 111 da reti non autorizzate, lasciandola accessibile solo ai client strettamente richiesti (eventuali NFS interni)

Risultati della scansione del socket di rete:



Risultati della cattura traffico (Socket Network Capture):

Durante la fase di test in ambiente virtualizzato, è stato eseguito lo sniffer sviluppato dal team su macchina Kali, con cattura in tempo reale del traffico sull'interfaccia eth0 e stampa a console dei principali metadati (timestamp, MAC sorgente/destinazione, tipo frame, IP e porte TCP/UDP quando presenti).
Nel campione osservato si rileva traffico IPv4 di tipo TCP riconducibile a sessioni HTTPS (porta 443) tra l'host in LAN e indirizzi esterni, coerente con le attività di connettività/operatività svolte nel laboratorio e con l'egress consentito durante la fase di troubleshooting.
Sono inoltre visibili frame broadcast con ethertype 0x0806 (ARP), compatibili con la normale

risoluzione IP→MAC e quindi attesi in una LAN. In questo contesto, la cattura non evidenzia pattern anomali “eclatanti” (es. flood evidente), ma soprattutto viene utilizzata come verifica di coerenza con le policy di segmentazione: un comportamento anomalo, nel nostro scenario, sarebbe stato osservare traffico in uscita dalla DMZ verso la LAN o verso la VLAN del NAS (movimento laterale), che dovrebbe risultare bloccato per impostazione e regole dedicate. Lo sniffer permette quindi di supportare il troubleshooting e la validazione delle regole firewall, evidenziando rapidamente se compaiono flussi non previsti tra i segmenti (LAN/DMZ/NAS) durante i test.

Preventivo - Theta

Immagine della tabella generale riassuntiva del preventivo che andremo a proporre all’azienda Theta

Categoria di Costo	Costo (€)	Commenti	Extra
Hardware & Periferiche	€ 148.850,00	*Comprende tutti i 120 PC, monitor, server, NAS, switch di piano, router di bordo, rack e UPS. La cifra si basa sulla configurazione: 20 Mac Grafica, 35 PC IT, 65 PC Dipendenti.*	*Preventivo scalabile in base al numero e tipologie differenti di PC richiesti*
Firewall (HW + Licenze)	€ 4.250,00	*Acquisto dell'Appliance hardware e licenza annuale per la protezione perimetrale avanzata e la gestione del traffico WAN/VPN.*	
IDP (HW + Licenze)	€ 5.850,00	*Soluzione (hardware/software) per la sicurezza interna, mirata al rilevamento e prevenzione delle intrusioni su punti critici della rete.*	
Software	€ 5.950,00	*Include l'acquisto in bulk delle 97 licenze Windows Pro (se non OEM), Licenza*	

		Server OS, Antivirus/EDR (annuale per 120 utenti) e Software per la gestione del Backup del NAS.	
Cablaggio & Infrastruttura Fisica	€ 25.000,00	*Comprende materiali e manodopera per l'installazione e la certificazione dei 120 punti rete (Cat. 6A/7), oltre ai lavori accessori per l'alloggiamento dei rack*	
Manodopera	€ 34.800,00	*Copre tutte le ore di lavoro per la Progettazione, la Configurazione specialistica di Server, Rete (VLAN, Routing), PC Deployment, e il Collaudo finale.*	
TOTALE	€ 224.700,00		*+ IVA 22%*

All'interno del progetto è stato redatto un preventivo economico con l'obiettivo di stimare in modo realistico i costi necessari per l'implementazione dell'infrastruttura della rete preposta. Tale strumento pianifica le scelte tecniche ai costi reali.

Il preventivo è stato suddiviso in diverse aree:

- **HARDWARE & PERIFERICHE:**

la prima riguarda l'hardware che include i PC, server, dispositivi di rete come switch e rack e i sistemi di continuità.
Questi elementi sono fondamentali per garantire affidabilità e continuità operativa;

- **FIREWALL (HW + LICENZE):**

La seconda area è dedicata alla sicurezza di rete, in particolare ai dispositivi firewall e ai sistemi di monitoraggio.
Queste voci sono orientate alla protezione delle infrastrutture;

- **DP (HW + LICENZE):**

La terza area si concentra sulla soluzione per la sicurezza interna mirata al rilevamento e alla prevenzione delle intrusioni su punti critici della rete;

- **SOFTWARE:**

La quarta area lavora sull’acquisto di Licenza Server OS, Antivirus/EDR (Annuale per i 120 dispositivi) e i Software per la gestione del Backup del NAS;

- **CABLAGGIO & INFRASTRUTTURA FISICA:**

La quinta area comprende manodopera, tutti i materiali per le installazione avvenute e la certificazione dei 120 punti di rete;

- **MANODOPERA:**

Questa sezione finale invece ricopre tutte le ore di lavoro dedicate alla progettazione dell'infrastruttura

TOTALE (+ IVA 22%):
Il totale preventivato dei costi di spesa eventualmente sostenuti si sommerà all' IVA al 22%

Ogni voce del preventivo è coerente con l'architettura della rete progettata.
Ad esempio la presenza di un ***DMZ(Server Web)*** e di un ***firewall*** perimetrale giustifica l'inclusione di specifici dispositivi di sicurezza e le relative licenze software.
Oltre ai costi materiali il preventivo include anche le attività operative come l'installazione dell'hardware, il cablaggio strutturato, la configurazione dei dispositivi di rete e il collaudo finale. Queste attività sono fondamentali perché garantiscono che l'infrastruttura venga correttamente implementata testata e resa operativa riducendo il rischio di errori o problemi in fase di utilizzo.

In conclusione il preventivo consente di avere una visione completa dei costi dell'intero progetto e dimostra sostenibilità economica dell'infrastruttura proposta.