Architettura di Rete

La rete interna della Theta è strutturata in una topologia gerarchica, con una suddivisione logica in sei sottoreti, una per ciascun piano dell'edificio.

Ciascun piano dispone di uno switch che collega i 20 PC presenti, e tutti gli switch sono poi connessi a un router centrale.

Il router funge da punto di aggregazione e permette la comunicazione tra i vari piani e il server NAS, garantendo l'accesso centralizzato ai dati.

Abbiamo scelto di dividere la rete con una subnet mask 255.255.255.224(/27) che segmenta gli indirizzi IP in intervalli di 32 indirizzi ciascuno.

La distribuzione è la seguente:

Subnet 1: 192.168.1.0 - 192.168.1.31
Subnet 2: 192.168.1.32 - 192.168.1.63
Subnet 3: 192.168.1.64 - 192.168.1.95
Subnet 4: 192.168.1.96 - 192.168.1.127
Subnet 5: 192.168.1.128 - 192.168.1.159
Subnet 6: 192.168.1.160 - 192.168.1.191

Vantaggi della Scelta Progettuale

- **Sicurezza:** La segmentazione della rete in sottoreti aumenta il livello di sicurezza, isolando il traffico di ciascun piano e limitando la propagazione di eventuali attacchi.
- **Scalabilità:** La disponibilità di 32 indirizzi IP per piano consente di aggiungere ulteriori dispositivi in futuro senza dover riconfigurare la rete.
- **Gestione semplificata:** La struttura gerarchica della rete facilita la gestione e la manutenzione, consentendo di isolare e risolvere eventuali problemi a livello di singolo piano o di router centrale.
- **Indipendenza dei piani:** Ciascun piano opera in modo indipendente, riducendo l'impatto di eventuali problemi su altri piani.

Dispositivi di Sicurezza Implementati nella Rete

La presente relazione approfondisce le motivazioni e i vantaggi specifici associati a ciascun dispositivo di sicurezza implementato nella rete, fornendo un quadro più dettagliato della strategia di protezione adottata.

Router con funzionalità IDS(Intrusion Detection System):

- **Motivazione:** Il router, in quanto choke point della rete, offre una posizione strategica per l'analisi del traffico in tempo reale. L'IDS integrato consente il rilevamento di anomalie e pattern sospetti, fornendo un primo livello di difesa contro intrusioni esterne e movimenti laterali interni.
- **Vantaggi:**
    - **Visibilità completa del traffico:** Il router processa tutto il traffico in entrata e in uscita, consentendo all'IDS di analizzare un ampio spettro di dati e correlare eventi per identificare attacchi sofisticati.
    - **Rilevamento in tempo reale:** L'analisi in linea permette di identificare e bloccare attacchi in corso, riducendo il dwell time e limitando i danni potenziali.
    - **Basso overhead:** L'integrazione dell'IDS nel router minimizza l'impatto sulle prestazioni della rete, evitando colli di bottiglia e latenze aggiuntive.

HIDS(Host Intrusion Detection System) su Server NAS:

- **Motivazione:** Il server NAS, repository centralizzato di dati sensibili, rappresenta un asset ad alto valore per gli attaccanti. L'HIDS offre una protezione mirata, monitorando l'attività a livello di sistema operativo e filesystem per rilevare compromissioni e manipolazioni non autorizzate.
- **Vantaggi:**
    - **Rilevamento di attacchi file-based:** L'HIDS può identificare modifiche sospette ai file, tentativi di accesso non autorizzato e attività anomale a livello di processo, segnalando potenziali intrusioni o malware.
    - **Integrità dei dati:** Il monitoraggio continuo dei file cruciali

garantisce l'immutabilità dei dati e previene la perdita o la corruzione causata da attacchi mirati.
    - **Analisi forense:** In caso di incidente, i log dettagliati dell'HIDS forniscono prove cruciali per ricostruire l'attacco, identificare il vettore di ingresso e valutare l'estensione della compromissione.

Firewall configurato come Web Application Firewall (WAF) e IPS per la protezione del Server Web:

- **Motivazione:** Il server web, esposto a Internet, è un obiettivo primario per attacchi esterni. Configurando il firewall come WAF, oltre alle funzionalità tradizionali di filtraggio del traffico, si aggiunge uno strato di protezione specifico per le applicazioni web.
- L'IPS aggiuntivo potenzia ulteriormente la sicurezza bloccando attivamente tentativi di sfruttamento di vulnerabilità.
- **Vantaggi:**
    - **Perimeter security e protezione applicativa:** Il firewall/WAF agisce come prima linea di difesa, controllando l'accesso alla rete e proteggendo il server web da attacchi specifici alle applicazioni, come SQL injection, cross-site scripting e altre minacce a livello HTTP/HTTPS.
    - **Prevenzione attiva:** L'IPS, attraverso l'analisi del traffico e l'utilizzo di firme e modelli comportamentali, blocca in tempo reale attacchi noti e sospetti, inclusi tentativi di sfruttamento di vulnerabilità a livello applicativo.
    - **Mitigazione DDoS:** Il firewall/WAF e l'IPS possono implementare meccanismi di rate limiting e filtraggio per mitigare gli effetti di attacchi DDoS, garantendo la disponibilità del servizio web anche sotto carico elevato.
    - **Virtual patching:** Il WAF può fornire una protezione temporanea per vulnerabilità note nelle applicazioni web, in attesa dell'applicazione di patch correttive, riducendo la finestra di esposizione agli attacchi.