EPICODE-CS0124
Build Week 1 - Team 1
Attacco Brute Force DVWA

Indice

Riferimenti e versioni

GdL Team 1:

Responsabile/referente del documento (di seguito Responsabile): Verdiana Germani

TL: Flaviano Sedici

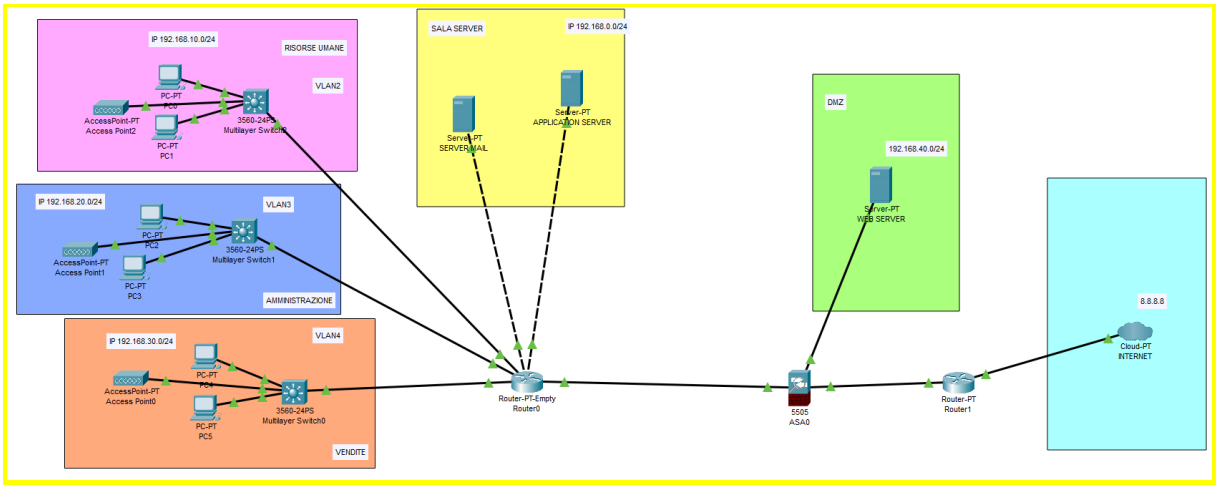
Risorse a supporto (di seguito Risorse): Francesco Mineo

Versionamento

Versione	**Descrizione**	**Ruolo**	**Data**
1.0	Redazione documento	Responsabili	15/12/2024
1.1	Formattazione documento	TL	15/12/2024
1.2	Revisione	Team 1	15/12/2024

---

1. Rappresentazione grafica della rete



2. Descrizione della rete

Rete	VLAN	DEFAULT GATEWAY
Risorse Umane	**192.168.10.0/24**	**192.168.10.1**
Amministrazione	**192.168.20.0/24**	**192.168.20.1**
Vendite	**192.168.30.0/24**	**192.168.30.1**
Sala Server	**192.168.0.0/24**	**192.168.0.1**
DMZ	**192.168.40.0/24**	**192.168.40.1**

3. VLAN

Nel progetto di rete per la compagnia Theta i dipartimenti hanno una VLAN dedicata. Ogni rete consente il collegamento di vari dispositivi (pc, server, stampanti ed altro). Per completezza sono stati aggiunti degli access-point al fine di consentire l'accesso ad un wifi protetto da password.
La divisione in VLAN consente di poter disporre di una connessione per 253 dispositivi per ogni dipartimento e contestualmente dà l'opportunità alla compagnia Theta di isolare a livello logico i vari dipartimenti tra loro.
Con una VLAN dedicata è stata posizionata nella rete interna anche la Sala Server nella quale risiede anche l'Application Server e-commerce disponibile ai soli dipendenti dell'azienda nonché un server DHCP che fornisce una corretta e automatica distribuzione degli indirizzi IP a tutti i dispositivi collegati.
Inoltre se configurato correttamente tramite le tabelle di routing, offre un ulteriore livello di protezione per la rete interna da potenziali minacce provenienti dall'esterno.

4. Router esterno (traffico in entrata)

Il router è stato configurato, per le comunicazioni in ingresso provenienti da Internet, con un protocollo di NAT (Network address translation) in modo che sia possibile, tramite un IP pubblico, raggiungere i server collegati nella DMZ ma non nella rete interna.
Tutte le altre comunicazioni verranno instradate secondo quanto descritto di seguito.

5. Router esterno (traffico in uscita)

Per le comunicazioni in uscita, ossia provenienti dalla rete interna e dirette verso l'esterno, il router non devia o blocca alcun passaggio di dati, instradando i dati verso Internet per entrambe le reti.

6. Firewall

Il Firewall è posizionato nella rete a protezione della DMZ e della rete interna.

7. Firewall Policy per il traffico in entrata

Il firewall è stato configurato per le comunicazioni in ingresso (provenienti da Internet) in modo da accettare solamente le comunicazioni instradate dal router verso i server collocati nella DMZ.
Tutti gli altri instradamenti o le richieste di comunicare con IP della rete Interna, saranno configurati sul firewall in modo che il firewall le scarti (DROP).
Si è pensato alla configurazione DROP al posto del DENY per dare meno informazioni possibili ad eventuali attaccanti sulla natura della eventuale mancata comunicazione.
Le uniche porte che saranno aperte per la DMZ saranno quelle necessarie ad offrire i servizi previsti dall'azienda e configurati sui server.

8. Firewall Policy per il traffico in uscita

Per le comunicazioni in uscita (verso internet) il firewall è stato impostato in modo da consentire la comunicazione della DMZ solamente sulle porte aperte per i servizi erogati dai server.
La rete interna potrà accedere ad Internet sulle principali porte standard (posta, internet, etc.) dedicate ai servizi utili in azienda o che l'azienda stessa riterrà opportuni.
Per le comunicazioni in uscita dalla rete interna sarà applicato anche un Filtraggio di Stato (Stateful filtering) in modo da consentire le comunicazioni in entrata solo se espressamente richiesto dagli host della rete interna.
Per le comunicazioni interne, ossia tra la rete interna e la DMZ, il firewall sarà configurato con una tabella di DENY in modo da impedire le comunicazioni tra le due reti e nello stesso tempo offrire agli utenti finali un messaggio di errore per evitare di ripetere la richiesta di accesso diretto.
Ovviamente gli utenti della rete interna, pur non potendo accedere direttamente ai server nella DMZ, possono accedere ai loro servizi esposti tramite la rete Internet.

9. DMZ (Zona demilitarizzata)

Nella DMZ è stato collocato il Web Server che esporrà i servizi dell'impresa su internet e quindi accessibili al pubblico.
La DMZ è l'area di rete tra la rete interna e la rete esterna (internet). Il traffico in questa zona è meno controllato rispetto alla zona di rete interna, ed è infatti un'area usata per inserire i vari server che devono essere accessibili dagli utenti esterni. Nel nostro progetto di rete all'interno della DMZ troviamo il Web server della compagnia Theta che espone vari servizi al pubblico.
Per creare la nostra DMZ useremo il firewall presente che lavora con le VLAN, ne presenta due di default: inside (di seguito rete aziendale interna) e outside (di seguito internet). La VLAN aziendale avrà un livello di sicurezza alto, in quanto a questa rete non devono poter accedere host esterni.
La DMZ deve essere configurata in modo che non possa comunicare con la rete interna, per questo sul firewall imposteremo "no forward interface VLAN inside" (la nostra rete aziendale). Andrebbero anche configurati gli ACL (lista di controllo accessi) per poter regolare il traffico in entrata ed in uscita.
Il firewall perimetrale quindi ci permette di mitigare e regolamentare il traffico da e verso internet; è il nostro primo livello di protezione.
Nella rete interna di Theta troviamo la Sala server in cui possiamo vedere l'Application server che espone sulla rete aziendale interna un applicativo e-commerce accessibile solo dagli impiegati della compagnia, dunque non accessibile da utenti esterni.
Il firewall perimetrale quindi andrebbe posizionato tra la rete interna e la rete esterna perché appunto serve a proteggere la rete interna dalle eventuali minacce provenienti dall'esterno/internet, per questo è anche importante che non comunichi direttamente con la DMZ. Con il filtraggio statico il firewall viene configurato proprio per consentire la ricezione o meno di un pacchetto andando a verificare se l'indirizzo IP di origine e quello di destinazione è consentito, se la porta di destinazione è autorizzata e se il protocollo usato è permesso.