Traccia 1:

Rappresentare graficamente un modello di rete per mettere in sicurezza le due componenti critiche, includendo l'analisi dei dispositivi che potrebbero servire per aumentare la protezione della rete.

Si è iniziato con la costruzione della rete, partendo da tre ambienti separati:

DMZ(Demilitarized Zone): Con all'interno tre server, un HTTP, per la comunicazione con l'esterno della rete, un server POP3/IMAP utile alla ricezione della mail, e un server SMTP utile all'invio delle mail all'esterno.

Ambiente LAN: In quest'ambiente, troviamo il router, a cui sono collegati i tre switch dell'azienda protetto da un Stateful Firewall sul confine di una rete in modo da filtrare tutto il traffico che questa scambia con l'esterno.

Server Room: dove all'interno troviamo tutta la parte sensibile dell'azienda quindi il NAS, l'app server e il DNS.

Per incrementare la sicurezza nella DMZ abbiamo optato per un WAF(Web Application Firewall) per proteggere una delle zone critiche, bersaglio principale di eventuali attacchi, in quanto è la zona di interfaccia con l'ambiente esterno, non essendo soggetta alla protezione di un Firewall. Essa poi è collegata al router tramite uno switch, dove si interpone un IPS, volto ad incrementare il controllo del traffico di rete tramite il rilevamento ed un eventuale blocco delle intrusioni, generando un alert per noi. La scelta di un componente attivo, fa si che si abbia una maggiore sicurezza a discapito delle performance.

La Server room è isolata, e collegata al router tramite uno switch dove si interpone un IDS, volto ad un controllo passivo delle connessioni dirette alla server room. Lo switch è configurato in modo tale da consentire l'accesso esclusivamente alla VLAN1 e alla VLAN3, attraverso l'impostazione della porta su TRUNK.

Abbiamo altresì suddiviso la rete interna, per compartimentalizzare le utenze, in modo da creare delle reti virtuali, che possano comunicare tra loro, aumentando così le performance e la sicurezza, e gestire più facilmente i permessi per l'accesso alla server Room.
la scelta di un componente attivo, fa si che si abbia una maggiore sicurezza a scapito delle performance.
In sintesi, il DMZ è una componente chiave nella progettazione di reti sicure, in quanto contribuisce a proteggere la rete interna da potenziali minacce esterne mantenendo servizi accessibili dall'esterno in un ambiente controllato.

Programma in python per l'enumerazione dei metodi http abilitati su un determinato target:

L'obiettivo di questo tool è avere la possibilità di enumerare tutti i metodi abilitati su un determinato indirizzo ip.

Dopo la scelta della libreria, passiamo alla definizione dei vari metodi che vogliamo enumerare (con l'aggiunta di un metodo fittizio, per verificare l'attendibilità delle risposte). Abbiamo deciso di utilizzare un ciclo 'for' per effettuare la richiesta http ad una delle 'url' che abbiamo dichiarato, per ogni metodo contenuto nella lista 'methods'.
Il risultato ottenuto è una stampa dei servizi abilitati con i codici corrispondenti.

Programma in Python per la valutazione dei servizi attivi (port scanning)

L'obiettivo di questo tool, è valutare la quantità dei servizi attivi, quindi eseguire uno scanning delle porte. Questo tipo di software può essere utilizzato come strumento di monitoraggio della sicurezza della rete, individuazione di problemi di configurazione , o altresì per evidenziare le vulnerabilità della stessa.

Questo programma solitamente utilizza librerie e moduli socket per aprire le connessioni alle diverse porte su un host e determinare se un servizio è in ascolto su quella porta o meno. È importante sottolineare che la scansione delle porte su un host senza autorizzazione può essere considerata una violazione della sicurezza.

Il programma è strutturato partendo dalla creazione del 'socket' e dalla richiesta di connessione. Una volta creata la connessione, si parte con la ricerca dei servizi attivi sulle porte definite in precedenza.
Una volta ottenuta una risposta, avviene una stampa delle porte ricercate, con i relativi servizi attivi.
Nel nostro caso specifico, veniva richiesto l'ascolto sulla porta 80, relativa ai servizi HTTP.

Report su attacchi a dizionario sulla DVWA, partendo dal livello di sicurezza più basso.

Un attacco a dizionario, è un tipo di attacco informatico che mira a scoprire una combinazione di accesso utente/password, utilizzando una lista predefinita di utenti e password più utilizzati, a differenza di un attacco BruteForce che invece tenta tutte le combinazioni possibili di caratteri. L'obiettivo è quello di riuscire a penetrare la sezione dedicata al Bruteforcing, all'interno del nostro server DVWA su metasploitable, partendo dal livello più basso di sicurezza, fino ad arrivare a penetrare il livello massimo.

Per superare i diversi livelli di sicurezza abbiamo utilizzato due programmi differenti: il primo è dedicato ai livelli LOW e MEDIUM, invece il secondo è dedicato al livello massimo di sicurezza.
La differenza principale, risiede nella presenza di un comando SLEEP, lato server, all'interno del codice, che ritarda i tempi di risposta per una quantità di tempo definita, ad ogni tentativo di accesso errato, rendendo l'attacco meno efficace.

Il software utilizzato per le difficoltà LOW e MEDIUM, è caratterizzato dalla presenza di un cookie di sessione, perché il nostro obiettivo è orientare l'attacco su una sezione specifica, bypassando così l'autenticazione iniziale del server DVWA, accedendo così ad una sessione già registrata ad un livello di sicurezza precedentemente dichiarato. Successivamente andiamo a riempire delle liste partendo dai nostri file di testo, rendendoli leggibili e fruibili dal software. Le combinazioni sono frutto dell'esecuzione di due cicli 'for' nidificati, generando così 'url' composti da variabili di

username e passwords e dando il via ad una reiterazione di richieste. Questa metodologia è resa possibile dall'utilizzo del solo verbo 'GET'.

Il risultato che vogliamo ottenere, sarà la visualizzazione delle credenziali di accesso corrette, mediante appunto una serie di tentativi.

Questo tool, è stato utilizzato per i due livelli di difficoltà, low e medium.

Per riuscire a superare il livello più alto, abbiamo la necessità di implementare il nostro software, per far fronte alla problematica aggiunta dal server, che per ogni richiesta non corretta, ci impone di attendere un lasso di tempo predefinito prima di reiterarne una nuova.

Report su attacchi a dizionario sulla DVWA, partendo dal livello di sicurezza più alto.

Per questo tentativo di intrusione abbiamo implementato il tool precedente per effettuare delle richieste http in parallelo