EPICODE

Cyber Security & Ethical Hacking

Build Week – Progetto

EPICODE

Traccia e requisiti

Progetto di Rete per la Compagnia Theta

Progetto di Rete per la Compagnia Theta

Specifiche del Progetto

Siamo stati ingaggiati dalla compagnia Theta per sviluppare un preventivo di spesa e un progetto di rete per la loro infrastruttura IT. Ecco i requisiti e i componenti necessari:

- Struttura dell'edificio: 6 piani
- Dispositivi previsti: 20 computer per piano, per un totale di 120 computer
- Componenti aggiuntivi:
  - 1 Web server (rappresentato dalla macchina DVWA di Metasploitable)
  - 1 Firewall perimetrale
  - 1 NAS (Network Attached Storage)
  - 3 IDS/IPS (Intrusion Detection System / Intrusion Prevention System)

Progetto di Rete per la Compagnia Theta

Rete Interna Aziendale

- **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 al 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.

Rete Esterna (Internet)

- **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

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) 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 la sicurezza e l'accessibilità delle varie porte di comunicazione.

Report Finale

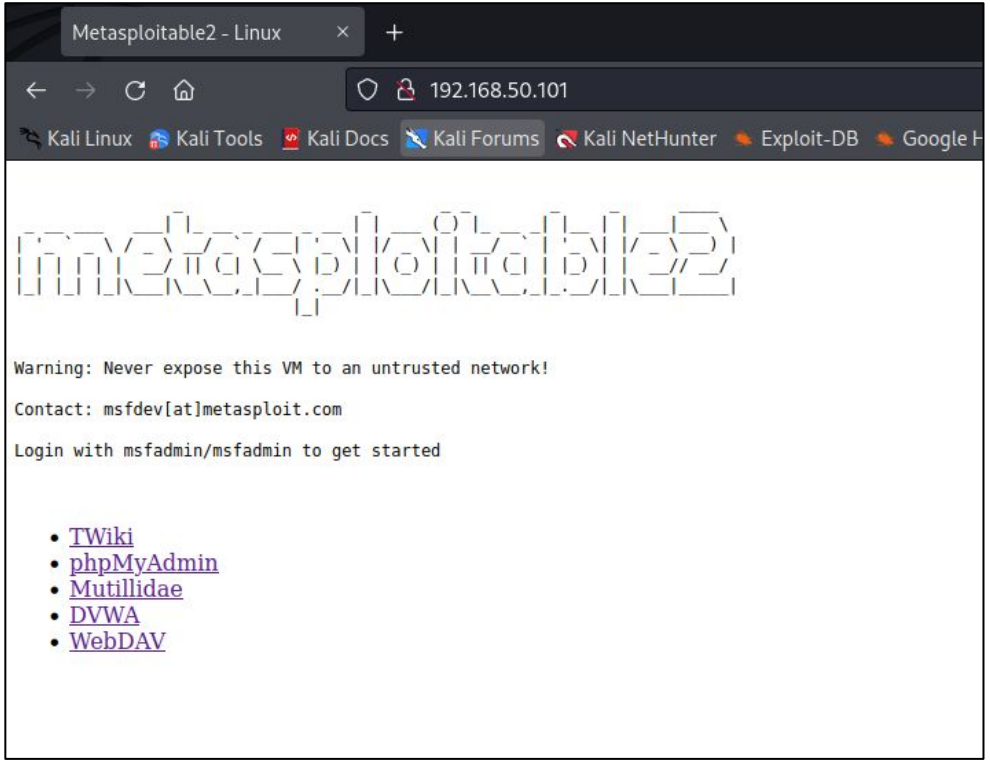
Alla conclusione dei test, redigeremo un report dettagliato che includerà:

- **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 e chiuse 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.

Linee guida per la risoluzione del progetto:

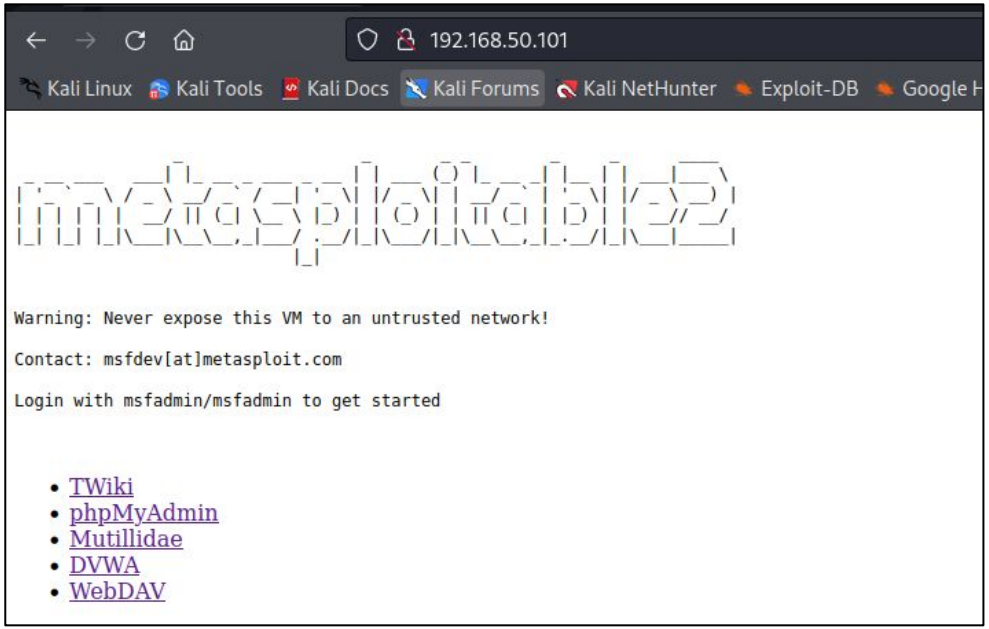
- Il Web Server di Theta verrà simulato dalla macchina Metasploitable
- Per la scansione dei servizi, non è possibile utilizzare i tool già pronti. Lo studente dovrà dunque scrivere in linguaggio Python un scanner che accetti in input un IP ed un range di porte da scansionare (la programmazione fa parte dell'esercizio). L'output del programma dovrà essere una lista delle porte con relativo stato (aperta/chiusa).
- La macchina Metasploitable espone un servizio web sulla porta 80, potete controllarlo da interfaccia grafica digitando l'indirizzo della vostra Metasploitable nella barra del browser da Kali (assicuratevi che ci sia comunicazione tra la macchina Kali e Metasploitable prima, Kali deve essere in grado in «pingare» la macchina Metasploitable).



Linee guida per la risoluzione del progetto:

Cliccate su phpMyAdmin e controllate quali verbi HTTP sono abilitati utilizzando un programma in Python anche in questo caso scritto da voi (la programmazione del tool fa parte dell'esercizio).

Il tool dovrà prendere input un path e dare in output come risultato una lista dei metodi abilitati su quel determinato path.



Bonus:

1. **Eseguire il subnetting per scegliere la subnet più appropriata per la rete.**

2. **Creare un programma in python che catturi il socket di rete.**

EPICODE

GRAZIE

Epicode