EPICODE-CS0124
Build Week 1 - Team 1
SAL 2

1. Descrizione delle attività odierne

1.1. Obiettivi della giornata

Redazione, revisione e test dei tre componenti Python necessari:

- Port Scanner
- Brute Force
- Method Scanner

Redazione schema di rete ottimale

Verifica delle funzionalità dei due laboratori virtuali predisposti

2. SAL

2.1. Redazione, revisione e test dei tre componenti Python

- **Port Scanner**

Il programma per la scansione delle porte è stato realizzato con successo in modo che individui le porte TCP aperte sulla macchina target.

Domani, durante le simulazioni in laboratorio, si valuterà se ampliare il programma anche per scansionare le porte UDP.

- **Brute Force**

Il programma per effettuare una simulazione di attacco brute force è stato compilato con successo.

Attualmente sono state utilizzate solo i dictionary standard inseriti in Kali Linux. Nella simulazione di domani verranno integrati anche altri dizionari provenienti dai repository GitHub.

Al momento il programma è impostato per aggredire il sistema di login di DVWA, domani replicato e modificato per la simulazione di attacco contro phpmyadmin.

- **Method Scanner**

Il programma per l'analisi dei metodi è stato sviluppato con successo e consente di verificare i metodi abilitati su un determinato socket.

Tutti i programmi sono stati testati e verificati nei laboratori creati, in particolare nei confronti dei servizi esposti su Metasploitable inerenti al server DVWA.

Nella giornata di domani una parte del team di occuperà di revisionare e ampliare il codice al fine di migliorarlo e svilupparne la riusabilità in modo da gestire ulteriori casistiche di attacco che emergeranno durante l'esecuzione dei test sul laboratorio.

2.2. Redazione schema di rete ottimale

Lo schema di rete è stato realizzato sulla base delle specifiche richieste. E' stato redatto un documento che ne spiega brevemente le funzionalità e verrà integrato, qualora sia necessario, a valle dei test di domani.

2.3. Verifica delle funzionalità dei due laboratori virtuali predisposti

Grazie alle verifiche effettuate sui programmi appena elencati, è stata verificata anche la corretta funzionalità dei due laboratori di creati per i test di domani.

2.4. GitHub

Tutta la documentazione necessaria è stata caricata correttamente dai rispettivi assegnatari all'interno del repository GitHub condiviso, compresa la documentazione di progetto.

---

3. Conclusioni

Il Team ha lavorato con grande solerzia non solo completando i singoli compiti affidati, ma dando completa disponibilità nei confronti dei colleghi nel risolvere non inerenti ai loro task personali.

Si fa riferimento in particolare alla programmazione dell'attacco Brute Force ha richiesto un impegno leggermente superiore al previsto in quanto erano presenti dei moduli che hanno richiesto una configurazione più accurata.

Non sono state rilevate frizioni all'interno del gruppo e tutti hanno lavorato costantemente negli orari imposti dal Team Leader.

Ad oggi la tabella di marcia e l'effort preventivato risultano rispettati.