BUILD WEEK GRUPPO ''IANNONE LUCA''

INDICE

- PREFAZIONE
- PRIMA GIORNATA
  SQL INJECTION

EPICODE

PREFAZIONE

PIO SRL

TEAM LEADER :

Iannone Luca

COLLABORATORI:

Francesco Pio Scopece

Francesco Perticaroli

Giorgio Ciaschini

Ahmed El Ashri

Marco Fasani

nessus Professional

KALI

In questa fase andremo a spiegare come configurare una macchina a livello e quali comandi eseguire su alcune di esse da TERMINALE

KALI LINUX

Mediante il comando da terminale :

<sudo nano /etc/network/interfaces>

Andiamo a configurare i parametiri di rete nel modo riportato nella figura accanto.

N.B

I campi vanno inseriti nel seguente modo

Auto eth0

Iface eth0 inet static

Address : ‘’inserire IP da dare alla macchina’’

Gateway : ‘’riscrivere ip con il primo indirizzo dispondibile’’

Network : ‘’indirizzo che identifica la rete in base all’IP che abbiamo impostato’’

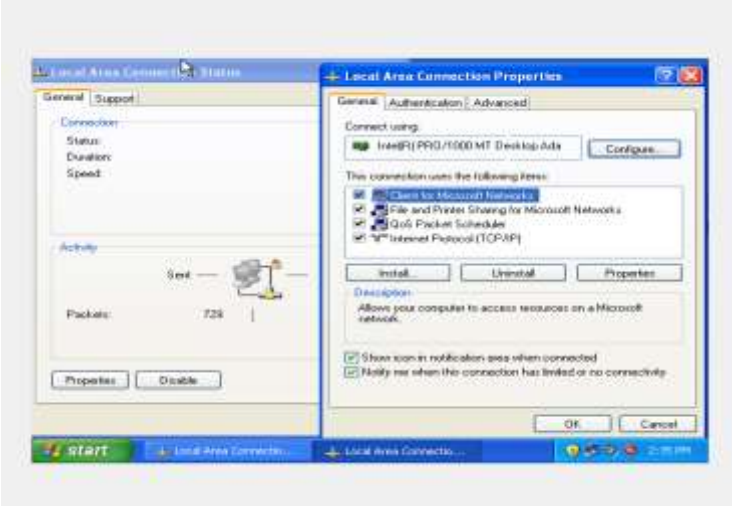
Successivamente dopo aver impostato la nostra configurazione andremo a salvare le nostre impostazioni premendo i tasti (**ctrl + x**) , quando il terminale ci chiederà di salvare le impostazioni digiteremo (**Y**) quindi «yes» e successivamente il tasto (**INVIO**)

PIO srl
So di non sapere

Dopo aver eseguito i vari comandi citati nelle slide precedenti andremo ad eseguire un riavvio del sistema di **KALI** in modo che le nostre impostazioni vengano caricate. Il comando da eseguire da terminale è il seguente :
< sudo reboot>

EPICODE

WINDOWS

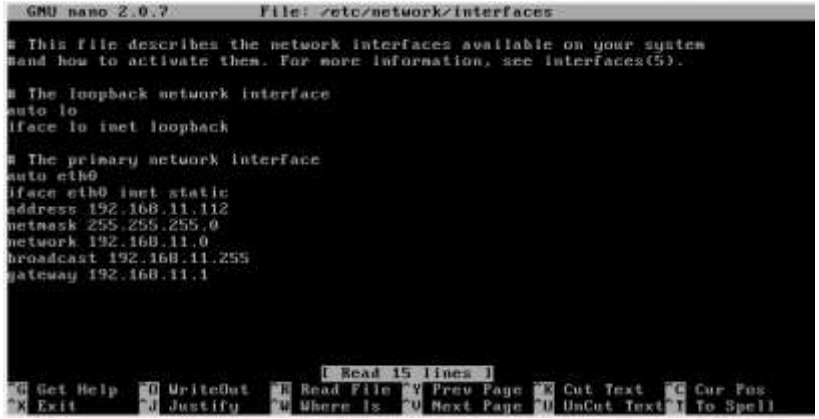


In questa fase andremo a vedere come settare le impostazioni di rete di una macchina WINDOWS

PROCEDIMENTO :

- SELEZIONIAMO la **''LOCAL AREA CONNECTION STATUS''**cliccando sui due computer sulla barra di ''**START**''
- CLICCHIAMO SULLE **''PROPETIES''**
- SELEZIONIAMO **''PROTOCOL TCP/IP''**
- ANDIAMO A MODIFICARLO IN BASE ALLE NOSTRE ESIGENZE

METASPLOITABLE



I comandi da eseguire sono sulla macchina **META** sono gli stessi che eseguiamo sulla macchina **KALI LINUX** Quindi li possiamo andare a vedere nelle slide precedenti.

IMPOSTAZIONE LIVELLO SICUREZZA DVWA

Nello svolgimento della nostra build week andremo a settare le impostazioni della ‘’**DVWA**‘’di metasploitable con un livello di sicurezza ‘’**BASSO**’’-‘’**LOW**’’

PRIMA GIORNATA

Il compito della prima giornata è stato svolto da :
FRANCESCO PERTICAROLI

SQL INJECTION

Il lavoro da svolgere prevede di decriptare l'hash della password di Pablo Picasso che troviamo nella **SQL** injection di **DVWA.**
Il tool di cracking utilizzato è '**John The Ripper**'.
La traccia è la seguente:

Traccia Giorno 1:
Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità **SQL** injection presente sulla Web Application **DVWA** per recuperare in chiaro la password dell'utente **Pablo Picasso** (ricordatevi che una volta trovate le password, c'è bisogno di un ulteriore step per recuperare la password in chiaro).

SVOLGIMENTO DEL LAVORO

La prima azione sarà quella di trovare le password criptate sul sito tramite il comando **“UNION SELECT user, password FROM users #”**.
L'iniezione SQL basata su UNION coinvolge l'uso dell'operatore UNION che combina i risultati di più istruzioni SELECT per recuperare dati da più tabelle come un singolo set di risultati. La query maliziosa con l'operatore UNION può essere inviata al database tramite l'URL del sito web o un campo di input dell'utente.
Trovata la password di Picasso, la copiamo e la salviamo su un file di nome ‘PW.txt’ .

JOHN THE RIPPER

Sul terminale di Kali Linux utilizziamo il comando di John The Ripper
‘ **john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5** ./Desktop/PW.txt ‘ e successivamente scriviamo la directory interessata; per decriptare la password dobbiamo inserire il formato md5 che ci servirà per convertirle.Questa funzione prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit.
Per farci mostrare tutto il contenuto usiamo “ --show --format=raw-md5 “ e vediamo che ci restituirà la password.