EPICODE

**Esercizio**
Nmap scan

**Traccia:**

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine.
E' molto importante in questa fase essere organizzati e strutturati.
Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:

- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

-Fonte dello scann -Target dello scann - Tipo di scann - Risultati ottenuti

| | | | |
|---|---|---|---|
| Servizio nmap utilizzato dalla macchina kali Linux 192.168.30.125 | Macchina metaspoitable2 con indirizzo 192.168.30.130 | Nmap -sT | Otteniamo risultati sullo stato della porta e i servizi disponibili |
| Servizio nmap utilizzato dalla macchina kali Linux 192.168.30.125 | Macchina metaspoitable2 con indirizzo 192.168.30.130 | Nmap -sS | Risultato sullo stato della porta e i servizi disponibili |
| Servizio nmap utilizzato dalla macchina kali Linux 192.168.30.125 | Macchina metaspoitable2 con indirizzo 192.168.30.130 | Nmap -A | I risultati ottenuti sono maggiori rispetto ai primi due. Otteniamo: porte aperte con servizi attivi,nome computer,tipo di sistema operativo,dominio di appartenenza, tipo di host e livello di autenticazione. |