Report

1. Gli aggressori possono effettuare la ricognizione di rete o il footprint della tua rete in molti modi diversi. Con l'aiuto di **nmap**, puoi facilmente effettuare una ricognizione attiva contro qualsiasi bersaglio come mostrato di sopra

2. **NetDiscover** è uno strumento molto utile per trovare host su reti wireless o commutate. Può essere utilizzato sia in modalità attiva che passiva.

3. Con l'opzione **–top-ports** , puoi identificare facilmente le prime 10 porte aperte in qualsiasi rete con il comando riportato qui sopra.

4. Attualmente, **–top-ports** seleziona le porte più diffuse dal file **nmap-services** o dall'elenco delle porte fornito sulla riga di comando.

5. **Unicornscan** è un nuovo motore di raccolta e correlazione di informazioni creato per e dai membri delle comunità di ricerca e test sulla sicurezza. È stato progettato per fornire un motore che sia scalabile, accurato, flessibile ed efficiente.

   Unicornscan imposta di default una scansione TCP/UDP, a differenza di nmap. Di default, invia una scansione SYN. Diciamo che volessimo scansionare il nostro IP (192.168.169.138), cercando tutte le porte e inviando 3000 pacchetti al secondo che potremmo scrivere come sopra riportato.

6. **hping** è un analizzatore/assemblatore di pacchetti TCP/IP orientato alla riga di comando. L'interfaccia è ispirata al comando ping unix, ma hping non è solo in grado di inviare richieste di echo ICMP. Supporta anche i protocolli TCP, UDP, ICMP e RAW-IP, ha una modalità traceroute, la capacità di inviare file tra un canale coperto e molte altre funzionalità.