nmap – brzi pregled osnovnih funkcija

nmap [tip skeniranja] [opcije] [specifikacija mete]

Tip skeniranja	Opis:
-sP	Ping scan – provjeravamo samo dali je poslužitelj online
-sS	Syn Scan – Skeniranje sa poluotvorenim TCP rukovanjem (Syn,SynAck)
-sT	Connect skeniranje – Skeniranje punim TCP rukovanjem (Syn,SynAck,Ack)

Opcije:	Opis:
-p X	Skeniraj samo port X (npr: -p22)
-pX-Y	Skeniraj portove od X do Y (-p1-65535)
--top-ports X	Skeniraj samo X najpopularnijih portova (--top-ports 10)
--version-all	Testiraj sve moguće metode identifikacije i pravljenja otiska servisa
--osscan-guess	Pokušaj agresivnije detektirati tip OS-a
-TX	Brzina skeniranja X (-T0 Sporo, -T3 Normalno, -T5 Agresivno) (X=0 do 5)
-A	Aktiviraj detekciju verzija, OS-a, skripte za testiranje i traceroute
-PN	Ne provjeravaj dali je računalo aktivno

Mete (TARGET):	Opis:
localhost, scanme.nmap.org	Po hostnameu
192.168.1.1/24	Po CIDR maski
192.168.1.1-254	Sa rasponom (1-254)
-iL DAT	Preko datoteke DAT

Primjer skeniranja:	Učinak:
nmap -sP 192.168.1.1-254	Provjeri koja su aktivna računala u rasponu 192.168.1.1 do 192.168.1.254
nmap -sS 192.168.1.1	Skeniraj najpopularnije otvorene portove na računalu 192.168.1.1
nmap -sS -p1-65535 192.168.1.1	Skeniraj sve otvorene portove na računalu 192.168.1.1
nmap -sS -p1-65535 -A --version-all -O --fuzzy -v -v 192.168.1.1	Detaljno skeniranje računala 192.168.1.1
nmap -sS -p22 -T0 -v -v 192.168.1.1-254	Sporo skeniranje samo računala koja imaju otvoreni port 22 (SSH) u rasponu od 192.168.1.1 do 192.168.1.254

Tonimir Kišasondi v.0.1