Basque CyberSecurity Centre

Nmap cheat sheet

Kode irekiko tresna bat da, **sareak eta atakak eskaneatzeko eta kalteberatasunak bilatzeko** erabiltzen dena. Segurtasun-auditoretzetan erabiltzen da, sareak monitorizatzeko.

1. Atakak zehazteko aukerak		
Sintaxia	**Adibidea**	**Azalpena**
-p	nmap -p 23 172.15.10.1	Atakak zehaztutako atakan eskaneatzen ditu
-p	nmap -p 23-100 172.16.1.1	Atakak zehaztutako ataka-barrutian eskaneatzen ditu
-p	nmap -pU:110,T:23-25,43 172.15.10.1	U-UDP T-TCP eskaneatze-motak
-p-	nmap -p 172.15.10.1	Ataka guztiak eskaneatzen ditu
-p	nmap -p -smtp,https 172.16.1.1	Berariazko protokoloak eskaneatzen ditu
-F	nmap -F 172.15.10.1	Atakak azkar eskaneatzen ditu
-p "*"	nmap -p "*" ftp 172.16.1.1	Atakak izenarekin eskaneatzen ditu
-r	nmap -r 172.15.10.1	Atakak sekuentziaren arabera eskaneatzen ditu

2. Eskaneatze-motak		
Sintaxia	**Adibidea**	**Azalpena**
-sS	nmap 172.15.10.1 -sS	TCP SYN ataka eskaneatzen du
-sT	nmap 172.15.10.1 -sT	TCP atakarako konexioa eskaneatzen du
-sA	nmap 172.15.10.1 -sA	TCP ACK ataka eskaneatzen du
-sU	nmap 172.15.10.1 -sU	UDP ataka eskaneatzen du
-Sf	nmap 172.15.10.1 -Sf	TCP FIN eskaneatzea
-sX	nmap 172.15.10.1 -sX	XMAS eskaneatzea
-sP	nmap 172.15.10.1 -sP	PING eskaneatzea
-Su	nmap 172.15.10.1 -sU	UDP eskaneatzea
-sA	nmap 172.15.10.1 -sA	TCP ACK eskaneatzea
-SL	nmap 172.15.10.1 -SL	Sareko ostalari bakoitza zerrendatzen du

Basque CyberSecurity Centre

3. Hainbat komando

nmap -6	Helburuen IPV6 eskaneatzea
nmap –proxies proxy 1 URL, proxy 2 URL	Proxyak dituzten helburuetan dabil
nmap –open	Ataka irekiak soilik erakusten ditu

4. Irteera-formatuak nmap-en

Lehenetsita	nmap -oN scan.txt 172.15.10.1
XML	nmap -oX scanr.xml 172.15.10.1
Grepable formatua	nmap -oG grep.txt 172.15.10.1
Formatu guztiak	nmap -oA 172.15.10.1

5. Eskaneatze-komandoak/Sintaxia

nmap [eskaneatze-mota] [aukerak] {171.20.20.1 espezifikazioa}

6. 172.16.1.1 espezifikazioa

nmap 172.16.1.1	IParen eskaneatze sinplea
nmap 172.16.1.1 172.16.100.1	IPen eskaneatze espezifikoa
nmap 172.16.1.1 -254	IPen barruti bat eskaneatzea
nmap xyz.org	Domeinu bat eskaneatzea
nmap 10.1.1.0/8	CIDR notazioa erabiliz eskaneatzea
nmap –iL scan.txt	Fitxategi baten 172.16.1.1 eskaneatzea
nmap –exclude 172.16.1.1	Eskaneatzetik kanpo utzitako IP espezifikoa

Basque CyberSecurity Centre

7. NSE scriptak NMAPen	
nmap --script= test script	Scripta exekutatzen du xedeko IP helbidearen kontra
nmap --script-update-db	Datu-basea eguneratzen du scripts/script.db-tik
nmap -sV -sC	Script lehenetsiak erabiltzen ditu eskaneatzeko
nmap –script-help=" Test script"	Scriptetarako tresnaren laguntza

8. Eskaneatze-aukerak	
nmap -sP 172.15.10.1	Ping eskaneatzea soilik
nmap -PU 172.15.10.1	Ping UDP eskaneatzea
nmap -PE 172.15.10.1	ICMP ping echo-a
nmap -PO 172.15.10.1	IP protokoloaren pinga
nmap -PR 172.15.10.1	ARP pinga
nmap -Pn 172.15.10.1	Pingik gabe eskaneatzea
nmap -traceroute 172.15.10.1	Traceroutea

9. Timing-aukerak NMAPen	
nmap -T0 172.15.10.1	Eskaneatze motelagoa
nmap -T1 172.15.10.1	IDSak saihesteko eskaneatzea
nmap -T2 172.15.10.1	Eskaneatze egokia
nmap -T3 172.15.10.1	Tenporizadore lehenetsiarekin eskaneatzea
nmap -T4172.15.10.1	Eskaneatze agresiboa
nmap -T5 172.15.10.1	Eskaneatze oso agresiboa