🔹 100+ Comandos de Nmap

📡 Escaneos Básicos (1–10)

1. `nmap 192.168.1.1` – Escaneo rápido por defecto
2. `nmap dominio.com` – Escanear dominio
3. `nmap 192.168.1.1 192.168.1.2` – Escanear varias IPs
4. `nmap 192.168.1.1-10` – Rango de IPs
5. `nmap 192.168.1.0/24` – Subred completa
6. `nmap -v 192.168.1.1` – Modo detallado (verbose)
7. `nmap -vv` – Modo muy detallado
8. `nmap -T4 192.168.1.1` – Velocidad de escaneo
9. `nmap -T5` – Muy agresivo (rápido pero detectable)
10. `nmap -T1` – Muy lento (evasivo)

🕵️ Tipos de Escaneo (11–20)

11. `nmap -sS` – Escaneo SYN (stealth)
12. `nmap -sT` – Escaneo TCP connect
13. `nmap -sU` – Escaneo UDP
14. `nmap -sN` – Escaneo TCP NULL
15. `nmap -sF` – Escaneo FIN
16. `nmap -sX` – Escaneo Xmas
17. `nmap -sA` – Detección de firewall ACK

18. `nmap -sW` – Escaneo Window
19. `nmap -sM` – Escaneo Maimon
20. `nmap -sZ` – Escaneo SCTP COOKIE-ECHO

🧠 Reconocimiento y Detección (21–30)

21. `nmap -sV` – Detección de versión de servicios
22. `nmap -sC` – Script básico por defecto (como -A)
23. `nmap -A` – Escaneo agresivo (SO, scripts, traceroute, versión)
24. `nmap -O` – Detectar sistema operativo
25. `nmap --osscan-guess` – Adivinar SO si no es claro
26. `nmap --version-all` – Detección profunda de versiones
27. `nmap -Pn` – Saltar descubrimiento (ping)
28. `nmap -n` – Desactiva resolución DNS
29. `nmap --traceroute` – Muestra ruta hasta el objetivo
30. `nmap --reason` – Mostrar razón del resultado

🔐 Puertos y Servicios (31–40)

31. `nmap -p 80` – Escanear puerto específico
32. `nmap -p 1-65535` – Todos los puertos
33. `nmap -p-` – Atajo para todos los puertos
34. `nmap -F` – Escaneo rápido (puertos más comunes)
35. `nmap --top-ports 100` – Top 100 puertos usados
36. `nmap --port-ratio 0.01` – Puertos con ratio alto

37. `nmap -sV --version-light` – Versión rápida
38. `nmap --open` – Mostrar solo puertos abiertos
39. `nmap -p 22,80,443` – Puertos separados por coma
40. `nmap -p T:80,U:53` – TCP y UDP especificados

🛠️ Opciones de Scripting NSE (41–60)

41. `nmap --script=default` – Scripts por defecto
42. `nmap --script=ssl-heartbleed` – Verificar Heartbleed
43. `nmap --script=auth` – Scripts de autenticación
44. `nmap --script=discovery` – Scripts de descubrimiento
45. `nmap --script=vuln` – Buscar vulnerabilidades
46. `nmap --script=http-enum` – Enumerar servicios web
47. `nmap --script=ftp-anon` – FTP anónimo
48. `nmap --script=smb-os-discovery` – Detección SMB
49. `nmap --script-help=vuln` – Descripción del script
50. `nmap --script-updatedb` – Actualizar base de scripts
51. `nmap --script-trace` – Ver tráfico generado
52. `nmap --script-args 'user=admin,pass=1234'` – Parámetros para scripts
53. `nmap --script http-title` – Obtener títulos web
54. `nmap --script dns-brute` – Bruteforce DNS
55. `nmap --script ssh-auth-methods` – Métodos de autenticación SSH
56. `nmap --script ssl-cert` – Obtener certificado SSL

57. `nmap --script smb-enum-shares` – Listar recursos compartidos
58. `nmap --script smtp-commands` – Comandos SMTP
59. `nmap --script telnet-ntlm-info` – Info NTLM
60. `nmap --script snmp-info` – Información SNMP

⚙️ Opciones Avanzadas (61–80)

61. `nmap --data-length 50` – Añadir padding a paquetes
62. `nmap --max-retries 2` – Número máximo de reintentos
63. `nmap --host-timeout 1m` – Tiempo máximo por host
64. `nmap --scan-delay 1s` – Retardo entre paquetes
65. `nmap --max-rate 100` – Límite de paquetes por segundo
66. `nmap --min-rate 50` – Mínimo de velocidad
67. `nmap --spoof-mac 0` – MAC aleatoria
68. `nmap --badsum` – Generar checksum inválido
69. `nmap -f` – Fragmentar paquetes
70. `nmap --source-port 53` – Puerto fuente especificado
71. `nmap -D RND:10` – Decoys aleatorios
72. `nmap -g 53` – Puerto origen manual
73. `nmap -S 192.168.1.100` – Spoof IP
74. `nmap -e eth0` – Interfaz de red específica
75. `nmap -6` – Escaneo IPv6
76. `nmap --exclude 192.168.1.5` – Excluir IP

77. `nmap --exclude-file lista.txt` – Excluir desde archivo
78. `nmap --packet-trace` – Traza de paquetes
79. `nmap -oN salida.txt` – Guardar en formato normal
80. `nmap -oX salida.xml` – Guardar XML

📋 Salida, Reportes y Logs (81–90)

81. `nmap -oG salida.gnmap` – Formato grepable
82. `nmap -oA todo` – Guardar en todos los formatos
83. `nmap --append-output` – Añadir a archivo
84. `nmap --webxml` – Salida para web
85. `nmap -v -v` – Más información
86. `nmap -d` – Modo debug
87. `nmap --reason` – Mostrar causas
88. `nmap --stats-every 10s` – Ver progreso
89. `nmap --stylesheet hoja.xsl` – Usar XSLT
90. `nmap -oX - | xsltproc hoja.xsl -` – Salida HTML

🔎 Ejemplos Completos (91–110)

91. `nmap -A -T4 192.168.1.1` – Escaneo agresivo rápido
92. `nmap -sS -Pn -T3 10.0.0.1-50` – Escaneo stealth sin ping
93. `nmap -sU -p 53 192.168.1.1` – Escanear DNS por UDP
94. `nmap -sV -p 80,443 --script=http-enum` – Enum web services
95. `nmap -p- -T5 10.10.10.10` – Todos los puertos al máximo

Diego Alexis Villafuerte

96. `nmap -O --osscan-guess 192.168.1.50` – Detección de SO avanzada
97. `nmap --script smb-os-discovery -p445 192.168.1.5` – Info de red SMB
98. `nmap --top-ports 200 --open -iL ips.txt` – Top puertos abiertos en lista
99. `nmap -sC -sV -oA escaneo_red 192.168.1.0/24` – Escaneo completo
100. `nmap -iR 10 -Pn -T4 --script=vuln` – Escaneo aleatorio de vulnerabilidades
101. `nmap -sS --badsum 192.168.1.1` – Técnicas evasivas
102. `nmap --script firewall-bypass -T4 10.10.10.1` – Intento de evadir firewall
103. `nmap -sS --data-length 200 192.168.1.1` – Llenar paquetes para evasión