

# Packet-Level Analysis of Network Reconnaissance Techniques Using Nmap and Wireshark

Author: Frankie Rodriguez Rivera  
Advisor: Dr. Jeffrey Duffany  
Master in Computer Science  
Polytechnic University of Puerto Rico

## Abstract

This project examines network reconnaissance methods, packet-level traffic inspection, and authentication security using Nmap and Wireshark. The study investigates how scanning activities manifest in network traffic and how defenders can identify these patterns. Experiments demonstrated that different scan types produce distinct TCP flag signatures. SYN scans generated half-open attempts, while ACK scans revealed firewall filtering. Authentication analysis showed weak credentials can be compromised rapidly. Results support defense-in-depth combining network visibility, packet analysis, and strong authentication.

## Introduction

As digital systems become more interconnected, cybersecurity is a central concern. Many cyberattacks begin with reconnaissance, where attackers collect details about possible targets. This project examines how reconnaissance tools generate observable network traffic patterns that defenders can use for early detection. The study combines Nmap scanning with Wireshark packet capture to compare theoretical expectations with real network behavior.

## Background

Modern networks are a common starting point for cyberattacks because exposed services and traffic patterns can be observed remotely. Reconnaissance involves checking which hosts are reachable, which ports are open, and what services are exposed. Nmap is widely used for host discovery, port scanning, service enumeration, and OS fingerprinting, supporting several scan types that behave differently at the transport layer. Wireshark enables researchers to capture and analyze packets produced during scans and routine traffic, providing concrete data such as TCP flag patterns and protocol distribution. Together, these tools allow security professionals to study reconnaissance as a protocol exchange rather than simply reviewing scan output summaries.

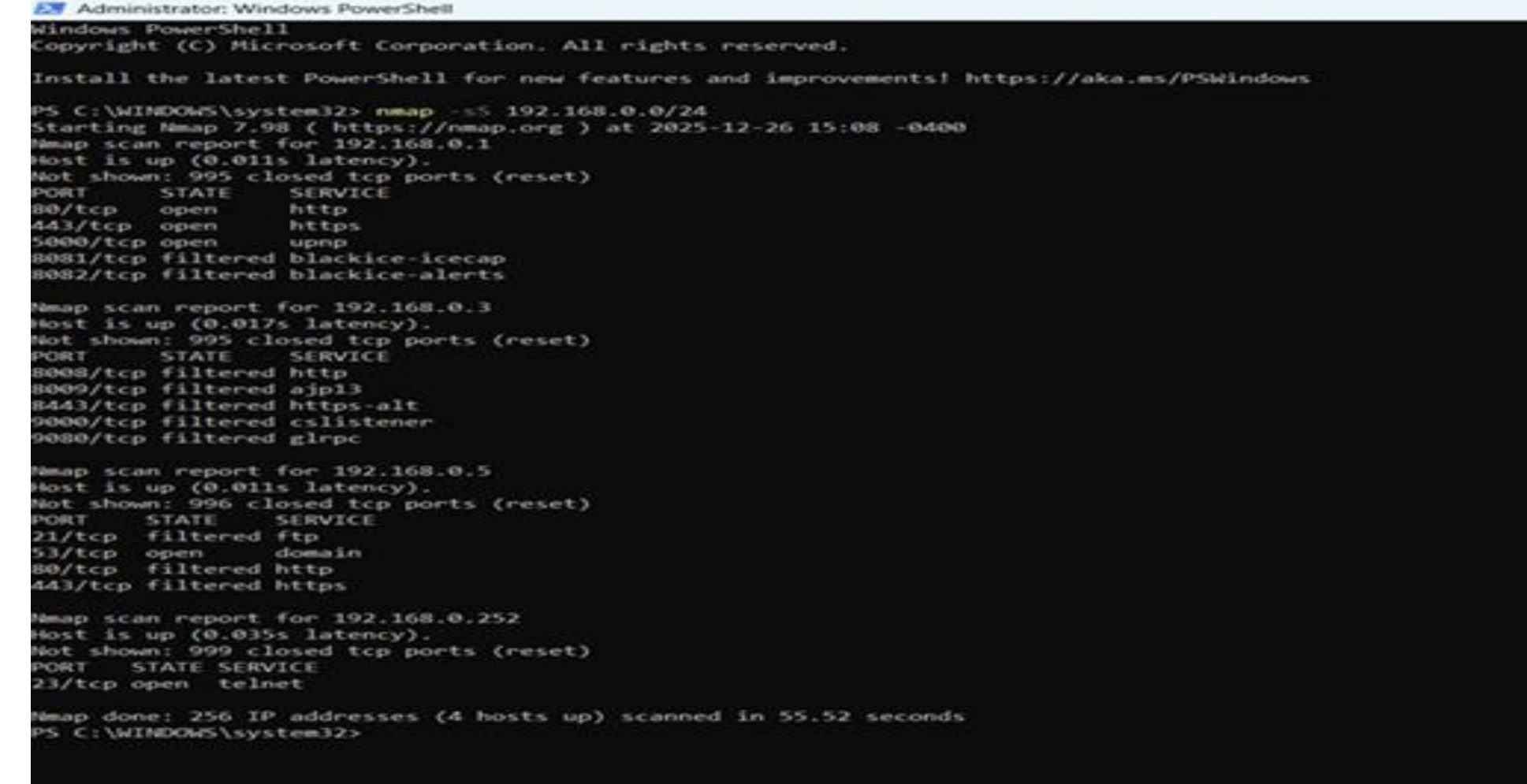
## Problem

Network reconnaissance is often the first step in a cyberattack but is frequently missed by defenders because it does not cause immediate visible disruption. Scanning methods produce different packet-level signatures in TCP control flags and protocol responses. Without packet-level inspection, it is difficult to distinguish host discovery from port scanning, firewall probing, or OS fingerprinting. Additionally, weak authentication controls significantly increased risk after reconnaissance identifies reachable services. This project addresses the gap in packet-level understanding of reconnaissance traffic and its relationship to authentication vulnerabilities.

## Methodology

The project followed four phases in a controlled environment:

1. Network Reconnaissance Using Nmap: Host discovery scans identified active devices on subnet 192.168.0.0/24. TCP SYN scanning revealed open ports (HTTP/80, HTTPS/443, UPnP/5000). Multiple scan types were compared: SYN, ACK, fast, and aggressive scans. External validation used [scanme.nmap.org](http://scanme.nmap.org).



```
PS C:\Users\Frankie> nmap -sS -iL 192.168.0.0/24
Nmap scan report for 192.168.0.0/24
Host: 192.168.0.0 (192.168.0.0)
Host: 192.168.0.1 (192.168.0.1)
Host: 192.168.0.2 (192.168.0.2)
Host: 192.168.0.3 (192.168.0.3)
Host: 192.168.0.4 (192.168.0.4)
Host: 192.168.0.5 (192.168.0.5)
Host: 192.168.0.6 (192.168.0.6)
Host: 192.168.0.7 (192.168.0.7)
Host: 192.168.0.8 (192.168.0.8)
Host: 192.168.0.9 (192.168.0.9)
Host: 192.168.0.10 (192.168.0.10)
Host: 192.168.0.11 (192.168.0.11)
Host: 192.168.0.12 (192.168.0.12)
Host: 192.168.0.13 (192.168.0.13)
Host: 192.168.0.14 (192.168.0.14)
Host: 192.168.0.15 (192.168.0.15)
Host: 192.168.0.16 (192.168.0.16)
Host: 192.168.0.17 (192.168.0.17)
Host: 192.168.0.18 (192.168.0.18)
Host: 192.168.0.19 (192.168.0.19)
Host: 192.168.0.20 (192.168.0.20)
Host: 192.168.0.21 (192.168.0.21)
Host: 192.168.0.22 (192.168.0.22)
Host: 192.168.0.23 (192.168.0.23)
Host: 192.168.0.24 (192.168.0.24)
Nmap scan report for 192.168.0.24
Host: 192.168.0.24 (192.168.0.24)
Nmap scan report for 192.168.0.25
Host: 192.168.0.25 (192.168.0.25)
Nmap scan report for 192.168.0.26
Host: 192.168.0.26 (192.168.0.26)
Nmap scan report for 192.168.0.27
Host: 192.168.0.27 (192.168.0.27)
Nmap scan report for 192.168.0.28
Host: 192.168.0.28 (192.168.0.28)
Nmap scan report for 192.168.0.29
Host: 192.168.0.29 (192.168.0.29)
Nmap scan report for 192.168.0.30
Host: 192.168.0.30 (192.168.0.30)
Nmap scan report for 192.168.0.31
Host: 192.168.0.31 (192.168.0.31)
Nmap scan report for 192.168.0.32
Host: 192.168.0.32 (192.168.0.32)
Nmap scan report for 192.168.0.33
Host: 192.168.0.33 (192.168.0.33)
Nmap scan report for 192.168.0.34
Host: 192.168.0.34 (192.168.0.34)
Nmap scan report for 192.168.0.35
Host: 192.168.0.35 (192.168.0.35)
Nmap scan report for 192.168.0.36
Host: 192.168.0.36 (192.168.0.36)
Nmap scan report for 192.168.0.37
Host: 192.168.0.37 (192.168.0.37)
Nmap scan report for 192.168.0.38
Host: 192.168.0.38 (192.168.0.38)
Nmap scan report for 192.168.0.39
Host: 192.168.0.39 (192.168.0.39)
Nmap scan report for 192.168.0.40
Host: 192.168.0.40 (192.168.0.40)
Nmap scan report for 192.168.0.41
Host: 192.168.0.41 (192.168.0.41)
Nmap scan report for 192.168.0.42
Host: 192.168.0.42 (192.168.0.42)
Nmap scan report for 192.168.0.43
Host: 192.168.0.43 (192.168.0.43)
Nmap scan report for 192.168.0.44
Host: 192.168.0.44 (192.168.0.44)
Nmap scan report for 192.168.0.45
Host: 192.168.0.45 (192.168.0.45)
Nmap scan report for 192.168.0.46
Host: 192.168.0.46 (192.168.0.46)
Nmap scan report for 192.168.0.47
Host: 192.168.0.47 (192.168.0.47)
Nmap scan report for 192.168.0.48
Host: 192.168.0.48 (192.168.0.48)
Nmap scan report for 192.168.0.49
Host: 192.168.0.49 (192.168.0.49)
Nmap scan report for 192.168.0.50
Host: 192.168.0.50 (192.168.0.50)
Nmap scan report for 192.168.0.51
Host: 192.168.0.51 (192.168.0.51)
Nmap scan report for 192.168.0.52
Host: 192.168.0.52 (192.168.0.52)
Nmap scan report for 192.168.0.53
Host: 192.168.0.53 (192.168.0.53)
Nmap scan report for 192.168.0.54
Host: 192.168.0.54 (192.168.0.54)
Nmap scan report for 192.168.0.55
Host: 192.168.0.55 (192.168.0.55)
Nmap scan report for 192.168.0.56
Host: 192.168.0.56 (192.168.0.56)
Nmap scan report for 192.168.0.57
Host: 192.168.0.57 (192.168.0.57)
Nmap scan report for 192.168.0.58
Host: 192.168.0.58 (192.168.0.58)
Nmap scan report for 192.168.0.59
Host: 192.168.0.59 (192.168.0.59)
Nmap scan report for 192.168.0.60
Host: 192.168.0.60 (192.168.0.60)
Nmap scan report for 192.168.0.61
Host: 192.168.0.61 (192.168.0.61)
Nmap scan report for 192.168.0.62
Host: 192.168.0.62 (192.168.0.62)
Nmap scan report for 192.168.0.63
Host: 192.168.0.63 (192.168.0.63)
Nmap scan report for 192.168.0.64
Host: 192.168.0.64 (192.168.0.64)
Nmap scan report for 192.168.0.65
Host: 192.168.0.65 (192.168.0.65)
Nmap scan report for 192.168.0.66
Host: 192.168.0.66 (192.168.0.66)
Nmap scan report for 192.168.0.67
Host: 192.168.0.67 (192.168.0.67)
Nmap scan report for 192.168.0.68
Host: 192.168.0.68 (192.168.0.68)
Nmap scan report for 192.168.0.69
Host: 192.168.0.69 (192.168.0.69)
Nmap scan report for 192.168.0.70
Host: 192.168.0.70 (192.168.0.70)
Nmap scan report for 192.168.0.71
Host: 192.168.0.71 (192.168.0.71)
Nmap scan report for 192.168.0.72
Host: 192.168.0.72 (192.168.0.72)
Nmap scan report for 192.168.0.73
Host: 192.168.0.73 (192.168.0.73)
Nmap scan report for 192.168.0.74
Host: 192.168.0.74 (192.168.0.74)
Nmap scan report for 192.168.0.75
Host: 192.168.0.75 (192.168.0.75)
Nmap scan report for 192.168.0.76
Host: 192.168.0.76 (192.168.0.76)
Nmap scan report for 192.168.0.77
Host: 192.168.0.77 (192.168.0.77)
Nmap scan report for 192.168.0.78
Host: 192.168.0.78 (192.168.0.78)
Nmap scan report for 192.168.0.79
Host: 192.168.0.79 (192.168.0.79)
Nmap scan report for 192.168.0.80
Host: 192.168.0.80 (192.168.0.80)
Nmap scan report for 192.168.0.81
Host: 192.168.0.81 (192.168.0.81)
Nmap scan report for 192.168.0.82
Host: 192.168.0.82 (192.168.0.82)
Nmap scan report for 192.168.0.83
Host: 192.168.0.83 (192.168.0.83)
Nmap scan report for 192.168.0.84
Host: 192.168.0.84 (192.168.0.84)
Nmap scan report for 192.168.0.85
Host: 192.168.0.85 (192.168.0.85)
Nmap scan report for 192.168.0.86
Host: 192.168.0.86 (192.168.0.86)
Nmap scan report for 192.168.0.87
Host: 192.168.0.87 (192.168.0.87)
Nmap scan report for 192.168.0.88
Host: 192.168.0.88 (192.168.0.88)
Nmap scan report for 192.168.0.89
Host: 192.168.0.89 (192.168.0.89)
Nmap scan report for 192.168.0.90
Host: 192.168.0.90 (192.168.0.90)
Nmap scan report for 192.168.0.91
Host: 192.168.0.91 (192.168.0.91)
Nmap scan report for 192.168.0.92
Host: 192.168.0.92 (192.168.0.92)
Nmap scan report for 192.168.0.93
Host: 192.168.0.93 (192.168.0.93)
Nmap scan report for 192.168.0.94
Host: 192.168.0.94 (192.168.0.94)
Nmap scan report for 192.168.0.95
Host: 192.168.0.95 (192.168.0.95)
Nmap scan report for 192.168.0.96
Host: 192.168.0.96 (192.168.0.96)
Nmap scan report for 192.168.0.97
Host: 192.168.0.97 (192.168.0.97)
Nmap scan report for 192.168.0.98
Host: 192.168.0.98 (192.168.0.98)
Nmap scan report for 192.168.0.99
Host: 192.168.0.99 (192.168.0.99)
Nmap scan report for 192.168.0.100
Host: 192.168.0.100 (192.168.0.100)
Nmap scan report for 192.168.0.101
Host: 192.168.0.101 (192.168.0.101)
Nmap scan report for 192.168.0.102
Host: 192.168.0.102 (192.168.0.102)
Nmap scan report for 192.168.0.103
Host: 192.168.0.103 (192.168.0.103)
Nmap scan report for 192.168.0.104
Host: 192.168.0.104 (192.168.0.104)
Nmap scan report for 192.168.0.105
Host: 192.168.0.105 (192.168.0.105)
Nmap scan report for 192.168.0.106
Host: 192.168.0.106 (192.168.0.106)
Nmap scan report for 192.168.0.107
Host: 192.168.0.107 (192.168.0.107)
Nmap scan report for 192.168.0.108
Host: 192.168.0.108 (192.168.0.108)
Nmap scan report for 192.168.0.109
Host: 192.168.0.109 (192.168.0.109)
Nmap scan report for 192.168.0.110
Host: 192.168.0.110 (192.168.0.110)
Nmap scan report for 192.168.0.111
Host: 192.168.0.111 (192.168.0.111)
Nmap scan report for 192.168.0.112
Host: 192.168.0.112 (192.168.0.112)
Nmap scan report for 192.168.0.113
Host: 192.168.0.113 (192.168.0.113)
Nmap scan report for 192.168.0.114
Host: 192.168.0.114 (192.168.0.114)
Nmap scan report for 192.168.0.115
Host: 192.168.0.115 (192.168.0.115)
Nmap scan report for 192.168.0.116
Host: 192.168.0.116 (192.168.0.116)
Nmap scan report for 192.168.0.117
Host: 192.168.0.117 (192.168.0.117)
Nmap scan report for 192.168.0.118
Host: 192.168.0.118 (192.168.0.118)
Nmap scan report for 192.168.0.119
Host: 192.168.0.119 (192.168.0.119)
Nmap scan report for 192.168.0.120
Host: 192.168.0.120 (192.168.0.120)
Nmap scan report for 192.168.0.121
Host: 192.168.0.121 (192.168.0.121)
Nmap scan report for 192.168.0.122
Host: 192.168.0.122 (192.168.0.122)
Nmap scan report for 192.168.0.123
Host: 192.168.0.123 (192.168.0.123)
Nmap scan report for 192.168.0.124
Host: 192.168.0.124 (192.168.0.124)
Nmap scan report for 192.168.0.125
Host: 192.168.0.125 (192.168.0.125)
Nmap scan report for 192.168.0.126
Host: 192.168.0.126 (192.168.0.126)
Nmap scan report for 192.168.0.127
Host: 192.168.0.127 (192.168.0.127)
Nmap scan report for 192.168.0.128
Host: 192.168.0.128 (192.168.0.128)
Nmap scan report for 192.168.0.129
Host: 192.168.0.129 (192.168.0.129)
Nmap scan report for 192.168.0.130
Host: 192.168.0.130 (192.168.0.130)
Nmap scan report for 192.168.0.131
Host: 192.168.0.131 (192.168.0.131)
Nmap scan report for 192.168.0.132
Host: 192.168.0.132 (192.168.0.132)
Nmap scan report for 192.168.0.133
Host: 192.168.0.133 (192.168.0.133)
Nmap scan report for 192.168.0.134
Host: 192.168.0.134 (192.168.0.134)
Nmap scan report for 192.168.0.135
Host: 192.168.0.135 (192.168.0.135)
Nmap scan report for 192.168.0.136
Host: 192.168.0.136 (192.168.0.136)
Nmap scan report for 192.168.0.137
Host: 192.168.0.137 (192.168.0.137)
Nmap scan report for 192.168.0.138
Host: 192.168.0.138 (192.168.0.138)
Nmap scan report for 192.168.0.139
Host: 192.168.0.139 (192.168.0.139)
Nmap scan report for 192.168.0.140
Host: 192.168.0.140 (192.168.0.140)
Nmap scan report for 192.168.0.141
Host: 192.168.0.141 (192.168.0.141)
Nmap scan report for 192.168.0.142
Host: 192.168.0.142 (192.168.0.142)
Nmap scan report for 192.168.0.143
Host: 192.168.0.143 (192.168.0.143)
Nmap scan report for 192.168.0.144
Host: 192.168.0.144 (192.168.0.144)
Nmap scan report for 192.168.0.145
Host: 192.168.0.145 (192.168.0.145)
Nmap scan report for 192.168.0.146
Host: 192.168.0.146 (192.168.0.146)
Nmap scan report for 192.168.0.147
Host: 192.168.0.147 (192.168.0.147)
Nmap scan report for 192.168.0.148
Host: 192.168.0.148 (192.168.0.148)
Nmap scan report for 192.168.0.149
Host: 192.168.0.149 (192.168.0.149)
Nmap scan report for 192.168.0.150
Host: 192.168.0.150 (192.168.0.150)
Nmap scan report for 192.168.0.151
Host: 192.168.0.151 (192.168.0.151)
Nmap scan report for 192.168.0.152
Host: 192.168.0.152 (192.168.0.152)
Nmap scan report for 192.168.0.153
Host: 192.168.0.153 (192.168.0.153)
Nmap scan report for 192.168.0.154
Host: 192.168.0.154 (192.168.0.154)
Nmap scan report for 192.168.0.155
Host: 192.168.0.155 (192.168.0.155)
Nmap scan report for 192.168.0.156
Host: 192.168.0.156 (192.168.0.156)
Nmap scan report for 192.168.0.157
Host: 192.168.0.157 (192.168.0.157)
Nmap scan report for 192.168.0.158
Host: 192.168.0.158 (192.168.0.158)
Nmap scan report for 192.168.0.159
Host: 192.168.0.159 (192.168.0.159)
Nmap scan report for 192.168.0.160
Host: 192.168.0.160 (192.168.0.160)
Nmap scan report for 192.168.0.161
Host: 192.168.0.161 (192.168.0.161)
Nmap scan report for 192.168.0.162
Host: 192.168.0.162 (192.168.0.162)
Nmap scan report for 192.168.0.163
Host: 192.168.0.163 (192.168.0.163)
Nmap scan report for 192.168.0.164
Host: 192.168.0.164 (192.168.0.164)
Nmap scan report for 192.168.0.165
Host: 192.168.0.165 (192.168.0.165)
Nmap scan report for 192.168.0.166
Host: 192.168.0.166 (192.168.0.166)
Nmap scan report for 192.168.0.167
Host: 192.168.0.167 (192.168.0.167)
Nmap scan report for 192.168.0.168
Host: 192.168.0.168 (192.168.0.168)
Nmap scan report for 192.168.0.169
Host: 192.168.0.169 (192.168.0.169)
Nmap scan report for 192.168.0.170
Host: 192.168.0.170 (192.168.0.170)
Nmap scan report for 192.168.0.171
Host: 192.168.0.171 (192.168.0.171)
Nmap scan report for 192.168.0.172
Host: 192.168.0.172 (192.168.0.172)
Nmap scan report for 192.168.0.173
Host: 192.168.0.173 (192.168.0.173)
Nmap scan report for 192.168.0.174
Host: 192.168.0.174 (192.168.0.174)
Nmap scan report for 192.168.0.175
Host: 192.168.0.175 (192.168.0.175)
Nmap scan report for 192.168.0.176
Host: 192.168.0.176 (192.168.0.176)
Nmap scan report for 192.168.0.177
Host: 192.168.0.177 (192.168.0.177)
Nmap scan report for 192.168.0.178
Host: 192.168.0.178 (192.168.0.178)
Nmap scan report for 192.168.0.179
Host: 192.168.0.179 (192.168.0.179)
Nmap scan report for 192.168.0.180
Host: 192.168.0.180 (192.168.0.180)
Nmap scan report for 192.168.0.181
Host: 192.168.0.181 (192.168.0.181)
Nmap scan report for 192.168.0.182
Host: 192.168.0.182 (192.168.0.182)
Nmap scan report for 192.168.0.183
Host: 192.168.0.183 (192.168.0.183)
Nmap scan report for 192.168.0.184
Host: 192.168.0.184 (192.168.0.184)
Nmap scan report for 192.168.0.185
Host: 192.168.0.185 (192.168.0.185)
Nmap scan report for 192.168.0.186
Host: 192.168.0.186 (192.168.0.186)
Nmap scan report for 192.168.0.187
Host: 192.168.0.187 (192.168.0.187)
Nmap scan report for 192.168.0.188
Host: 192.168.0.188 (192.168.0.188)
Nmap scan report for 192.168.0.189
Host: 192.168.0.189 (192.168.0.189)
Nmap scan report for 192.168.0.190
Host: 192.168.0.190 (192.168.0.190)
Nmap scan report for 192.168.0.191
Host: 192.168.0.191 (192.168.0.191)
Nmap scan report for 192.168.0.192
Host: 192.168.0.192 (192.168.0.192)
Nmap scan report for 192.168.0.193
Host: 192.168.0.193 (192.168.0.193)
Nmap scan report for 192.168.0.194
Host: 192.168.0.194 (192.168.0.194)
Nmap scan report for 192.168.0.195
Host: 192.168.0.195 (192.168.0.195)
Nmap scan report for 192.168.0.196
Host: 192.168.0.196 (192.168.0.196)
Nmap scan report for 192.168.0.197
Host: 192.168.0.197 (192.168.0.197)
Nmap scan report for 192.168.0.198
Host: 192.168.0.198 (192.168.0.198)
Nmap scan report for 192.168.0.199
Host: 192.168.0.199 (192.168.0.199)
Nmap scan report for 192.168.0.200
Host: 192.168.0.200 (192.168.0.200)
Nmap scan report for 192.168.0.201
Host: 192.168.0.201 (192.168.0.201)
Nmap scan report for 192.168.0.202
Host: 192.168.0.202 (192.168.0.202)
Nmap scan report for 192.168.0.203
Host: 192.168.0.203 (192.168.0.203)
Nmap scan report for 192.168.0.204
Host: 192.168.0.204 (192.168.0.204)
Nmap scan report for 192.168.0.205
Host: 192.168.0.205 (192.168.0.205)
Nmap scan report for 192.168.0.206
Host: 192.168.0.206 (192.168.0.206)
Nmap scan report for 192.168.0.207
Host: 192.168.0.207 (192.168.0.207)
Nmap scan report for 192.168.0.208
Host: 192.168.0.208 (192.168.0.208)
Nmap scan report for 192.168.0.209
Host: 192.168.0.209 (192.168.0.209)
Nmap scan report for 192.168.0.210
Host: 192.168.0.210 (192.168.0.210)
Nmap scan report for 192.168.0.211
Host: 192.168.0.211 (192.168.0.211)
Nmap scan report for 192.168.0.212
Host: 192.168.0.212 (192.168.0.212)
Nmap scan report for 192.168.0.213
Host: 192.168.0.213 (192.168.0.213)
Nmap scan report for 192.168.0.214
Host: 192.168.0.214 (192.168.0.214)
Nmap scan report for 192.168.0.215
Host: 192.168.0.215 (192.168.0.215)
Nmap scan report for 192.168.0.216
Host: 192.168.0.216 (192.168.0.216)
Nmap scan report for 192.168.0.217
Host: 192.168.0.217 (192.168.0.217)
Nmap scan report for 192.168.0.218
Host: 192.168.0.218 (192.168.0.218)
Nmap scan report for 192.168.0.219
Host: 192.168.0.219 (192.168.0.219)
Nmap scan report for 192.168.0.220
Host: 192.168.0.220 (192.168.0.220)
Nmap scan report for 192.168.0.221
Host: 192.168.0.221 (192.168.0.221)
Nmap scan report for 192.168.0.222
Host: 192.168.0.222 (192.168.0.222)
Nmap scan report for 192.168.0.223
Host: 192.168.0.223 (192.168.0.223)
Nmap scan report for 192.168.0.224
Host: 192.168.0.224 (192.168.0.224)
Nmap scan report for 192.168.0.225
Host: 192.168.0.225 (192.168.0.225)
Nmap scan report for 192.168.0.226
Host: 192.168.0.226 (192.168.0.226)
Nmap scan report for 192.168.0.227
Host: 192.168.0.227 (192.168.0.227)
Nmap scan report for 192.168.0.228
Host: 192.168.0.228 (192.168.0.228)
Nmap scan report for 192.168.0.229
Host: 192.168.0.229 (192.168.0.22
```