任务四: Nmap 扫描

1. 主机探测

使用命令: nmap -sP 172.18.1.207

```
C:\Users\Franpin>nmap -sP 172.18.1.207
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:33 中国标准时间
Nmap scan report for DESKTOP-FBGS9FI.1an (172.18.1.207)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

2. 端口扫描

使用命令: nmap -p 5000-8088 172.18.1.207

扫描端口 5000-8088

```
C:\Users\Franpin>nmap -p 5000-8088 172.18.1.207
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:55 中国标准时间
Nmap scan report for DESKTOP-FBGS9FI.1an (172.18.1.207)
Host is up (0.000061s latency).
Not shown: 3084 closed tcp ports (reset)
PORT STATE SERVICE
5040/tcp open unknown
5357/tcp open wsdapi
7680/tcp open pando-pub
8082/tcp open blackice-alerts
8083/tcp open us-srv

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

wireshark 抓包:

No.	Time	Source	Destination	Protocol	Length Info
Tr.	9 0.524006	172.18.1.207	172.18.1.207	TCP	48 56186 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
L	10 0.524096	172.18.1.207	172.18.1.207	TCP	44 5900 → 56186 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
	11 0.525264	172.18.1.207	172.18.1.207	TCP	48 56186 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	12 0.525356	172.18.1.207	172.18.1.207	TCP	44 8080 → 56186 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
	13 0.525371	172.18.1.207	172.18.1.207	TCP	48 56186 → 5409 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	14 0.525419	172.18.1.207	172.18.1.207	TCP	44 5409 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	15 0.525432	172.18.1.207	172.18.1.207	TCP	48 56186 → 6589 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	16 0.525469	172.18.1.207	172.18.1.207	TCP	44 6589 → 56186 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
	17 0.525478	172.18.1.207	172.18.1.207	TCP	48 56186 → 6608 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	18 0.525511	172.18.1.207	172.18.1.207	TCP	44 6608 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	19 0.525519	172.18.1.207	172.18.1.207	TCP	48 56186 → 8059 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	20 0.525552	172.18.1.207	172.18.1.207	TCP	44 8059 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	21 0.525560	172.18.1.207	172.18.1.207	TCP	48 56186 → 5731 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	22 0.525592	172.18.1.207	172.18.1.207	TCP	44 5731 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	23 0.525600	172.18.1.207	172.18.1.207	TCP	48 56186 → 6839 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	24 0.525636	172.18.1.207	172.18.1.207	TCP	44 6839 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	25 0.526238	172.18.1.207	172.18.1.207	TCP	48 56186 → 7620 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	26 0.526307	172.18.1.207	172.18.1.207	TCP	44 7620 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	27 0.526316	172.18.1.207	172.18.1.207	TCP	48 56186 → 6886 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	28 0.526351	172.18.1.207	172.18.1.207	TCP	44 6886 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	29 0.526680	172.18.1.207	172.18.1.207	TCP	48 56186 → 5937 [SYN] Seg=0 Win=1024 Len=0 MSS=1460

3. 操作系统扫描

使用命令: nmap -O 172.18.1.207

```
C:\Users\Franpin>nmap -0 172.18.1.207
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:35 中国标准时间
Nmap scan report for DESKTOP-FBGS9FI.1an (172.18.1.207)
Host is up (0.00077s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open microsoft-ds
5357/tcp open wsdapi
8082/tcp open blackice-alerts
8083/tcp open us-srv
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
```

Wireshark 抓包:

No.	Time	Source	Destination	Protocol	Protocol Length Info	
	82 3.624802	172.18.1.207	172.18.1.207	TCP	48 58375 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	83 3.624842	172.18.1.207	172.18.1.207	TCP	44 21 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
	84 3.624851	172.18.1.207	172.18.1.207	TCP	48 58375 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	85 3.624930	172.18.1.207	172.18.1.207	TCP	48 135 → 58375 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=65495	
	86 3.624939	172.18.1.207	172.18.1.207	TCP	44 58375 → 135 [RST] Seq=1 Win=0 Len=0	
	87 3.624955	172.18.1.207	172.18.1.207	TCP	48 58375 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	88 3.624990	172.18.1.207	172.18.1.207	TCP	44 8080 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
	89 3.624998	172.18.1.207	172.18.1.207	TCP	48 58375 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	90 3.625030	172.18.1.207	172.18.1.207	TCP	44 256 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
	91 3.625038	172.18.1.207	172.18.1.207	TCP	48 58375 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	92 3.625069	172.18.1.207	172.18.1.207	TCP	44 143 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
T)	93 3.625077	172.18.1.207	172.18.1.207	TCP	48 58375 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	94 3.625129	172.18.1.207	172.18.1.207	TCP	48 445 + 58375 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=65495	
	95 3.625137	172.18.1.207	172.18.1.207	TCP	44 58375 → 445 [RST] Seq=1 Win=0 Len=0	
N.	96 3.625149	172.18.1.207	172.18.1.207	TCP	48 58375 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	97 3.625183	172.18.1.207	172.18.1.207	TCP	44 5900 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
	98 3.625191	172.18.1.207	172.18.1.207	TCP	48 58375 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	99 3.625223	172.18.1.207	172.18.1.207	TCP	44 113 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
	100 3.625231	172.18.1.207	172.18.1.207	TCP	48 58375 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	101 3.625262	172.18.1.207	172.18.1.207	TCP	44 110 → 58375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
	102 3.625561	172.18.1.207	172.18.1.207	TCP	48 58375 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
	103 3.625609	172.18.1.207	172.18.1.207	TCP	44 23 → 58375 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0	

4. 服务识别

使用命令: nmap -sV 172.18.1.207

```
C:\Users\Franpin>nmap -sV 172.18.1.207

Starting Nmap 7.92 (https://nmap.org ) at 2022-04-03 11:00 中国标准时间
Nmap scan report for DESKTOP-FBGS9FI.1an (172.18.1.207)
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8082/tcp open us-srv?
```

Wireshark 抓包:

138 53.039631	172.18.1.207	172.18.1.207	TCP	48 54029 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139 53.040049	172.18.1.207	172.18.1.207	TCP	44 5900 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140 53.040183	172.18.1.207	172.18.1.207	TCP	48 54029 + 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
141 53.040247	172.18.1.207	172.18.1.207	TCP	44 113 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142 53.040260	172.18.1.207	172.18.1.207	TCP	48 54029 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
143 53.040300	172.18.1.207	172.18.1.207	TCP	44 993 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144 53.040310	172.18.1.207	172.18.1.207	TCP	48 54029 + 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
L 145 53.040347	172.18.1.207	172.18.1.207	TCP	44 21 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146 53.040355	172.18.1.207	172.18.1.207	TCP	48 54029 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
147 53.040398	172.18.1.207	172.18.1.207	TCP	44 8888 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
148 53.040407	172.18.1.207	172.18.1.207	TCP	48 54029 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
149 53.040444	172.18.1.207	172.18.1.207	TCP	44 554 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
150 53.040453	172.18.1.207	172.18.1.207	TCP	48 54029 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
151 53.040579	172.18.1.207	172.18.1.207	TCP	48 135 → 54029 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=65495
152 53.040600	172.18.1.207	172.18.1.207	TCP	48 54029 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
153 53.040645	172.18.1.207	172.18.1.207	TCP	44 54029 → 135 [RST] Seq=1 Win=0 Len=0
154 53.040683	172.18.1.207	172.18.1.207	TCP	44 587 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 53.040738	172.18.1.207	172.18.1.207	TCP	48 54029 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
156 53.040802	172.18.1.207	172.18.1.207	TCP	44 110 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
157 53.041388	172.18.1.207	172.18.1.207	TCP	48 54029 + 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
158 53.041461	172.18.1.207	172.18.1.207	TCP	44 1720 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159 53.041476	172.18.1.207	172.18.1.207	TCP	48 54029 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
160 53.041520	172.18.1.207	172.18.1.207	TCP	44 1723 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 53.041530	172.18.1.207	172.18.1.207	TCP	48 54029 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
162 53.041575	172.18.1.207	172.18.1.207	TCP	44 1025 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
163 53.041584	172.18.1.207	172.18.1.207	TCP	48 54029 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
164 53.041665	172.18.1.207	172.18.1.207	TCP	48 139 → 54029 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
165 53.041681	172.18.1.207	172.18.1.207	TCP	48 54029 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
166 53.041722	172.18.1.207	172.18.1.207	TCP	44 54029 → 139 [RST] Seq=1 Win=0 Len=0
167 53.041757	172.18.1.207	172.18.1.207	TCP	44 8080 → 54029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 53.041777	172.18.1.207	172.18.1.207	TCP	48 54029 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

5. 漏洞扫描

使用命令: nmap -p- -sV --version-all --script vuln 172.18.1.207

wireshark 抓包:

100 105 515001	470 40 4 207	472 40 4 207	TCD	40 54540 443 55393 5 0 10 4004 1 0 955 4450
192 105.616804	172.18.1.207	172.18.1.207	TCP	48 54619 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
193 105.616846	172.18.1.207	172.18.1.207	TCP	44 443 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194 105.616856	172.18.1.207	172.18.1.207	TCP	48 54619 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
195 105.616891	172.18.1.207	172.18.1.207	TCP	44 111 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196 105.616900	172.18.1.207	172.18.1.207	TCP	48 54619 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
197 105.616934	172.18.1.207	172.18.1.207	TCP	44 21 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
198 105.616942	172.18.1.207	172.18.1.207	TCP	48 54619 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
199 105.616976	172.18.1.207	172.18.1.207	TCP	44 1025 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200 105.616985	172.18.1.207	172.18.1.207	TCP	48 54619 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
201 105.617018	172.18.1.207	172.18.1.207	TCP	44 53 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
202 105.617027	172.18.1.207	172.18.1.207	TCP	48 54619 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
203 105.617060	172.18.1.207	172.18.1.207	TCP	44 1723 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
204 105.617068	172.18.1.207	172.18.1.207	TCP	48 54619 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
205 105.617101	172.18.1.207	172.18.1.207	TCP	44 23 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206 105.617109	172.18.1.207	172.18.1.207	TCP	48 54619 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
207 105.617142	172.18.1.207	172.18.1.207	TCP	44 256 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
208 105.617151	172.18.1.207	172.18.1.207	TCP	48 54619 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
209 105.617185	172.18.1.207	172.18.1.207	TCP	44 113 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210 105.617603	172.18.1.207	172.18.1.207	TCP	48 54619 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
211 105.617656	172.18.1.207	172.18.1.207	TCP	44 80 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
212 105.617668	172.18.1.207	172.18.1.207	TCP	48 54619 → 110 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
213 105.617706	172.18.1.207	172.18.1.207	TCP	44 110 → 54619 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214 105.617715	172.18.1.207	172.18.1.207	TCP	48 54619 → 139 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
215 105.617788	172.18.1.207	172.18.1.207	TCP	48 139 → 54619 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
216 105.617804	172.18.1.207	172.18.1.207	TCP	48 54619 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
217 105.617844	172.18.1.207	172.18.1.207	TCP	44 54619 → 139 [RST] Seg=1 Win=0 Len=0
218 105.617898	172.18.1.207	172.18.1.207	TCP	48 445 → 54619 [SYN, ACK] Seg=0 Ack=1 Win=64240 Len=0 MSS=65495
219 105.617913	172.18.1.207	172.18.1.207	TCP	44 54619 → 445 [RST] Seg=1 Win=0 Len=0
220 105.617965	172.18.1.207	172.18.1.207	TCP	48 54619 → 8888 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
221 105.618019	172.18.1.207	172.18.1.207	TCP	44 8888 + 54619 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
222 105,618030	172,18,1,207	172.18.1.207	TCP	48 54619 → 22 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
223 105.618069	172.18.1.207	172.18.1.207	TCP	44 22 → 54619 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
224 105.618078	172.18.1.207	172.18.1.207	TCP	48 54619 → 8080 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
225 105.618114	172.18.1.207	172.18.1.207	TCP	44 8080 → 54619 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
226 105,618123	172.18.1.207	172,18,1,207	TCP	48 54619 → 25 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
L 227 105.618160	172.18.1.207	172.18.1.207	TCP	44 25 → 54619 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
228 105,618169	172.18.1.207	172.18.1.207	TCP	48 54619 → 3389 [SYN] Seg=0 Win=1024 Len=0 MSS=1460
				C