

Assignment 2

Name: Tarek Mohamed Nawara

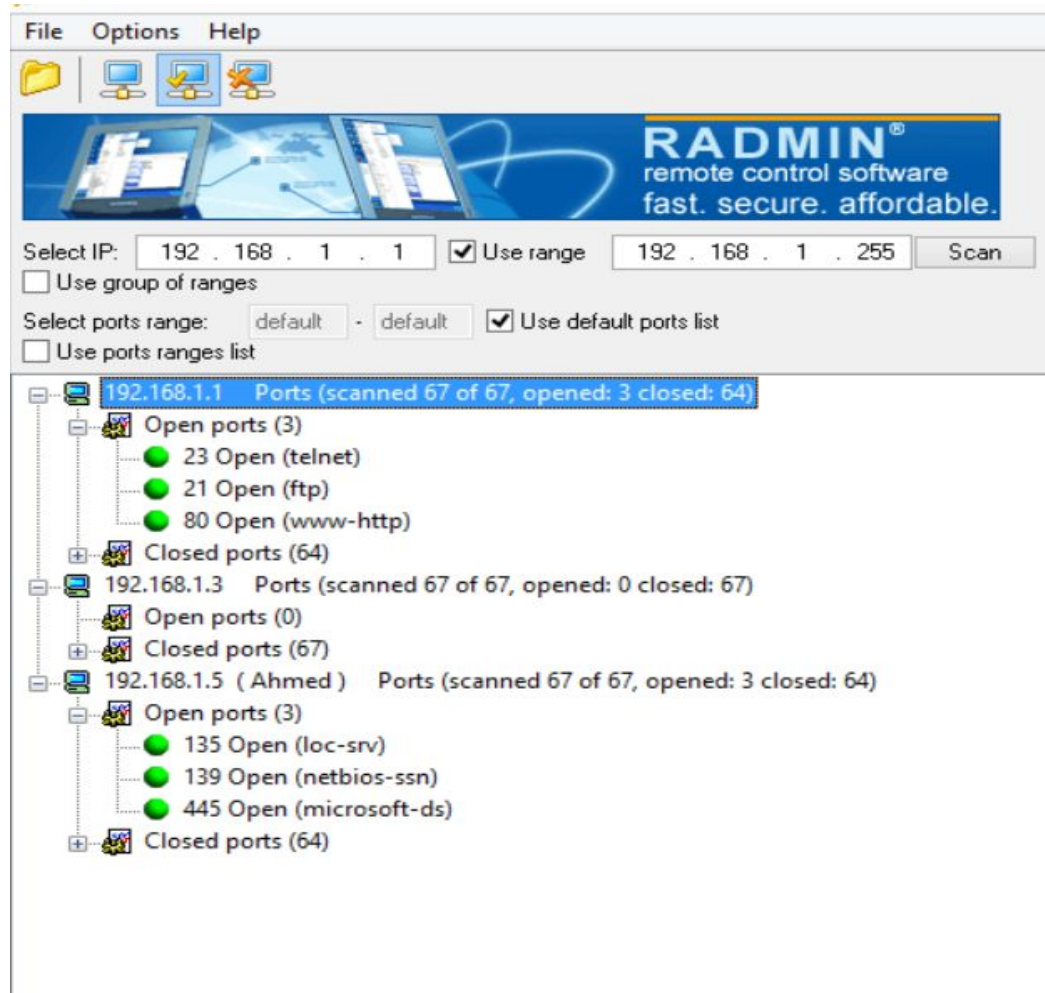
Number: 38

Problem one

Use advanced port scanner to scan one to three hosts on your local net to find their open ports.

Answer

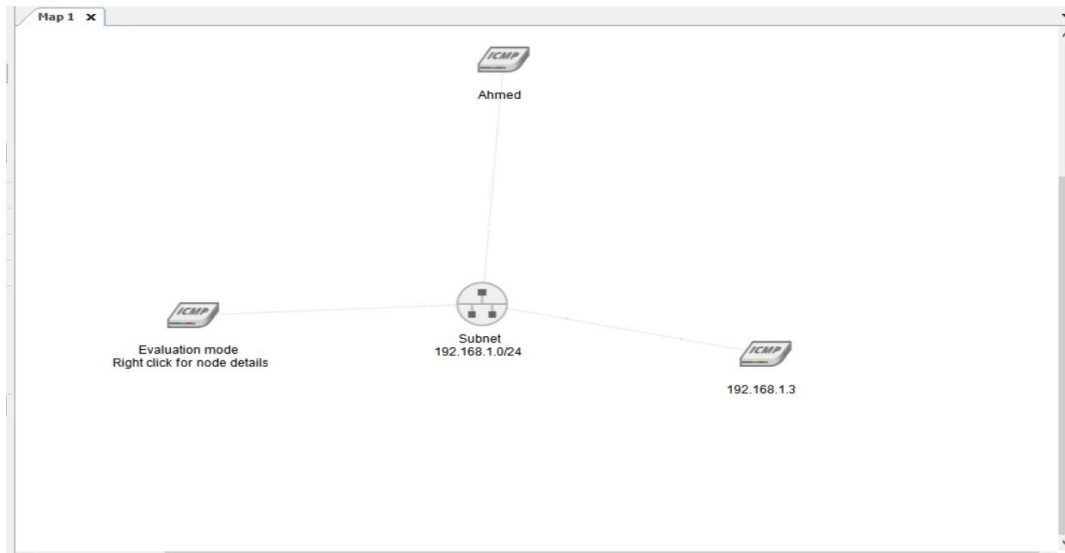
It shows my device (192.168.1.5) opening three ports (135, 139, 445) and 192.168.1.1 is a default gateway opening (21, 23, 80) and there's another device (192.168.1.3) opening no ports .



Problem two

Use network surveyor to show the map of all hosts on your local net.

Answer



Problem three

Ping www.wustl.com to find its address. Start Wireshark. Set capture filter option `\IP Address` to capture all traffic to/from this address. Open a browser window and Open www.wustl.com. Stop Wireshark. Submit a screen capture showing the packets seen.

```

tarek : bash — Konsole
File Edit View Bookmarks Settings Help
[tarek@tarek-pc]$ ping www.wustl.com
PING www.wustl.com (209.15.13.134) 56(84) bytes of data.
^C
--- www.wustl.com ping statistics ---
73 packets transmitted, 0 received, 100% packet loss, time 72966ms

[tarek@tarek-pc]$ █

```

By using the filter ip.addr==209.15.13.134

No.	Time	Source	Destination	Protocol	Length	Info
607	11.342755	192.168.1.5	209.15.13.134	TCP	66	58766 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
608	11.343224	192.168.1.5	209.15.13.134	TCP	66	58767 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
614	11.511995	209.15.13.134	192.168.1.5	TCP	66	80 → 58766 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1
615	11.512188	192.168.1.5	209.15.13.134	TCP	54	58766 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
616	11.512383	209.15.13.134	192.168.1.5	TCP	66	80 → 58767 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1
617	11.512511	192.168.1.5	209.15.13.134	TCP	54	58767 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
618	11.512922	192.168.1.5	209.15.13.134	HTTP	448	GET / HTTP/1.1
628	11.735387	209.15.13.134	192.168.1.5	TCP	68	80 → 58766 [ACK] Seq=1 Ack=395 Win=65792 Len=0
631	12.026930	209.15.13.134	192.168.1.5	HTTP	568	HTTP/1.1 302 Found (text/html)
632	12.027186	192.168.1.5	209.15.13.134	TCP	54	58766 → 80 [ACK] Seq=395 Ack=508 Win=65280 Len=0
633	12.029003	192.168.1.5	209.15.13.134	TCP	54	58766 → 80 [FIN, ACK] Seq=395 Ack=508 Win=65280 Len=0
638	12.193338	209.15.13.134	192.168.1.5	TCP	68	80 → 58766 [ACK] Seq=508 Ack=396 Win=65792 Len=0
671	21.864921	192.168.1.5	209.15.13.134	ICMP	74	Echo (ping) request id=0x0001, seq=1424/36809, ttl=128 (no response found!)
675	26.493655	192.168.1.5	209.15.13.134	ICMP	74	Echo (ping) request id=0x0001, seq=1425/37125, ttl=128 (no response found!)
685	31.494329	192.168.1.5	209.15.13.134	ICMP	74	Echo (ping) request id=0x0001, seq=1426/37381, ttl=128 (no response found!)
689	36.494871	192.168.1.5	209.15.13.134	ICMP	74	Echo (ping) request id=0x0001, seq=1427/37637, ttl=128 (no response found!)
711	56.521252	192.168.1.5	209.15.13.134	TCP	55	[TCP Keep-Alive] 58767 → 80 [ACK] Seq=0 Ack=1 Win=65792 Len=0
712	56.680909	209.15.13.134	192.168.1.5	TCP	66	[TCP Window Update] 80 → 58767 [ACK] Seq=1 Ack=1 Win=65792 Len=0 SLE=0 SRE=1
786	101.781226	192.168.1.5	209.15.13.134	TCP	55	[TCP Keep-Alive] 58767 → 80 [ACK] Seq=0 Ack=1 Win=65792 Len=0
787	101.864099	209.15.13.134	192.168.1.5	TCP	66	[TCP Keep-Alive ACK] 80 → 58767 [ACK] Seq=1 Ack=1 Win=65792 Len=0 SLE=0 SRE=1

▸ Frame 607: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 ▸ Ethernet II, Src: HonHaiPr_76:07:f9 (00:71:cc:76:07:f9), Dst: AskeyCom_dd:ef:03 (4c:ed:de:dd:ef:03)
 ▸ Destination: AskeyCom_dd:ef:03 (4c:ed:de:dd:ef:03)
 ▸ Source: HonHaiPr_76:07:f9 (00:71:cc:76:07:f9)
 Type: IPv4 (0x0800)
 ▸ Internet Protocol Version 4, Src: 192.168.1.5, Dst: 209.15.13.134
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x7e40 (32320)
 ▸ Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0xdc40 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.5