LABORATORIUM BEZPIECZEŃSTWO TECHNOLOGII INFORMATYCZNYCH

Data wykonania ćwiczenia:	03.10.2023
Rok studiów:	3
Semestr:	5
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	2

Temat: Skanowanie Sieci w Poszukiwaniu Otwartych Portów.

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Skanowanie Sieci w Poszukiwaniu Otwartych Portów.

Cel zadania:

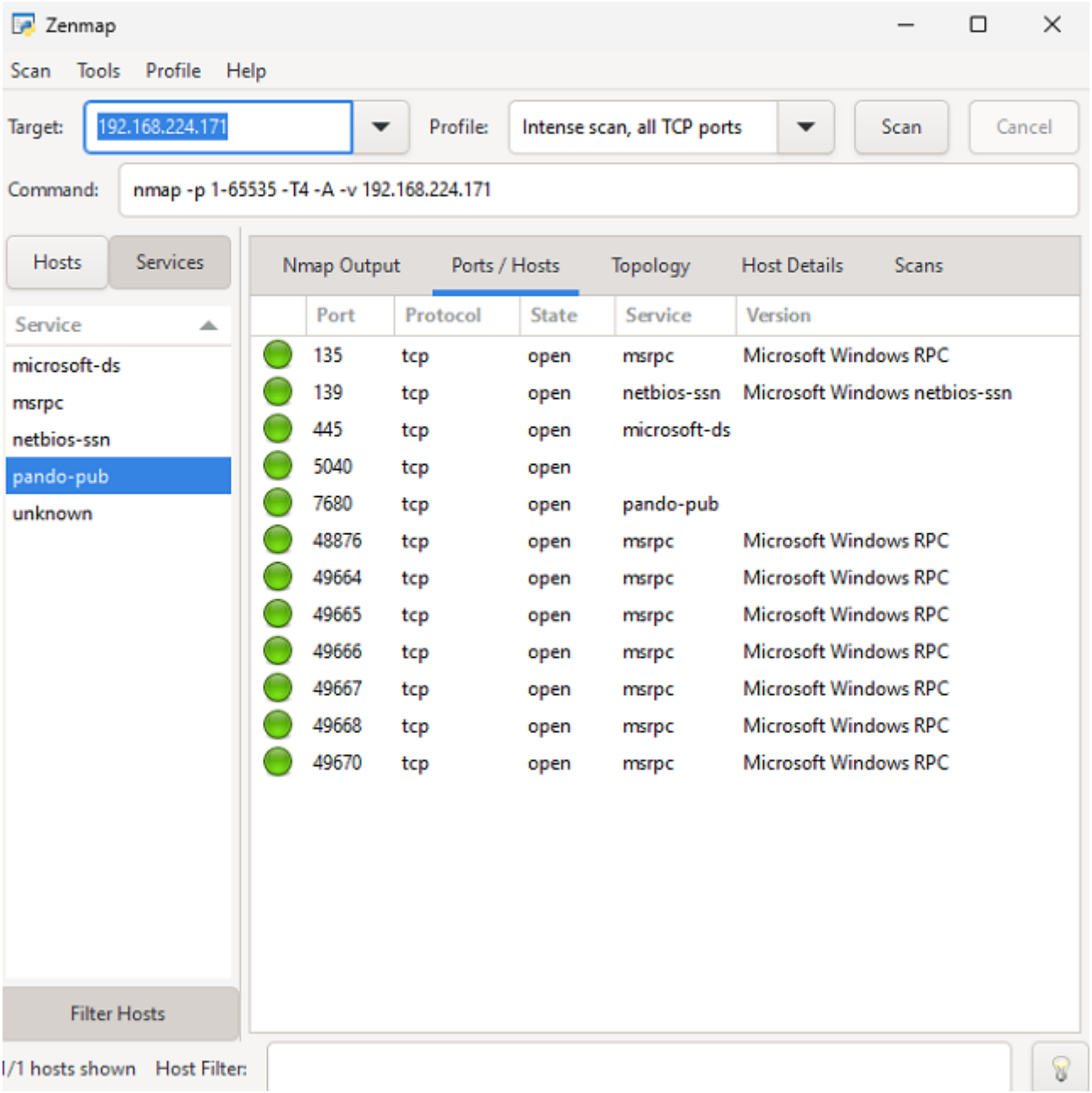
Celem tego laboratorium jest zapoznanie studentów z podstawami skanowania sieci w celu identyfikacji otwartych portów i działających usług, a także z umiejętnością korzystania z narzędzi do skanowania sieci, takich jak nmap i Wireshark.

Część 1: Skanowanie przy użyciu nmap (Network Mapper)

Po zainstalowaniu narzędzia NMap postanowiłem wybrać swój własny komputer za cel i za pomocą polecenia

```
nmap -p 1-65535 -T4 -A -v 192.168.224.171
```

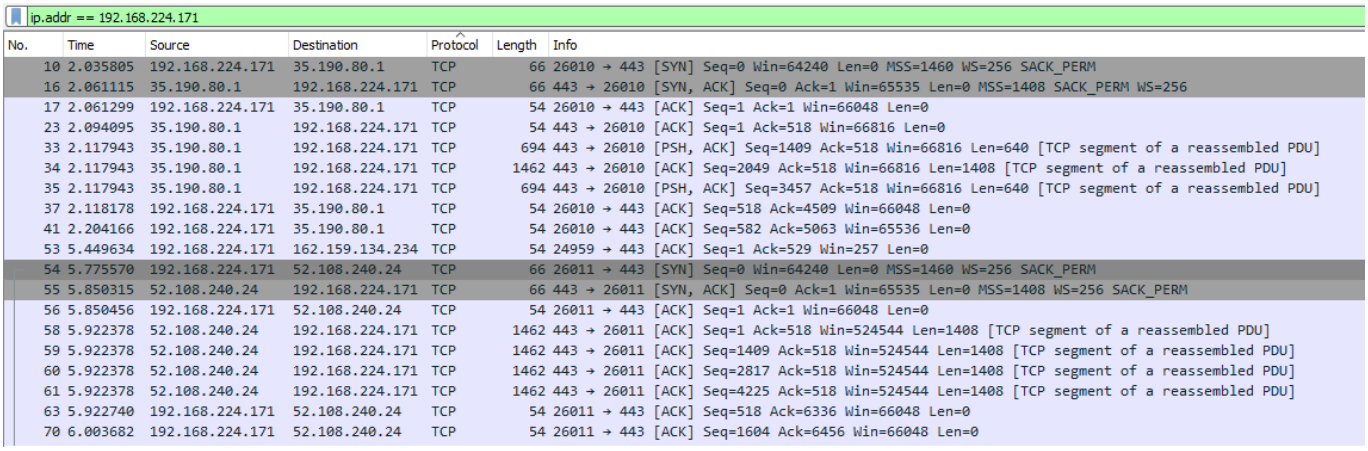
Przeprowadziłem skan mojej sieci za pomocą lokalnego IPv4.



Możemy zauważyć że większość otwartych portów pochodzi z serwisów microsoftu, oprócz tego możemy zauważyć jeszcze jedene niezidentyfikowany otwarty port.

Część 2: Skanowanie przy użyciu Wireshark

Po zeskanowaniu własnej sieci możemy przez do analizy, zwrócimy szczególną uwagę protokół TCP.



ip.addr == 192.168.224.171

No.	Time	Source	Destination	Protocol	Length	Info
10	2.035805	192.168.224.171	35.190.80.1	TCP	66	26010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16	2.061115	35.190.80.1	192.168.224.171	TCP	66	443 → 26010 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 SACK_PERM WS=256
17	2.061299	192.168.224.171	35.190.80.1	TCP	54	26010 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
23	2.094095	35.190.80.1	192.168.224.171	TCP	54	443 → 26010 [ACK] Seq=1 Ack=518 Win=66816 Len=0
33	2.117943	35.190.80.1	192.168.224.171	TCP	694	443 → 26010 [PSH, ACK] Seq=1409 Ack=518 Win=66816 Len=640 [TCP segment of a reassembled PDU]
34	2.117943	35.190.80.1	192.168.224.171	TCP	1462	443 → 26010 [ACK] Seq=2049 Ack=518 Win=66816 Len=1408 [TCP segment of a reassembled PDU]
35	2.117943	35.190.80.1	192.168.224.171	TCP	694	443 → 26010 [PSH, ACK] Seq=3457 Ack=518 Win=66816 Len=640 [TCP segment of a reassembled PDU]
37	2.118178	192.168.224.171	35.190.80.1	TCP	54	26010 → 443 [ACK] Seq=518 Ack=4509 Win=66048 Len=0
41	2.204166	192.168.224.171	35.190.80.1	TCP	54	26010 → 443 [ACK] Seq=582 Ack=5063 Win=65536 Len=0
53	5.449634	192.168.224.171	162.159.134.234	TCP	54	24959 → 443 [ACK] Seq=1 Ack=529 Win=257 Len=0
54	5.775570	192.168.224.171	52.108.240.24	TCP	66	26011 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
55	5.850315	52.108.240.24	192.168.224.171	TCP	66	443 → 26011 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 WS=256 SACK_PERM
56	5.850456	192.168.224.171	52.108.240.24	TCP	54	26011 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
58	5.922378	52.108.240.24	192.168.224.171	TCP	1462	443 → 26011 [ACK] Seq=1 Ack=518 Win=524544 Len=1408 [TCP segment of a reassembled PDU]
59	5.922378	52.108.240.24	192.168.224.171	TCP	1462	443 → 26011 [ACK] Seq=1409 Ack=518 Win=524544 Len=1408 [TCP segment of a reassembled PDU]
60	5.922378	52.108.240.24	192.168.224.171	TCP	1462	443 → 26011 [ACK] Seq=2817 Ack=518 Win=524544 Len=1408 [TCP segment of a reassembled PDU]
61	5.922378	52.108.240.24	192.168.224.171	TCP	1462	443 → 26011 [ACK] Seq=4225 Ack=518 Win=524544 Len=1408 [TCP segment of a reassembled PDU]
63	5.922740	192.168.224.171	52.108.240.24	TCP	54	26011 → 443 [ACK] Seq=518 Ack=6336 Win=66048 Len=0
70	6.003682	192.168.224.171	52.108.240.24	TCP	54	26011 → 443 [ACK] Seq=1604 Ack=6456 Win=66048 Len=0

Pomimo natłoku informacji możemy zidentyfikować porty dla których wartość celowego portu DST wyniosi 443 oznacza to zazwyczaj otawrty port HTTPS, taka sama sytuacja jest dla portu 80 - HTTP, 22 - SSH, 25 - SMTP.

Możemy teraz przejśc przez takie rekordy i na podstawie adresu ip jesteśmy w stanie zindentyfikować z jakiego serwisu pochodzą dane rekordy.

Np.

```
Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
\Device\NPF_{32714C3E-D261-4C1B-B959-82F5192BA025}, id 0 Ethernet II, Src:
IntelCor_08:8e:00 (a0:a8:cd:08:8e:00), Dst: 9e:a1:57:5a:e9:9c (9e:a1:57:5a:e9:9c)
Internet Protocol Version 4, Src: 192.168.224.171, Dst: 52.108.240.24 Transmission
Control Protocol, Src Port: 26011, Dst Port: 443, Seq: 0, Len: 0
```

Z powyższego rekordu możemy zauważyć że adres IP prowadzi do platformy Office, co potwierdza nasze wnioski uzyskane w aplikacji NMap, gdzie widzieliśmy że część otwartych portów pochodzi z usług microsoftu.

Część 3: Analiza i obrona przed skanowaniem sieci

1. Przeprowadź analizę wyników z części 1 i części 2, gdzie skanowaliście sieć. Zastanów się, jakie informacje można było uzyskać z wyników skanowania i jakie potencjalne zagrożenia mogą wynikać z tych informacji.

Podczas skanowania sieci mogliśmy uzyskać różne informacje, takie jak otwarte porty, dostępne usługi i konfiguracje sieciowe. Po przeanalizowaniu tych informacji możemy dojść do następujących zagrożeń:

- Potencjalne ataki hakerskie na znalezione otwarte porty i usługi.
- Nieautoryzowany dostęp do zasobów sieciowych.
- Możliwość uruchomienia ataków typu "man-in-the-middle" w celu przechwycenia danych.
- Eksploracja systemów pod kątem znalezienia luk w zabezpieczeniach.

Na podstawie wyników skanowania sieci, przemyśl, jakie działania można podjąć w celu zabezpieczenia sieci przed atakami lub nieautoryzowanym dostępem.

Na podstawie wyników skanowania, musimy podjąć działania w celu zabezpieczenia sieci przed potencjalnymi atakami i nieautoryzowanym dostępem. Możemy rozważyć następujące działania:

- Zamknięcie zbędnych otwartych portów i usług: Wyłączamy usługi i porty, które nie są niezbędne do działania naszej sieci, aby zminimalizować potencjalne ataki.
- Aktualizacja oprogramowania i systemów: Zapewniamy, że wszystkie urządzenia i oprogramowanie w sieci są regularnie aktualizowane, aby zaktualizować zabezpieczenia i łaty.
- Wdrożenie silnego firewalla: Konfigurujemy firewalla w taki sposób, aby kontrolować ruch sieciowy i blokować nieautoryzowane połączenia.
- Monitorowanie ruchu sieciowego: Używamy narzędzi monitorujących, takich jak IDS (Systemy Wykrywania Włamań) i IPS (Systemy Zapobiegania Włamań), aby śledzić i reagować na podejrzane działania w sieci.

Opracuj strategię obrony przed skanowaniem i testowaniem podatności sieci, takie jak odpowiednie konfiguracje firewalla, monitorowanie ruchu sieciowego lub aktualizacje oprogramowania.

- Regularne testy podatności: Planujemy regularne testy skanowania podatności w celu wykrywania i usuwania potencjalnych luk w zabezpieczeniach.
- Szkolenia dla personelu: Zapewniamy odpowiednie szkolenia dla pracowników w zakresie bezpieczeństwa sieci i świadomości zagrożeń.
- Zasady dostępu i kontroli dostępu: Wdrażamy restrykcyjne zasady dostępu oraz kontrolujemy dostęp do zasobów sieciowych w oparciu o zasady "zasad najmniejszego uprzywilejowania."
- Plan reagowania na incydenty: Opracowujemy plan reagowania na incydenty, aby efektywnie reagować na potencjalne ataki i naruszenia bezpieczeństwa.

Podsumowując, analiza wyników skanowania sieci powinna prowadzić do konkretnych działań w celu zabezpieczenia sieci przed potencjalnymi zagrożeniami. Regularna troska o bezpieczeństwo sieci i monitoring są kluczowe w utrzymaniu bezpiecznej i odporniej infrastruktury.