

Ze względów bezpieczeństwa, usunąłem pierwsze cztery zadania, ponieważ wykonywałem tam operacje sieciowe na maszynach działających w mojej lokalnej sieci domowej.

For security reasons, I removed the first four tasks because I was performing network operations there on machines running on my local home network.

ZADANIE 5:

The image shows a Wireshark packet capture window titled "Export_IS_2021.pcap". The packet list shows 10 packets. The first packet is a DNS query from 172.16.17.131 to 172.16.17.2. The packet details pane shows the structure of this packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.17.131	172.16.17.2	DNS	78	Standard
2	1.606894	172.16.17.131	239.255.255.250	SSDP	175	M-SEARCH
3	3.931885	172.16.17.131	172.16.17.2	DNS	85	Standard
4	3.955009	172.16.17.2	172.16.17.131	DNS	158	Standard
5	4.009396	172.16.17.131	172.16.17.2	DNS	78	Standard
6	8.019457	172.16.17.131	172.16.17.2	DNS	78	Standard
7	9.032584	172.16.17.131	172.16.17.2	DNS	78	Standard
8	11.045871	172.16.17.131	172.16.17.2	DNS	78	Standard
9	15.056076	172.16.17.131	224.0.0.252	LLMNR	66	Standard
10	15.164388	172.16.17.131	224.0.0.252	LLMNR	66	Standard

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: 00:0c:29:24:d0:a3 (00:0c:29:24:d0:a3), Dst: 01:00:5e:f1:1d:1a (01:00:5e:f1:1d:1a)
Internet Protocol Version 4, Src: 172.16.17.131, Dst: 172.16.17.2
User Datagram Protocol, Src Port: 64538, Dst Port: 53
Domain Name System (query)

a) Analizie został poddany adres IPv4 172.16.17.131

b) Gateway: 172.16.17.2

c) To działo się w ramach wirtualnych maszyn. Z przesyłanych pakietów można wyciągnąć informacje, że są to wirtualne maszyny.

d) Jesteśmy w stanie, ruch pakietów z początku pliku jest typowy dla skanowania w poszukiwaniu portów otwartych. Adres 172.16.17.131 otrzymał wiele pakietów TCP na różnych portach. Zatem ktoś szukał otwartego portu.

e) Atak polegał na wysyłaniu pakietów TCP na wybrane przez atakującego porty. Następnie czekał on na odpowiedź. Jeżeli odpowiedź się pojawiła, oznaczało to, że port jest otwarty.
IP: 172.17.17.128

f)

24 30.530014	172.16.17.131	239.255.255.250	SSDP	175 M-SEARCH → HTTP/1.1	
25 31.715128	172.16.17.128	172.16.17.131	TCP	60 57324 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
26 31.715128	172.16.17.128	172.16.17.131	TCP	60 57324 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
27 31.715309	172.16.17.128	172.16.17.131	TCP	60 57324 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
28 31.715370	172.16.17.128	172.16.17.131	TCP	60 57324 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
29 31.715370	172.16.17.128	172.16.17.131	TCP	60 57324 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
30 31.715568	172.16.17.128	172.16.17.131	TCP	60 57324 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
▶ Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethernet II, Src: 00:0c:29:ec:8a:14 (00:0c:29:ec:8a:14), Dst: 00:0c:29:24:d0:a3 (00:0c:29:24:d0:a3) Destination: 00:0c:29:24:d0:a3 (00:0c:29:24:d0:a3) Address: 00:0c:29:24:d0:a3 (00:0c:29:24:d0:a3) ...0. = LG bit: Globally unique address (factory default) ...0. = IG bit: Individual address (unicast) Source: 00:0c:29:ec:8a:14 (00:0c:29:ec:8a:14) Address: 00:0c:29:ec:8a:14 (00:0c:29:ec:8a:14) ...0. = LG bit: Globally unique address (factory default) ...0. = IG bit: Individual address (unicast) Type: IPv4 (0x0800) Padding: 0000 Internet Protocol Version 4, Src: 172.16.17.128, Dst: 172.16.17.131 Transmission Control Protocol, Src Port: 57324, Dst Port: 256, Seq: 0, Len: 0					0000 00 0c 29 24 d0 a3 00 0c 29 ec 8a 14 00 00 45 00 0010 00 2c e1 c5 00 00 2b 06 32 e3 ac 10 11 80 ac 10 0020 11 83 df ec 01 00 ea 17 5a 70 00 00 00 00 02 0030 04 00 f3 84 00 00 02 04 05 b4 00 00

Ten adres mac należy do sprawy ataku.

g)

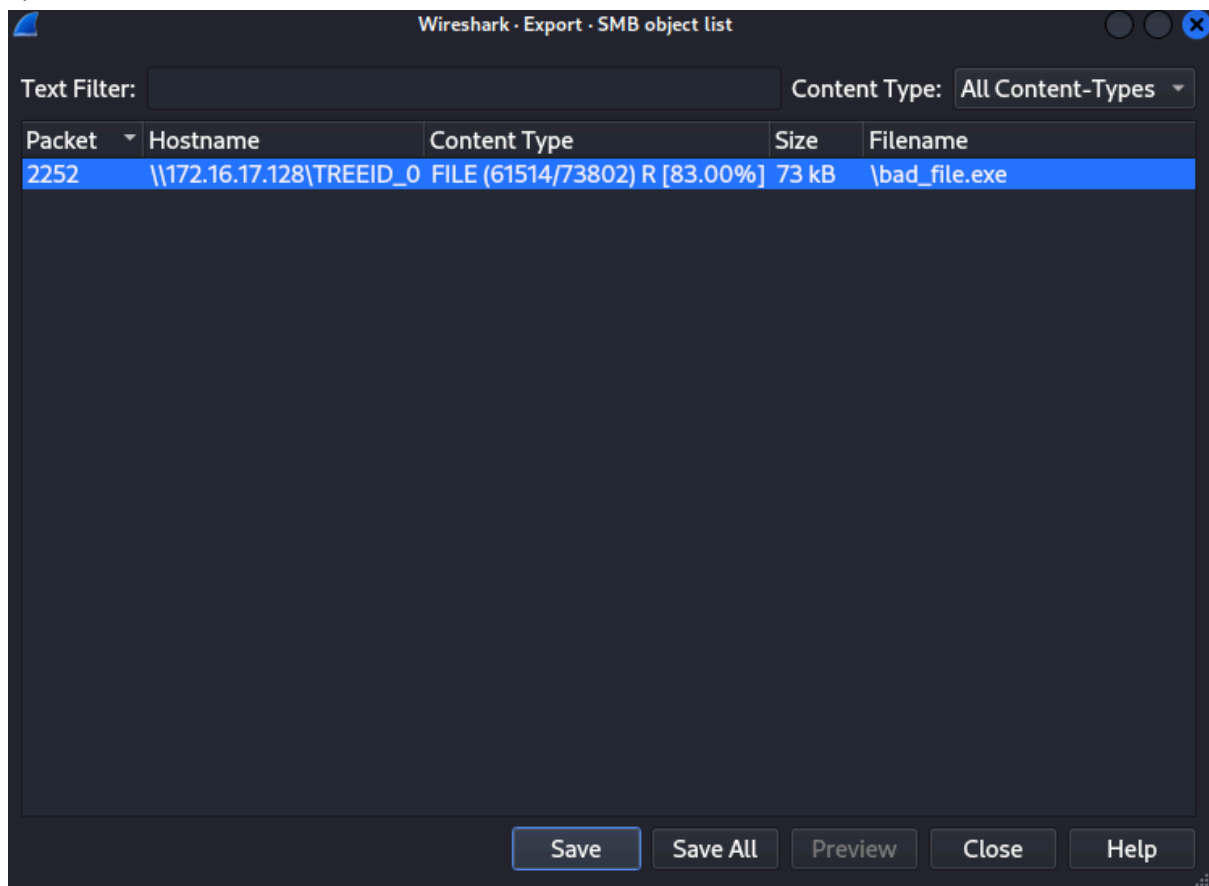
2254 365.307001	172.16.17.131	172.16.17.128	SMB	166 Trans2 Request, FIND_FIRST2, Pattern: \bad_file.exe
2255 365.310066	172.16.17.128	172.16.17.131	SMB	241 Trans2 Response, FIND_FIRST2, Files: bad_file.exe
2256 365.310369	172.16.17.131	172.16.17.128	SMB	166 Trans2 Request, FIND_FIRST2, Pattern: \bad_file.exe
2257 365.313358	172.16.17.128	172.16.17.131	SMB	241 Trans2 Response, FIND_FIRST2, Files: bad_file.exe
2258 365.313647	172.16.17.131	172.16.17.128	SMB	144 Trans2 Request, FIND_FIRST2, Pattern: *
2259 365.316225	172.16.17.128	172.16.17.131	SMB	93 Trans2 Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE
2260 365.316595	172.16.17.131	172.16.17.128	SMB	170 NT Create AndX Request, FID: 0xdead, Path: \bad_file.exe

Plik nazywa się bad_file.exe

▶ Frame 2254: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0 Encapsulation type: Ethernet (1) Arrival Time: Nov 24, 2021 18:35:52.345166000 CET [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1637775352.345166000 seconds [Time delta from previous captured frame: 0.000283000 seconds] [Time delta from previous displayed frame: 0.000283000 seconds] [Time since reference or first frame: 365.307001000 seconds] Frame Number: 2254 Frame Length: 166 bytes (1328 bits) Capture Length: 166 bytes (1328 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp:nbss:smb] [Coloring Rule Name: SMB] [Coloring Rule String: smb nbss nbns netbios]		▶ Ethernet II, Src: 00:0c:29:24:d0:a3 (00:0c:29:24:d0:a3), Dst: 00:0c:29:ec:8a:14 (00:0c:29:ec:8a:14) ▶ Internet Protocol Version 4, Src: 172.16.17.131, Dst: 172.16.17.128 ▶ Transmission Control Protocol, Src Port: 49162, Dst Port: 445, Seq: 2895, Ack: 5759, Len: 112 ▶ NetBIOS Session Service ▶ SMB (Server Message Block Protocol)	
--	--	---	--

został pobrany ok. 18:35:52 z adresu atakującego(172.16.17.128), co możemy zobaczyć na 1 rzucie ekranu.

h)



```
(szmpns@kali)-[~/InformatykaSledcza/InfSl_LAB05]  
$ md5sum %5cbad_file.exe  
e3d7589286e151061b8720b10f8cab45 %5cbad_file.exe
```

i) Z jakiegoś powodu suma została źle policzona i skrót nie istniał w bazie virus total.
Inne narzędzie zrobiło to poprawnie:
f8e82827fb5ab265d6e50abce401029b

52

/ 68

52 security vendors and 1 sandbox flagged this file as malicious

Reanalyze
Similar
More

e2b440dc8aaba8c2fe16687e497c05a0f364a6c4564b7be7c9e3390b04e33be

Size72.07 KB

Last Analysis Date2 years ago

EXE

ab.exe

peexeoverlayidle

Community Score

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.swort/cryptz

Threat categoriestrojan

Family labelsswortcryptzrozena

Security vendors' analysis

Do you want to automate checks?

Ten plik zawiera bardzo wiele niebezpiecznych programów. Backdoory do 32-bitowych Windowsów oraz trojany.

Microsoft	Trojan.Win32/Meterpreter.O	NANO-Antivirus	Virus.Win32.Gen-Crypt.cnc
Panda	Trj/GdSda.A	QuickHeal	Trojan.Swort.A
Rising	HackTool.Swort!t.6477 (CLASSIC)	Sangfor Engine Zero	Trojan.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	ML/PE-A + Mal/EncPk-ACE	SUPERAntiSpyware	Trojan.Backdoor-Shell
Symantec	Packed.Generic.347	TACHYON	Backdoor/W32.Agent.73802.BN
Tencent	Trojan.Win32.Cryptz.za	Trellix (FireEye)	Generic.mg.f8e82827fb5eb265
TrendMicro	Backdoor.Win32.SWRORT.SMAL01	TrendMicro-HouseCall	Backdoor/Win32.SWRORT.SMAL01
VIPRE	Trojan.Win32.Swort.B (v)	ViRobot	Trojan.Win32.Elzob.Gen
WithSecure	Trojan.TR/Patched.Gen2	Yandex	Trojan.Rozena.Gen.1

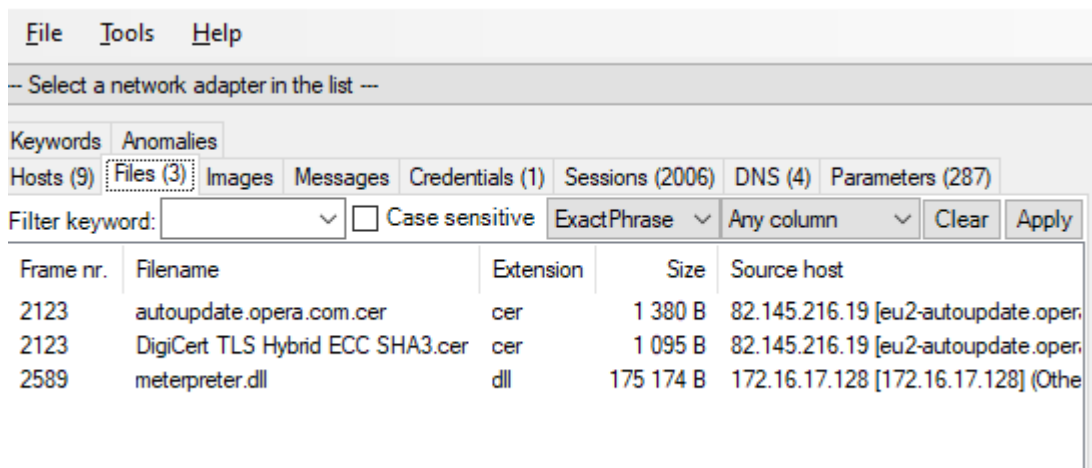
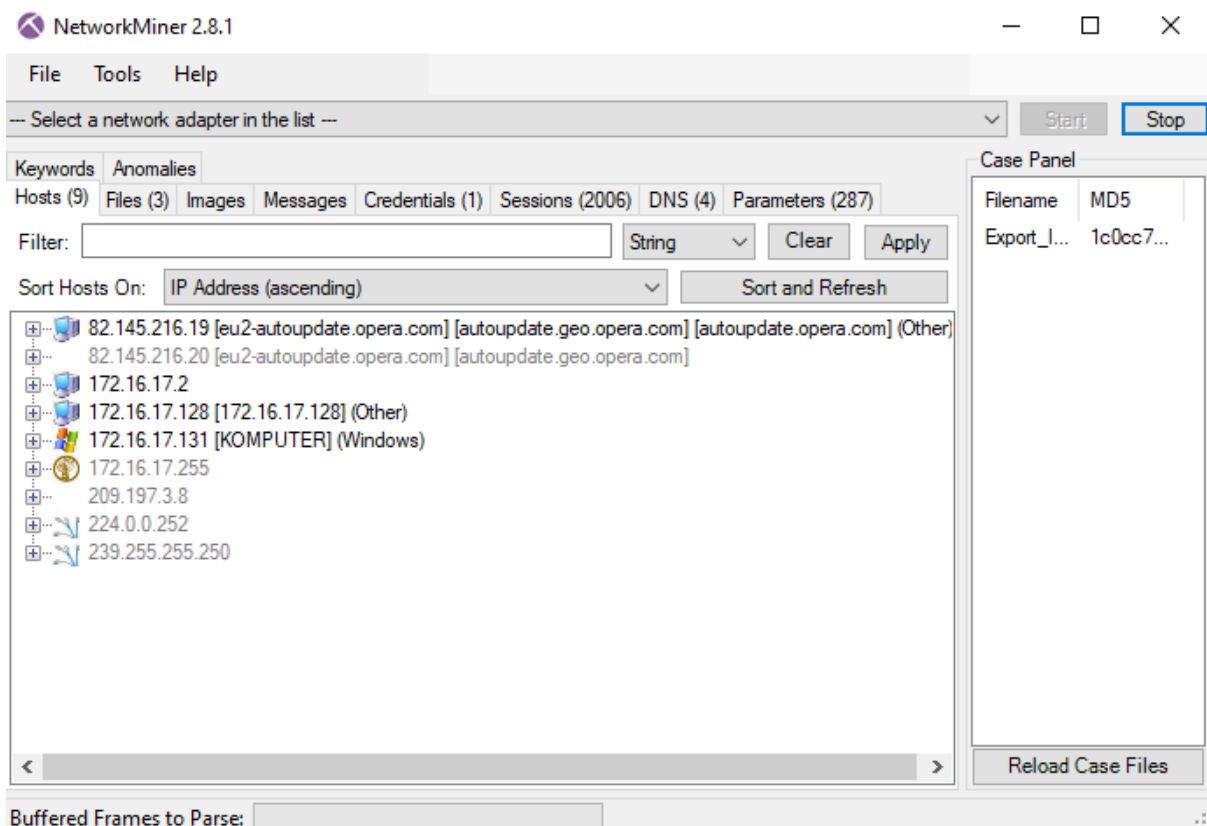
j) Był to port 49165.

k)

10.000000	172.16.17.131	172.16.17.2	DNS	78 Standard query 0x040a A isatap.localdomain
2980.392.588053	172.16.17.131	172.16.17.255	BROWSER	243 Host Announcement KOMPUTER, Workstation, Server, NT Workstation
2105.152.494128	172.16.17.131	172.16.17.255	BROWSER	243 Host Announcement KOMPUTER, Workstation, Server, NT Workstation
45.32.858300	172.16.17.131	172.16.17.255	BROWSER	243 Host Announcement KOMPUTER, Workstation, Server, NT Workstation

Nazywał się KOMPUTER

ZADANIE 6:



W zakładce files nie widać tego pliku.

Plik został wysłany(informacja z analizy wireshark) za pomocą protokołu SMB, istnieje zatem szansa, że narzędzie NetworkMiner nie obsługuje w ogóle plików przesyłanych za pomocą tego protokołu.

W latach 2016-2017 podjęto kroki, aby program skuteczniej wyciągał pliki z protokołów SMB.

Po przeczytaniu kilku forów internetowych, można stwierdzić, że program ma dalej ten sam problem do dziś.

Nie pomaga nawet sugerowana zmiana uprawnień na takie, w których może zapisywać dane m.in. w pliku Assembled Files.

Program dalej ma problemy z ekstrakcją plików o rozszerzeniu .exe przesłanych za pomocą protokołu SMB.