# **BSidesJeddah-Part1**

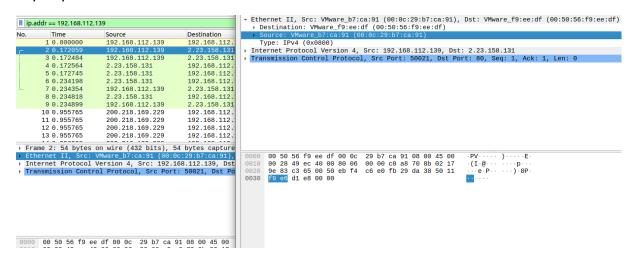
1. What is the victim's MAC address?

Wraz z plikiem pcap otrzymaliśmy plik suricata.rules który jest sygnaturami systemu IDS/IPS możemy go użyć do przeskanowania pliku pcap suricatą bądź snortem w moim przypaku suricata.

Z wygenerowanych logów możemy dowiedzieć się że adresacja ip w sieci LAN opiera się na klasie adresu C 192... dzięki tej informacji możemy wyfiltrować same adresy zaczynające się na 192.

```
michal@linux:~/Desktop/log$ cat fast.log | cut -d " " -f 21 | sort | uniq -c | sort | grep 192
11 192.168.112.128:443
1 192.168.112.139:110
1 192.168.112.139:59491
1 192.168.112.2:137
27 192.168.112.2:880
3 192.168.112.139:0
michal@linux:~/Desktop/log$
```

Jak można zauważyć najwięcej podejrzanego ruchu zostało zalogowane miedzy adresami 192.168.112.139 oraz 192.168.112.128 ale kiedy przyjrzymy się ruchowi w wiresharku można łatwo wywnioskować że ofiarą jest 192.168.112.139. Pozostaje odczytać jego adres fizyczny:



Answer: 00:0C:29:B7:CA:91

2. What is the address of the company associated with the victim's machine MAC address?

Dla przykładu ja użyłem tego narzędzia do znalezienia adresu: https://www.ipchecktool.com/tool/macfinder

Answer: 3401 Hillview Avenue Palo Alto CA 94304 US

### 3. What is the attacker's IP address?

Uzyjemy tego polecenia aby wyfiltrować z logów suricaty wszystkie adresy oraz informacje ile razy się powtarzają i zapiszemy je do pliku out1.txt może się nam to przydać w późniejszym czasie.

cat fast.log | cut -d " " -f 21 | sort | uniq -c | sort > out1.txt

```
michal@linux:~/Desktop/log$ cat out1.txt | grep -i 192.

11 192.168.112.128:443

1 192.168.112.139:110

1 192.168.112.2:39:59491

1 192.168.112.2:137

27 192.168.112.128:80

3 192.168.112.139:0

michal@linux:~/Desktop/log$
```

Jeden z adresów wysyłał podejrzanie dużo ruchu do ofiary oraz wielokrotnie był uważany przez sygnatury jako potencjalna exploitacja.

Answer:192.168.112.128

4. What is the IPv4 address of the DNS server used by the victim machine?

Wyfiltrujmy ruch dns związany z adresem ip ofiary:

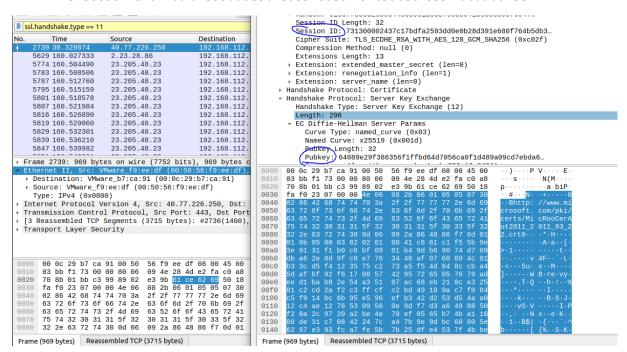
Jak można zaobserwować adres ofiary odpytywał tylko jeden serwer DNS

Answer:192.168.112.2

5. What domain is the victim looking up in packet 5648?

Answer: omextemplates.content.office.net

6. What is the server certificate public key that was used in TLS session: 731300002437c17bdfa2593dd0e0b28d391e680f764b5db3c4059f7abadbb28e



Answer: 64089e29f386356f1ffbd64d7056ca0f1d489a09cd7ebda630f2b7394e319406

7. What domain is the victim connected to in packet 4085?

```
38.329874 40.77.226.250 →192.168.112.139 TLSV1.2 969 Server Hello, Certificate, Server Key Exchange, Server Hello Done
38.33438 192.168.112.139 →40.77.226.250 TLSV1.2 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
38.43033 40.77.226.250 →192.168.112.139 TLSV1.2 105 Change Cipher Spec, Encrypted Handshake Message
38.424137 192.168.112.139 →40.77.226.250 TLSV1.2 824 Application Data
38.424317 192.168.112.139 →40.77.226.250 TLSV1.2 824 Application Data
38.424512 40.77.226.250 →192.168.112.139 TCP 60 443 →50073 [ACK] Seq=3767 Ack=1076 Win=64240 Len=0
38.424748 192.168.112.139 →40.77.226.250 TLSV1.2 856 Application Data
38.425037 40.77.226.250 →192.168.112.139 TCP 60 443 →50073 [ACK] Seq=3767 Ack=1678 Win=64240 Len=0
38.693254 40.77.226.250 →192.168.112.139 TLSV1.2 824 Application Data
38.701642 192.168.112.139 →40.77.226.250 TLSV1.2 824 Application Data
38.701642 192.168.112.139 →40.77.226.250 TLSV1.2 824 Application Data
38.70287 192.168.112.139 →40.77.226.250 TLSV1.2 406 Application Data
38.70287 192.168.112.139 →40.77.226.250 TLSV1.2 406 Application Data
39.017474 40.77.226.250 →192.168.112.139 TLSV1.2 349 Application Data
39.017407 40.77.226.250 →192.168.112.139 TLSV1.2 824 Application Data
39.024823 192.168.112.139 →40.77.226.250 TLSV1.2 825 Application Data
39.024823 40.77.226.250 →192.168.112.139 TLSV1.2 349 Application Data
39.024823 40.77.226.250 →192.168.112.139 TLSV1.2 825 Application Data
39.02467 40.77.226.250 →192.168.112.139 TLSV1.2 825 Application Data
39.024767 40.77.226.250 →192.168.112.139 TLSV1.2 825 Application Data
39.024676 40.77.226.250 →192.168.112.139
```

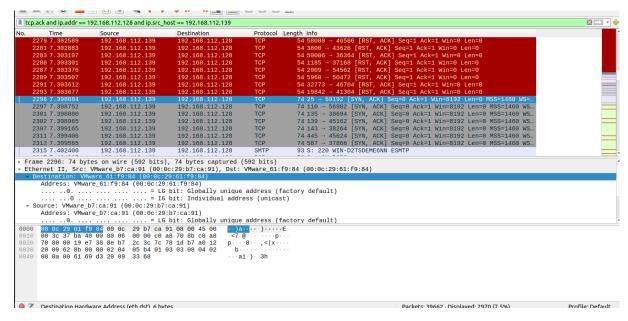
W pakiecie 4085 nasza ofiara komunikuje się z adresem 40.77.226.250 czyli z adresem logicznym ip nie mamy podanej tutaj domeny jednak kiedy wrócimy do screena z pytania 4 i 5 zauważmy że ofiara odpytywała już serwer DNS w poszukiwaniu adresu 40.77.226.250:

```
nt.office.net CNAME omextemplates.content.office.net.edgekey.net CNAME e584.g.akamaledge.net
      oft.com CNAME settingsfd-geo.trafficmanager.net A 51.104.136.2
oft.com CNAME settingsfd-geo.trafficmanager.net A 51.104.136.2
```

Answer: v10.vortex-win.data.microsoft.com

8. The attacker conducted a port scan on the victim machine. How many open ports did the attacker find?

Atakujący skanował serwer / adres ofiary w poszukiwaniu otwartych portów na których działają usługi. W skrócie polega to na tymże narzędzie skanujące wysyła do określonego zakresu portów flage SYN tcp oraz oczekuje od danej usługi odpowiedzi w postaci flagi SYN, ACK



#### Answer:7

9. Analyze the pcap using the provided rules. What is the CVE number falsely alerted by Suricata?

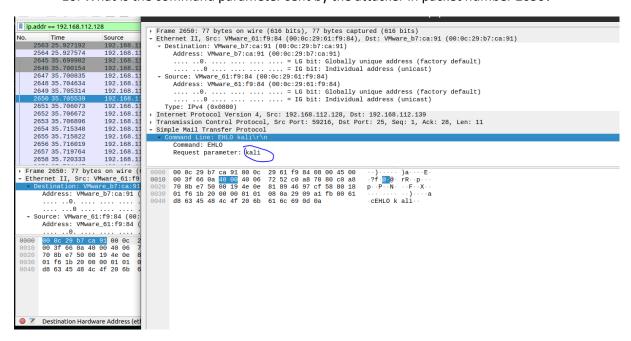
Wracamy do logów wygenerowanych przez suricate tzn fast.log oraz filtrujemy słowa kluczowego "CVE":

```
michal@linux:~/Desktop/log$ cat fast.log | grep -i CVE
10/01/2021-14:31:54.593627 [**] [1:2030387:1] ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read [**] [Classification: At 000:0000:d4aa:8d54:3230:720b:52484 -> ff02:0000:0000:0000:0000:0000:0000:53555
michal@linux:~/Desktop/log$ |
```

Mamy jeden wynik i zawiera on poprawną odpowiedz.

Answer: CVE-2020-11899

10. What is the command parameter sent by the attacker in packet number 2650?



Answer: kali

11. What is the stream number which contains email traffic?

Answer:1183

12. What is the victim's email address?

Filtrujemy tcp.stream == 1183 i szukamy adresu docelowego SMTP RCPT TO:

	tcp.stream == 1183								
No.	Time	Source	Destination	Protocol	Length Info				
	2645 35.699982	192.168.112.128	192.168.112.139	TCP	74 59216 → 25 [SYN] Seq=0 Win=64240 Len=0 M				
	2646 35.700154	192.168.112.139	192.168.112.128	TCP	74 25 → 59216 [SYN, ACK] Seq=0 Ack=1 Win=81				
	2647 35.700835	192.168.112.128	192.168.112.139	TCP	66 59216 → 25 [ACK] Seq=1 Ack=1 Win=64256 L				
	2648 35.704634	192.168.112.139	192.168.112.128	SMTP	93 S: 220 WIN-D2TSDEME6NN ESMTP				
	2649 35.705314	192.168.112.128	192.168.112.139	TCP	66 59216 → 25 [ACK] Seq=1 Ack=28 Win=64256				
	2650 35.705539	192.168.112.128	192.168.112.139	SMTP	77 C: EHLO kali				
	2651 35.706073	192.168.112.139	192.168.112.128	SMTP	132 S: 250-WIN-D2TSDEME6NN   SIZE 20480000				
	2652 35.706672	192.168.112.128	192.168.112.139	TCP	66 59216 → 25 [ACK] Seq=12 Ack=94 Win=64256				
	2653 35.706896	192.168.112.128	192.168.112.139	SMTP	106 C: MAIL FROM: <support@cyberdefenders.org< td=""></support@cyberdefenders.org<>				
	2654 35.715348	192.168.112.139	192.168.112.128	SMTP	74 S: 250 OK				
	2655 35.715822	192.168.112.128	192.168.112.139	TCP	66 59216 → 25 [ACK] Seq=52 Ack=102 Win=6425				
	2656 35.716019	192.168.112.128	192.168.112.139	SMTP	103 C: RCPT TO: <joshua@cyberdefenders.org></joshua@cyberdefenders.org>				
	2657 35.719764	192.168.112.139	192.168.112.128	SMTP	74 S: 250 OK				

Answer: joshua@cyberdefenders.org

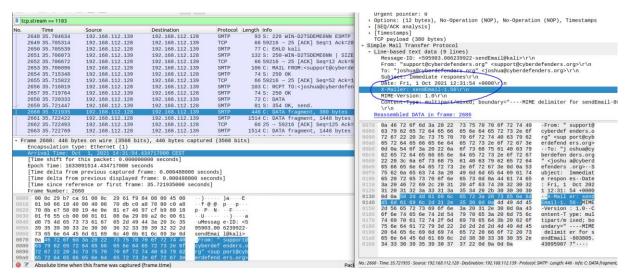
13. What was the time attacker sent the email?

Filtrujemy strumień po raz kolejny i odczytujemy godzinę z e-maila

Answer: 12:31:54

## 14. What is the version of the program used to send the email?

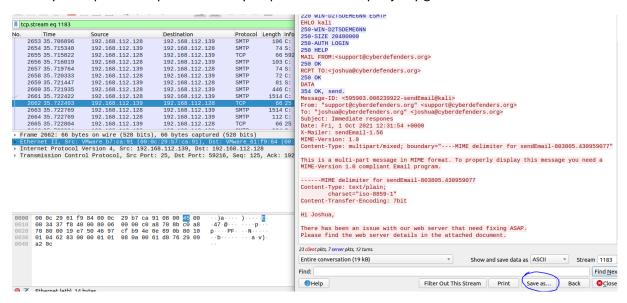
W pakiecie 2660 znajduje się zawartość wiadomości z informacji warstwy 7 można odczytać narzędzie za pomocą którego prawdopodobnie wysłano wiadomość



Answer: 1.56

#### 15. What is the MD5 hash of the email attachment?

Robimy zrzut pakietu odpowiedzi ofiary na pakiet SMTP i zapisujemy go z rozszerzeniem .eml



Answer: 55e7660d9b21ba07fc34630d49445030

16. What is the CVE number the attacker tried to exploit using the malicious document?

Zrzucony plik wrzucamy na strone virustotal jest to sandbox zawierający silniki wielu antywirusów.

Answer: CVE-2021-40444

17. The malicious document file contains a URL to a malicious HTML file. Provide the URL for this file.

Filtrujemy w poszukiwaniu ruchu http z adresem docelowym atakującego:

ip	ip.dst == 192.168.112.128 and http									
No.	Time	Source	Destination	Protocol	Length Info					
	2940 60.364064	192.168.112.139	192.168.112.128	HTTP	229 OPTIONS / HTTP/1.1					
	2949 60.403141	192.168.112.139	192.168.112.128	HTTP	217 HEAD /word.html HTTP/1.1					
	2959 60.419163	192.168.112.139	192.168.112.128	HTTP	229 OPTIONS / HTTP/1.1					
+	2968 60.438714	192.168.112.139	192.168.112.128	HTTP	381 GET /word.html HTTP/1.1					
	2985 60.449673	192.168.112.139	192.168.112.128	HTTP	200 HEAD /word.html HTTP/1.1					
	2996 60.457949	192.168.112.139	192.168.112.128	HTTP	200 HEAD /word.html HTTP/1.1					
	3007 60.470053	192.168.112.139	192.168.112.128	HTTP	229 OPTIONS / HTTP/1.1					
	3016 60.498931	192.168.112.139	192.168.112.128	HTTP	217 HEAD /word.html HTTP/1.1					
	3026 60.510041	192.168.112.139	192.168.112.128	HTTP	229 OPTIONS / HTTP/1.1					
	3035 60.521039	192.168.112.139	192.168.112.128	HTTP	444 GET /word.html HTTP/1.1					
	3046 60.529126	192.168.112.139	192.168.112.128	HTTP	200 HEAD /word.html HTTP/1.1					
	3057 60.536577	192.168.112.139	192.168.112.128	HTTP	200 HEAD /word.html HTTP/1.1					
	3076 61.461908	192.168.112.139	192.168.112.128	HTTP	423 GET /word.cab HTTP/1.1					
	CET /word html U	TTD/1 1\r\n	100 100 110 100	HTTP	OOO OPTIONO / UTTP /4 4					
,	GET /word.html HTTP/1.1\r\n  Accept: */*\r\n									
		lla/4 0 (compatible:	MSTE 7 A: Windows NT	6 2: Win64	. v64: Tridopt/7 0: NET4 00: NET4 0E: NE					
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trident/7.0; .NET4.00										
Accept-Encoding: gzip, deflate\r\n										
	Host: 192.168.11									
	\r\n	Connection: Keep-Alive\r\n								
	[Full request URI: http://192.168.112.128/word.html]									
	[HTTP request 1/									
[Response in frame: 2977]										

Answer: <a href="http://192.168.112[.]128/word.html">http://192.168.112[.]128/word.html</a>

20. The malicious HTML contains a js code that points to a malicious CAB file. Provide the URL to the CAB file?

Na Screenie z zadania 17 w pakiecie 3076 widzimy plik /word.cab jego lokalizacja jest bardzo podobna:

Answer: <a href="http://192.168.112[.]128/word.cab">http://192.168.112[.]128/word.cab</a>

21. The exploit takes advantage of a CAB vulnerability. Provide the vulnerability name?

Troche googlowania i odpowiedzą jest podatność ZipSlip jest to krytyczna podatność która umożliwia wykonanie kodu umieszczonego w pliku html.

Answer: ZipSlip

22. The CAB file contains a malicious dll file. What is the tool used to generate the dll?

Funkcje generowania złośliwych bibliotek dll lub innych revshelli daje np. pakiet metasploit

Answer: metasploit

23. What is the path of the dropped malicious dll file? Replace your username with IEUser Po analizie pliku word.html i deobfuskacji możemy znaleźć lokalizacje gdzie złośliwy plik został zapisany:

Answer: C:\Users\IEUser\Appdata\Local\Temp\msword.inf

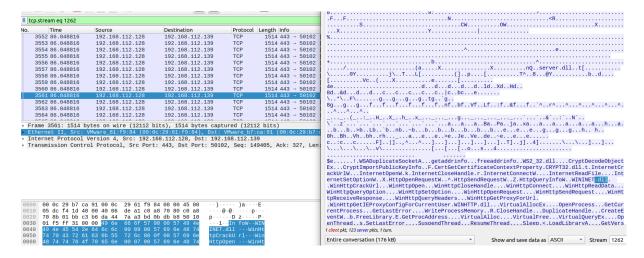
24. Analyzing the dll file what is the API used to write the shellcode in the process memory?

Możemy się tego dowiedzieć poprzez wypakowanie pliku z archiwum word.cap za pomocą polecenia: 7z e word.cab następnie sprawdzamy stringi wyodrębnionego pliku gdzie znajdujemy odpowiedz:

```
chal@linux:~/Desktop$ strings msword.inf -n 8
!This program cannot be run in DOS mode.
text$mn
idata$5
rdata$zzzdbg
idata$2
idata$3
idata$4
idata$6
CloseHandle
ReleaseSemaphore
WaitForSingleObject
CreateEventA
OpenEventA
ExitThread
ResumeThread
CreateProcessA
GetThreadContext
SetThreadContext
VirtualAllocEx
WriteProcessMemory
CreateSemaphoreA
KERNEL32.dll
```

Answer: WriteProcessMemory

25. Extracting the shellcode from the dll file. What is the name of the library loaded by the shellcode



Adres atakującego generował bardzo dużo ruchu z portu 443 do ofiary w pakiecie 3561 można odczytać bibliotekę .dll która prawdopodobnie była załadowana do pamięci

26. Which port was configured to receive the reverse shell?

W dalszym etapie ataku adres ofiary wysyła bardzo dużo flag tcp.ack tak jakby wysyłał jakieś dane jest to typowe zachowanie revershella, Oprócz tego wysyła żądania do serwera http na adres atakującego z którego zostały wcześniej pobrane dwa złośliwe pliki

ip.src == 192.168.112.139 and ip.dst == 192.168.112.128						
No.	Time	Source	Destination	Protocol	Length Info	
	5142 137.765661	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11151514 Ack=259637 Win=524032 Len=6424	
	5143 137.765911	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11215754 Ack=259637 Win=524032 Len=6424	
	5144 137.766163	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11279994 Ack=259637 Win=524032 Len=6424	
	5145 137.766405	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11344234 Ack=259637 Win=524032 Len=6424	
	5146 137.766630	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11408474 Ack=259637 Win=524032 Len=6424	
	5147 137.766853	192.168.112.139	192.168.112.128	TCP	17574 50103 → 443 [ACK] Seq=11472714 Ack=259637 Win=524032 Len=1752	
	5161 137.767086	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11490234 Ack=259637 Win=524032 Len=6424	
	5162 137.767375	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11554474 Ack=259637 Win=524032 Len=6424	
	5163 137.767605	192.168.112.139	192.168.112.128	HTTP	3446 POST /Trm_QWz3GPappqinyPBWSgeXk3iW8bOMcj1yj-CAk3zd2WRScqc9Ity	
	5177 138.117526	192.168.112.139	192.168.112.128	HTTP	362 GET /Trm_QWz3GPappqinyPBWSgeXk3iW8bOMcj1yj-CAk3zd2WRScqc9ItyY	
	5179 138.141122	192.168.112.139	192.168.112.128	HTTP	362 GET /Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd2WRScqc9ItyY	
	5181 138.145380	192.168.112.139	192.168.112.128	HTTP	362 GET /Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd2WRScqc9ItyY	
	5183 138.147620	192.168.112.139	192.168.112.128	HTTP	362 GET /Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd2WRScqc9ItyY	
	5185 138.155842	192.168.112.139	192.168.112.128	TCP	388 50103 → 443 [PSH, ACK] Seq=11623338 Ack=260357 Win=525056 Len	
	5186 138.156458	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11623672 Ack=260357 Win=525056 Len=6424	
	5187 138.156862	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11687912 Ack=260357 Win=525056 Len=6424	
	5188 138.157110	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11752152 Ack=260357 Win=525056 Len=6424	
	5190 138.157378	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11816392 Ack=260357 Win=525056 Len=6424	
	5192 138.157614	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seq=11880632 Ack=260357 Win=525056 Len=6424	
	5195 138.157865	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Seg=11944872 Ack=260357 Win=525056 Len=6424	
	5197 138.158122	192.168.112.139	192.168.112.128	TCP	64294 50103 → 443 [ACK] Sea=12009112 Ack=260357 Win=525056 Len=6424	
→ F	rame 3547: 54 bytes	on wire (432 bits),	54 bytes captured	(432 bits)		
→ E	thernet II, Src: VM	ware_b7:ca:91 (00:0c	:29:b7:ca:91), Dst:	VMware_61:	f9:84 (00:0c:29:61:f9:84)	
> Internet Protocol Version 4, Src: 192.168.112.139, Dst: 192.168.112.128						
Transmission Control Protocol Sec Bort: 50102 Det Bort: 443 Sec. 327 Ack: 130425 Len: 0						

Answer: 443