RACTF2020 Writeup – Peculiar Packet Capture

Agent,

We have a situation brewing. Last week there was an attack on the prime minister of Morocco. His motorcade was stopped by a road blockade where heavily armed men opened fire on them. Fortunately, the prime minister was able to escape safely but many personnel and a few other ministers did not.

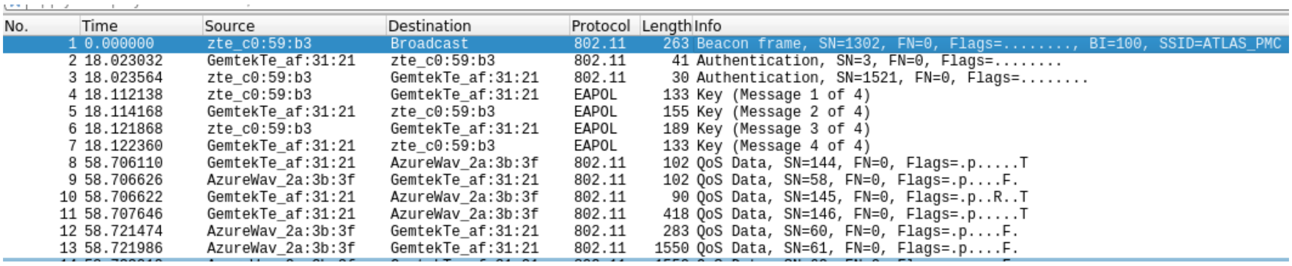
ATLAS, a multi-national Private Military Corporation (PMC) based in Colorado, USA, is our main suspect. We believe they were hired to conduct the hit by the opposition political party.

We flew Agent Jason to Colorado to investigate further. He gained access to their building's reception area dressed in a suit acting as a potential client with an appointment. He was able to intercept wireless network traffic from their corporate wireless network before being escorted out by guards when they realised the bluff.

The network capture is attached below, see if you can recover any important documents which could help us tie ATLAS to the Morocco incident.

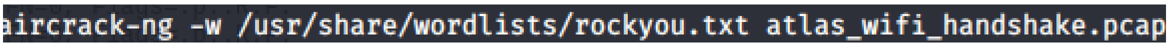
400 Points

In this challenge a packet capture was provided. Opening this in Wireshark produced the following:

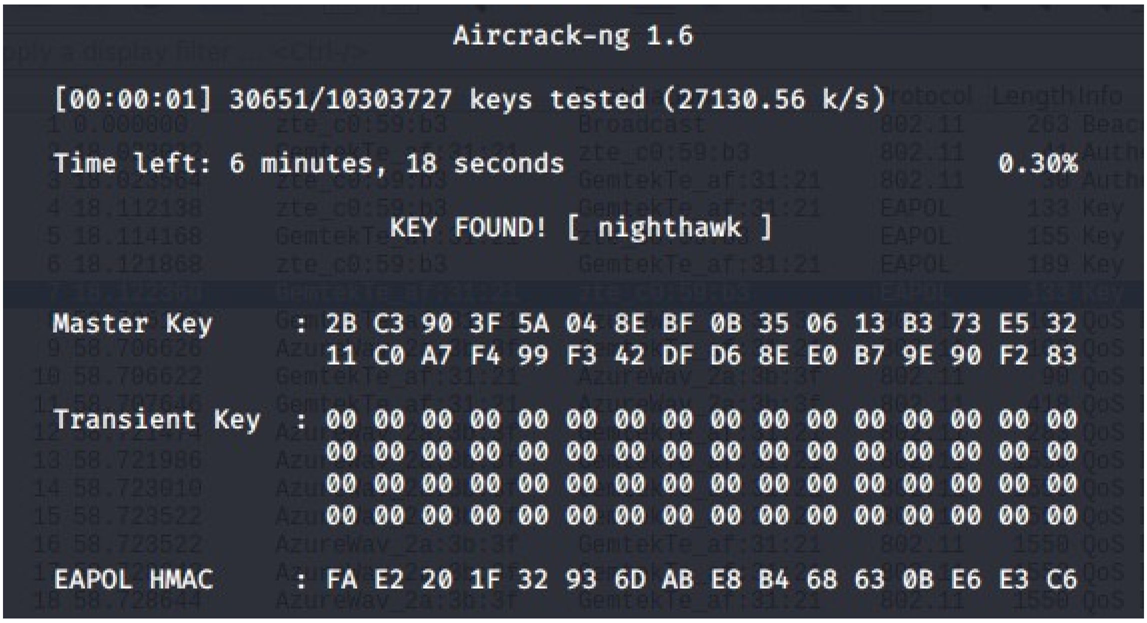


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	zte_c0:59:b3	Broadcast	802.11	263	Beacon frame, SN=1302, FN=0, Flags=........, BI=100, SSID=ATLAS_PMC
2	18.023032	GemtekTe_af:31:21	zte_c0:59:b3	802.11	41	Authentication, SN=3, FN=0, Flags=........
3	18.023564	zte_c0:59:b3	GemtekTe_af:31:21	802.11	30	Authentication, SN=1521, FN=0, Flags=........
4	18.112138	zte_c0:59:b3	GemtekTe_af:31:21	EAPOL	133	Key (Message 1 of 4)
5	18.114168	GemtekTe_af:31:21	zte_c0:59:b3	EAPOL	155	Key (Message 2 of 4)
6	18.121868	zte_c0:59:b3	GemtekTe_af:31:21	EAPOL	189	Key (Message 3 of 4)
7	18.122360	GemtekTe_af:31:21	zte_c0:59:b3	EAPOL	133	Key (Message 4 of 4)
8	58.706110	GemtekTe_af:31:21	AzureWav_2a:3b:3f	802.11	102	QoS Data, SN=144, FN=0, Flags=.p.....T
9	58.706626	AzureWav_2a:3b:3f	GemtekTe_af:31:21	802.11	102	QoS Data, SN=58, FN=0, Flags=.p....F.
10	58.706622	GemtekTe_af:31:21	AzureWav_2a:3b:3f	802.11	90	QoS Data, SN=145, FN=0, Flags=.p..R..T
11	58.707646	GemtekTe_af:31:21	AzureWav_2a:3b:3f	802.11	418	QoS Data, SN=146, FN=0, Flags=.p.....T
12	58.721474	AzureWav_2a:3b:3f	GemtekTe_af:31:21	802.11	283	QoS Data, SN=60, FN=0, Flags=.p....F.
13	58.721986	AzureWav_2a:3b:3f	GemtekTe_af:31:21	802.11	1550	QoS Data, SN=61, FN=0, Flags=.p....F.

Seeing the first 7 frames, I guessed this was a handshake between a client and a wireless access point, so I took these frames and separated them into a separate PCAP file. Using aircrack-ng I was able to identify it was a WPA passphrase and crack it with the rockyou password list:

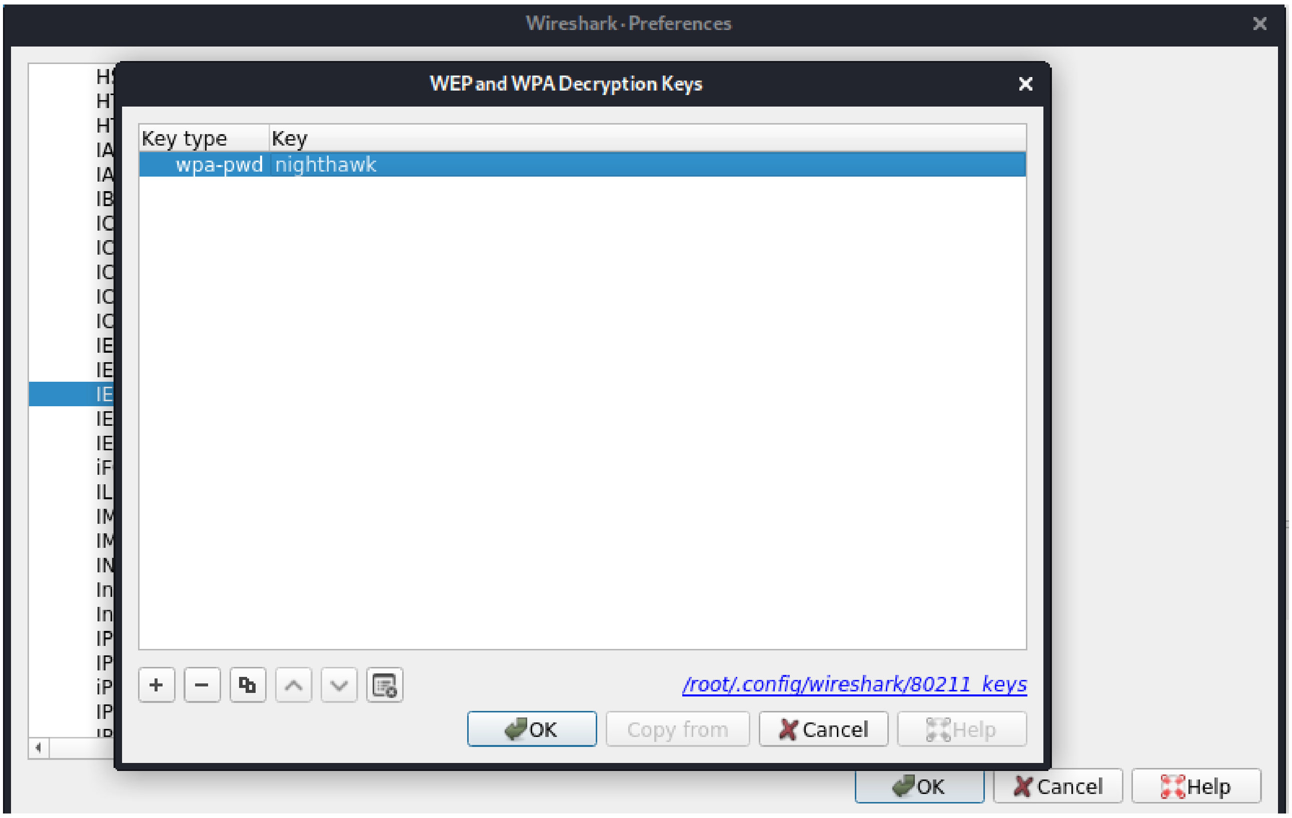


```
aircrack-ng -w /usr/share/wordlists/rockyou.txt atlas_wifi_handshake.pcap
```



```
                        Aircrack-ng 1.6

   [00:00:01] 30651/10303727 keys tested (27130.56 k/s)

   Time left: 6 minutes, 18 seconds                          0.30%

                      KEY FOUND! [ nighthawk ]


   Master Key     : 2B C3 90 3F 5A 04 8E BF 0B 35 06 13 B3 73 E5 32
                    11 C0 A7 F4 99 F3 42 DF D6 8E E0 B7 9E 90 F2 83

   Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   EAPOL HMAC     : FA E2 20 1F 32 93 6D AB E8 B4 68 63 0B E6 E3 C6
```

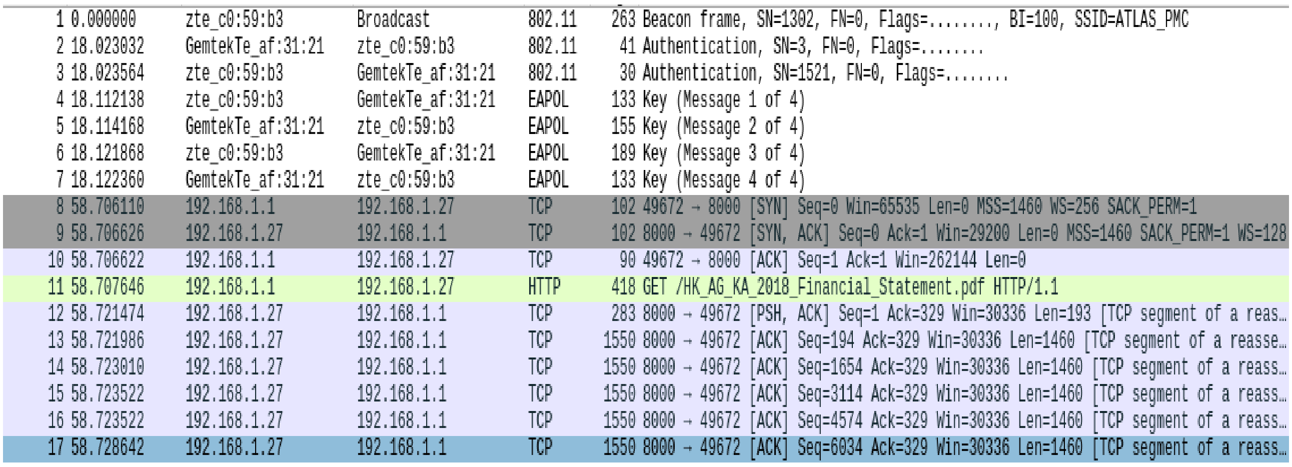
Back to the original PCAP file, I added nighthawk to the IEEE 802.11 protocol decryption keys:



Key type	Key
wpa-pwd	nighthawk

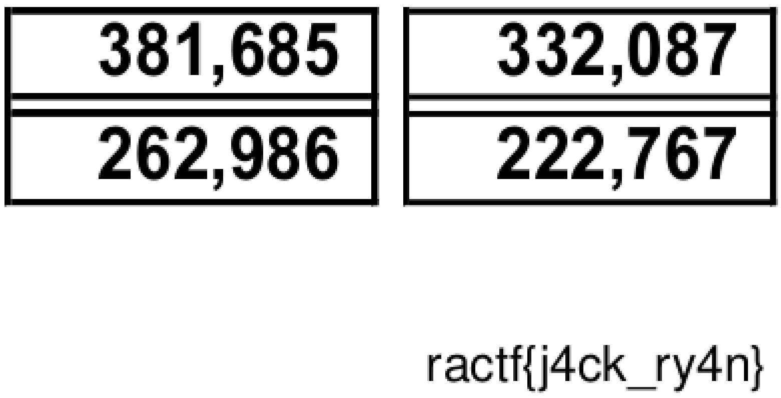
/root/.config/wireshark/80211_keys

This decrypted the packets within the PCAP file and found a PDF that had been transferred.



```
 1 0.000000   zte_c0:59:b3      Broadcast         802.11   263 Beacon frame, SN=1302, FN=0, Flags=........, BI=100, SSID=ATLAS_PMC
 2 18.023032  GemtekTe_af:31:21 zte_c0:59:b3      802.11    41 Authentication, SN=3, FN=0, Flags=........
 3 18.023564  zte_c0:59:b3      GemtekTe_af:31:21 802.11    30 Authentication, SN=1521, FN=0, Flags=........
 4 18.112138  zte_c0:59:b3      GemtekTe_af:31:21 EAPOL    133 Key (Message 1 of 4)
 5 18.114168  GemtekTe_af:31:21 zte_c0:59:b3      EAPOL    155 Key (Message 2 of 4)
 6 18.121868  zte_c0:59:b3      GemtekTe_af:31:21 EAPOL    189 Key (Message 3 of 4)
 7 18.122360  GemtekTe_af:31:21 zte_c0:59:b3      EAPOL    133 Key (Message 4 of 4)
 8 58.706110  192.168.1.1       192.168.1.27      TCP      102 49672 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 9 58.706626  192.168.1.27      192.168.1.1       TCP      102 8000 → 49672 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
10 58.706622  192.168.1.1       192.168.1.27      TCP       90 49672 → 8000 [ACK] Seq=1 Ack=1 Win=262144 Len=0
11 58.707646  192.168.1.1       192.168.1.27      HTTP     418 GET /HK_AG_KA_2018_Financial_Statement.pdf HTTP/1.1
12 58.721474  192.168.1.27      192.168.1.1       TCP      283 8000 → 49672 [PSH, ACK] Seq=1 Ack=329 Win=30336 Len=193 [TCP segment of a reas…
13 58.721986  192.168.1.27      192.168.1.1       TCP     1550 8000 → 49672 [ACK] Seq=194 Ack=329 Win=30336 Len=1460 [TCP segment of a reasse…
14 58.723010  192.168.1.27      192.168.1.1       TCP     1550 8000 → 49672 [ACK] Seq=1654 Ack=329 Win=30336 Len=1460 [TCP segment of a reass…
15 58.723522  192.168.1.27      192.168.1.1       TCP     1550 8000 → 49672 [ACK] Seq=3114 Ack=329 Win=30336 Len=1460 [TCP segment of a reass…
16 58.723522  192.168.1.27      192.168.1.1       TCP     1550 8000 → 49672 [ACK] Seq=4574 Ack=329 Win=30336 Len=1460 [TCP segment of a reass…
17 58.728642  192.168.1.27      192.168.1.1       TCP     1550 8000 → 49672 [ACK] Seq=6034 Ack=329 Win=30336 Len=1460 [TCP segment of a reass…
```

As it had been transmitted over HTTP, I was able to export the document and open it up. From this I was able to reveal the flag, hidden in the bottom right corner of the document:



381,685	332,087
262,986	222,767

ractf{j4ck_ry4n}