

DawgCTF 2020 Free WiFi Part 4

Saturday, March 7, 2020 12:16 PM

Given a .pcapng file that opens in wireshark. (same pcap, same site)

Hint: You need to generate your own key from the nonce provided each time.

30	2.857838198	3.82.133.247	10.0.2.15	HTTP	887	HTTP/1.0 200 OK (text/html)
85	23.199319815	10.0.2.15	3.82.133.247	HTTP	811	POST /staff.html HTTP/1.1 (application/x-www-form-urlencoded)
89	23.233862336	3.82.133.247	10.0.2.15	HTTP	2694	HTTP/1.0 200 OK (text/html)
113	25.474065080	10.0.2.15	3.82.133.247	HTTP	368	GET /static/bootstrap/css/bootstrap.min.css.map HTTP/1.1
115	25.583354568	3.82.133.247	10.0.2.15	HTTP	447	HTTP/1.0 404 NOT FOUND (text/html)
147	41.173437196	10.0.2.15	3.82.133.247	HTTP	555	GET /staff.html HTTP/1.1
151	41.210495515	3.82.133.247	10.0.2.15	HTTP	1148	HTTP/1.0 200 OK (text/html)
175	43.175598790	10.0.2.15	3.82.133.247	HTTP	368	GET /static/bootstrap/css/bootstrap.min.css.map HTTP/1.1
177	43.205132464	3.82.133.247	10.0.2.15	HTTP	447	HTTP/1.0 404 NOT FOUND (text/html)
217	65.196002237	10.0.2.15	3.82.133.247	HTTP	811	POST /staff.html HTTP/1.1 (application/x-www-form-urlencoded)
221	65.233219285	3.82.133.247	10.0.2.15	HTTP	2694	HTTP/1.0 200 OK (text/html)
233	67.305673226	10.0.2.15	3.82.133.247	HTTP	368	GET /static/bootstrap/css/bootstrap.min.css.map HTTP/1.1
235	67.334796028	3.82.133.247	10.0.2.15	HTTP	447	HTTP/1.0 404 NOT FOUND (text/html)
261	73.495438275	10.0.2.15	3.82.133.247	HTTP	553	GET /jwtlogin HTTP/1.1
263	73.525602558	3.82.133.247	10.0.2.15	HTTP	381	HTTP/1.0 401 UNAUTHORIZED (application/json)
285	99.689973636	10.0.2.15	3.82.133.247	HTTP	555	GET /staff.html HTTP/1.1
289	99.725239803	3.82.133.247	10.0.2.15	HTTP	1148	HTTP/1.0 200 OK (text/html)
313	101.607489295	10.0.2.15	3.82.133.247	HTTP	368	GET /static/bootstrap/css/bootstrap.min.css.map HTTP/1.1
Accept-Encoding: gzip, deflate\r\n						
Referer: http://freewifi.ctf.umbccd.io/staff.html\r\n						
Content-Type: application/x-www-form-urlencoded\r\n						
Content-Length: 134\r\n						
[Content length: 134]						
Cookie: WifiKey nonce=MjAyMC0wNC0wOCAxNzowMQ==; session=eyJjc3JmX3Rva2VuIjoIYtY4ZWQxZjVkd0hhZTgyZDEzMWY4ODhmZWExZjYwNDRmNTEwMDgyMCJ9.Xo35d0.zpNEVjf6uG_5vhqNCE7						
Cookie pair: WifiKey nonce=MjAyMC0wNC0wOCAxNzowMQ==						
Cookie pair: session=eyJjc3JmX3Rva2VuIjoIYtY4ZWQxZjVkd0hhZTgyZDEzMWY4ODhmZWExZjYwNDRmNTEwMDgyMCJ9.Xo35d0.zpNEVjf6uG_5vhqNCE7bS8QEz0						
Connection: keep-alive\r\n						
Upgrade-Insecure-Requests: 1\r\n						
\r\n						
[Full request URI: http://freewifi.ctf.umbccd.io/staff.html]						
[HTTP request 1/1]						
[Response in frame: 89]						
File Data: 134 bytes						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "csrf_token" = "ImE4OGVhZWQxZjVkd0hhZTgyZDEzMWY4ODhmZWExZjYwNDRmNTEwMDgyMCJ9.Xo35d0.zpNEVjf6uG_5vhqNCE7bS8QEz0"						
Form item: "passcode" = "5004f47a"						
Form item: "submit" = "Submit"						


They suggest the passcode is a function of the nonce.

I tried taking the nonce MjAyMC0wNC0wOCAxNzowMQ==
(decodes into: 2020-04-08 17:01)

and pasted it into a site that produces all the hashes:

<https://www.browserling.com/tools/all-hashes>

MiAvMC0wNC0wOCAxNzowMQ==

Calculate Hashes!  (undo)

NTLM	58097D2F7FD1F82F6370E7EED3BE48FA	MD2	fa6dd74d6052a6775a19eb6a9d0ef37b
MD4	ff5ace977274de42e0baa8fb66d48c21	MD5	5179d1417da290b9073e27ffb8df9349
MD6-128	a93822510f4a8a8910e2ce227008ad49	MD6-256	98f6cdc71b490ec917eb96a1bf61dc87767b65b6f9ff9bc
MD6-512	2cf2b84fc03a0aaf2a1d164e230faf6497db486382e665	RipeMD-128	e788e52f200badf864d2584a480abd71
RipeMD-160	4469231f5251da10fbb276dff4676e3317394108	RipeMD-256	1bdd7ce6f860ace22816a2c41e6d8be89d309f7ca7db2c
RipeMD-320	f900df24e10fa7c70fe9a92d8454f0df47e57efbcaa660f4	SHA1	5004f47ae3e2e7c1c9a5ea4d1666f95e6b06b062
SHA3-224	532d1d2ad3e421525ebcef1453a9f6f5cd536d494393e	SHA3-256	f8751222fa55dca371a84c2f6c5d10d1ad5c31013c4e72f
SHA3-384	cfdcc0743bc226ea5c2d6d3e36af089627c2a7f5c332f	SHA3-512	09a14b8075bf373faadf3c20953fda24d1b6eeb18ba759
SHA-224	cae20d86f02ba6cd372c229375e390eedd676c7473d5e	SHA-256	574566f41c70e58b8f46b8379d8d0689832a1ffcd124c6
SHA-384	5c13882802d213afeba272f0217f28aa38fe40eb758c21f	SHA-512	65558a7d9e8a2a3b350191479f9b1b3434390476d810
CRC16	ef2e	CRC32	3e2e3417
Adler32	62fd07f2	Whirlpool	8547a620b1da9ea41760bbaecb8f3fdfe18eb49003788

and I see the SHA1 hash: 5004f47ae3e2e7c1c9a5ea4d1666f95e6b06b062

The first 8 chars match with the passcode in wireshark!

So, I played with this page and got the nonce and decoded it. It changes every minute, so I increased the minute by one to give me time and re b64'd it. Generated the sha1 hash from that.

The I entered that sha1 hash and kept pressing enter. Once that minute clicked past, it revealed this flag:

Welcome to the staff login page!

Staff login

You may use either of the following methods to logon.

Username:

Password:

Submit

[Forgot your password?](#)

OR

Login with WifiKey:

Submit

DawgCTF{k3y_b@s3d_l0g1n!}