Devin Lewis

When I first attempted to make contact with the server “your webpage” I noticed a new protocol being used in blue that was DNS, where it said “standard query” and “standard query response” which I assume was to make contact with the server.

Afterwards, I send the standard GET method to try and get the webpage “/basicauth/”, however unlike usual where I go to the website I get hit with a request to enter a username and password. The server, at that moment, responded to my request by sending me “Unauthorized (text/html)” so I assume that this is the request page for my username and password.

11	0.070467196	192.168.2.129	45.79.89.123	HTTP	395	GET /basicauth/ HTTP/1.1
12	0.070861615	45.79.89.123	192.168.2.129	TCP	60	80 → 40654 [ACK] Seq=1 Ack=342 Win=64240 Len=0
13	0.116508049	45.79.89.123	192.168.2.129	HTTP	457	HTTP/1.1 401 Unauthorized (text/html)

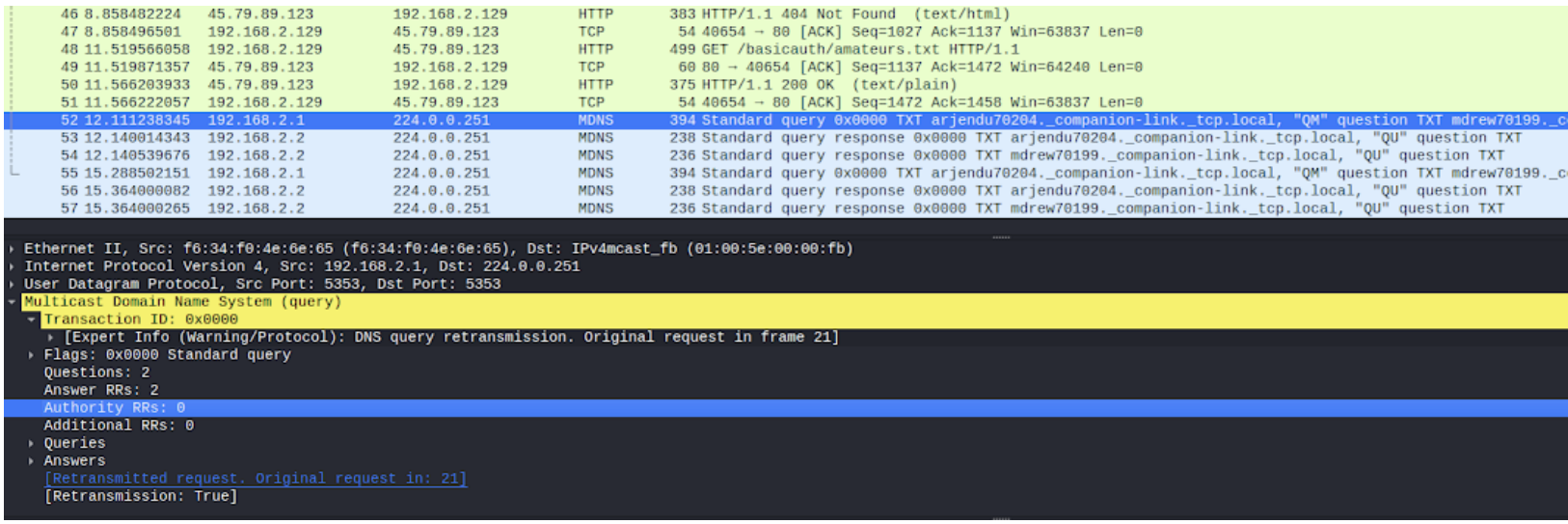
While I’m typing in the username and password, what’s strange was that I saw a lot of ACK (which acknowledges the connection and requests) but I also saw from both the server and my computer a lot of FIN, even though the connection didn’t end at all. I also saw a new three letter word called PSH, though I’m not sure what that does.

I then saw a series of MDNS protocols from my computer to the server, then at the end of that my computer made the request to access the website again with the same GET method. With that in mind I can safely assume that in those MDNS protocols are my answers for the username and password.

19	5.244492530	VMware_5f:4e:7e	VMware_f3:a4:6d	ARP	42	Who has 192.168.2.2? Tell 192.168.2.129
20	5.244904911	VMware_f3:a4:6d	VMware_5f:4e:7e	ARP	60	192.168.2.2 is at 00:50:56:f3:a4:6d
21	7.256757726	192.168.2.1	224.0.0.251	MDNS	291	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question TXT wcc02760326._compa
22	7.257762375	192.168.2.2	224.0.0.251	MDNS	597	Standard query response 0x0000 PTR _ipp._tcp.local, "QU" question PTR WCC225-CC5550 @ wnordq62292._ipp._tcp.local SRV 0 0 631
23	7.257762592	192.168.2.2	224.0.0.251	MDNS	611	Standard query response 0x0000 PTR _ipp._tcp.local, "QU" question PTR OKI DATA CORP C331 @ biolstu62160._ipp._tcp.local SRV 0
24	7.257762648	192.168.2.2	224.0.0.251	MDNS	341	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR sanderson266942._companion-link._tcp.local S
25	7.257762705	192.168.2.2	224.0.0.251	MDNS	396	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question TXT arjendu70204._companion-link._tcp.local, "QU
26	7.257881014	192.168.2.2	224.0.0.251	MDNS	332	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR avanenge68356._companion-link._tcp.local SRV
27	7.258161985	192.168.2.2	224.0.0.251	MDNS	385	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR SMOHRING67565._companion-link._tcp.local SRV
28	7.258162175	192.168.2.2	224.0.0.251	MDNS	384	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR mdrew70199._companion-link._tcp.local SRV 0
29	7.258345990	192.168.2.2	224.0.0.251	MDNS	272	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR jstrand65553._companion-link._tcp.local SRV
30	7.258618465	192.168.2.2	224.0.0.251	MDNS	324	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR ehazlett62531._companion-link._tcp.local SRV
31	7.258982785	192.168.2.2	224.0.0.251	MDNS	335	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR rhoffner68346._companion-link._tcp.local SRV
32	7.259215144	192.168.2.2	224.0.0.251	MDNS	332	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR sgaldeen68357._companion-link._tcp.local SRV
33	7.259488646	192.168.2.2	224.0.0.251	MDNS	350	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR lpearson67009._companion-link._tcp.local SRV
34	7.259686539	192.168.2.2	224.0.0.251	MDNS	325	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR aknodell65360._companion-link._tcp.local SRV
35	7.260101354	192.168.2.2	224.0.0.251	MDNS	275	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question TXT wcc02760326._companion-link._tcp.local, "QU"
36	7.260290693	192.168.2.2	224.0.0.251	MDNS	326	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR bhaileab59824._companion-link._tcp.local SRV
37	7.260487316	192.168.2.2	224.0.0.251	MDNS	337	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR mzimmerm63315._companion-link._tcp.local SRV
38	7.260658251	192.168.2.2	224.0.0.251	MDNS	398	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question PTR DevSpace._companion-link._tcp.local SRV 0 0
39	7.261022835	192.168.2.2	224.0.0.251	MDNS	275	Standard query response 0x0000 PTR _companion-link._tcp.local, "QU" question TXT rhagen59159._companion-link._tcp.local, "QU"

What's also worth pointing out was this new protocol at the very top called ARP, which actually checked with my VMware software to see what what my current server was running on, so it is interesting knowing that it checks where you're trying to access the website from, or maybe that's only a VMware thing i'm not sure.

Once I've connected to the site I try to connect to amateurs.txt with the get method, the server returns an ok and returns the file but on wireshark you actually see it go through another standard query / standard query response chain. On the very first frame of that chain it also references back to the original DNS request (which was apparently in frame 21) and also retransmitts that request, which means it checks your authentication even when you've already gained access to the site.



In every MDNS protocol frame there was a section labeled queries and answers, which I assume are in correlation with the authentication process for computers. From that I could see that the passwords were encrypted but I'm not sure on where the encryption key came from, but it does relate back to HTTP Basic Authentication since I can at least tell it's not encoding the text since it's not using the basic encoding screen.

I still have a lot of questions though, like why are there several MDNS protocols in a row, and why are all of the sources sourced from my computer? What is ARP? What exactly is Unauthorized text/html? And the biggest one, why did it seem like I saw a bunch of other carleton usernames while I was looking at each frame in the MDNS chain? They were all next to something called a “companion-link” but I wouldn’t even know where to start with that.