Alanna Richerson

November 7, 2024

IT 315 Intro to Network & Security

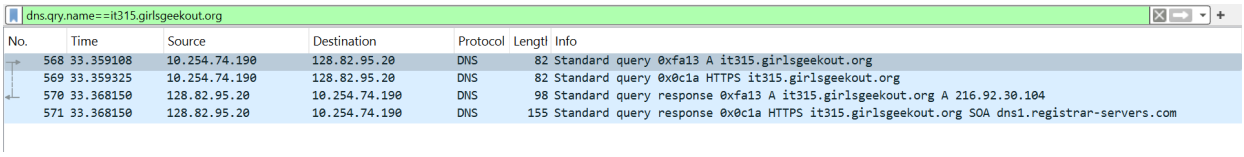
Install Wireshark on your computer or use one of the lab computers with Wireshark installed on it.

Wireshark Install: www.wireshark.org... NOT www.wireshark.com

Do the following:

1. Open Wireshark and start a packet capture. (There are lots of videos on YouTube that explain it, like this one: https://www.youtube.com/watch?v=jvuiI1Leg6w)
2. Switch to your web browser and connect to http://IT315.girlsgeekout.org; NOTE: This is http, not https.
3. Type your name in the form and click Submit.
4. Switch back to Wireshark and stop the packet capture.

Do the following in Wireshark and submit answers to the questions:

1. Use the display filter "dns". Find the packet with the info that says "Standard Query Response" for IT315.girlsgeekout.org. What is the IP address of http://IT315.girlsgeekout.org?Links to an external site. Hint: It's the IP address on the far right of the entry, next to "A".
    1. The IP address for IT315.girlsgeekout.org is 216.92.30.104.
    2. 

dns.qry.name==it315.girlsgeekout.org

No.	Time	Source	Destination	Protocol	Length	Info
568	33.359108	10.254.74.190	128.82.95.20	DNS	82	Standard query 0xfa13 A it315.girlsgeekout.org
569	33.359325	10.254.74.190	128.82.95.20	DNS	82	Standard query 0x0c1a HTTPS it315.girlsgeekout.org
570	33.368150	128.82.95.20	10.254.74.190	DNS	98	Standard query response 0xfa13 A it315.girlsgeekout.org A 216.92.30.104
571	33.368150	128.82.95.20	10.254.74.190	DNS	155	Standard query response 0x0c1a HTTPS it315.girlsgeekout.org SOA dns1.registrar-servers.com

2. Use the display filter "ip.addr == " with the IP address of http://IT315.girlsgeekout.org to limit the display to show only traffic to and from http://IT315.girlsgeekout.org. Find the packet where your browser application sent a GET command with your name. How did the website know your first and last name?
    1. 577 GET /index.php?firstname=Alanna&lastname==Richerson HTTp/1.1

2. ip.addr == 216.92.30.104

No.	Time	Source	Destination	Protocol	Lengtl	Info
611	33.467419	216.92.30.104	10.254.74.190	HTTP	450	HTTP/1.1 404 Not Found (text/html)
613	33.517032	10.254.74.190	216.92.30.104	TCP	54	49859 → 80 [ACK] Seq=826 Ack=993 Win=130048 Len=0
623	38.480051	216.92.30.104	10.254.74.190	TCP	56	80 → 49859 [FIN, ACK] Seq=993 Ack=826 Win=131328 Len=0
624	38.480128	10.254.74.190	216.92.30.104	TCP	54	49859 → 80 [ACK] Seq=826 Ack=994 Win=130048 Len=0
627	39.608619	10.254.74.190	216.92.30.104	TCP	54	49859 → 80 [FIN, ACK] Seq=826 Ack=994 Win=130048 Len=0
628	39.608807	10.254.74.190	216.92.30.104	TCP	66	49862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
629	39.609080	10.254.74.190	216.92.30.104	HTTP	577	GET /index.php?firstname=Alanna&lastname=Richerson HTTP/1.1
637	39.622266	216.92.30.104	10.254.74.190	TCP	56	80 → 49859 [ACK] Seq=994 Ack=827 Win=131264 Len=0

3.

3. Find the server's response to that GET command (it should say "HTTP/1.1 200 OK). What type of data is contained in this packet?
    1. 661 HTTP/1.1 200 O (text/html)
    2. ip.addr == 216.92.30.104

No.	Time	Source	Destination	Protocol	Lengtl	Info
628	39.608807	10.254.74.190	216.92.30.104	TCP	66	49862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
629	39.609080	10.254.74.190	216.92.30.104	HTTP	577	GET /index.php?firstname=Alanna&lastname=Richerson HTTP/1.1
637	39.622266	216.92.30.104	10.254.74.190	TCP	56	80 → 49859 [ACK] Seq=994 Ack=827 Win=131264 Len=0
641	39.622266	216.92.30.104	10.254.74.190	TCP	66	80 → 49862 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1382 WS=64 SACK_PERM
643	39.622740	10.254.74.190	216.92.30.104	TCP	54	49862 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
646	39.628476	216.92.30.104	10.254.74.190	HTTP	661	HTTP/1.1 200 OK (text/html)

    3. The type of data that is contained in this packet is Line-based text data: text/html (21 lines)
4. Think about what you have seen in this packet capture. Why is it important to have network traffic encrypted rather than appearing in clear text?
    1. It is important to have network traffic encrypted rater than appearing in clear text because it prevents unauthorized interception and reading of sensitive data. A significant risk arises with unencrypted traffic because it can be easily intercepted and viewed by anyone with network access, possibly leading to data breaches and security vulnerabilities. Encryption serves as a protective measure, making sensitive information unreadable to unauthorized parties.