M Gmail   **Adicherla VenkataSai <adicherlavenkatasai5@gmail.com>**

[MTech-CSE-21] PKI Assignment 1
1 message

shivanshu mehta <shivanshudm@gmail.com>   Wed, Jan 8, 2020 at 4:03 PM
To: mtech-cse-21@googlegroups.com
Cc: baluparne@gmail.com

Hello All,

Please find below. The due date is 29-JAN-2020.

Assignment 1:

A. Use wireshark to caputre the packet showing the username and the password in the clear text from the SVNIT mail server. (mail.svnit.ac.in)
B. Use wireshark to capture the packet showing credentials on any HTTPS website (e.g. gmail, facebook etc.) and show that the content is encrypted in wireshark.
C. Install a local web server. (e.g. Apache).
D. Generate and install self-certified SSL certificate on local web server installed in C.
E. Use wireshark to capture the packets being transmitted to and from local web server and show that the content is encrypted.
F. Use Private Key of Generated SSL certificate (in D) to decrypt the packets captured in wireshark as in (E).
G. When you make an encrypted connection to any public HTTPS website, your browser stores the negotiated session key. This key is normally stored in a file called "SSLKEYLOGFILE". Use wireshark to use the key stored in this file and decrypt the content of packets transferred between your machine and the public HTTPS website.
HINT for F: Wireshark only supports a certain TLS encryption algorithm for Decryption part. So, you will need to find out which algorithm wireshark supports and then you will need to ensure that the server always picks only that encryption algorithm for any connection.
Hint for G: It only works on specific OS and specific browser.

Thanks and Regards,

Shivanshu Mehta.

--
You received this message because you are subscribed to the Google Groups "MTECH CSE '21" group.
To unsubscribe from this group and stop receiving emails from it, send an email to mtech-cse-21+unsubscribe@googlegroups.com.
To view this discussion on the web, visit https://groups.google.com/d/msgid/mtech-cse-21/CAN%2B_N8ujT0z6DOQV4bbQ-5M5y%2BKcHdux2ffSawo8a_9Du-5nLg%40mail.gmail.com.