Decrypt SSL Traffic

Using wireshark to decrypt SSL traffic on a server.

Step-by-step guide

1. Download wireshark and libsmi to the server: ' sudo yum install wireshark ' will install both.
    a. If the server is behind a proxy, get with your team/tech lead to allow the server to reach the rpm repos through iron port.
2. Download wireshark-devel: ' sudo yum install wireshark-devel '.
    a. If the server is behind a proxy, get with your team/tech lead to allow the server to reach the rpm repos through iron port.
3. Verify wireshark has GnuTLS and Gcrypt modules: ' tshark -v '.
4. Create the tshark capture ' sudo tshark '.
    a. Add the attribute to group SSL packets together. Ironically, the command is: ' -o "ssl.desegment_ssl_records:TRUE" '.
    b. Add the attribute to group application data packets together: ' -o "ssl.desegment_ssl_application_data:TRUE" '.
    c. Add the attribute to decrypt the data with a pem/cert: ' -o "ssl.keys_list:127.0.0.1,443,http,key.pem" ' <ssl.keys_list: ip_address, ssl_port, decode_data_as, key_file>
        i. Server keys can generally be found in /etc/httpd/conf/ folder in Linux. Must be root to view the contents of the folder.
    d. Add the verbose attribute: ' -V ' to show packet data.
    e. For the best results, send the data to a txt file: ' > file_name.txt '

    Whole example:

    ```
    sudo tshark -o "ssl.desegment_ssl_records:TRUE" -o
    "ssl.desegment_ssl_application_data:TRUE" -o
    "ssl.keys_list:127.0.0.1,443,http,key.pem" -V > auth_test.txt
    ```

    Other options are available here: https://www.wireshark.org/docs/wsug_html_chunked/ChCustCommandLine.html or using the command: 'man tshark' or 'tshark --help'
    The most useful options:
        i. Putting a separator between packets: ' -S <separator> '. Example ' -S _____ '
        ii. Specifying a specific network interface to capture: ' -i <interface> '. Example ' -i eth0 '
        iii. Capture data on a specific port: ' -R <protocol>.port == <port> '. Example ' -R tcp.port==80 '
5. Starting a tshark run will show the lines:
    a. Running as user "root" and group "root". This could be dangerous.
    b. Capturing on eth0.
6. Open your browser and go to the website. Generally a POST result shows up best in the logs.
7. Close tshark (CTRL + C).
8. After the run, read the contents of the file. Most of the data is gibberish. Search for "GET" or "POST"

References

https://wiki.wireshark.org/SSL#SSL_dissection_in_Wireshark

Related articles

- Import Code Styles to an IDE
- Technology Stack
- BSL Network Room IT Startup/Shutdown Procedures
- Install .NET Framework 3.5 on Windows 10
- Decrypt SSL Traffic