בס"ד

TLS Exercise (Barak Gonen):

I. Cypher suites (20 points)

1. In this section, we will check the security level of domains using Cipher suites enumeration.

Run (using Linux or WSL) the following command on three sites of your choice.

```
nmap –script ssl-enum-ciphers -p 443 domain_name > domain_name.txt
```

Specify for each site:

A. What is the lowest security level of the Cipher suits?

B. Is there any support for TLS versions with poor security?

C. Are there any other security issues?

D. Run the command on the ***ohel-shem.iscool.co.il*** domain and repeat the questions A B C.

Note: Nmap is a source Linux command-line tool, used for network exploration, host discovery, and security auditing. Gordon Lyon created it to help map an entire network easily and find its open ports and services.

To install nmap on WSL: "sudo apt-get update && apt-get install nmap" and/or "sudo apt install nmap".

II. Certificates (20 points)

2. In this section, we will investigate certificates. Using WSL or Linux, perform a certificate investigation as demonstrated in the video. Answer the following questions on a site of your choice:

A. What is the certificate chain?

B. What is the Common Name (CN) of the domain to which the certificate belongs?

C. What is the signature and hash algorithm of the certificate?

D. How many bits are there in the encryption key?

For the following domains, specify what the error message is in the certificate (the text

which is found after Verify error) . If there is no error- capture the “verify return” value:

E. ***revoked.badssl.com***

F. ***untrusted.badssl.com***

G. ***self-signed.badssl.com***

III. TLS v1.2 handshake (30 points)

Open the snipping file **TLSsniffEx.pcapng**.

3. How many packets contain Client Hello? What is the filter that allows you to find packets of this type only?

4. Focus on the first Client Hello packet. What is the domain name to which you are browsing to?

5. What filter can be put in Wireshark to receive only the Client Hello, which is intended for a Server Name of our choice?

6. What is the TLS version?

7. What is the Cipher Suite chosen by the server? What algorithm is used for the following operations?

a. Hashing
b. Encryption
c. Authentication
d. Key Exchange

8. How many certificates are sent by the server? What is their common name?

9. Is the certificate also valid for other URLs that are under hattrick.org?

10. Between which dates is the hattrick.org certificate valid?

11. Who is the Root Certificate Authority and was his certificate sent to the client?

12. How does the customer verify that the hattrick.org certificate is not revoked? Is it through the Certificate Revocation List, through the OCSP protocol (Online Certification Status Protocol) or through OCSP Stapling?

13. Which Record is sent from the server to the client and would not have been sent if the key exchange was with the RSA algorithm? What does this record include when it is sent?

14. What is the handshake type of the Client Key Exchange and what does it include? Does the customer sign it?

15. Use the SSL log file to decrypt the encrypted information. How can wireshark pick a specific set of keys, from all the keys in the file, which is the correct key set for the TLS session? There is a value which appears both in the sniffing and in the Wireshark log. What is the name of that field, in wireshark?

16. What is the first resource that the client does a GET for? What is the received status code? Explain what the customer will do as a result.

17. Follow TLS Stream. In the search screen, search for **Username** and **Password**.

IV. TLS v1.3 Handshake (30 points)

Browse to a website of your choise, who uses TLS v1.3. Provide proof of your responses (using screen captures)

Client Hello:

18. What version exists in the Record Header? What version exists in the Client Hello Version field?

19. What are the first 6 hex digits of the Client Random number?

20. What are the first 6 hex digits of the Session ID?

21. How many Cipher Suites did the client propose?

22. Which Cipher Suites are TLS 1.3?

23. Use the Extension “Key_Share”. Which Diffie-Hellman curve is chosen by the client?

24. At this point, does the client know that this DH curve is supported by the server?

Server Hello:

25. What version exists in the Record Header? What version exists in the Server Hello Version field?

26. What are the first 6 hex digits of the Server Random number?

27. What are the first 6 hex digits of the Session ID? How does it compare to the client Session ID? Why?

28. Which Cipher Suites did the server choose?

29. Use the Extension “Key_Share”. Which Diffie-Hellman curve is chosen by the server?

30. Did the client guess correctly? What would happen if not?

Certificate:

Decrypt the TLS communication.

31. What is the certificate chain used?

32. Which field indicates that this certificate belongs to the server you connected?

The End, Good luck!