University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 11: Network Perimeter Security

Question 1: TLS/SSL Inspection

a. How can a firewall decrypt and read TLS traffic, and what is the name of this technique?
b. How can a user know whether TLS traffic is being decrypted by a firewall ?

Question 2: CAA and CT combined with TLS/SSL Inspection

See the lecture on Key Management and PKI to recap the principles of DNS CAA (Certificate Authority Authorization) and CT (Certificate Transparency).

a. Is CAA compatible with TLS Inspection? Explain why or why not.
b. Is CT compatible with TLS Inspection? Explain why or why not.
c. Is Certificate Pinning compatible with TLS Inspection? Explain why or why not. Certificate Pinning has not been explained in the lectures, but you can read about it on e.g. https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

Question 3: Windows Defender Firewall

Windows Defender Firewall is integrated with Windows 10. If you have Windows 10 on your computer, take a look at the inbound rules and outbound rules. Identify inbound rules made for 3rd party applications that you have installed, i.e. not generic rules for Windows 10 or for your computer. What would happen if you removed an application specific rule?

Question 4: Base-Rate Fallacy in Intrusion Detection

The so-called base-rate fallacy is a reasoning error which can lead to false alarms in an IDS.

a. What is meant by the base-rate fallacy?
b. The base-rate fallacy is a typical reasoning error in medical diagnostics as well as in legal reasoning about evidence (where it is called “the prosecutor’s fallacy”). Give an example of the base-rate fallacy in these two disciplines.
c. What can be done to avoid the base-rate fallacy?
d. Assume that A denotes an Attack, and that D denotes the Detection of signature of attack. The meaning of the conditional probability p(D|A) is then: The probability of Detected signature given that Attack occurs. How can conditional probabilities be inverted, i.e. how to convert p(D|A) into p(A|D), and which base-rate probability is needed to do that ?

Question 5: WLAN Security

a. What do the abbreviations STA, AP, AS, BSS, ESS and DS mean in relation to IEEE 802.11 WLAN? Briefly describe each concept and how they are related.
b. List and briefly describe the 5 IEEE 802.11i phases of operation.