CS 418/618 System and Usable Security: End Semester Exam

Dr. Neminath Hubballi

24-11-2021, 10:00 AM to 01:00 PM

Instructions

1. Scanning should be consistent (only portrait mode), clearly visible and only one pdf document should be uploaded after doing all sanity checks. Incomplete and improperly scanned and invisible answer scripts will not be evaluated.
2. Marks for each question is shown at the end in bold lettered number within bracket.

Questions

1. Differentiate between Random Access Memory (RAM) and Content Addressable Memory (CAM). Can RAM be useed in networking devices ? Why CAM is preferred over RAM ? (**4**)
2. A user selects password as ”rainbow”. Assuming this is processed and stored using Windows LAN password manager, outline the step by step operation (need not show the actual hash values). (**5**)
3. Mention 3 types of Phishing attacks and give a two lines description with an example. (**4**)
4. What is delegation DNS signer ? How many delegation signers can be there in the DNS hierarchy ? (**2**)
5. Give an example scenario for the lest common mechanism security principle. (**2**)
6. Write a firewall rule to (i)Accept connection from IP prefix of 30.10.0.0/16 on port number 25 (ii) of TCP (iii) going to a web server with IP address 100.10.10.10 (**3**)
7. What is SYN Cookie ? and how it helps in preventing SYN flood attacks ? (**3**)
8. Assuming you are a system admin in-charge of maintaining a network and you are asked to configure a firewall which by default is using a deny-all strategy, write a firewall rule to permit a user on the external network to connect to a server in the internal network with IP address 10.2.1.1 on port number 5000. (**3**)
9. What is rainbow table and how it is used to crack passwords ? (**3**)
10. Which of the following TCP congestion control based attack does not preserve the end-to-end reliability semantics (**1**)

    (a) ACK division

(b) DupACK

(c) Optimistic ACKing

11. Write a snort rule to detect TCP-SYN flood attack mounted on a web server which is running on port 80 having IP 192.168.10.1. Assume for the current scenario a system is said to be under syn-flood attack if it receives more than 1000 connections request in an interval of 10 seconds. (**4**)

12. Write a snort rule to search for content using perl compatible regular expression to search string google.php?id=<some integer>. Here the length of some integer ranges between 1-5. Example for some valid and invalid searches are: (**4**)

    - google.php?id=1 is valid
    - google.php?id= 14678 is valid
    - google.php?id= 123654 is invalid

13. Write hping3 commands to do the following on a web server running on port 80 having IP address 192.168.10.1 (**4**)

    (a) SYN flood attack

    (b) Port Scan for port range 0-500

    (c) send 10 spoofed ICMP messages using random source

14. Write wireshark capture filter to grab tcp packets with syn flag set. (**2**)

15. An adversary is is trying to login to a remote server using SSH. She is trying different passwords by systematically generating them. Can you suggest a method to detect such attacks using Intrusion Detection System ? Briefly tell how your proposed solution will detect them. (**3**)

16. Mention different techniques used to detect spoofed IP packets. Briefly elaborate how TTL value will be useful in this scenario. (**3**)