IIT 3221 COMPUTER AND NETWORK SECURITY YEAR 2 SEM 2

DURATION: 2HRS

Instructions

1. This paper contains FIVE questions
2. Answer one (compulsory) and any other TWO questions
3. Answer each question on a new page.

QUESTION ONE (COMPULSORY) [30 MARKS]

(a) Explain the significance of the following abbreviations to network security. [4 Marks]

(i) DMZ (iii) MD5

(ii) IPsec (iv) SSL

(b) Daniel wants to protect himself against rootkits, so he runs a virtual Windows XP system on top of Mac OS X. Is Daniel vulnerable to Windows XP rootkits? Explain. [4 Marks]

(c) Differentiate between the following as applies to network security [4 Marks]

(i) Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

(ii) Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS)

(d) Name any TWO intelligent gathering tools that can be used in a network. [2 Marks]

(e) Explain how a targeted worm or virus can avoid detection by virus scanner. [2 Marks]

(f) "Firewalls can be used to block all distributed denial of service attacks while allowing all authorized communications".

(i) Do you agree with the above statement? Explain your answer. [3 Marks]

(ii) Identify any THREE network threats that a firewall does not protect against. [3 Marks]

(iii) Explain one weakness of firewall at network perimeter in defending servers, desktop machines, and laptops against network threats. [2 Marks]

(g) In a Mandatory Access Control system, how can an insider with access to high-security file leak information to a low-security process using the virtual memory system? [2 Marks]

(h) Give FOUR security issues commonly found with corporate VOIP implementation. [4 Marks]

QUESTION TWO **[20 MARKS]**

(a) Explain any THREE common sources of security vulnerabilities problems in computer networks. [6 Marks]

(b) Using a well labeled diagram, explain the components of an operating systems security environment. [6 Marks]

(c) How does file permissions implementation on Windows differs with UNIX? Use an example to support your answer. [4 Marks]

(d) Describe two fundamentally different conceptual approaches that can be used for user authentication. [4 Marks]

QUESTION THREE **[20 MARKS]**

(a) Studies have shown that on-line banking services have become primary targets of cyber attacks. Phishing, password database theft, Man-in-the-Middle attack, Man-in-the Browser attack, key logging and pharming are among the top threats identified in on-line banking services. Explain how any four of the mentioned attacks is performed and respective countermeasure. [8 Marks]

(b) Consider the Biashara Authentication Web Server, which uses a web page with a user name and user password (the password must be between 9 and 255 characters, and must contain at least three of the following: uppercase letters, lowercase letters, numbers, punctuation, and all other characters), connected via SSL to net-auth.biashara.co.ke. The web server sits behind a firewall that examines the contents of packets including reconstructing connection streams.

(i) Briefly explain THREE different plausible ways to attack such a system and gain unauthorized access. [6 Marks]

(ii) Use a diagram to explain how Biashara Company Limited could use firewall to protect against transmitting unencrypted credit card numbers over the network. [6 Marks]

QUESTION FOUR **[20 MARKS]**

(a) With the aid of well labeled diagram, explain the following; [12 Marks]

(i) DNS Rebinding Attack

(ii) SYN Flooding Attack

(iii) Smurf DOS Attack

(iv) TCP Connection Spoofing

(b) A software company is selling a new defense against DDoS attacks. Their software looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 1% of traffic over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. Their marketing folks are claiming that this will stop all DDoS attacks cold in the water. Is this a good solution to the problem? Give one reason to support your answer. [4 Marks]

(c) The military runs a multi-user computer that all government employees can log into; programs that require access to top-secret data are run inside a virtual machine. Suppose Captain Peter is given an account on this computer so that he can install emacs. Colonel Oguta runs a copy of Peter's emacs program inside a virtual machine and uses it to edit the top-secret list stored in warehouses. (Only Oguta has an account on the guest OS running inside the virtual machine.) If Captain Oguta were malicious, could he arrange to learn the contents of this list? If yes, explain how; if no, say why not. [4 Marks]

QUESTION FIVE **[20 MARKS]**

(a) SSL (Secure Socket Layer) is widely used to counter threats to Web security. What protocols does SSL comprise? Outline the functions or services provided by each of the SSL protocols. [6 Marks]

(b) The Kerberos authentication system supports client-server authentication in distributed environments. Describe the role of the authenticator used in the Kerberos protocol, and

explain why an authenticator is NOT required when a client requests a ticket-granting ticket from an authentication server. [4 Marks]

(c) Consider yourself being approached by Machakos County Governor to help in implementing a new IEEE802.11 WLAN (Wireless Local Area Network) for their county office with 80 computer users. The county has already got a wired network facility and it is required that this WLAN should be integrated with the existing wired network facility. Identify *three* security threats that are introduced as the result of this wireless network installation and integration, and outline security services that are required to address these threats. [6 Marks]

(d) Suggest a Disaster Recovery Plan (DRP) that the county in Q 5 (c) can use to arrest any threats originating from network downtime. [4 Marks]

- END -