TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

UNIVERSITY EXAMINATION FOR:

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

BIT 2317 : FUNDAMENTALS OF COMPUTER SECURITY

END OF SEMESTER EXAMINATION

SERIES: DECEMBER 2016

TIME: 2 HOURS

DATE : DECEMBER 2016

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of **five** questions. QUSTION ONE is Compulsory. Attempt any other TWO questions

Do not write on the question paper.

Question ONE

a) Define the following terms:

i) Trojan Horses

ii) Cookies

iii) Time bomb (6 Marks)

b) Give your views on why protecting information systems is generally a difficult process. (2 Marks)

c) A company that relies on electronic transactions for its livelihood could suffer serious financial damage if its systems are taken off line for even a short time. Indeed, cases have been reported where an e-commerce company's competitor launched a denial of service (DoS) attack against the company's Web site, hoping that

customers would abandon the target's nonresponsive servers and take their businesses to the attacker's Web site.

Critically discuss the denial of service (DoS) attacks and defenses against these attacks. (4 Marks)

d) Explain the difference "Substitution cipher" and "transposition cipher" techniques (4 Marks)

e) Twenty-five thousand messages arrive at an organization each year. Currently, there are no firewalls. On the average, there are 1.2 successful hacking each year. Each successful hacking will result in a loss to the company of about $130,000.

A major firewall is proposed at a cost of $66,000 and a maintenance cost of $5,000. The estimated useful life is 3 years. The chance that an intruder will break through the firewall is 0.0002. In such a case, the damage will be $100,000 (30%), or $200,000 (50%), or no damage at all. There is an annual maintenance cost of $20,000 for the firewall.

i) Should management buy the firewall? (2 marks)

ii). An improved firewall that is 99.9988% effective costs $84,000 with a life of 3 years and annual maintenance cost of $16,000 is available. Should this one be purchased instead of the first one? (2marks)

Question TWO

a) In real life systems, describe a simple model of conventional (or secret key) encryption, identifying the problems inherent in the described approach. (10 Marks)

b). Briefly explain the Data Encryption Standard (DES) (2 marks)

c) The application of computer techniques in banking business has produced the need to translate all banking operations into a form accepted by computers. Discuss any four properties that digital signature's should have to be able to sign documents using their local computers or terminals. (8 marks)

Question THREE

a) As our computing infrastructures have grown more network-centric and much of our lives revolve around networked computers, attackers have devised very clever means for undermining computer communications. Therefore, various techniques exist for gaining access to computing resources using network-based attacks.

Critically discuss the following three techniques used in network-based attacks, and recommend defenses against both attack techniques: (10 marks)

b) Using the rail-fence method, encrypt the message "APPLE PIE SECRET" (4 Marks)

c) Explain the difference between "Cryptography" and "Steganography" (4 Marks)

d) Define the term “Security Plan” (2 Marks)

Question FOUR
Study the given scenario and answer the questions that follow:

Scenario: Dial “M” for Modem

Darth was having a bad day. His name wasn’t really Darth, but in chat sessions, email and even his own Website, he was simply Darth.

The reason for Darth’s bad day involved some junk he had purchased at the mall. He had saved up for a couple of weeks to buy a really cool widget from the Widgets-R-Us store. He spent most of his shopping dollars online, trolling online auctions looking for a bargain. When Darth brought his widget home and plugged it in, the damn thing didn’t have any of the features he had read about on the Web site. The company manufacturing this thing, Acme Widgets, had lied to him. Darth was very, very upset.

Acme Widgets, Inc., the worldwide leader in widget manufacturing, had implemented the network architecture shown in Fig. 1. Their company consisted of about 1,000 employees, all connected via an internal IP network. They weren’t yet into selling widgets on the Internet, but did implement a Web site that included various static Web pages showing off their widget wares. Their Internet connectivity included the classic, textbook tri-homed firewall. The DMZ (**D**e**M**ilitarized **Z**one) included a Web server for sending static Web pages to potential customers and a DNS server. Acme administrators controlled the firewall and DMZ systems from a management console on the internal network. This simple, familiar architecture, or small variations from it, is in widespread use throughout the world for a variety of organizations.

Darth began his adventure against Acme Widgets by doing some reconnaissance. He had to know some more information about his victim before starting to knock on their (virtual) doors. Darth cruised over to InterNIC and looked up information on Acme Widgets, Inc. The results of his InterNIC search proved quite useful. Acme had an assigned IP address space of w.x.y.0-255. Furthermore, the administrator, John Doe, had a telephone number listed ABC-1024.

Darth used this information to begin scanning. He set up a router, Fragrouter, to help evade any intrusion detection systems that Acme might be using. He routed all scanning traffic through a system installed with Fragrouter installed to avoid any detection.

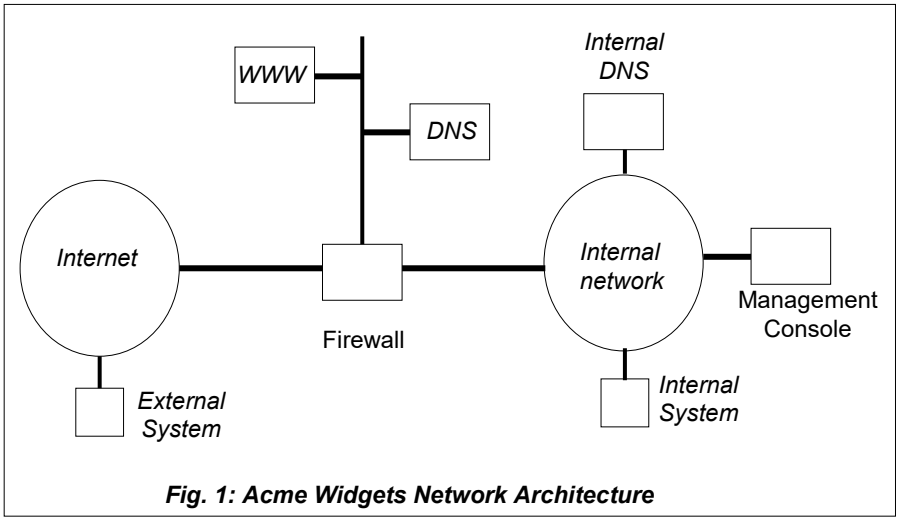

Fig. 1: Acme Widgets Network Architecture

He started scanning Acme's network using Cheops to discover which systems were alive on the target network, resulting in the discovery of three Internet-accessible systems. Using Cheops' integrated traceroute capabilities, Darth developed a basic idea of the architecture. One of the three systems was in front of the other two. A quick Nmap SYN scan revealed TCP port 80 open on one of the systems; the other system had no TCP ports open, but the Nmap UDP scanner showed UDP port 53 open. The other system had no ports open, but Firewalk showed that it was indeed a packet filter with rules allowing TCP port 80 and UDP port 53 to the DMZ machines. At this point, Darth had discerned the general architecture of Acme's Internet DMZ and firewall. He scribbled down all of this information, creating a basic sketch of the target.

Darth also ran a vulnerability scan using Nessus, just to see if Acme made any simple mistakes, leaving vulnerable or unpatched services accessible to the Internet. Unfortunately for Darth, Nessus came up dry. No known vulnerabilities were present on the DMZ.

Without any holes/vulnerabilities on the DMZ, Darth next fired up his war-dialer: THC-Scan. He configured the tool to dial the 1,000 numbers around the administrator's line, ranging from ABC-1000 to ABC-1999. The entire range should be done in one evening.

After a couple of hours, THC-scan turned up three modems asking for one-time passwords, but no obvious way to get in yet. After two more hours of running THC-Scan, a far more interesting modem turned up at ABC-1234, with a response that appeared quite compelling. Darth consulted his modem response database and the target system was running ControlMeAnywhere (CMA), a commercial remote access and control program. Darth just happened to have a CMA client on his hard drive. He ran the client, telling it to dial ABC-1234 to connect without a password. Darth equally awaited as his modem pumped out the dialing tones. Cha-Ching! What a rush! The CMA server did not require a password. Darth had found a way in!

Scenario Questions

a). Identify the motivation for the attack on the Acme Widgets network. (2marks)

b). Give a concise definition of the following concepts in relation to the given CASE

i) Threat
ii) Attack
iii) Vulnerability
iv) Firewall
v) Demilitarised zone (DMZ)
v) Intrusion Detection System (IDS) (12 marks)

c) Why was it important for Darth to try to evade Intrusion Detection Systems (IDSs)? (2 marks)
d) Which services listen at TCP port 80 and UDP port 53 respectively? (4 marks)
e) Identify the mistake(s) in organizational security policy in the above scenario and state possible defenses. (10 Marks)

Question FIVE

Security management must manage risks in terms of causes, effects and costs of a security loss. The costs resulting from a security breach must be balanced with the costs resulting from enhanced security measures This means that systematic security management allows countermeasures to be chosen in a planned and managed way, since too much security wastes money while too little security wastes IS capability. Explain your understanding to the following stages in the systematic management of security. (20 marks)

i) Risk Identification.

ii) Risk Analysis or Assessment.

iii) Risk Handling
iv) Disaster Recovery