YILDIZ TECHNICAL UNIVERSITY
FACULTY of ELECTRICAL & ELECTRONICS ENG. / DEPT. of COMPUTER ENGINEERING

Student Name Surname:	**Number:**			**Signature:**	
Course: BLM4011 Gr1,2,3	**Date/Time: 23/11/2021 16:30**			**Duration: 60 min.**	
Exam. Type: Midterm	**MidT 1 ☒**	**MidT 2**	**MakeUp**	**Final**	**MUFinal**
Instructors: Prof. Dr. Hasan Hüseyin BALIK					

Q1) In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Assume the attacker has compromised a number of broadband-connected residential PCs to use as zombie systems. Also assume each such system has an average uplink capacity of 256 kbps. What is the maximum number of 100-byte ICMP echo request (ping) packets a single zombie PC can send per second? How many such zombie systems would the attacker need to flood a target organization using a 10-Mbps link? A 16-Mbps link? Or a128-Mbps link? **(30p)**

A1) In the distributed variant of the attack, a single zombie PC can send 256000 / (100 × 8) = 320 packets per second. **(10p)**

for a 10-Mbps link (10000/256) about 40 are needed **(7p)**

for a 16-Mbps link (16000/256) about 63 are needed **(7p)**

for a 16-Mbps link (16000/256) about 500 are needed **(6p)**

Q2) Assume you have found a USB memory stick in the university campus area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick? **(25p)**

A2) It may carry a program infected with an executable virus, or document infected with a macro virus, which if run or opened can allow the virus to run and spread. **(5p)**

It could carry a malicious worm that may be run automatically using the autorun capability, or by exploiting some vulnerability when the USB stick is viewed. **(5p)**

It could contain a trojan horse program or file that would threaten the system if installed or allowed to run. **(5p)**

You can mitigate these threats, and try to safely determine the contents of the memory stick, by scanning the memory stick with suitable, up-to-date anti-virus software for any signs of malware. **(5p)**

You could examine the memory stick in a controlled environment, such as a live-boot linux or other system, or in some emulation environment, which cannot be changed even if the malware does manage to run. **(5p)**

Q3) Consider user accounts on a system with a Web server configured to provide access to user Web areas. In general, this uses a standard directory name, such as 'public_html,' in a user's home directory. This acts as their user Web area if it exists. However, to allow the Web server to access the pages in this directory, it must have at least search (execute) access to the user's home directory, read/execute access to the Web directory, and read access to any Web pages in it. What consequences does this requirement have? Note that a Web server typically executes as a special user, and in a group that is not shared with most users on the system. Are there some circumstances when running such a Web service is simply not appropriate? Explain. **(20p)**

Hepinize sınavınızda başarılar dilerim.

A3) In order to provide the Web server access to a user's 'public_html' directory, then search (execute) access must be provided to the user's home directory (and hence to all directories in the path to it), read/execute access to the actual Web directory, and read access to any Web pages in it, for others (since access cannot easily be granted just to the user that runs the web server). However this access also means that any user on the system (not just the web server) has this same access. Since the contents of the user's web directory are being published on the web, local public access is not unreasonable (since they can always access the files via the web server anyway). However in order to maintain these required permissions, if the system default is one of the more restrictive (and more common) options, then the user must set suitable permissions every time a new directory or file is created in the user's web area. Failure to do this means such directories and files are not accessible by the server, and hence cannot be access over the web. This is a common error. As well the fact that at least search access is granted to the user's home directory means that some information can be gained on its contents by other user's, even if it is not readable, by attempting to access specific names. It also means that if the user accidentally grants too much access to a file, it may then be accessible to other users on the system. If the user's files are sufficiently sensitive, then the risk of accidental leakage due to inappropriate permissions being set may be too serious to allow such auser to have their own web pages. **(20p)**

Q4) Assume that passwords are limited to the use of the 95 printable ASCII characters and that all passwords are 16 characters in length. Assume a password cracker with an encryption rate of 12.8 million encryptions per second. How long will it take to test exhaustively all possible passwords on a UNIX system? **(20p)**

A4) There are $95^{16} \approx 44 \times 10^{30}$ possible passwords. **(10p)**

The time required is $44x10^{30} / 12{,}8x10^{06} = 3{,}44x10^{24}$ second or $1{,}09\ x10^{17}$ yıl **(10p)**

Q5) What is the difference between a private key and a secret key? **(15p)**

A5) The key used in conventional encryption is typically referred to as a **secret key**. The two keys used for public-key encryption are referred to as **the public** key and the **private key**. **(15p)**

Q6) How many keys are required for two people to communicate via a symmetric cipher? **(15p)**

A6) One secret key. **(15p)**

Hepinize sınavınızda başarılar dilerim.