**THE UNIVERSITY OF DODOMA**



COLLEGE OF EDUCATION

SCHOOL OF CURRICULUM AND TEACHER EDUCATION

**COURSE CODE:** TE: 221

**COURSE TITLE**: SYSTEM SUPPORT AND MANAGEMENT

**NATURE OF THE WORK**: GROUP ASSIGNMENT-PRESENTATION

**COURSE COORDINATOR**: Mr. MAZOYA A.

**SUBMISSION DATE**: 02ndJUNE 2O17

**PARTICIPANT’S DETAILS*.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S/N | NAME | REG.NUMBER | DEG.PROG | SEX | SIGNATURE |
| 1 | HUSSEIN RICHARD | T/UDOM/2015/15762 | BED SC ICT | M |  |
| 2 | BAKARI,HUSSEIN | T/UDOM/2015/15761 | BED SC ICT | M |  |
| 3 | BLASSIO, DEUSDEDITH | T/UDOM/2014/05705 | BED SC ICT | M |  |
| 4 | CHAGULA, PIUS | T/UDOM/2015/03062 | BED SC ICT | M |  |
| 5 | COSMAS, DATIUS | T/UDOM/2015/03065 | BED SC ICT | M |  |
| 6 | NCHEMBELE, AMBROCE C. | T/UDOM/2015/03150 | BED SC ICT | M |  |
| 7 | KILLO, HALIMA | T/UDOM/2015/15759 | BED SC ICT | F |  |
| 8 | NATHANAEL, OMBENI | T/UDOM/2015/15771 | BED SC ICT | M |  |
| 9 | MTEKELE, EMMANUEL E. | T/UDOM/2015/03142 | BED SC ICT | M |  |
| 10 | MWALONGO, VALESTA L. | T/UDOM/2015/03145 | BED SC ICT | F |  |
| 11 | KIUMBO, HAMISI R. | T/UDOM/2015/03104 | BED SC ICT | M |  |
| 12 | ANYABWILE DANKEN | T/UDOM/2015/15722 | BED SC ICT | M |  |
| 13 | CHARLES TUMAINI | T/UDOM/2015/15748 | BED SC ICT | F |  |
| 14 | MUDATHIRU NAUSHAD | T/UDOM/2015/15726 |  | M |  |
| 15 | HARUNA SAID | T/UDOM/2015/03083 |  | M |  |

**QUESTION**. *Presentation on threats and attack*

**THREATS AND ATTACK**

**THREATS**

**Threats** A set of circumstances or events that has the potential to course loss or harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable. Threats can be avoided by blocking of vulnerabilities.

**Vulnerabilities** refer to a weakness in an information system or its components that might be **exploited** to compromise the security of the system.

**Four primary classes of threats in network security**

**Unstructured threats**. Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts which used command line interpreter and password crackers.

**Structured threats**. Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses.

**External threats**. External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

**Internal threats**. Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.

**Negative effects of threats in information systems**

* Weaken computer security or provide backdoor into protected networked computer
* It reduce computer performance due to interference of systems
* Lead to destroying information or data in the computer system
* It cause modifications of information or data in the information systems
* Lead to unavailability of essentials information or data in the computer systems

**ATTACK**

Attack is the deliberate act that exploits vulnerability OR Is the actual attempt to violate security.

Attackers need **MOM** (M**ethod –Opportunity –Motive)**

**Method**; It is the Skills, knowledge and tools which is used to attempt an attack

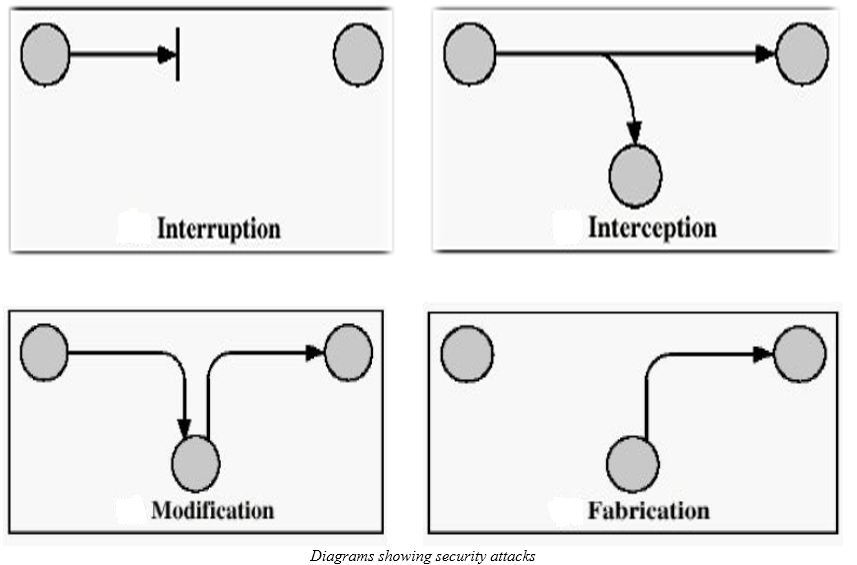
**Opportunity**; Time and access to attempt an attack

**Motive**; A reason to attempt an attack

**Types of attack**

Harm to information systems can be affected on four different ways

* **Interruption:** This is an attack on availability
* **Interception:** This is an attack on confidentiality
* **Modification:** This is an attack on integrity
* **Fabrication:** This is an attack on authenticity

****

**Four primary classes of attacks**

* **Reconnaissance:** Is unauthorized discovery and mapping of systems, services, or vulnerabilities it is also known as information gathering.
* **Access**: System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have authority to access usually involves running a tool that exploits a known vulnerability of the system or application being attacked.
* **Denial of service:** Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information.
* **Worms, viruses, and Trojan horses:** Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or bounce back to other systems.

**Measures which can be used to protect the computer system from security threats and attacks**

* Locking your computer with a password.
* Installing Anti-Virus software and ensure it is up-to-date.
* Using up-to-date software (operating systems and user applications)
* Logging off or shutting down your computer when going away.
* Make a backup of your important documents and data.
* Protect your files with passwords
* Before clicking on any e-mail attachment, make sure that the attachment is scanned even if you know the source.
* Before using media given to you by someone else, scan it to remove viruses

REFERENCES

Stallings,W.(2002), *Cryptography and Network Security*. Second Edition

Andress and Amanda. (2004). *Surviving Security:* How to Integrate People, Process, and Technology. Second Edition, AuerbachPublications

Anderson, Ross, J and Wiley,J. *Security Engineering:* A Guide to Building Dependable Distributed Systems.