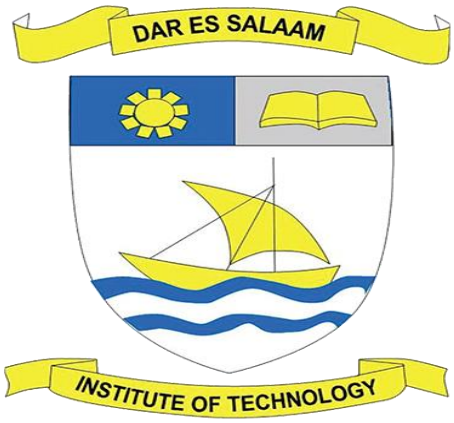
DAR-ES-SALAAM INSTITUTE OF TECHNOLOGY



GROUP NO 09 ASSIGNMENT O2

MODULE NAME: CYBER SECURITY AND PRIVACY

MODULE CODE: ITT 06218

FACILITATOR: SAKINA MSONDE

CLASS: OD21-IT

S/N	NAMES	REGISTRATION NUMBER
1	PRISCA EZEKIEL MAYALA	2102209118191
2	ELLY GERADY	210210920513
3	DENIS JOASH JOSEPHAT	2102209213281
4	LORRVIN.K. LONGINUS	2102209213992
5	SOUD PETER	210210920612
6	MKAMELDA KALIOMO	2102209112921

QUESTION: Identify essential Cyber security tools

ANSWERS:

1. Antivirus Software:

Antivirus software scans files and compares them against a database of known malware signatures. If a match is found, the antivirus software takes action, such as quarantining or deleting the infected file, to protect the system from malware infections.

Example: Norton Antivirus, McAfee Antivirus, Kaspersky

2. Firewalls:

Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. They create a barrier between a trusted internal network and untrusted external networks, filtering traffic to block malicious or unauthorized access while allowing legitimate traffic to pass through.

Example: Cisco ASA (Adaptive Security Appliance), pfSense

3. Intrusion Detection Systems (IDS):

IDS monitors network or system activities for malicious or suspicious behaviour and generates alerts when potential security threats are detected. It works by analysing network traffic patterns, signatures, and anomalies to identify potential security incidents.

Example: Snort, Suricata

4. Intrusion Prevention Systems (IPS):

IPS builds upon IDS capabilities by actively blocking or preventing identified threats from compromising the network or system. It automatically takes action to block malicious traffic or close vulnerabilities identified by the IDS, helping to mitigate security risks in real-time.

Example: Palo Alto Networks IPS, Check Point IPS

5. Virtual Private Networks (VPNs):

VPNs create a secure and encrypted connection between a user's device and a private network, typically over the internet. They work by encrypting data transmitted between the user's device and the VPN server, ensuring privacy and security by preventing unauthorized access or interception of sensitive information. Example: NordVPN, ExpressVPN

6. Encryption Tools:

Encryption tools use cryptographic algorithms to convert plaintext data into ciphertext, making it unreadable to unauthorized users. They work by applying encryption algorithms to data at rest (stored data) or data in transit (data being transmitted over a network), ensuring confidentiality and protecting sensitive information from unauthorized access or interception.

Reference:

https://www.nist.gov/cyberframework

https://linuxsecurity.com/howtos/learn-tips-and-tricks/improve-your-digital-security-as-a-linux-user-tips-to-keep-your-business-safe

https://www.sans.org/white-papers/454/

https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

Cybersecurity & Infrastructure Security Agency (CISA).

(n.d.). Free cybersecurity services & tools. https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

SANS Institute. (n.d.). Reading room. Retrieved from https://www.sans.org/white-papers/454/

Open Web Application Security Project (OWASP). (n.d.). OWASP cheat sheet series. Retrieved from https://cheatsheetseries.owasp.org/

GitHub. (n.d.). Security Lab. Retrieved from https://github.com/topics/security-tools