Assignment 1

(Individual Assignment)

Instructions:

Due Date: Feb 13, 2023

- **You have to present in class and viva will be taken for understanding of code and tasks**
- **Strong plagiarism policy apply**
- **There may be some intentional errors in the code research and correct them**
- **Helping initial code is attached**
- **Take screen shots where necessary i.e victim computer RAM utilization, Ports reply etc.**
- **Only those students who submit on time will be allowed to present**

Q1: Make a setup of injecting TCP/IP custom made packet using python programming, the code should perform following properties

- Build custom TCP header
- Build custom IP header
- Use Spoofed IP address
- Modify code for high-rate and low-rate Denial of service. Apply your own algorithm to justify
- Extra marks for building another malicious scenario out of this code other than DoS.

Show results on resources being overwhelm on victim machine using change in RAM and processor utilization

Q2: Modify this code to make it an “Port Scanning” script. It should able to check custom range of ports using XMAS scanning technique. Implement all scenarios given in the image just by modifying the given code used in question 1.

Scan Type	Initial Flags Set	Open Port Response	Closed Port Response	Notes
Full (TCP Connect)	SYN	SYN/ACK	RST	Noisiest but most reliable*
Half open (Stealth or SYN Scan)	SYN	SYN/ACK	RST	No completion of three-way handshake; designed for stealth but may be picked up on IDS sensors
XMAS	FIN/URG/PSH	No response	RST/ACK	Doesn't work on Windows machines
FIN	FIN	No response	RST/ACK	Doesn't work on Windows machines
NULL	No flags set	No response	RST/ACK	Doesn't work on Windows machines
ACK	ACK	RST	No response	Used in firewall filter tests

Q3: Implement a simple backdoor sub-process to any victim that is connected to a malicious server. Perform following operations on the connected victim

1. Run following commands on victim machine
    a. Ipconfig
    b. Sysinfo
    c. Process information and status
    d. Extra marks for more commands that give more information of victim
2. Inject DoS(made in Q1) simple packet injector using this back door, use appropriate python function to inject.
3. Show high rate traffic on victim machine using simple wireshark dump
4. Show unusual traffic being generated using one or two tools from Sysinternals(https://learn.microsoft.com/en-us/sysinternals/downloads/)