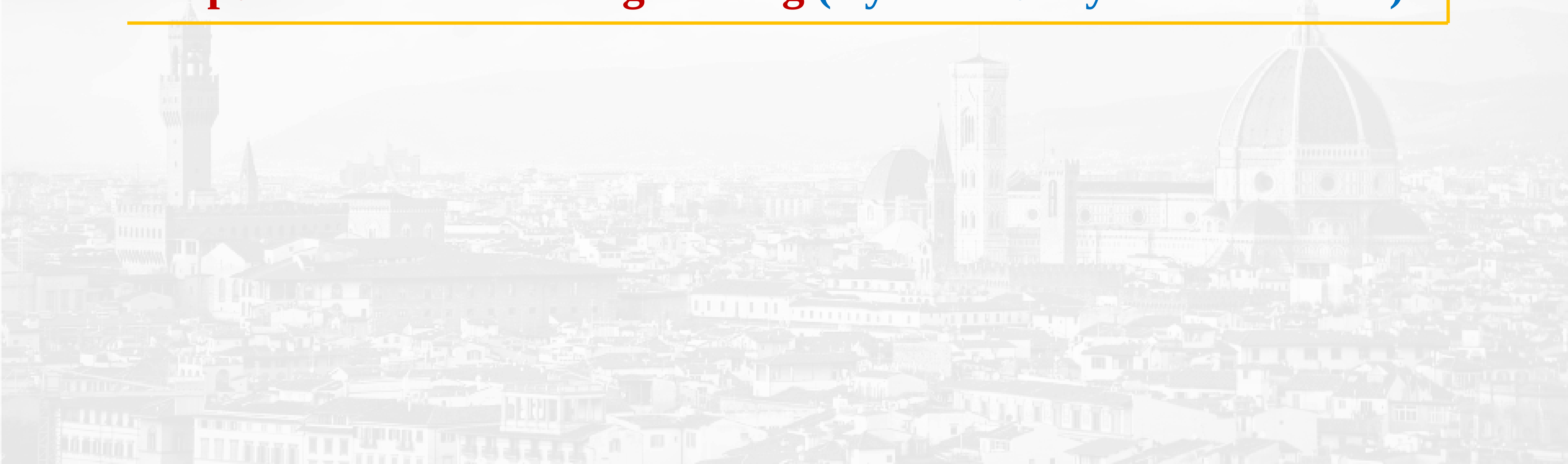
SY B.Tech Semester-IV (AY 2022-23)

Computer Science and Engineering (Cybersecurity and Forensics)



Assign No.	List of Assignments
1.	Write a program using JAVA or Python or C++ to implement any classical cryptographic technique.
2.	Write a program using JAVA or Python or C++ to implement Feistal Cipher structure
3.	Write a program using JAVA or Python or C++ to implement S-AES symmetric key algorithm.
4.	Write a program using JAVA or Python or C++ to implement RSA asymmetric key algorithm.
5.	Write a program using JAVA or Python or C++ to implement integrity of message using MD5 or SHA
6.	Write a program using JAVA or Python or C++ to implement Diffie Hellman Key Exchange Algorithm
7.	Write a program using JAVA or Python or C++ to implement Digital signature using DSA.
8.	Demonstrate Email Security using - PGP or S/MIME for Confidentiality, Authenticity and Integrity.
9.	Demonstration of secured web applications system using SSL certificates and its deployment in Apache tomcat server
10.	Configuration and demonstration of Intrusion Detection System using Snort.
11.	Configuration and demonstration of NESSUS tool for vulnerability assessment.

Configuration and demonstration of Intrusion Detection System using Snort.

IDS-Snort

- IDS
- IDS Tools: Snort, Zeek, Segan, OSSEC, Kismet etc..
- Snort Installation in Windows
  - www.snort.org
  - Snort 2.9.17_Installer.x86.exe
  - Registered and Install Rules (snortrules-snapshot-29111.tar)
- www.winpcap.org → download the library: WinPcap4.1.3
- Follow the steps to configure and run

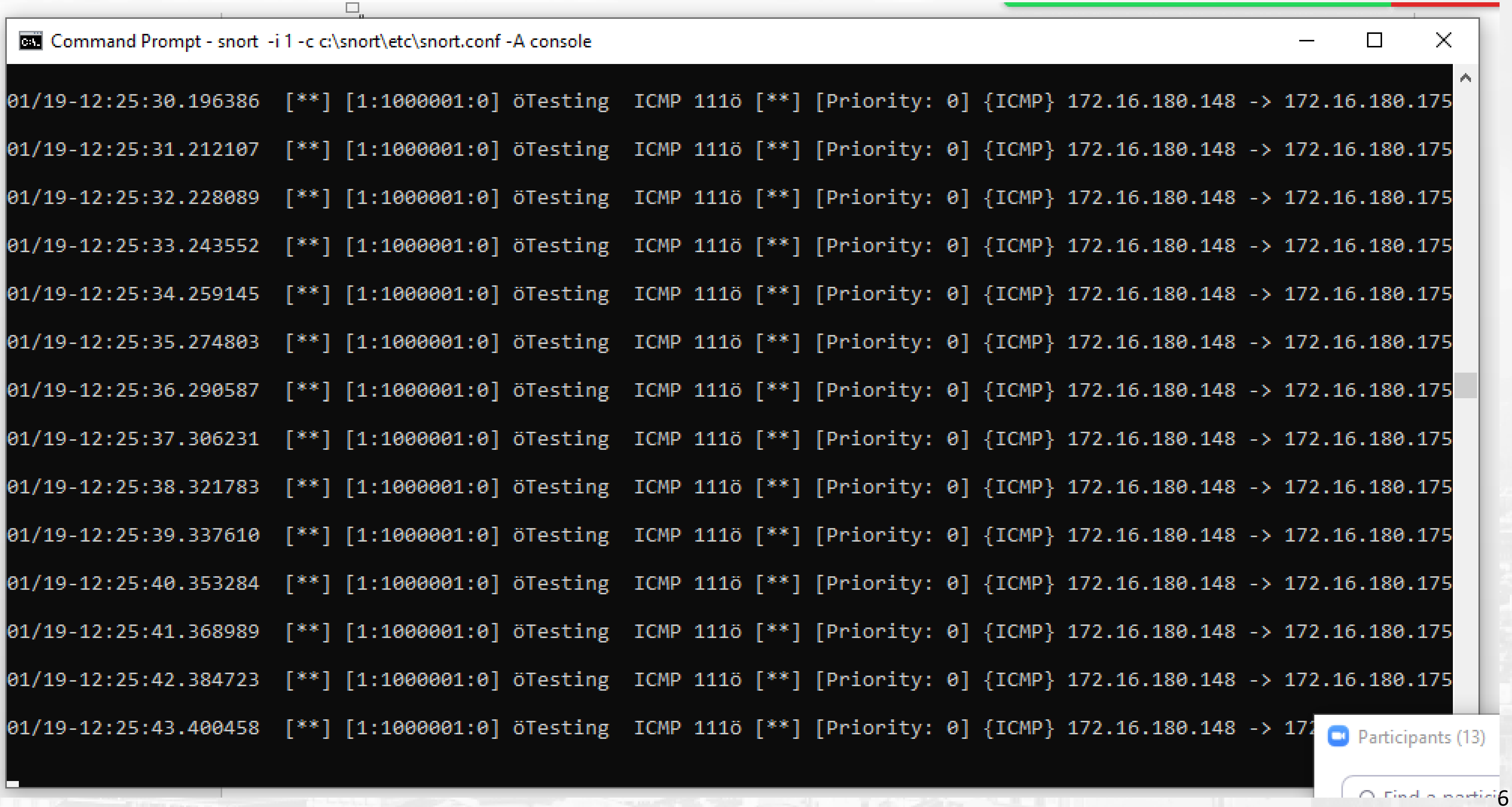
Steps

- Open the snort.conf file in word and set the rules
- Open command prompt and check following commands
  - c:\snort\bin> snort -V   # Version
  - c:\snort\bin> snort -W   # Information about LAN card
  - c:\snort\bin> snort -i 1 -c c:\snort\etc\snort.conf -T   # validation the configuration
- Open local file in word [C:\snort\rule\local]
- Go to at the end of the file

```
        alert icmp any any → any any (msg: “Testing ping/ICMP”; sid:1000001;)

alert icmp 172.16.180.148 any → 172.16. 180.175 any (msg: “Testing”; sid:1000011;)
```

- c:\snort\bin> snort -i 1 -c c:\snort\etc\snort.conf -A console



Command Prompt - snort -i 1 -c c:\snort\etc\snort.conf -A console

```
01/19-12:25:30.196386  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:31.212107  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:32.228089  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:33.243552  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:34.259145  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:35.274803  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:36.290587  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:37.306231  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:38.321783  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:39.337610  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:40.353284  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:41.368989  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:42.384723  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 172.16.180.175
01/19-12:25:43.400458  [**] [1:1000001:0] öTesting  ICMP 111ö [**] [Priority: 0] {ICMP} 172.16.180.148 -> 17
```