राष्ट्रीय प्रौद्योगिकी संस्थान हमीरपुर
हमीरपुर (हि.प्र.) – 177 005 (भारत)

NATIONAL INSTITUTE OF TECHNOLOGY HAMIRPUR
HAMIRPUR (H.P.) - 177 005 (INDIA)
(An Institute of National Importance under Ministry of HRD)

संगणक विज्ञान एवम् अभियांत्रिकी विभाग
Department of Computer Science & Engineering

Intrusion Detection System (CS-742) Assignment-2

AS02/2020

SEMESTER-II CLASS-M.Tech. CSE

All Assignment will be checked and evaluated by plagiarism software.

LAST DATE OF ONLINE SUBMISSION: 03/04/2020

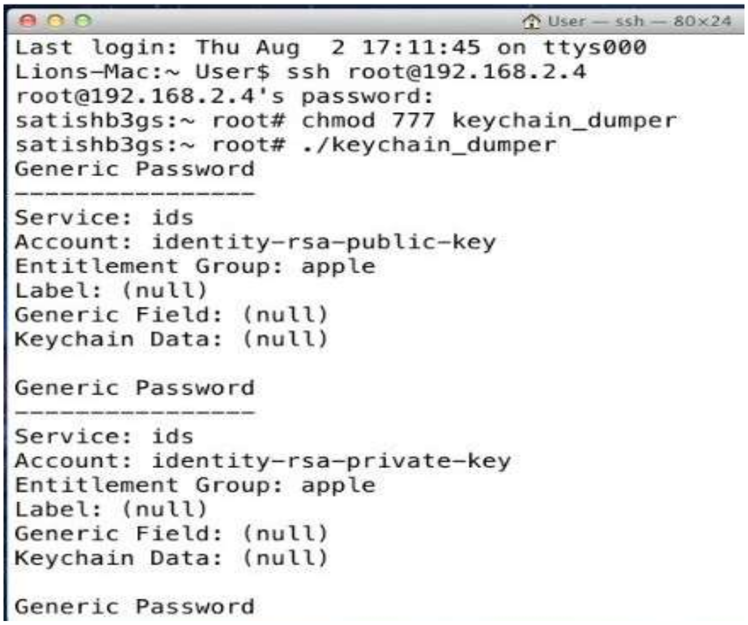
Submit your assignment in pdf format with Name and roll No

To E-mail only: lokeshhamirpur@gmail.com

Attempt All Questions:

1. Describe Pattern matching with respect to detection.
2. Define False Positives with respect to NIDS.
3. Define Evasion of signatures?
4. Consider the following situation:
5. *We saw a case a while back where someone used their **google** account at a computer lab on campus. She made sure her **google** account was no longer open in the browser window before leaving the lab. Someone came in behind her and used the same browser to re-access her account. They started sending emails from it and caused all sorts of mayhem.*
   Identify the type of attack in above scenario? What should you do?
6. Explain following rules/commands with respect to ***snort scenario***:

i. elaborate following screenshot of snort:



```
Last login: Thu Aug  2 17:11:45 on ttys000
Lions-Mac:~ User$ ssh root@192.168.2.4
root@192.168.2.4's password:
satishb3gs:~ root# chmod 777 keychain_dumper
satishb3gs:~ root# ./keychain_dumper
Generic Password
----------------
Service: ids
Account: identity-rsa-public-key
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: (null)

Generic Password
----------------
Service: ids
Account: identity-rsa-private-key
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: (null)

Generic Password
```

ii. Explain the command:

- ***tcpdump –n –r /var/log/snort/snort.log.<timestamp>***
- ***Alert tcp !192.168.100.0/24 any → 192.168.100.0/24 any***
- ***ipvar MY_IP_ADDRESSES***