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-3

AS03/2020

SEMESTER-II CLASS-M.Tech. CSE

All Assignment will be checked and evaluated by plagiarism software.

LAST DATE OF ONLINE SUBMISSION: 17/04/2020 Till 06:00 PM

Submit your assignment in pdf format with Name and roll No

and UPLOAD to google classroom and E-mail to: lokeshhamirpur@gmail.com

Attempt All Questions:

1. Why location of sensor is important in deployment of WLAN-based IDS? Explain the important considerations for selecting the sensor locations in WLAN-IDS.
2. Define WEP cracking
3. You are an employee for a tech department in a non-management position. A high-level executive demands that you break protocol and allow him to use his home laptop at work. What do you do?
4. What's more secure, SSL, TLS, or HTTPS?
5. How exactly does traceroute/tracert work at the protocol level?
6. How would you implement a secure login field on a high traffic website where performance is a consideration?
7. What is salting, and why is it used?
8. What Does It Mean When You Receive An Ntfs Error: 5?
9. Demonstrate following rules and captures the screenshots from snort:
   a. *alert tcp any any -> 192.168.1.0/24 21 (content: "USER root"; nocase; msg: "FTP root user access attempt";)*
   b. *alert udp any any -> 192.168.1.0/24 111 (rpc: 100083,*,*; msg:"RPC ttdb";)*
   c. *output xml: log, protocol=https host=air.cert.org file=alert.snort cert=mycert.crt key=mykey.pem ca=ca.crt server=srv_list.lst*
10. Demonstrate following rules and captures the screenshots from Wireshark:
    A.

```
tcp src port 443 and (tcp[((tcp[12] & 0xF0) >> 4 ) * 4] = 0x18) and
(tcp[((tcp[12] & 0xF0) >> 4 ) * 4 + 1] = 0x03) and (tcp[((tcp[12] & 0xF0) >>
4 ) * 4 + 2] < 0x04) and ((ip[2:2] - 4 * (ip[0] & 0x0F)  - 4 * ((tcp[12] &
0xF0) >> 4) > 69))
```

B.

```
udp[1] & 1 != 1 && udp[3] & 1 != 1 && udp[8] & 0x80 == 0x80 && length < 250
```