Exp – 6 Identify network reconnaissance tools/commands and describe its output.

1. ping google.com
2. ipconfig
3. hostname
4. getmac
5. arp -a
6. nslookup google.com
7. tracert google.com
8. netstat
9. systeminfo

10. Perform brute force attack to find the password using Burp suite on any demo website. (Demo website means a website which allows users to perform any attack on it for study purpose only)

1. Burp suite – proxy setting – select – edit – 8080 to 8081 .
2. Firefox – setting – proxy – manual – proxy = 127.0.0.1 – port = 8081 - checkbox tick ok
3. Import/export der format – rename - .der
4. Firefox – certificates – authorities – upload
5. Burp suite – open browser – acuart – enter user id n psswrd – intercept on – login hit –
6. Burp suite – right click on psswrd – send to intruder – payload – add – new psswrd + original psswrd – start attack – greatest length is ans. (actual psswrd) .

12. Use network sniffing tools to demonstrate the difference between http and https.

1. Wireshark – capture stop – tcet erp – enter credential
2. Wireshark – capture on – hit login – find http (info-POST) – right click – follow – tcp stream – visible user id + psswrd
3. Wireshark – capture stop
4. Mail / leetcode / any website - enter credential - capture on – hit login – find TLS - right click – follow – tcp stream – not visible user id + psswrd (encrypted form) .

13. Use network sniffing tools to demonstrate the TCP three-way handshake.

1. Wireshark – capture stop
2. Firefox/chrome – search altoro mutual – Wireshark – capture on - open altoro mutual site – close altoro mutual site
3. Wireshark – in filter exclude all other protocols except TCP – search 1st three TCP that consist ([SYN] + seq=0) ,([SYN , ACK] + seq=0 + ack=1)and ([ACK] + seq=1 + ack=1)