PRACTICAL LAB Exercises –Part 2

Section -A

Perform the following scans in NMAP and give the purpose of each of the commands listed below: Take snapshot of each scans. (the ipaddr should be the vulnerable website address)

nmap –sS IPADDR

nmap -sV -p 443 --script=ssl-heartbleed ipaddr

nmap -sV ipaddr

nmap -v ipaddr (what is the output given in the note, highlight)

nmap www.vit.ac.in **(determine the rdns record value and which are filtered and open ports)**

nmap -sT ipaddr

nmap --script http-title ipaddr

nmap --script http-headers ipaddr

nmap --script http-enum ipaddr

nmap -p 80,443 ipaddr (which port is open and closed)

nmap -p T:8888,443 ipaddr (what is the service name which is closed on 8888)

nmap --iflist

nmap -f ipaddr

nmap -A ipaddr

nmap -p 1-65535 localhost (which are the open and known ports)

nmap --top-ports 20 ipaddr

nmap -T4 -A cloudflare.com (from the complete output, give only the trace route result)

nmap -Pn --script vuln ipaddr (how many ports are filtered)

nmap -sV --script http-malware-host ipaddr (find out this statement from the result and highlight-- ---http-malware-host: Host appears to be clean)

Also , determine the commands for the questions given below:

1. **find the command to output the scan result to files?**
2. **What is the command to scan ipv6 address?**

Section –B

IBM QRADAR

Create an anomaly offense rule (name of the rule should contain anomaly_candidateID)

Filters to be applied

- Offense severity, credibility and relevance are greater than 8.
- When the source ip address is the vulnerable ip address given in the morning session of 26.12.20
- when the offense occurs after 5th day of the month
- when the offense occurs after 5 am
- When the number of flows making this offense is greater than 200
- When the number of destinations under attack is greater than 5