Advanced Enumeration and Packet Capturing Technique

- `netstat` **[To see the hostname of the system]**
- `nbtscan` **[NetBIOS information will be shown]**

1. `nbtscan -n <IP>`
2. `nbtscan <IP> -vh` **[In human-readable format]**
3. `nbtscan <IP> -d` **[To dump the packet]**
4. `nbtscan -f address.txt` **[To scan IP from file]**
5. `nbtscan <IP> abc.txt` **[To scan IP from file]**
6. `nmap -sT -Pn -iL address.txt` **[To scan IP from file]**
7. `nmap -sT -Pn -p139 address.txt` **[Scan IP from file for specific port]**
8. `nmap --script nbstat.nse -p139 <IP>`
9. `nmap -p 22 --script ssh-brute --script-ares userdb=username.list, passdb=passwords.list <IP>`
10. `nmap -p 22 --script ssh-brute --script-args userdb=username.list, passdb=passwords.lst \--script-args ssh-brute, timeout=45 <IP>`
11. `nmap --script vnc-brute -p 5900 <IP>` **[To share scan Virtual Network Computing]**
12. `nmap --script irc-info -p 6666 <IP>`
13. `nmap --script irc-brute -p 6666 <IP>`
14. `nmap --script broadcast-ping <IP>` **[Used for broadcast ping]**

Packet Capturing Technique

- Open **VMware** → **Kali** → Open terminal → Write → **select "any"** → Then it will start capturing the data packets.
- Now, go to Firefox and search: `testphp.vulnweb.com` → **username: "abcdef"** → **password: "123456"`** → Login.
- Now, go to **Wireshark** → Filter → `http.request.method=="POST"` → You will be able to view the captured packets.

Hypertext Transfer Protocol

- HTML from URL Encoded : **application/x-www-form-url encoded**
  - From item: **"uname" = abcd**
  - From item: **"pass" = 12345**