Web application vulnerability scanning

Enumeration
Open Kali Linux
NETBIOS AND SMB ENUMERATION
ON WINDOWS
OPEN POWERSHELL
Enter Commands
1. nbtstat
2. nbtstat –A &lt;IP ADDRESS of Target&gt;
ON KALI
1.nbtscan
2. nbtscan –r &lt;IP ADDRESS OF TARGET&gt;
3. nbtscan -v –r &lt;IP ADDRESS OF TARGET&gt;

SMB ENUMERATION PORT 139 ,445
Allow sharing files and resources
ON KALI
Tool used smbclient
1.smbclient
2. Smbclient -I &lt;IP ADDRESS&gt;
3. Smbclient -L &lt;IP ADDRESS&gt;
Vulnerlability Scanning

1. Namp -sV &lt;IP ADDRESS TARGET(METASPOLITABLE)&gt; -T4
-sV = show version of Port ans services
2. ls -al /usr/share/nmap/scripts | grep ftp
3.nmap --script vuln &lt;IP ADDRESS TARGET&gt; -T4 -V
4. ls -al /usr/share/nmap/scripts | grep ssh
5. nmap --script ssh-brute.nse &lt;IP ADDRESS TARGET(METASPOLITABLE)&gt;

NESSUS FOR VULNERLABILITY SCANNING
Search NESSUS
NESSUS ESSENTIAL
Enter credentials
Download NESSUS in kali
1. Cd downloads
2. Sudo dpkg -I Nessus-10.8.4-ubuntu1604_amd64.deb
COPY /bin/systemctl start nessusd.service
3. Netstat –ntlup
4.Paste /bin/systemctl start nessusd.service
5.Netstat –ntlup
Search on firefox
https://&lt;IP ADDRESS METASPOLITABLE2&gt;.8834

use nikto
github nikto