ant wak

Web application Security Project

Task 1: Using your metasploitable VM, check for the ip settings. Let's say for example the IP address is 192.168.x.x

Enter the IP address in the address bar in your browser. You will see the GUI of the metasploitable environment. Click on DVWA

Tasks to be performed:
1. Privilege escalation
2. CSRF
3. SQL injection
4. XSS

Document the above attack methodology and explain your findings. Make use of tools like Burp Suite, ZAP.

Task 2: Download and Install Zone Alarm firewall in your windows VM.

- Try performing a ping scan from kali linux.(You must be able to perform this.)
- Now open settings in the Zone alarm firewall go to Advanced settings>zones>add host.
- Add kali linux Ip address and from the drop down select block.
- Now try pinging the windows VM. (You shouldnt be able to ping).
- Go to tool>logs. You should be able to identify all the logs made by the firewall. Take a screenshot of both the logs and the kali terminal where ping cannot be done.

Optional: Try adding a website to your block list and try to access that website from your browser on windows. Make a report of how you can allow and block hosts and ip addresses on the

Task 3: With the help of Shodan, try to find as many vulnerable webcams across the globe. Include screenshots. Also use shodan to show how it can detect the presence of a web application firewall in a particular website. (Examples : Amazon EC2, Cloudflare etc.)