

Question-5 Web Server Hacking

Vulnerability Explanation:

The **Icecast application** running on **192.168.1.22** allows for a buffer overflow exploit wherein an attacker can remotely gain control of the victim's system by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

After gaining control we can execute following tasks like:

- File discovery and editing.
- Screen capture ,Key Logging , Knowing passwords etc
- Privilege escalation to Administrator



