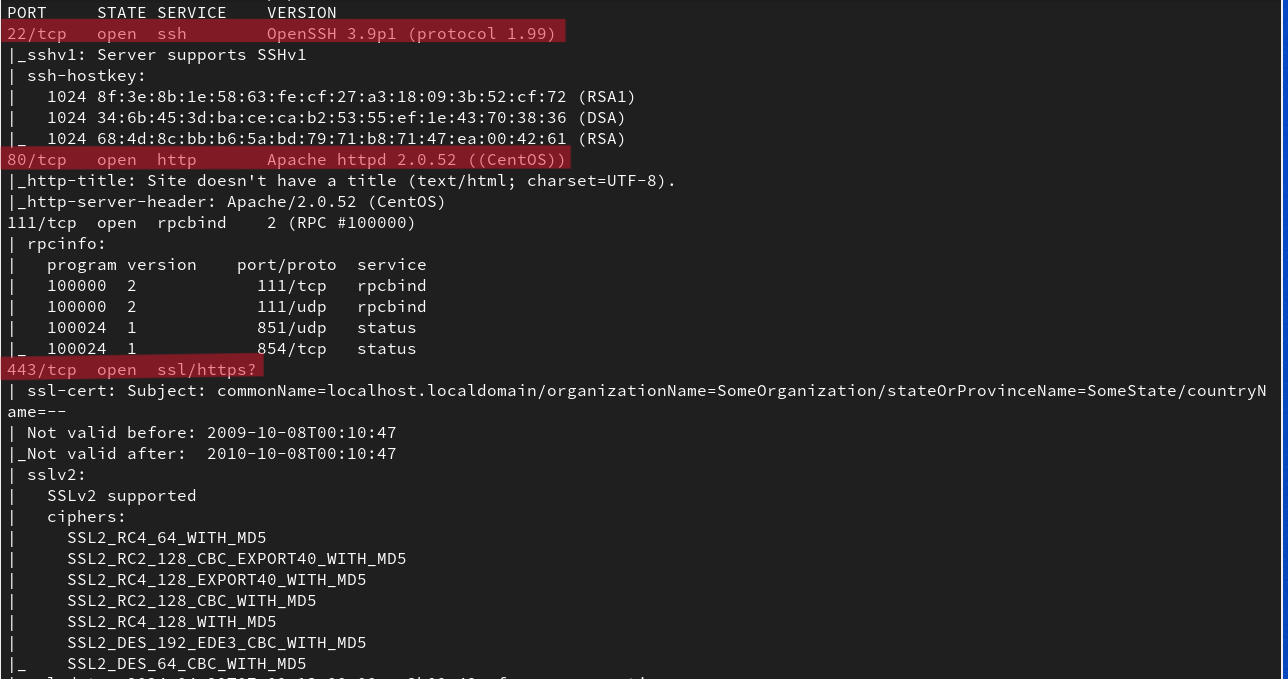
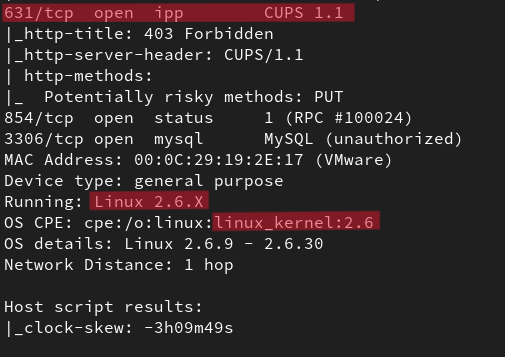
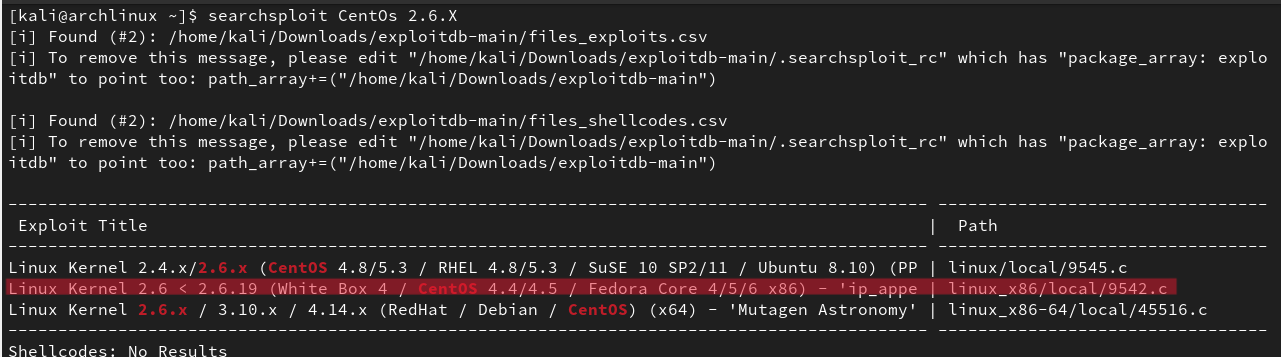
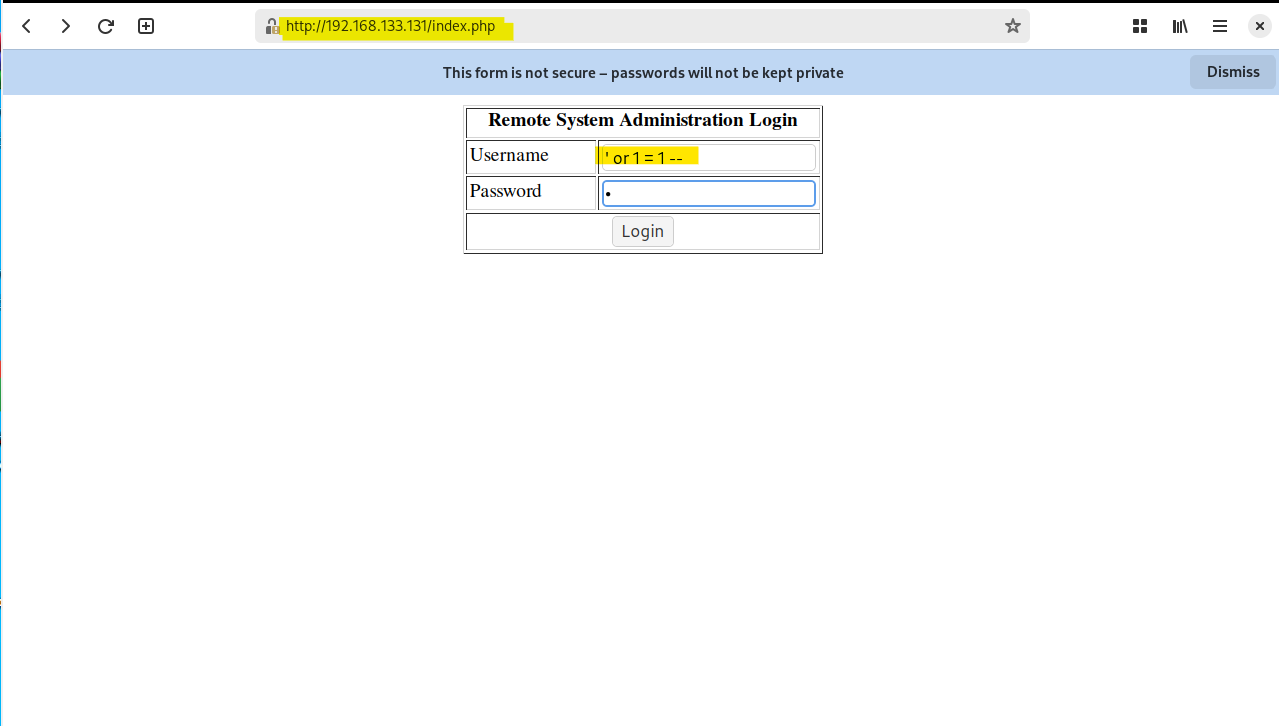
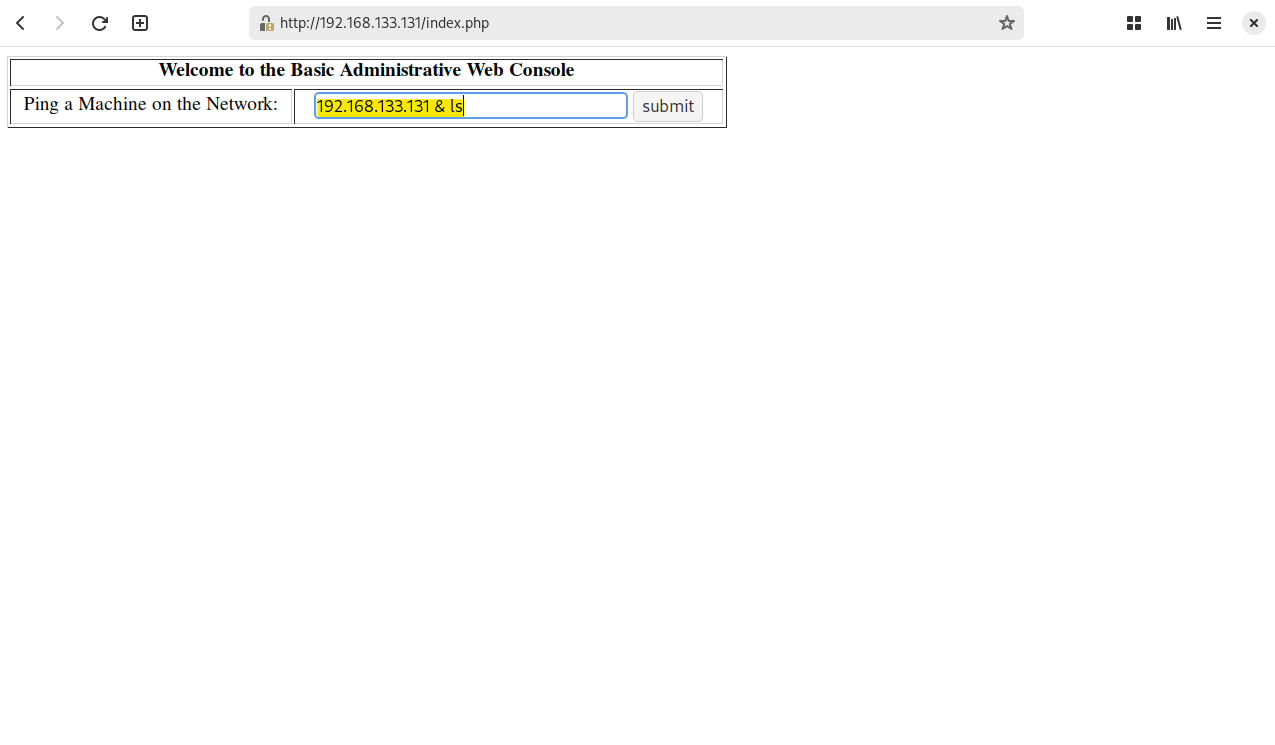
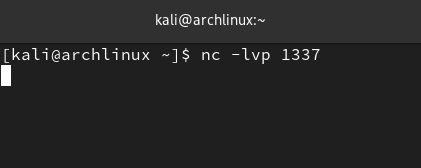
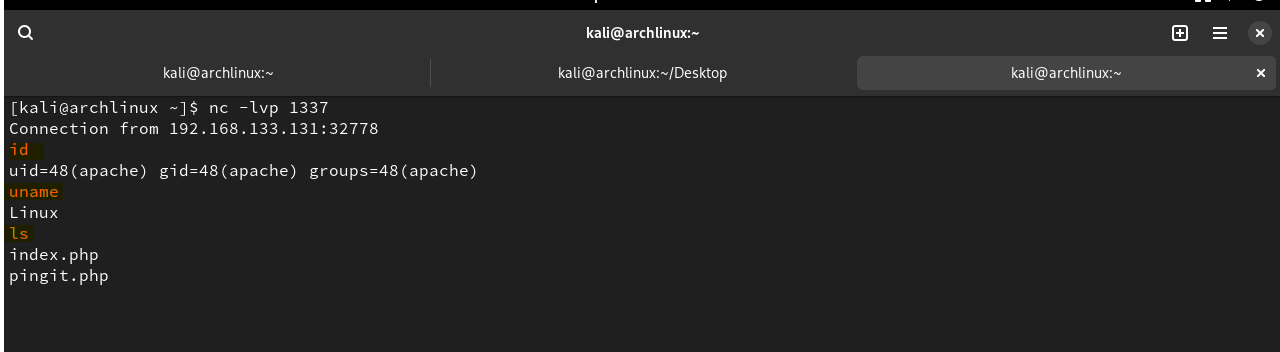
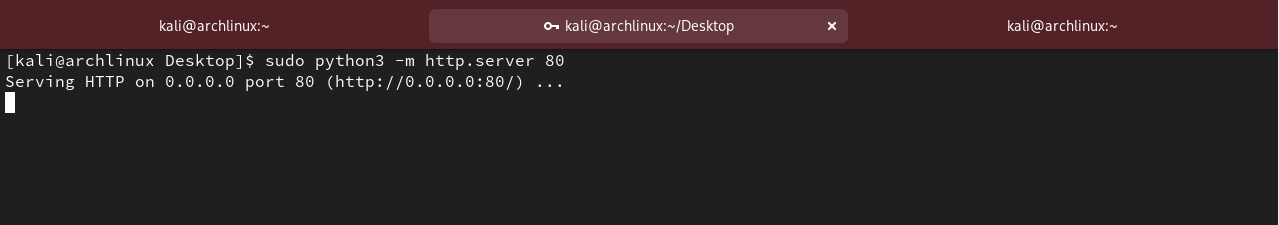
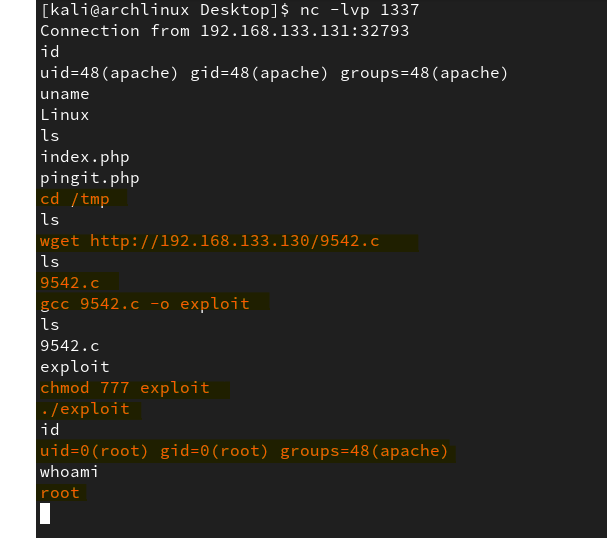
**Enumeration:**

1. **Network Discovery:**
   * Utilized **netdiscover** to identify active hosts on the network.
   * Discovered target machine at IP address 192.168.133.130.
2. **Port Scanning:**
   * Conducted port scan using **nmap** to identify open ports on the target.
   * Identified port 80 as open, indicative of a web server running.
   * 
   * 

**Exploitation:**

1. **Vulnerability Assessment:**
   * Utilized **searchsploit** to search for exploits relevant to CentOS with kernel version 2.6.
   * Discovered a potential exploit for further exploitation.
   * 
2. **Web Application Testing:**
   * Discovered a web application running on port 80.
   * Detected authentication bypass vulnerability using SQL injection.
   * Successfully logged in as admin to the web application.
   * 
3. **Command Injection:**
   * Exploited command injection vulnerability within the web application.
   * Executed commands to gather system information and escalate privileges.
   * 
   * 

**Post-Exploitation:**

1. **Reverse Shell:**
   * Established reverse shell connection using **netcat**.
   * Monitored listening port using **nc -lvp 1337**.
   * 
2. **Exploit Delivery and Execution:**
   * Set up an HTTP server to host the exploit payload.
   * Delivered the exploit to the target system using **wget**.
   * Executed the exploit to gain root privileges on the target system.
   * 
   * 
   * 
   * 

**Recommendations:**

* Patch vulnerable software and update system packages regularly.
* Implement strong authentication mechanisms and input validation in web applications.
* Conduct regular security assessments and penetration testing to identify and mitigate vulnerabilities.

**Conclusion:** The penetration test revealed significant vulnerabilities within the target system, including authentication bypass, command injection, and privilege escalation. It is imperative that appropriate remediation measures are taken to secure the system and prevent potential exploitation by malicious actors.