Ethical Hacking Practice #1: Sumo1 Writeup

Clay Jones

Objective:
Get root privileges of the vm.

Nmap Scans:

1. Performed an nmap scan to find the host.
2. Performed a TCP-SYN scan to collect information on the host
3. Findings
    a. Open Ports 22 and 80
    b. OS: Linux
    c. Network Distance: One hop
    d. SSH: OpenSSH Debian
    e. HTTP: Apache httpd 2.2.22

Server Check:
Since port 80 was open, the IP was typed into the search engine to prove a server was up. No network data was found.

Nikto Scan:
Ran a Nikto scan to find potential web vulnerabilities. Discovered this application contained the "Shellshock" vulnerability.

Metasploit:
The metasploit framework was used to search for exploits for the shellshock vulnerability. The exploitation script was found and ran.

Exploitation:
The working directory was printed and a whoami was run to show that the exploit worked. The uname command was used to find more information on the operating system and a searchsploit was run on the Ubuntu version. The exploit was ran and root privileges were gained.