Linux Command Scavenger Hunt #2

The Perimeter Is Open

Team name: _____ Members:

_____

THE SCENARIO + THE LAB

It is 04:47. An alert fires: cell-071 is accepting inbound connections on every port and a rogue process is beaconing out on port 8888. You SSH in before the attacker can establish persistence. Your job: inspect the damage, lock the perimeter, harden the SSH daemon, audit the failed-login log, sweep for malware, and verify the openssh-server binary has not been tampered with. Open the W2 Scavenger Hunt #2 CTF box from the W2 hub. For each row below: write the exact command (or minimal flag combination) you ran in the lab to complete that step. **First team to finish all eight correctly AND capture all eight lab flags wins.**

RULES

Teams of 2–3. Use any course resources (man pages, the W2 lecture deck, the W2 operator field manual). **First team correct: 100/100.** Other correct teams: 95/100. Each wrong answer: −2 points. All eight lab flags must be captured for full credit.

#	Description	Command
1	Inspect the current firewall rules on cell-071. What is the default policy on the INPUT chain? Step 1 — assess the perimeter	
2	Apply a default-deny policy so all NEW inbound connections are blocked. Add the established-sessions rule first — do NOT lock yourself out. Step 2 — close the perimeter	
3	Explicitly allow new SSH connections on port 22 so future logins are possible. Step 3 — whitelist SSH	
4	Identify every service listening on a TCP port. There is a rogue process running on an unexpected port — which port is it? Step 4 — hunt the implant	
5	Disable root SSH login in the SSH daemon configuration, syntax-check the config, then apply the change without dropping active connections. Step 5 — harden SSH	

#	Description	Command
6	Identify the account that was targeted by a brute-force attack and check how many login failures it has recorded. Step 6 — audit the failed logins	
7	Scan /tmp and /home recursively for malware and move any infected files to quarantine. Step 7 — AV sweep	
8	Verify the integrity of the openssh-server package against its stored checksums. What does the output tell you? Step 8 — package integrity check	

LAB FLAGS

Each worksheet row corresponds to one lab flag. When you run the correct command in the CTF box the engine auto-awards the flag. Copy each FLAG{...} value into the table below.

#	Flag value (FLAG{...})
1	
2	
3	
4	
5	
6	
7	
8	

Score (instructor): Sheet ____/100 Flag 1 ☐ Flag 2 ☐ Flag 3 ☐ Flag 4 ☐ Flag 5 ☐ Flag 6 ☐ Flag 7 ☐ Flag 8 ☐ Final: ____/100