

Linux Command Scavenger Hunt #3

Lost Authority

Team name: _____ Members: _____

THE SCENARIO + THE LAB

It is 02:14 UTC. Grid Security has flagged cell-071: DNS authority for sector7.matrix.net is lost. At 02:11 an attacker (203.0.113.99) gained root access and edited the BIND zone file — introducing a parse error that crashed named AND poisoning the grid-api A record to redirect traffic to their own server. They then installed a rogue cron job (/etc/cron.d/grid-resync) that re-applies the poison every 5 minutes to undo any fix. Open the W3 Scavenger Hunt #3 CTF box from the W3 hub. For each row below: write the exact command you ran to complete that step. **First team to capture all seven flags AND finish the worksheet wins.**

RULES

Teams of 2–3. Use any course resources (man pages, the W3 lecture deck, the W3 operator field manual).

First team correct: 100/100. Other correct teams: 95/100. Each wrong answer: –2 points. All seven lab flags must be captured for full credit.

#	Description	Command
1	Confirm that DNS resolution is broken on cell-071. Query the local nameserver for grid-api. What status do you get? Step 1 -- DNS Diagnose	
2	Run the BIND configuration and zone-file validator. Which file has an error, and what is the error on line 20? Step 2 -- BIND Checkconf	
3	After fixing the CNAME syntax error in the zone file, reload only the sector7.matrix.net zone. What does rndc report on success? Step 3 -- BIND Reload	
4	With BIND running again, query grid-api with +short. What IP address does the zone currently return? Step 4 -- DNS Integrity	
5	List the system cron drop-in directory. Which file should not be there? Step 5 -- Automation	
6	Read the malicious script that the rogue cron job runs. What IP address does the script re-poison the A record to? Step 6 -- Bash/Automation	

#	Description	Command
7	After removing the rogue cron job, correcting the poisoned A record, and reloading the zone, confirm resolution is restored. What IP does grid-api now return? Step 7 -- Verify	

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	

Score (instructor): Sheet ____/350 Flag 1 ☐ Flag 2 ☐ Flag 3 ☐ Flag 4 ☐ Flag 5 ☐ Flag 6 ☐
Flag 7 ☐ Final: ____/350