Ethical Hacking Linux Readiness Checklist

Professional Self-Assessment (25 Points)

Check each item honestly.

Workspace & Environment

☐ I maintain a stable Linux security workstation with updated packages.
☐ I organise every assessment into dedicated evidence folders.
☐ I understand root vs non-root execution implications.
☐ I routinely save command outputs and logs.

Linux Command-Line Fluency

☐ I can comfortably navigate, search, inspect, and filter files in terminal.
☐ I use grep/awk/sed or equivalent text filtering efficiently.
☐ I can inspect local network state without GUI tools.

Reconnaissance Capability

☐ I can gather DNS, whois, host, and metadata intelligence effectively.
☐ I know how to enumerate subdomains and external target footprint.
☐ I document passive findings before active scans begin.

Network Scanning Discipline

☐ I can perform structured host and port discovery.
☐ I understand service fingerprinting and banner interpretation.
☐ I save and compare scan results methodically.

Web Testing Readiness

☐ I can identify hidden directories and web technology clues.
☐ I inspect headers, cookies, and application responses manually.
☐ I know how to prioritise web findings by business sensitivity.

Credential Testing Maturity

☐ I understand authorised password auditing boundaries.
☐ I can test credential resilience responsibly.
☐ I know how to interpret password findings beyond “weak password found.”

Packet & Traffic Analysis

☐ I can capture and inspect packets using Linux tools.
☐ I know how to identify plaintext leakage or suspicious protocol behaviour.

Vulnerability Validation

☐ I understand the difference between scanner alerts and verified findings.
☐ I manually validate serious exposures before reporting them.
☐ I prioritise vulnerabilities by exploitability and business impact.

Automation & Workflow

☐ I use scripts or chained commands to reduce repetitive manual work.
☐ I maintain repeatable assessment methodology instead of random tool usage.
☐ I preserve evidence suitable for professional reporting.

SCORING RESULTS

21–25 Checks — Strong Maturity

You demonstrate solid Linux-based ethical hacking workflow discipline and are operating with professional assessment habits.

13–20 Checks — Moderate Exposure

You have foundational capability but still show inconsistency in methodology, automation, or evidence management.

0–12 Checks — High Vulnerability

Current tool familiarity is fragmented. Additional Linux operational discipline and structured ethical hacking workflow development are strongly needed.