OSCP Exam Report Template

Fill-in structure for the OffSec OSCP / OSCP+ exam report. Replace bracketed placeholders. Keep every command and screenshot reproducible.

> **Before you start:** confirm the current report requirements in the official PEN-200 course material and the exam guide for your attempt. Structures change between exam revisions. This template is a starting point, not a substitute for the official instructions.

1. Candidate and exam details

Field	Value
Candidate name	*[full name]*
OSID	*[OSID]*
Exam date / window	*[date and start time]*
Certification	*[OSCP or OSCP+]*

2. Executive summary

[3–6 sentences: what was assessed, how many targets were compromised, what level of access was achieved, and the overall risk. Write this last, but place it first.]

3. Scope and environment

Target	IP / hostname	OS	Result	Points
[Standalone 1]	*[10.10.x.x]*	*[Linux]*	*[root]*	*[20]*
[Standalone 2]	*[10.10.x.x]*	*[Windows]*	*[SYSTEM]*	*[20]*
[Standalone 3]	*[10.10.x.x]*	*[Linux]*	*[root]*	*[20]*
[AD set]	*[10.10.x.x]*	*[Windows]*	*[Domain Admin]*	*[40]*

4. Methodology

[Short paragraph: enumeration approach, toolset, how findings were validated, how evidence was captured. Do not paste a generic methodology essay; describe what you actually did in this exam.]

5. Findings per target

5.x [Hostname] — [IP]

Field	Detail
Hostname / IP	*[host / 10.10.x.x]*
Operating system	*[version]*
Initial access	*[service, vulnerability, CVE if applicable]*

Privilege escalation	*[path and mechanism]*
Final access	*[user / root / SYSTEM]*

Enumeration

[Commands run, services discovered, what each result told you. Keep output trimmed to the lines that matter.]

Exploitation

[Exact command or request, the response that confirms success, and a short explanation of why it worked.]

Privilege escalation

[Misconfiguration, vulnerable service or credential path. Show the before and after privilege level.]

Evidence

- *[Screenshot: whoami / hostname showing final access]*
- *[Screenshot: proof file or flag]*
- *[Screenshot: key exploitation step]*

Remediation

[Specific fix: patch level, configuration change, credential rotation, network control. Not "apply updates".]

6. Active Directory chain

6.1 Attack path overview

[Domain user → privilege escalation → lateral movement → Domain Admin. One line per hop.]

6.2 Domain enumeration

[LDAP / BloodHound queries, users, groups, ACLs, delegation findings. Annotate the BloodHound graph with the path you actually used.]

6.3 Credential access

[Kerberoasting, AS-REP roasting, password reuse, shares. Show both the request command and the resulting ticket or hash.]

6.4 Lateral movement and pivots

[Each hop: source host, destination host, credential used, technique. Add a simple diagram labelling interfaces and port forwards.]

6.5 Domain Admin proof

[Command output proving administrative control of the domain, plus the step that granted it. A final hash alone is not enough.]

7. Command log

[Optional appendix: commands in order, one per line, in monospaced blocks. Useful when a grader needs to replay a step.]

8. Submission checklist

- Every target in the scope table has a matching findings section.
- Every exploitation step has a command and a confirming output.
- Every screenshot is readable and shows host identity or privilege level.
- AD chain shows each hop, not only the final Domain Admin proof.
- Remediation is specific to the finding.
- Report opens cleanly in the required format and file name.
- No placeholder text left in the document.

Template provided by CyberServices.Store for study use. Confirm against the official OffSec requirements before submitting.