



Content store x portaltbittentechsolutions.in/vu x Bash for Beginners | Learn Shell x +

portaltbittentechsolutions.in/viewPdf

Why?

- Penetration Testing is a **process**, not a **deliverable**
- Documentation is an **eye** to the **process**
- PT makes you **skilled**, reporting makes you a **professional**
- OffSec allocates **24hr** for labs, and **24hr** for reporting
- First 24hr < Next 24hr
- **All flags** obtained, can **still** fail with 0!

What to Document?

2 What to Document?

What?

- ▶ All
 - ▶ Steps
 - ▶ Commands
 - ▶ Outputs
 - ▶ Exploit code
- ▶ Flag screenshots, local and proof
 - ▶ File **contents** and system **network address together**

What?

► What?

► Exploit code

- **Modified** code, and **why**
- **URL** to the script
- **Shellcode** generation commands



CyberProactive
@1632021307

3 ► Where to Document?



CyberProactive
@1632021307

CyberProactive
@1632021307

Content store x portalbittentechsolutions.in/vu x Bash for Beginners | Learn Shell x +

portalbittentechsolutions.in/viewPdf

Where?

- Official OffSec Report [Template](#)
- You can **build your own**
- Bring all the **proofs** gathered from attacking machine
- Show your **MS Word skills!**

4 How to Document?

4

How to Document?

How?

- Documentation is a **part of the process**
- Use a **note making app**
 - OneNote
 - KeepNote
 - CherryTree
- **Draft** a rough report **along**
- **Copy** all **outputs**
- **Save screenshots** for all the steps

Content store x portalbittentechsolutions.in/v... x Bash for Beginners | Learn Shell - X | +

portalbittentechsolutions.in/viewPdf

- Save screenshots for all the steps

10

► How?

- Target audience is a technically competent reader
- Detailed enough for a professional, concise enough for a stakeholder
- Don't assume anything!
- No grammar or spelling mistakes
- Stick to the point
- Put as many screenshots as possible
- Proof read 2-3 times

11

► How? [IMPORTANT]

- Your exam report is in PDF format
- PDF file name "OSCP-OS-XXXXX-Exam-Report.pdf"
- Your PDF has been archived into a .7z file (NO password)
- .7z file name "OSCP-OS-XXXXX-Exam-Report.7z"

- ▶ Target audience is a technically competent reader
- ▶ Detailed enough for a professional, concise enough for a stakeholder
- ▶ Don't assume anything!
- ▶ No grammar or spelling mistakes
- ▶ Stick to the point
- ▶ Put as many screenshots as possible
- ▶ Proof read 2-3 times

▶ How? [IMPORTANT]

- ▶ Your exam report is in PDF format
- ▶ PDF file name "OSCP-OS-XXXXX-Exam-Report.pdf"
- ▶ Your PDF has been archived into a .7z file (NO password)
- ▶ .7z file name "OSCP-OS-XXXXX-Exam-Report.7z"
- ▶ Archive is not more than 200MB
- ▶ Upload your .7z file to <https://upload.offsec.com>