Staying Organized

Whether we are performing client assessments, playing CTFs, taking a course in Academy or elsewhere, or playing HTB boxes/labs, organization is always crucial. It is essential to prioritize clear and accurate documentation from the very beginning. This skill will benefit us no matter what path we take in information security or even other career paths.

Folder Structure

When attacking a single box, lab, or client environment, we should have a clear folder structure on our attack machine to save data such as: scoping information, enumeration data, evidence of exploitation attempts, sensitive data such as credentials, and other data obtained during recon, exploitation, and post-exploitation. A sample folder structure may look like follows:

```
MichaelLuka@htb[/htb]$ tree Projects/

Projects/
└── Acme Company
    ├── EPT
    │   ├── evidence
    │   │   ├── credentials
    │   │   ├── data
    │   │   └── screenshots
    │   ├── logs
    │   ├── scans
    │   ├── scope
    │   └── tools
    └── IPT
        ├── evidence
        │   ├── credentials
        │   ├── data
        │   └── screenshots
        ├── logs
        ├── scans
        ├── scope
        └── tools
```

Here we have a folder for the client `Acme Company` with two assessments, Internal Penetration Test (IPT) and External Penetration Test (EPT). Under each folder, we have subfolders for saving scan data, any relevant tools, logging output, scoping information (i.e., lists of IPs/networks to feed to our scanning tools), and an evidence folder that may contain any credentials retrieved during the assessment, any relevant data retrieved as well as screenshots.

It is a personal preference, but some folks create a folder for each target host and save screenshots within it. Others organize their notes by host or network and save screenshots directly into the note-taking tool. Experiment with folder structures and see what works best for you to stay organized and work most efficiently.

Note Taking Tools

Productivity and organization are very important. A very technical but unorganized penetration tester will have a difficult time succeeding in this industry. Various tools can be used for organization and note-taking. Selecting a note-taking tool is very individual. Some of us may not need a feature that another person requires based on their workflow. Some great options to explore include:

Cherrytree	Visual Studio Code	Evernote
Notion	GitBook	Sublime Text
Notepad++		

Some of these are more focused on note-taking, while others such as Notion and GitBook have richer features that can be used to create Wiki-type pages, cheat sheets, and more. It is important to make sure that any client data is only stored locally and not synced to the cloud if using one of these tools on real-world assessments.

Tip: Learning Markdown language is easy and very useful for note taking, as it can be easily represented in a visually appealing and organized way.

Other Tools and Tips

Every infosec professional should maintain a knowledge base. This can be in the format of your choosing (though the tools above are recommended.) This knowledge base should contain quick reference guides for setup tasks that we perform on most assessments and cheat sheets for common commands that we use for each phase of an assessment.

As we complete boxes, labs, assessments, training courses, etc., we should be aggregating every payload, command, tip as we never know when one may come in handy. Having them accessible will increase our overall efficiency and productivity. Each HTB Academy Module has a cheat sheet of relevant commands showcased within the Module sections, which you can download and keep for future reference.

We should also maintain checklists, report templates for various assessment types, and build a findings/vulnerability database. This database can take the form of a spreadsheet or something more complex and include a finding title, description, impact, remediation advice, and references. Having these findings already written will save us considerable time and re-work during the reporting phase as the bulk of the findings will be written already and likely only require some customization to the target environment.

Moving On

Try out various note-taking tools and develop the folder structure that works for you and matches your methodology. Start early, so this becomes a habit! The Nibbles walkthrough later in this Module is an excellent opportunity to practice our documentation. Also, this Module contains many commands that are useful to add to our common commands cheat sheet.

- Basic Tools
- Service Scanning
- Web Enumeration
- Public Exploits
- Types of Shells
- Privilege Escalation
- Transferring Files

Getting Started with Hack The Box (HTB)

- Starting Out
- Navigating HTB

Attacking Your First Box

- Nibbles - Enumeration
- Nibbles - Web Footprinting
- Nibbles - Initial Foothold
- Nibbles - Privilege Escalation
- Nibbles - Alternate User Method - Metasploit

Problem Solving

- Common Pitfalls
- Getting Help

What's Next?

- Next Steps
- Knowledge Check

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left