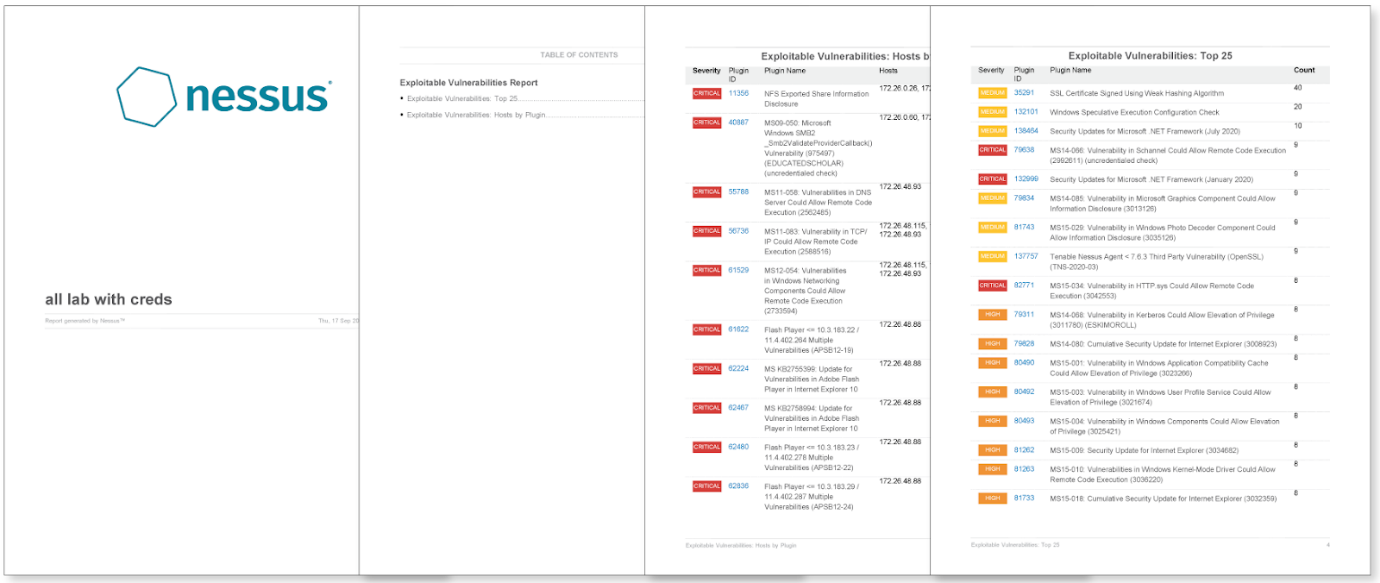
[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@b64f6edaeece4b50be6d48d0ffcb4343?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Generate a Report after Performing a Scan**

When the time comes to present the results of Nessus scans, you must first choose between reports and exports (although, strictly speaking, all of the options below involve exporting files):

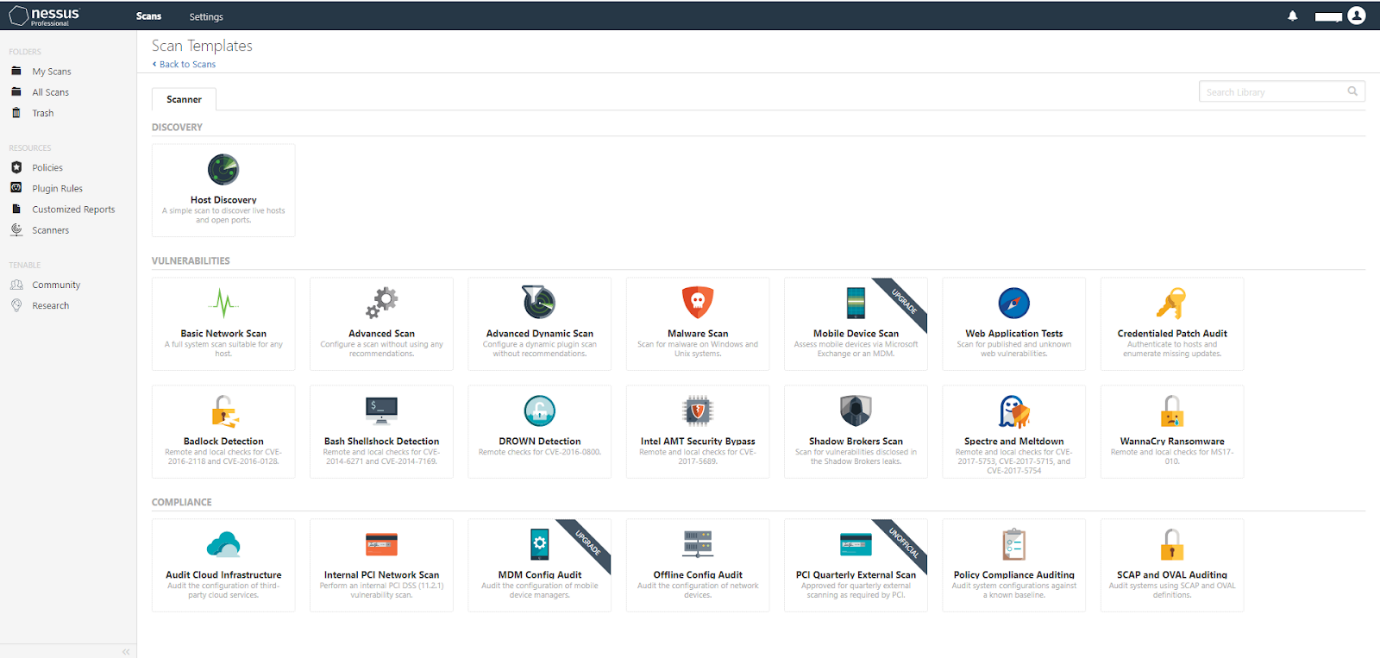
1. Reports: You have the most versatility with the presentation of your vulnerability scan findings if you decide to turn them into reports. Reports can be PDFs or HTML-based and are easily customizable in terms of what information you include, how it is presented, and their overall visual aesthetic.
2. Exports: Scans themselves can be exported as files in .XML, CSV or Nessus's proprietary DB format. .CSV is especially useful for importing into external databases, and .XML files can be imported into other tools, kept as a historical reference for auditing purposes or also later used as a policy template for future Nessus scans.



So you have to decide what you want most out of the report: Do you need to distribute and present it to a client team for remediation or put it into practice as a policy template for future efforts? Or are you building a historical record of scanning practices? Nessus has you covered for both of these reporting needs and many more.

**Nessus scan reporting step by step**

In some ways, the reports you end up with are only as strong as the policy you use to establish the parameters of your vulnerability scan. First, you need a clear understanding of the scan scope so that you're looking through the network areas you (or your client, if you're scanning as a consultant) are most concerned about and seeking out priority targets. To get started quickly, you can choose the proper template from among the pre-built options available in Nessus, or use any custom policies you may have added to the library.



Once the scan is complete and you've taken the time to look at your results, it's time to create your report:

1. If exporting in the .XML, or .CSV formats for future importation into a policy library or other database, simply click Export in the upper right-hand corner of the scan's results page and choose the desired format from a drop-down menu.
2. For PDF and HTML reports that display the scan results without any alterations, select the Executive Summary option, choose a file format and then click Export. (If choosing PDFs, remember that you need either Java or an open-source version of the Java Development Kit to generate them.)
3. To put together customized reports in either of those styles, select the Custom option on the scan results page. Then choose which scan results you want to include - Vulnerabilities, Remediations, Hosts, Notes, History, and Dashboard view can all be shown or hidden depending on your needs (and those of your client.)
4. Last but not least, determine whether you want to group any vulnerabilities you've discovered by hosts or plugins affected, and then click Export.



**Report reading pointers**

How you look at reports depends largely on your position and responsibilities within your organization - or, if you're consulting, what the client expects to learn from the vulnerability scanning, assessment, and reporting processes.

If you're part of the infosec or IT team, you'll certainly want to read your scan reports as thoroughly as possible. It's on you and your colleagues to review system vulnerabilities, project the levels of risk these issues create, and determine the best strategy for ridding the network, servers, and hosts of the most critical threats. Given how meticulously you need to understand your vulnerabilities, it may be best to create reports in multiple formats, and with different configurations: Specifically looking at ERP tech stack vulnerabilities and nothing else, for example, might help you dig into those problems, and then you'd switch back to a full-scan report or one displaying flaws in another asset type. Nessus makes this simple, and also allows you to easily compare the results of different scans.

Things are a bit different from the consultant's perspective. You still need to understand scan details front to back, but consider your audience - how much of that information does the client need immediately? You can start by presenting a succinct version of the report that covers essential details – especially when creating .HTML reports, which have an Executive Summary template – while including links to additional content for those who want more information.

Nessus Professional includes many predefined reports which are configured to provide useful summaries of scan results. Some of the reports you can create include:

* Unsupported software: provides insight into unsupported software found in your environment
* Exploitable vulnerabilities: details all detected vulnerabilities that have known exploits
* Operating system detections: lists all operating systems found on the scanned targets

However you need to configure your reports for optimal effectiveness, Nessus Professional can accommodate you.