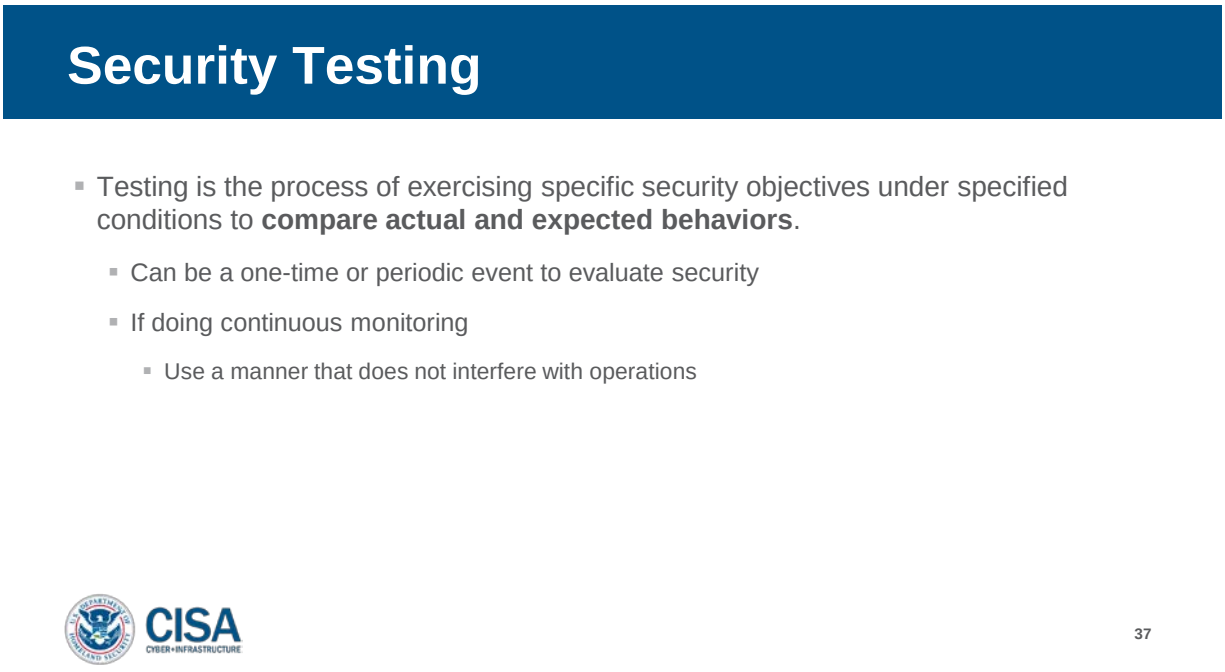
Security Testing and Assessments

Table of Contents

Security Testing and Assessments

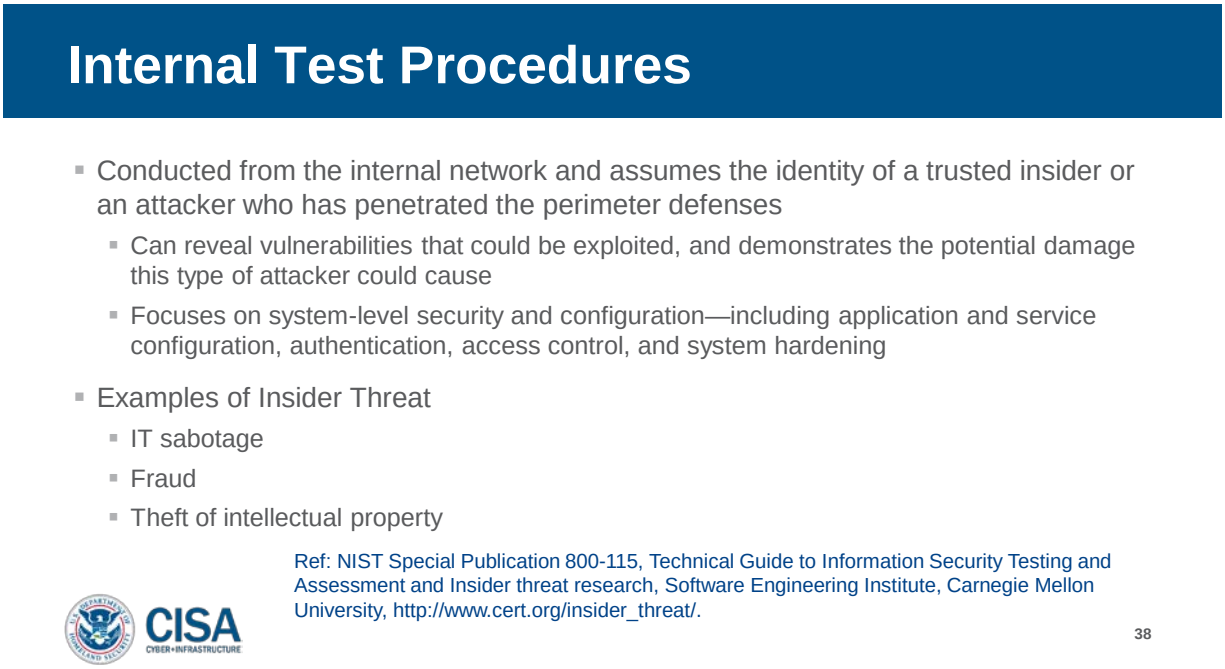
**036 Instructor: I want to talk about security testing and assessments.



**037 Let's review where we're at, first of all. Remember, we've identified the risks to the enterprise, which was nothing more than understanding the uncertainty related to threats that you may have that are looking to incur an impact on your organization, and they're going to do it by exploiting certain vulnerabilities. We've selected some security controls; we've actually implemented them; we maybe have even assessed them by this point; and we've implemented those mitigation strategies. We may be even continually monitoring them for how they're actually performing; and now we want to actually test the system. So we want to actually think about what we're expecting in terms of the actual system behavior. Now, this can be done one time or it can be periodically and quite regularly if you want it.

Now, if you're doing continuous monitoring, you may want to do testing such that it doesn't interfere necessarily with operations. There are some ways to do this we're going to discuss here, but if you think about it, at the heart of it, basically if you keep people informed, it may do a lot and go a long way to minimizing that interference.

Internal Test Procedures

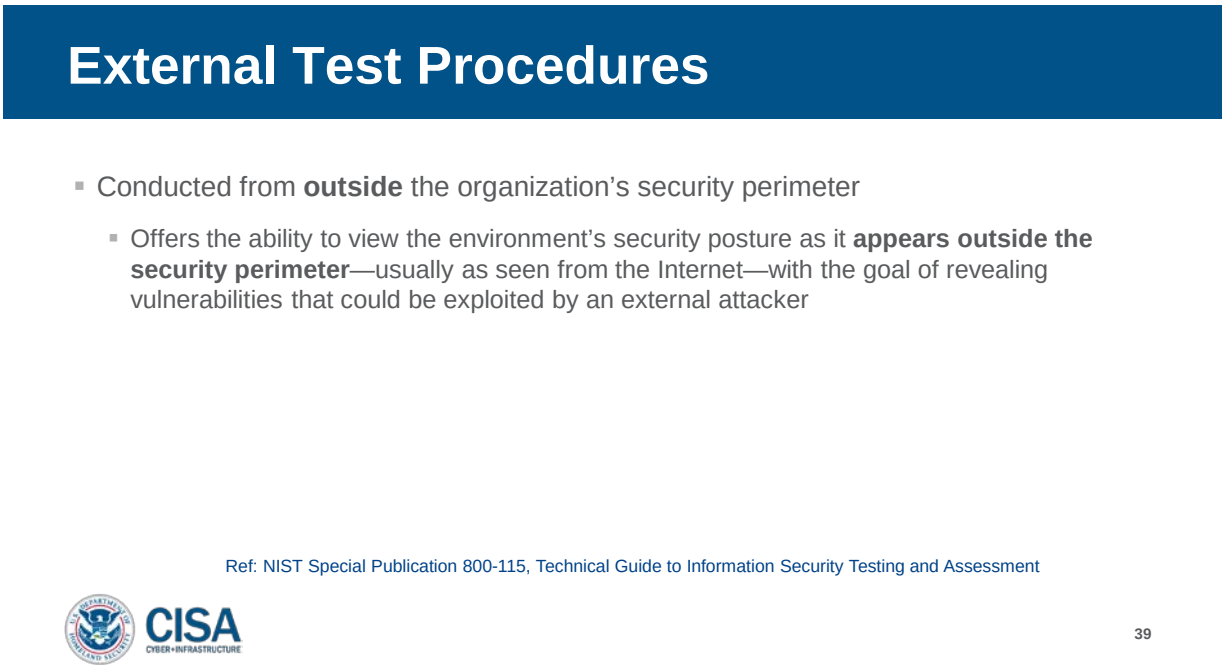


**038 So let's talk about some test procedures here and what you might have internal to your organization. What we're speaking about here is the notion that your threat actors may actually be inside the walls of your organization. So what you want to do is you want to think of a trusted insider or someone who can act as an attacker and if they've gotten inside your fences what they can actually do.

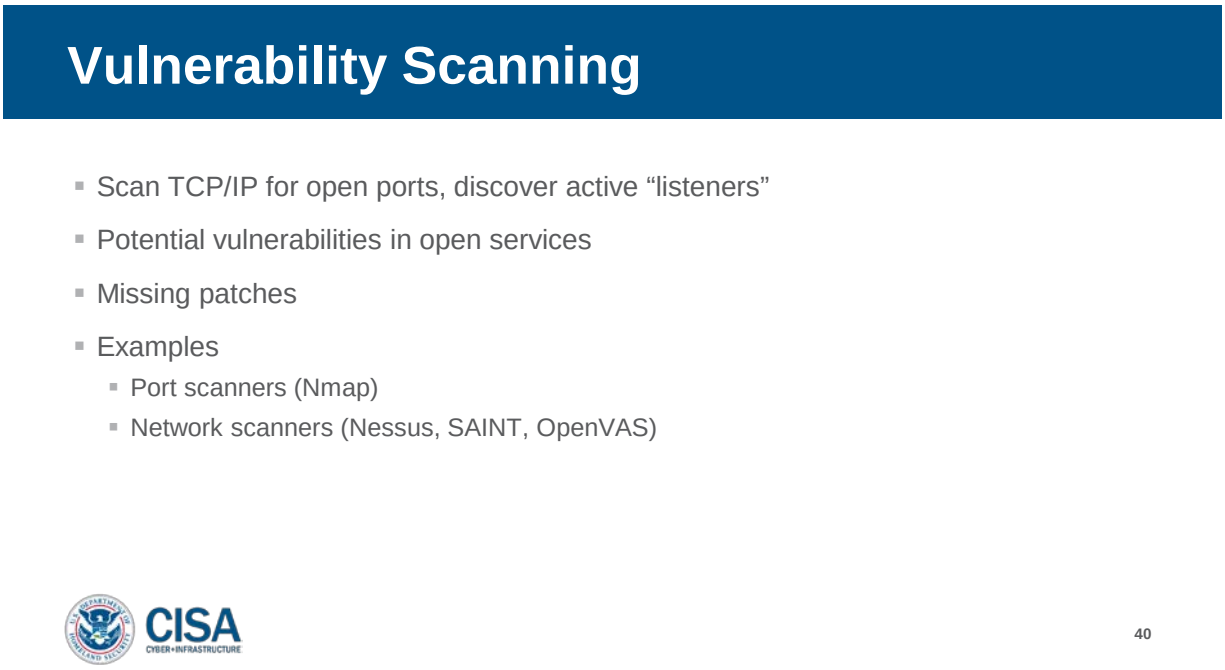
So if you give an attacker that kind of access, you really want to look at what vulnerabilities could be exploited, and you also want to look at the system-level security configuration and make sure that you have proper system hardening, such that even if an insider were to get through, they would be limited in exactly what they can actually find.

There's a whole bunch of different strategies here that we can talk about. For example, suppose you actually provide need-to-know type control on your personnel. Now the insider may only be able to access the things that specifically they need to know to executive their job, and you're insulating other information assets in your organization in that manner.

You want to also think about this in terms of the nature of the threat. Could be sabotage. In that case, you're worried truly about the integrity of the system. Maybe it's an issue of fraudulence, or fraudulent actions. Also, it could be the idea of theft of intellectual property, and that speaks directly to your confidentiality of your information assets.



**039 Now, you may actually want to look at test procedures that will actually test the system externally. So imagine if I had a castle and the castle's my primary asset, and I have walls that are around the castle. Those are my security controls that I have in place to keep outsiders from actually coming into my system and doing damage. I want to get a good picture as to what that wall looks like from the outside. What does it look like from outside the security perimeter if I had an adverse attacker trying to get into the system?



**040 There's this other notion too that I want to understand what are the gaps or what are the chinks in my armor, and I could look for vulnerabilities in a number of ways. One is I could look at ports that are actually transmitting and/or receiving data. I could also look to see that they systems are being updated and patched quite regularly. I have a lot of different tools that I could go through on this one, but for port scanners, an example would be like nmap. Network scanners, I could use a tool, for example, like Nessus.

Penetration Test

- **May** provide
  - A focused view of the network security posture
  - An analysis of how effective network defenses are to specific attacks
  - A view of how vulnerable specific users are
  - Metrics or scores based on test results
- **May not** provide
  - A list of all vulnerabilities on the network
  - A comprehensive and holistic view of defenses
  - A threat-based look at the network

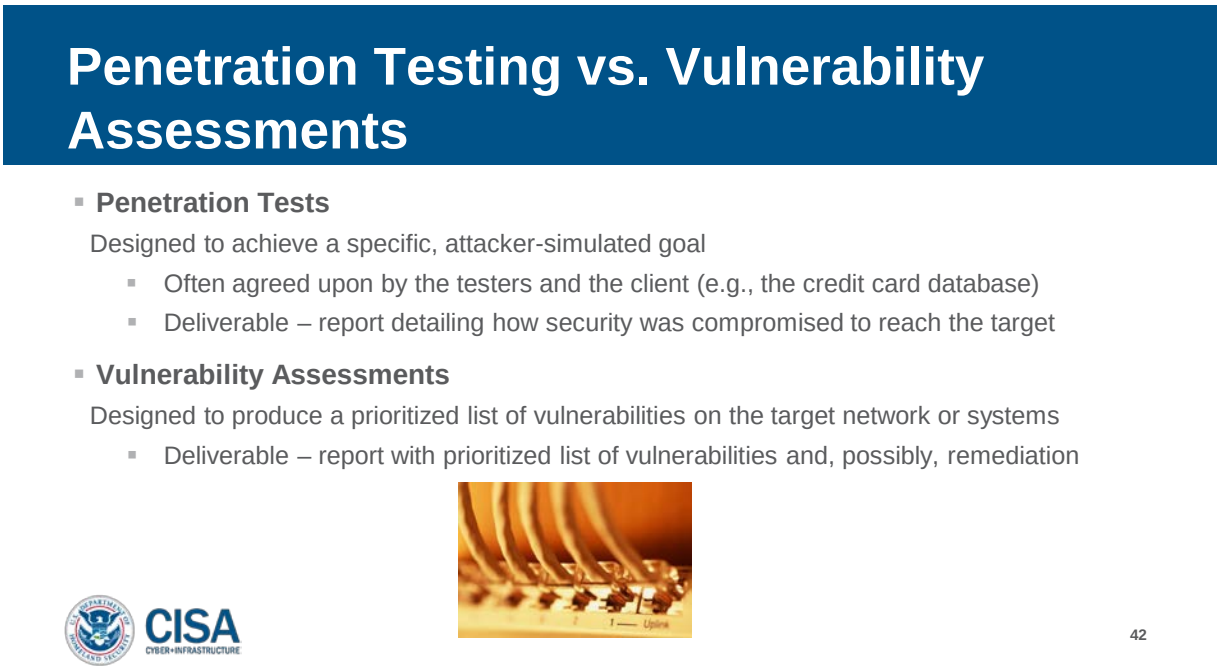
CISA CYBER+INFRASTRUCTURE

41

**041 Now, what I've talked to this point, I've actually tried to identify vulnerabilities or gaps in my system. But what if I want a more detailed sniper shot, if you will, at my system? Penetration testing may accomplish this for you. It gives you a very focused view at what you may have in terms of your with security. It also looks at how effective your defenses are against very specific attacks. If you specify the attack, you may actually find out that you actually have vulnerabilities not only technically in the system, but it may be related too to specific users who are using that system. What it really is not going to get you though is a broad understanding of vulnerabilities that you have on your system. If you want that more holistic view of your defenses, you're going to want to actually use maybe some other tool.

At least understand the gaps, for example, you have vulnerability scanning. You also may want to take a more threat-based look at your network if you want something a little broader.

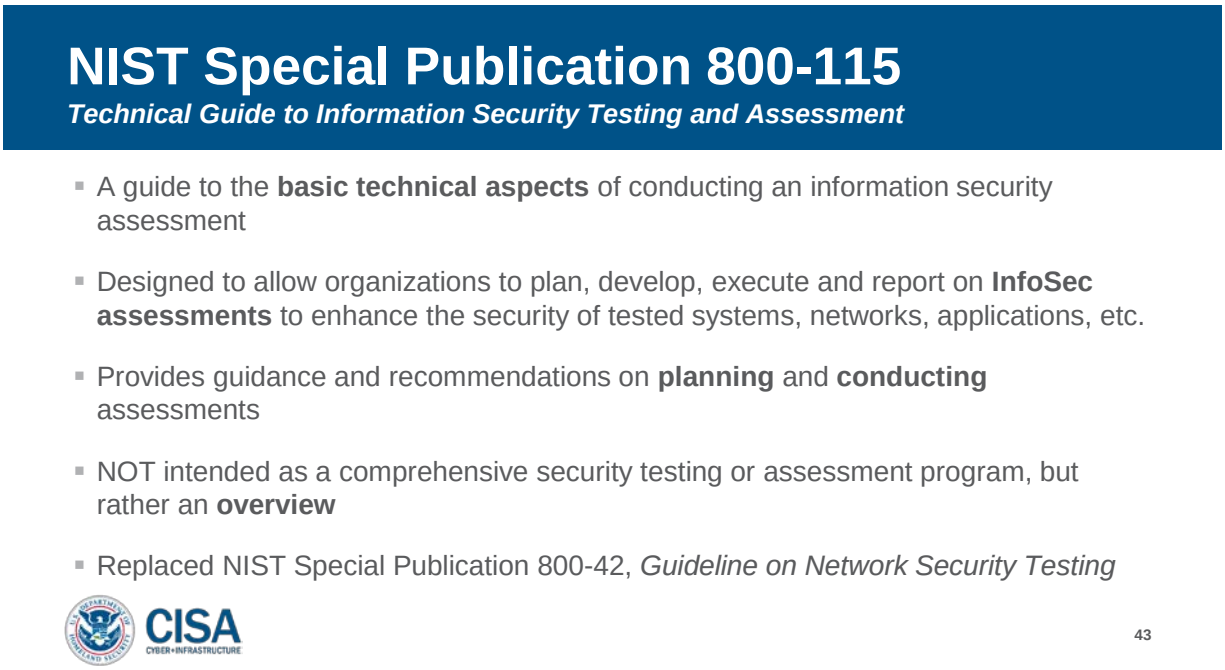
Penetration Testing vs. Vulnerability Assessments



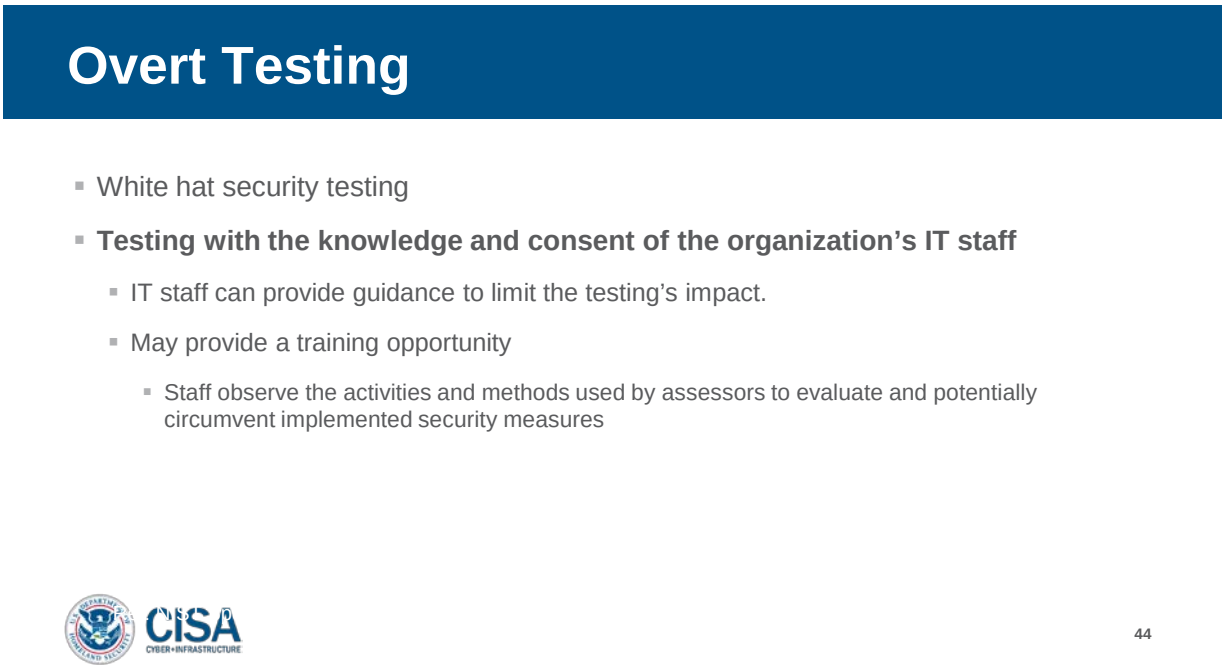
**042 So let's be clear. The difference between penetration tests and vulnerability assessments are quite distinct. Remember that penetration test is a sniper shot at your system. It's a simulated attack, and typically what you're doing is there's an agreed-upon tester and you have the person who is being attacked, and normally what you're going to get is a report on how the system was compromised, or if it was-- if they were able to reach that overall objective that was set. Vulnerabilities-- remember, once again, I'm looking for the chinks in

the armor where people can actually get through, and what I would like there is a prioritized list of what those gaps are so that way I can go back and remediate them.

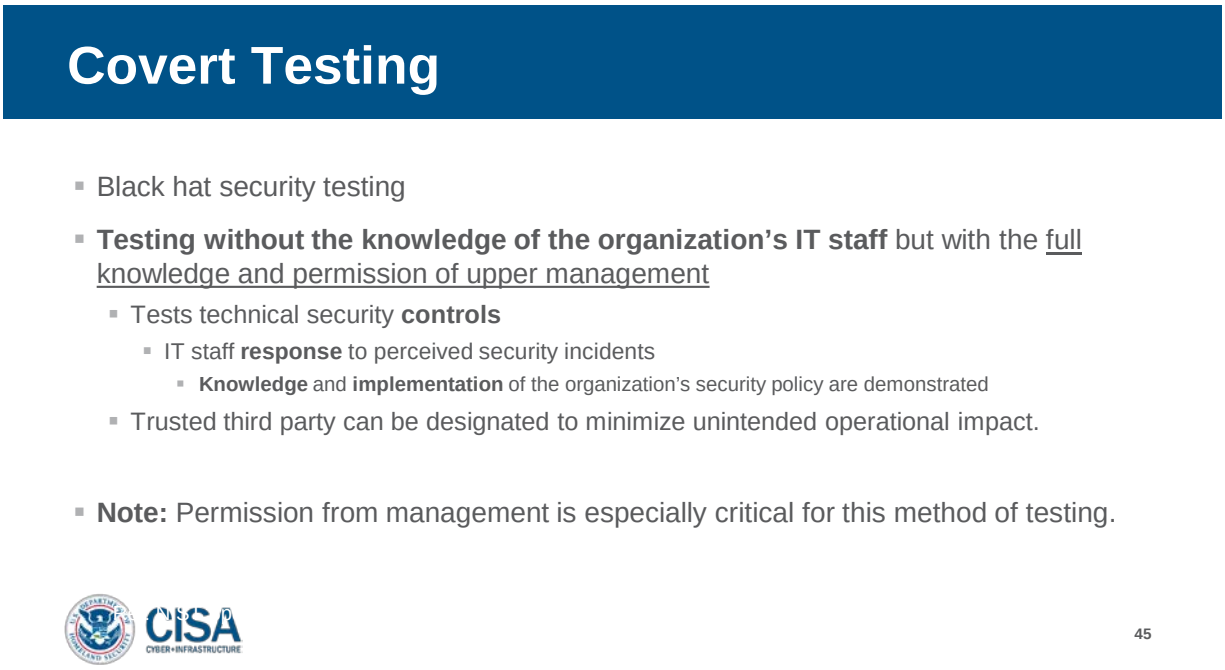
NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment



**043 If you look at NIST SP 800-115, you can learn a little bit more about this information security testing business. So, it will give you the technical aspects of what you're going to do in this assessment, and to be honest with you, it'll actually help you plan and conduct your assessments a lot more effectively. It's not comprehensive, but it can definitely give you a good overview if you want to learn more about how you're going to test your system.



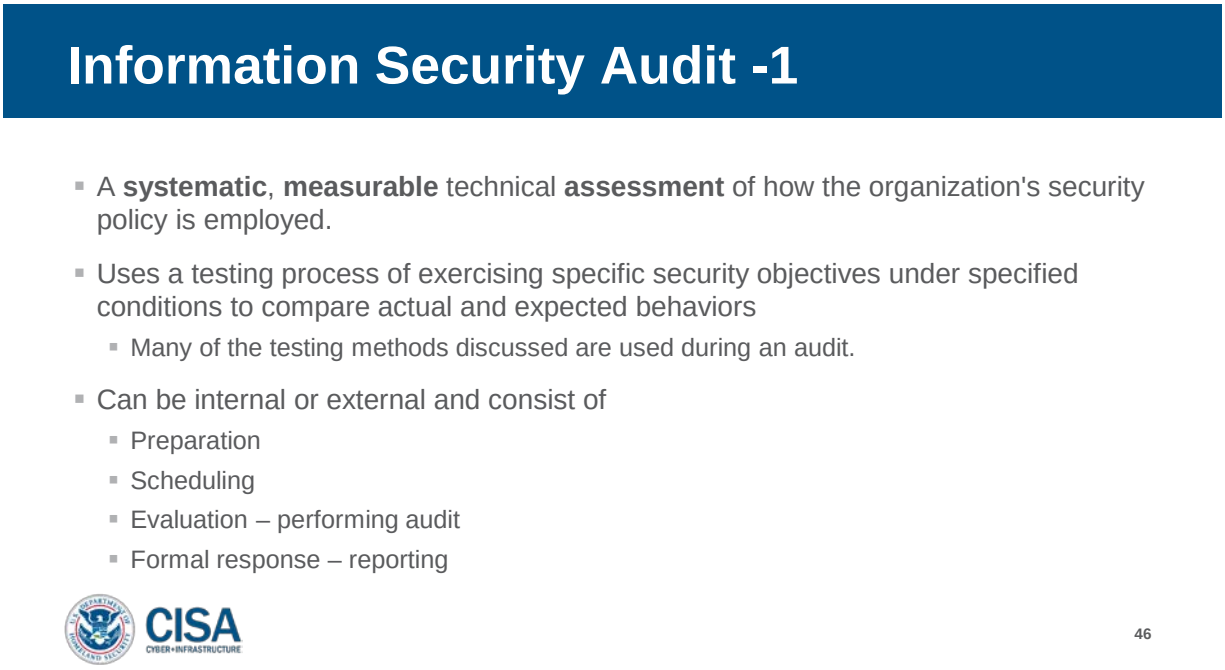
**044 There are different types of tests too. There's overt testing. This can be called white hat testing at times, and what we're doing is really testing the knowledge of the system, but we actually know that the actual person is attacking the system. The IT staff is actually sitting there and they can give guidance to actually limit what is going to take place in that test. It's a good training opportunity for your people too to see how things actually go down if I'm an attacker and I'm trying to actually attack the system to kind of understand at least how security controls can be circumvented.



**045 But there's also this covert testing idea. That's also called black hat security testing. Now what we have here is we have maybe an external provider, or it could be internal, but they're going to go off the grid, if you will, and they're going to talk to the management team and say, "Hey, we are going to conduct this penetration test and we're not going to tell anybody on the staff that it's taking place." By the way, if you're going to do this, you really need that manager's permission to actually go do that test, because there will be alarms that may go off and people may actually take specific actions to implement controls and incident responses. If that's the case, this means that there could be interference in normal day-to-day activities and you want to be very

aware as to what the impacts are from such an event.

Information Security Audit -1

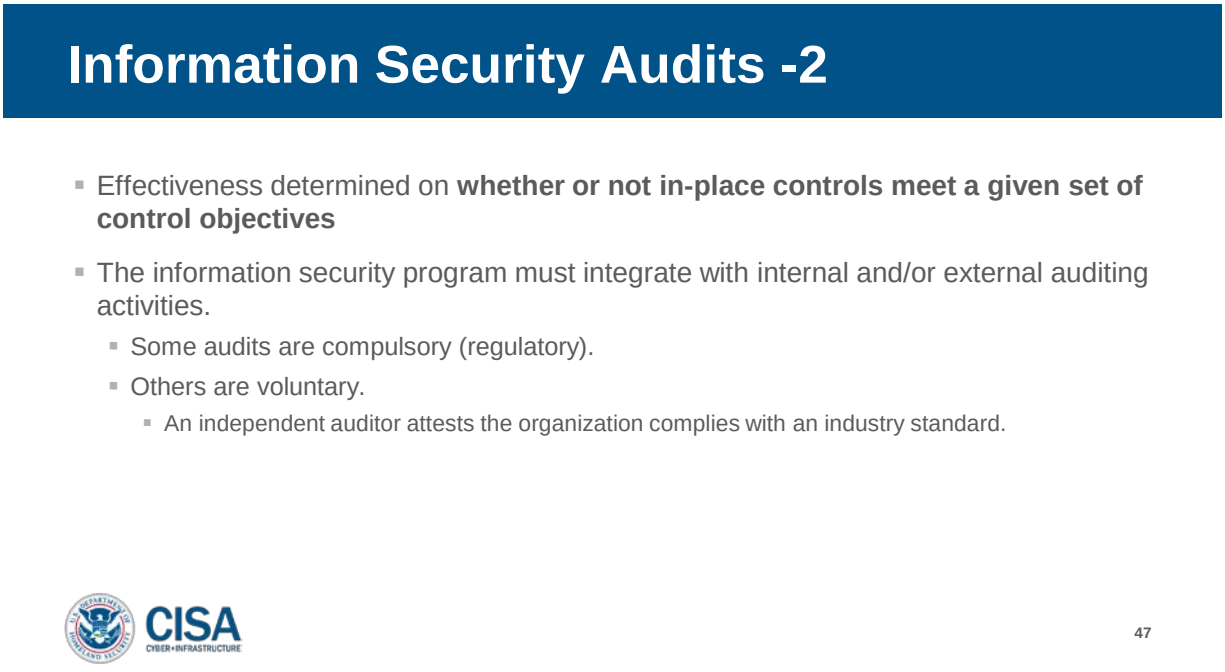


**046 Now, I could also audit my system. If you think about it, this is a very systematic process where I'm going to actually go measure how policy is being employed in an organization, and really what I'm trying to do here is I have a set of security objectives and I'm trying to make sure that they're actually being achieved with the behaviors of people in the organization and the behaviors of the technology; the expectations are being met by the security stack that I've implemented.

So the distinct steps that you may want to take here is you're going to prepare for that audit-- and by the way, it may be an internal auditor that's doing this, or it may be an

external auditor. They're going to establish a schedule around how long they want to conduct this audit, and they're actually going to think about what the specific scope is that they're auditing. Then they're actually going to perform that audit, and they're going to develop a report and provide it to your management team.

Information Security Audits -2

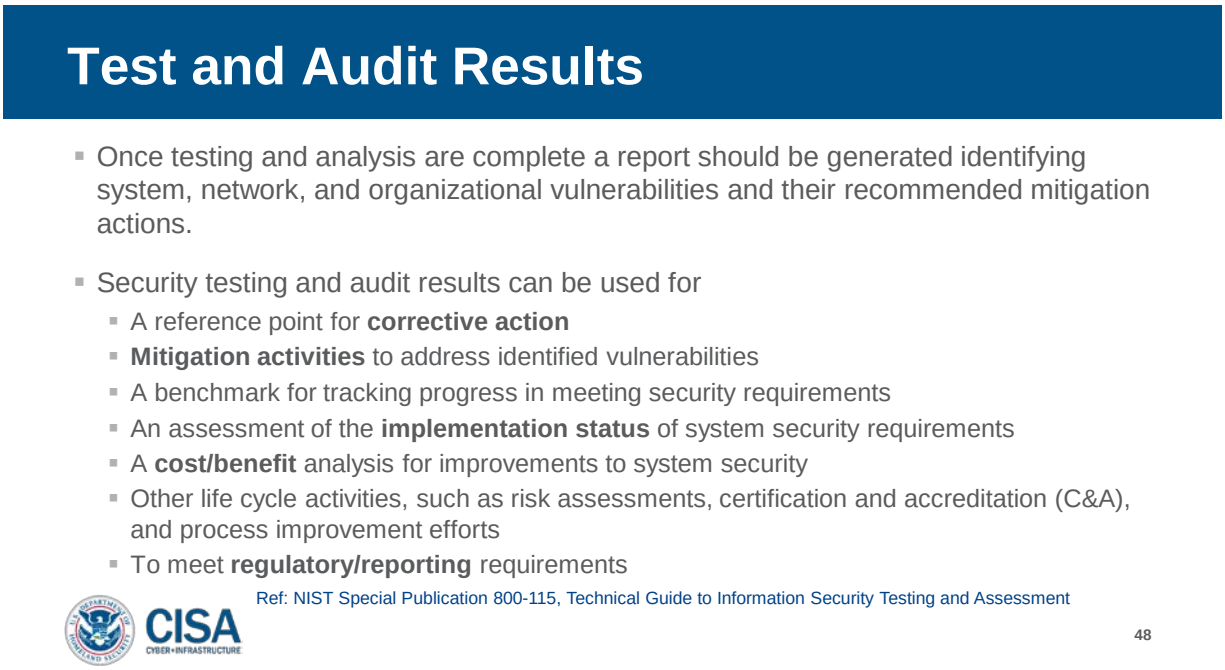


**047 Hopefully what we're going to get from this audit is to know whether or not you have the right controls in place. That said, you have control objectives that you set. You may also learn that existing controls that you have actually in place are maybe not meeting muster in terms of what your expectations are.

Now, some of these audits, you may have to actually do just because it's a

regulatory necessity. Others you may want to do because you know you have systems you have low confidence in in terms of meeting certain risks or managing certain risks. In that case, you want to actually have a voluntary audit.

Test and Audit Results



**048 Once the audit is through, they're going to compile the results and they're going to have to report them to somebody, most likely your management team, and I bet you if you're a front-line professional, you're going to get those results as well, because you're going to be the one who's actually implementing the corrective actions. You also want to think about, "Hey, now I have a benchmark," or something that I can use to compare with peers in my industry, maybe, or in my sector, so I understand how I'm performing, so I

understand what maturity level I am in terms of having security implemented in my organization.

Also, I could have a certain set of controls that are midway into implementation, and I can learn more about the status of that implementation. This may include the fact that they're actually running, but maybe I have personnel in the organization who are not fully trained yet to understand how to actually use the actual controls themselves to make sure that those requirement are being met.

I can maybe also get an understanding if I'm getting a return on investment for my risk investment that I've made, kind of a cost-benefit analysis in that regard.

Also, I may actually ultimately have to submit this report to meet regulatory expectations.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098