

# Security Testing and Assessments

## Table of Contents

Security Testing and Assessments .....	2
Security Testing .....	3
Internal Test Procedures .....	4
External Test Procedures .....	6
Vulnerability Scanning .....	7
Penetration Test .....	8
Penetration Testing vs. Vulnerability Assessments .....	9
NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment .....	10
Overt Testing .....	11
Covert Testing .....	12
Information Security Audit -1 .....	13
Information Security Audits -2 .....	14
Test and Audit Results .....	15
Notices .....	17

## Security Testing and Assessments



## Security Testing and Assessments

36

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

# Security Testing

- Testing is the process of exercising specific security objectives under specified conditions to **compare actual and expected behaviors**.
  - Can be a one-time or periodic event to evaluate security
  - If doing continuous monitoring
    - Use a manner that does not interfere with operations



37

\*\*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

# Internal Test Procedures

- Conducted from the internal network and assumes the identity of a trusted insider or an attacker who has penetrated the perimeter defenses
  - Can reveal vulnerabilities that could be exploited, and demonstrates the potential damage this type of attacker could cause
  - Focuses on system-level security and configuration—including application and service configuration, authentication, access control, and system hardening
- Examples of Insider Threat
  - IT sabotage
  - Fraud
  - Theft of intellectual property

Ref: NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment and Insider threat research, Software Engineering Institute, Carnegie Mellon University, [http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/).



38

**\*\*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 execute 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.

# External Test Procedures

- Conducted from **outside** the organization's security perimeter
  - Offers the ability to view the environment's security posture as it **appears outside the security perimeter**—usually as seen from the Internet—with the goal of revealing vulnerabilities that could be exploited by an external attacker

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



39

\*\*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?

# Vulnerability Scanning

- Scan TCP/IP for open ports, discover active “listeners”
- Potential vulnerabilities in open services
- Missing patches
- Examples
  - Port scanners (Nmap)
  - Network scanners (Nessus, SAINT, OpenVAS)



40

\*\*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

# 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



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

# Penetration Testing vs. Vulnerability Assessments

### ▪ Penetration Tests

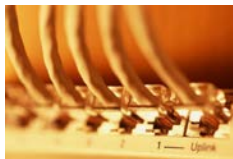
Designed to achieve a specific, attacker-simulated goal

- Often agreed upon by the testers and the client (e.g., the credit card database)
- Deliverable – report detailing how security was compromised to reach the target

### ▪ Vulnerability Assessments

Designed to produce a prioritized list of vulnerabilities on the target network or systems

- Deliverable – report with prioritized list of vulnerabilities and, possibly, remediation



42

\*\*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

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

- A guide to the **basic technical aspects** of conducting an information security assessment
- Designed to allow organizations to plan, develop, execute and report on **InfoSec assessments** to enhance the security of tested systems, networks, applications, etc.
- Provides guidance and recommendations on **planning** and **conducting** assessments
- NOT intended as a comprehensive security testing or assessment program, but rather an **overview**
- Replaced NIST Special Publication 800-42, *Guideline on Network Security Testing*



43

\*\*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.

## Overt Testing

# Overt Testing

- White hat security testing
- **Testing with the knowledge and consent of the organization's IT staff**
  - IT staff can provide guidance to limit the testing's impact.
  - May provide a training opportunity
    - Staff observe the activities and methods used by assessors to evaluate and potentially circumvent implemented security measures



44

\*\*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.

# Covert Testing

- Black hat security testing
- **Testing without the knowledge of the organization's IT staff** but with the full knowledge and permission of upper management
  - Tests technical security **controls**
    - IT staff **response** to perceived security incidents
      - **Knowledge** and **implementation** of the organization's security policy are demonstrated
  - Trusted third party can be designated to minimize unintended operational impact.
- **Note:** Permission from management is especially critical for this method of testing.



45

\*\*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

# Information Security Audit -1

- A **systematic, measurable** technical **assessment** of how the organization's security policy is employed.
- Uses a testing process of exercising specific security objectives under specified conditions to compare actual and expected behaviors
  - Many of the testing methods discussed are used during an audit.
- Can be internal or external and consist of
  - Preparation
  - Scheduling
  - Evaluation – performing audit
  - Formal response – reporting



46

\*\*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

# Information Security Audits -2

- Effectiveness determined on **whether or not in-place controls meet a given set of control objectives**
- The information security program must integrate with internal and/or external auditing activities.
  - Some audits are compulsory (regulatory).
  - Others are voluntary.
    - An independent auditor attests the organization complies with an industry standard.



47

\*\*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

# Test and Audit Results

- Once testing and analysis are complete a report should be generated identifying system, network, and organizational vulnerabilities and their recommended mitigation actions.
- Security testing and audit results can be used for
  - A reference point for **corrective action**
  - **Mitigation activities** to address identified vulnerabilities
  - A benchmark for tracking progress in meeting security requirements
  - An assessment of the **implementation status** of system security requirements
  - A **cost/benefit** analysis for improvements to system security
  - Other life cycle activities, such as risk assessments, certification and accreditation (C&A), and process improvement efforts
  - To meet **regulatory/reporting** requirements



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

48

\*\*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 requirements 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

# Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu). Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098



1