Introduction to Laboratory Assignment 3
Vulnerability scanning with OpenVAS

Computer Security Course
EDA263 / DIT641

Chalmers University of Technology

February 12^{th}, 2015

Vulnerability assessment?

Overview

1. What is Vulnerability assessment?
2. Lab 3 - Vulnerability scanning with OpenVAS
3. Formal Report tips

Vulnerability assessment (identification)

Vulnerability

A weakness in an asset or a group of assets that can be exploited by one or more threats.

The goal of vulnerability assessment is to obtain a (prioritized) list of vulnerabilities with brief description of how and why they might occur.

Vulnerability assessment (identification)

Vulnerability

A weakness in an asset or a group of assets that can be exploited by one or more threats.

The goal of vulnerability assessment is to obtain a (prioritized) list of vulnerabilities with brief description of how and why they might occur.

What is vulnerability scanning?

Vulnerability scanning is an automated process whose goal is to identify *security vulnerabilities* of computer systems in a network.

Vulnerability assessment (identification)

Vulnerability

A weakness in an asset or a group of assets that can be exploited by one or more threats.

The goal of vulnerability assessment is to obtain a (prioritized) list of vulnerabilities with brief description of how and why they might occur.

What is vulnerability scanning?

Vulnerability scanning is an automated process whose goal is to identify *security vulnerabilities* of computer systems in a network.

How is it performed?

Automated tools - *Vulnerability scanners* - software used to assess computer systems for weaknesses using a database of known vulnerabilities.

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing
2. Port scanning
3. Service fingerprinting
4. Vulnerability scanning
5. Assessment and recommendations
6. Assessment follow-up

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing
   - get familiar with the vulnerability scanner used
   - obtain information about the system (system configuration, network topology, etc.)
2. Port scanning
3. Service fingerprinting
4. Vulnerability scanning
5. Assessment and recommendations
6. Assessment follow-up

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing ✓
2. Port scanning
   - obtain a list of open ports (open port ↔ listening service)
   - find information about the open ports - what services are you expecting to find there? (`http(80)`, `SSH(22)`)
3. Service fingerprinting
4. Vulnerability scanning
5. Assessment and recommendations
6. Assessment follow-up

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing ✓
2. Port scanning ✓
3. Service fingerprinting
    - find more about each service behind each open port (version)
    - is it the expected one? (compare results with Step 2)
4. Vulnerability scanning
5. Assessment and recommendations
6. Assessment follow-up

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing ✓
2. Port scanning ✓
3. Service fingerprinting ✓
4. Vulnerability scanning
   - scan the discovered services for potential vulnerabilities
5. Assessment and recommendations
6. Assessment follow-up

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing ✓
2. Port scanning ✓
3. Service fingerprinting ✓
4. Vulnerability scanning ✓
5. Assessment and recommendations
    - use the vulnerability scan report generated by your tool to make recommendations about improving the security status of the system/systems tested
6. Assessment follow-up

Vulnerability assessment

Performed in a number of steps

1. Know your tools and the system you are testing ✓
2. Port scanning ✓
3. Service fingerprinting ✓
4. Vulnerability scanning ✓
5. Assessment and recommendations ✓
6. Assessment follow-up
   - propose a strategy for keeping the system secure
   - propose a list of actions that should be done regularly to keep the system secure
   - the report will help the system owner to reproduce your findings and take the appropriate actions

Vulnerability assessment

Performed in a number of steps

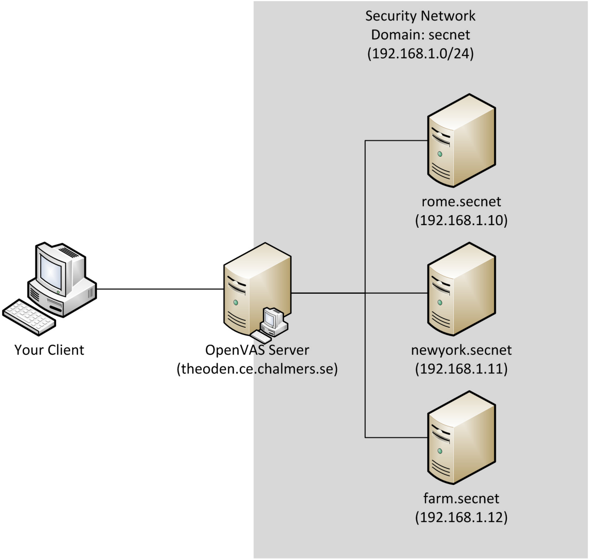
1. Know your tools and the system you are testing ✓
2. Port scanning ✓
3. Service fingerprinting ✓
4. Vulnerability scanning ✓
5. Assessment and recommendations ✓
6. Assessment follow-up ✓

Lab 3 - Vulnerability scanning with OpenVAS

During CW 4–6

- `theoden.ce.chalmers.se` can be accessed from every computer in the Chalmers domain
- Remote access using SSH is possible for this assignment outside the lab session hours.
  (More Info in PingPong - `pingpong.chalmers.se`)

The target network



Tips regarding the formal report

- don't present only the results, but also the steps you took to obtain them → this will help in reproducing your results

Tips regarding the formal report

- don't present only the results, but also the steps you took to obtain them → this will help in reproducing your results
- if you find too many vulnerabilities → focus on the most important ones and motivate your choice

Tips regarding the formal report

- don't present only the results, but also the steps you took to obtain them → this will help in reproducing your results
- if you find too many vulnerabilities → focus on the most important ones and motivate your choice
- follow the tips from the templates and LabPM

Tips regarding the formal report

- don't present only the results, but also the steps you took to obtain them → this will help in reproducing your results
- if you find too many vulnerabilities → focus on the most important ones and motivate your choice
- follow the tips from the templates and LabPM
- use the structure of the template to report your findings

Tips regarding the formal report

- don't present only the results, but also the steps you took to obtain them → this will help in reproducing your results
- if you find too many vulnerabilities → focus on the most important ones and motivate your choice
- follow the tips from the templates and LabPM
- use the structure of the template to report your findings
- don't forget to properly reference the sources used

Tips regarding the formal report

- don't present only the results, but also the steps you took to obtain them → this will help in reproducing your results
- if you find too many vulnerabilities → focus on the most important ones and motivate your choice
- follow the tips from the templates and LabPM
- use the structure of the template to report your findings
- don't forget to properly reference the sources used
- your report will help the network owners in improving the security of their system