

# Penetration Testing Timeline



## SCHEDULING

2-4 Months Before Penetration Test



## TESTING PREPARATION

5 Weeks Before Penetration Test



## AUTOMATED/MANUAL TESTING

During Penetration Test



## REPORTING

0-6 Weeks After Penetration Test



## REMEDIATION

0-3 Months After Penetration Test



## RETESTING

0-3 Months After Penetration Test



## AFTER RETESTING

Ongoing



## SCHEDULING (2-4 Months Before Penetration Test)

You've been given a timeline for your assessment, it is important to consider all factors before scheduling a test.

### Choose a pentester by verifying that:

- | They follow industry best practice standards
- | They communicate their testing methodologies

### Determine your pentest date by answering these questions:

- | Is the pentest starting early enough to leave time for remediation later?
- | Is this during a busy time of the year?
  - | Will office operations be interrupted?
  - | How much notice should we give everyone?

### Confirm your timeline with the pentester



## Testing Preparation (5 Weeks Before Penetration Test)

You have your technical questionnaire, now you need to address all aspects of testing preparation.

### Fill out your questionnaire

### Collect and deliver documentation

- | Provide as much information as you can by answering:
  - | What is your motivation?
  - | What do you really want to find out?
  - | What are your compliance requirements?

### Schedule penetration test

### Coordinate with personnel and prepare office

- | Inform your entire staff
- | Assign team members to assist with pentest

## Coordinate with personnel and prepare office

Verify this is done in your IPS (Intrusion Prevention System)  
or IDS (Intrusion Detection System)



## Automated/Manual Testing *(During Penetration Test)*

During this step, automated scans and manual testing is performed to further assess the security of the target while your team assists to make the process smooth and straightforward.

### Ensure that team members are available to assist with questions or issues during testing

Be available and responsive

Don't change the environment

Raise concerns if production is impacted

Plan enough in advance, holidays can be a popular time to book a pentest

Don't change your environment in the middle of the pentest

### Pick a time of day for automated scans

Determine how busy your environment is during this time



## Reporting *(0-6 Weeks After Penetration Test)*

Now that your penetration test is complete and you've received your report, you should review it to see if the penetration tester was able to identify the root causes of issues.

### Evaluate your report, taking note of:

Date of your report

Mark 90 days later on a calendar as the end of retesting window

The executive summary

Statement of the scope

Methodologies

Limitations

Narrative of steps they went through when they found a problem

What tools they used

How vulnerabilities were identified

### Begin planning for remediation

Analyze findings

Sometimes they can only see the symptoms of the issue

Look to see if the tester was able to identify root causes

### Start addressing root causes



## Remediation *(0-3 Months After Penetration Test)*

It's time to review your report and consider the logistics of your remediation and retesting plans.

### Remediate items

### Schedule retesting

### Your development team will want to:

Review changes

Install patches

Reconfigure software

Update code for all applications

Eliminate old OS (Operating System)

Close any non-critical network ports

Restrict Access

Double-check which personnel have access to what

Evaluate how much access every employee actually requires

Confirm all staff only have essential access



## Retesting *(0-3 Months After Penetration Test)*

During remediation, you can send your test back over to the penetration testing firm for retesting, and receive a revised report.

### Retest (within 90 days of initial report date)

- Certify that fixes are working

- Repeat remediation processes until all fixes are implemented correctly



## After Retesting *(Ongoing)*

Now that remediation and retesting is over, you should make process and policy changes to avoid future vulnerabilities.

### Develop an improvement plan by considering these questions:

- How can we make our environment a little more secure every time?

- Do we need additional training for our developers and network engineers?

- Do they have the resources they need to be successful?

### Assess your experience for next year's pentest:

- Did you have enough time to get everything done?

- Re-evaluate your timeline

### Plan a date for next year's pentest

### Ensure continued maintenance

- Regular updates

- Port scans

- App scans

- Incorporate new security practices