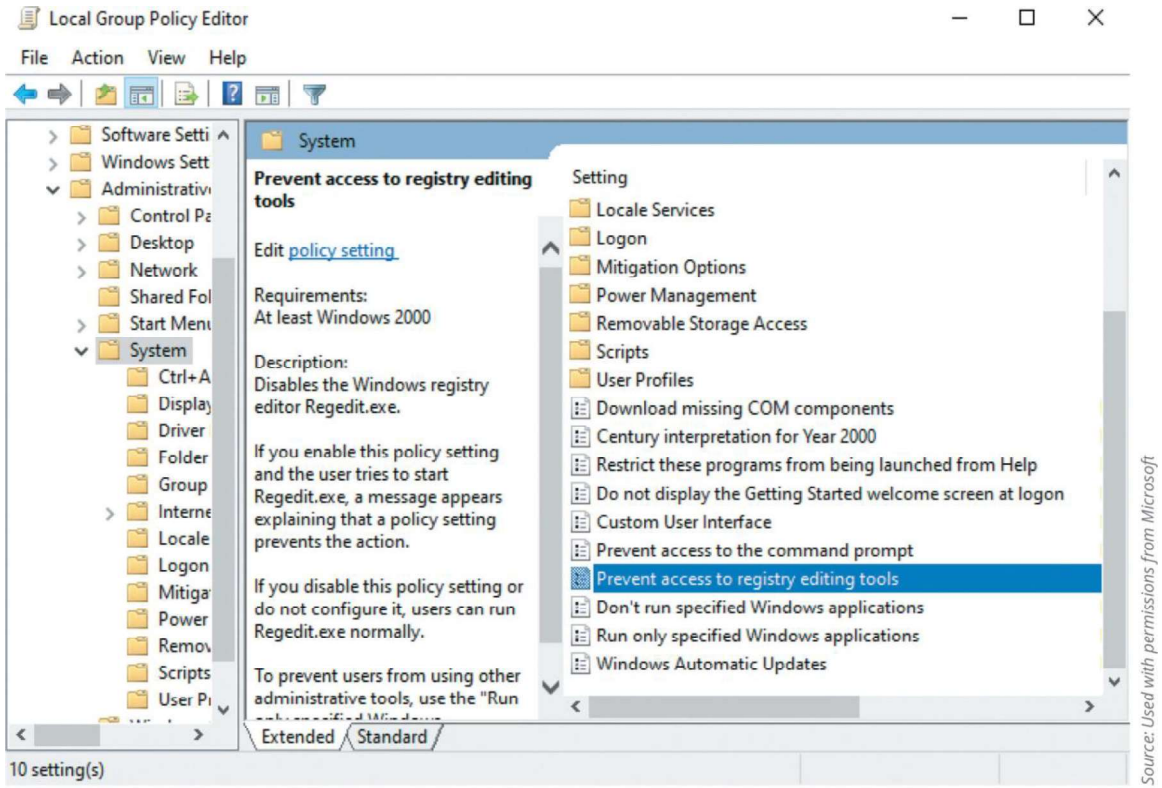
Harden Endpoints (1 of 6)

- Hardening endpoints involves patch management and OS protections
- Patch Management
  - Effective patch management involves two types of patch management tools to administer patches
    - Patch distribution using an *automated patch update service*
    - Patch reception in Microsoft Windows 10 includes the following options:
      - *Forced updates*
      - *No selective updates*
      - *More efficient distribution*

Harden Endpoints (2 of 6)

- Operating Systems
  - Securing an OS involves proper security configurations and using confinement tools
  - A typical OS security configuration should include the following:
    - *Disabling unnecessary ports and services*
    - *Disabling default accounts/passwords*
    - *Employing least functionality*
  - In Microsoft Windows, a *security template* is a collection of security configuration settings that can be used to deploy security settings to multiple computers
  - Windows 10 Tamper Protection security feature prevents Windows security settings from being changed or disabled by a threat actor who modifies the registry
    - A Group Policy setting can also *prevent access to registry editing tools* (see Figure 4-7)

Harden Endpoints (3 of 6)



Source: Used with permissions from Microsoft

Figure 4-7 Prevent access to registry editing tools

Figure 4-7 Prevent access to registry editing tools

Harden Endpoints (4 of 6)

- Operating Systems (continued)
  - Confinement Tools – several tools can be used to restrict malware:
    - *Application whitelisting/blacklisting*
    - *Sandbox*
    - *Quarantine*

Harden Endpoints (5 of 6)

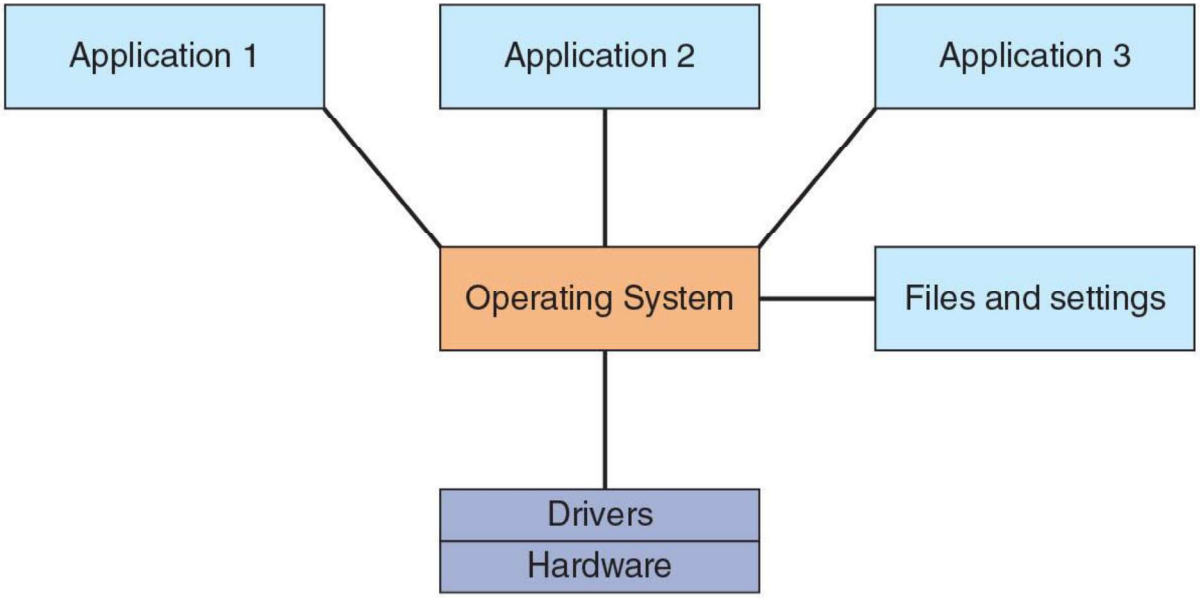


Figure 4-8 Applications interacting with an OS

Figure 4-8 Applications interacting with an OS

Harden Endpoints (6 of 6)

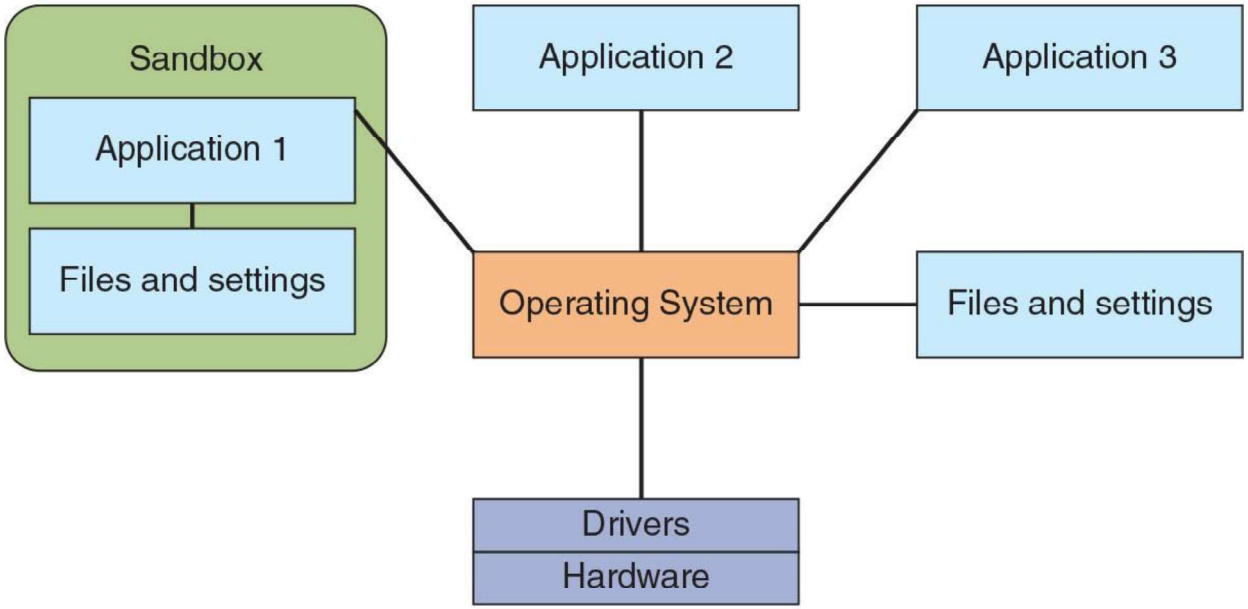


Figure 4-9 Using a sandbox

Figure 4-9 Using a sandbox

Knowledge Check Activity 2

Which of the following is NOT a tool that can be used to confine or restrict malware?

a. Whitelisting
b. Quarantine
c. Sandbox
d. Legacy boot

Knowledge Check Activity 2: Answer

Which of the following is NOT a tool that can be used to confine or restrict malware?

Answer: Legacy boot

A computer configured for legacy boot uses the BIOS to boot the system, which has little or no security features.

Creating and Deploying SecDevOps (1 of 2)

- An unsecure application can open the door for attackers to exploit the application, the data that it uses, and even the underlying OS
- A **directory traversal attack** takes advantage of vulnerability in the web application program or the web server software so that a user can move from the root directory to other restricted directories
- The ability to move could allow an unauthorized users to view confidential files or enter commands to execute on a server known as *command injection*
- Other dangerous weaknesses in an application can create vulnerabilities in computer memory or buffer areas that can be easily exploited
  - **Poor memory management vulnerabilities** result in attacks such as buffer overflow, integer overflow, pointer/object deference, and DLL injection attacks

Creating and Deploying SecDevOps (2 of 2)

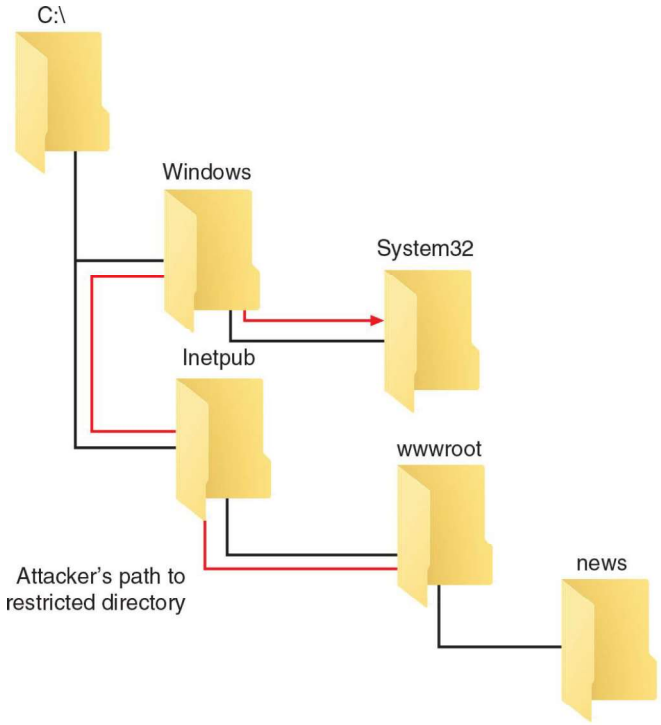


Figure 4-10 Directory traversal attack

Figure 4-10 Directory traversal attack

Application Development Concepts (1 of 3)

- The two levels of application development concepts include general concepts that apply to all application development and those that apply to a rigorous security-based approach
- General Concepts
  - Developing an application requires completing the following stages:
    - *Development*
    - *Testing*
    - *Staging*
    - *Production*
  - **Software diversity** is a software development technique in which two or more functionally identical variants of a program are developed from the same specification but by different programmers or programming teams
    - The intent is to provide error detection, increased reliability, and additional documentation

Application Development Concepts (2 of 3)

- General Concepts (continued)
  - **Provisioning** is the enterprise-wide configuration, deployment, and management of multiple types of IT system resources
  - **Deprovisioning** in application development is removing a resource that is no longer needed
  - **Integrity measurement** is an "attestation mechanism" designed to be able to convince a remote party that an application is running only a set of known and approved executables
- SecDevOps
  - An *application development lifecycle model* is a conceptual model that describes the stages involved in creating an application and are usually one of the following two:
    - *Waterfall model* – uses a sequential design process
    - *Agile model* – takes an incremental approach

Application Development Concepts (3 of 3)

- SecDevOps (continued)
  - *SecDevOps* is the process of integrating secure development best practices and methodologies into application software development and deployment processes using the agile model
  - SecDevOps applies **automated courses of action** to develop code as quickly and securely as possible
  - This automation enables:
    - **Continuous monitoring**
    - **Continuous validation**
    - **Continuous integration**
    - **Continuous delivery**
    - **Continuous deployment**

Secure Coding Techniques

- Several coding techniques should be used to create secure applications and limit data exposure or disclosing sensitive data to attackers
- These techniques include:
  - Determining how encryption will be implemented
  - Ensuring that memory management is handled correctly so as not to introduce memory vulnerabilities

Code Testing (1 of 3)

- Testing is one of the most important steps in SecDevOps
- Testing should be performed during the implementation and verification phases of a software development process
- Testing involves static code analysis and dynamic code analysis
- Static Code Analysis
  - **Static code analysis** are tests ran before the source code is even compiled and may be accompanied by manual peer reviews
- Dynamic Code Analysis
  - Security testing performed after the source code is compiled is called **dynamic code analysis**
  - **Fuzzing** is used by dynamic code analysis tools and provides random input to a program in an attempt to trigger exceptions

Code Testing (2 of 3)

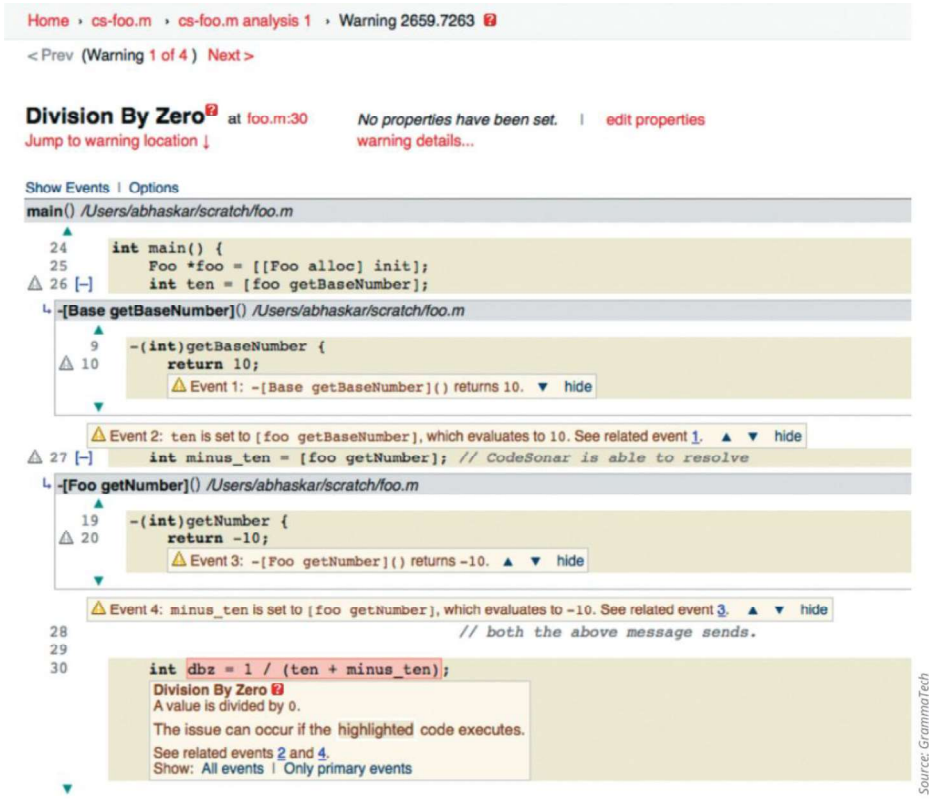


Figure 4-11 Automated static code analysis tool

Figure 4-11 Automated static code analysis tool

Code Testing (3 of 3)

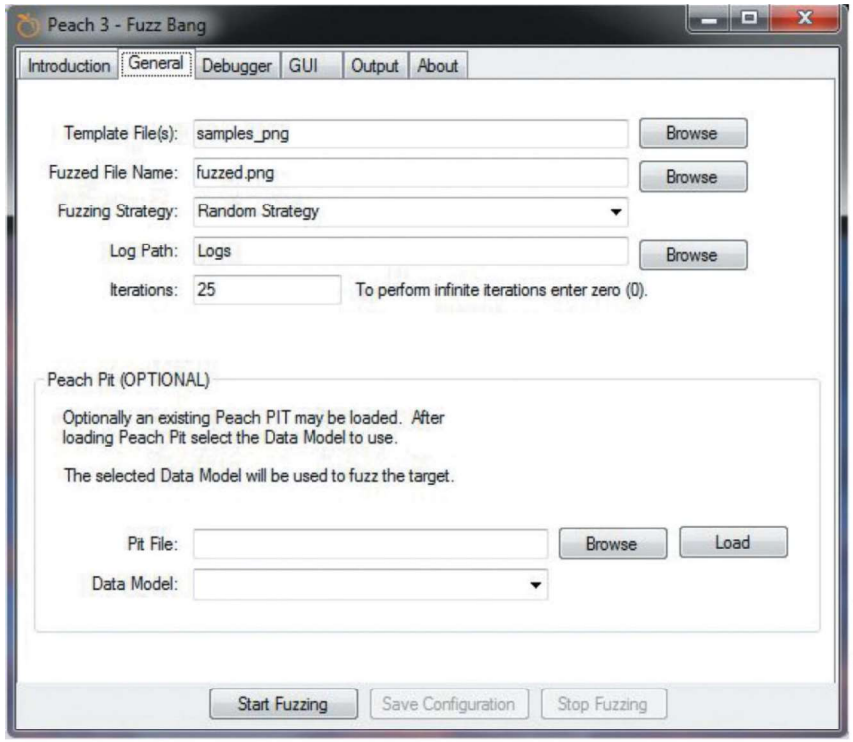


Figure 4-12 Fuzzer input generator

Figure 4-12 Fuzzer input generator

Knowledge Check Activity 3

Which of the following best describes static code analysis?

a. Testing uses a suite of pre-built attacks.
b. Tests are run before the source code is compiled.
c. Random input is used to trigger exceptions.
d. Used after all components are integrated.

Knowledge Check Activity 3: Answer

Which of the following best describes static code analysis?

Answer: b. Tests are run before the source code is compiled.

Static code analysis is performed before the source code is compiled and may be accompanied by manual peer reviews. Dynamic code analysis is performed on a running system.

Self-Assessment

1. Consider the importance of the system boot process in the security of endpoint computers. What are some of the dangers of using legacy boot procedures? Why are computers that use legacy boot firmware more susceptible to attacks?

Summary (1 of 2)

- Organizations are pooling their experiences and knowledge gained about the latest attacks with the broader security community because sharing this type of information has become an important aid to help other organizations shore up their defenses
- Several sources of threat intelligence are useful: a vulnerability database, a cybersecurity threat map, and file and code repositories are examples
- One of the steps that is often overlooked in securing endpoint computers is to confirm that the computer has started without any malicious activity taking place
- Antivirus (AV) software can examine a computer for any file-based virus infections and monitor computer activity and scan new documents that might contain a virus
- Web browsers have a degree of security that can protect endpoint computers
- A host intrusion detection system (HIDS) is a software-based application that runs on an endpoint computer and can detect that an attack has occurred

Summary (2 of 2)

- One of the most important steps in securing an endpoint computer is to promptly install patches
- An unsecure application can open the door for attackers to exploit the application, the data that it uses, and even the underlying OS
- Testing is one of the most important steps in SecDevOps