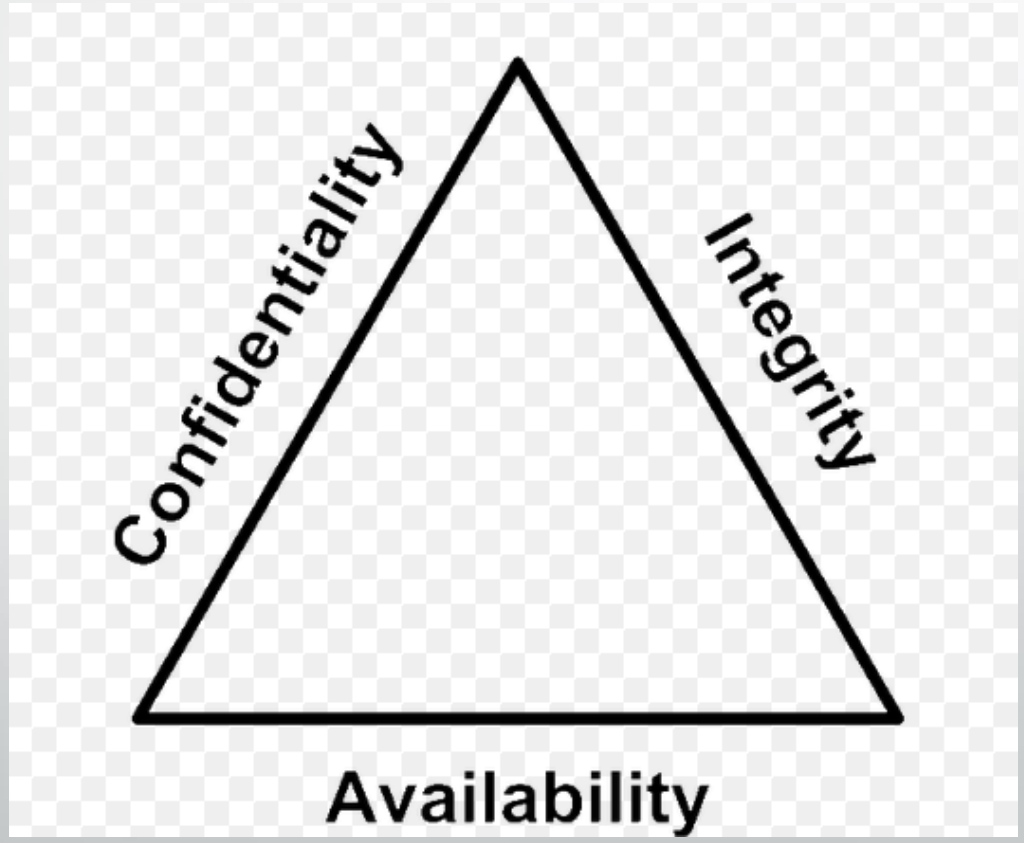
Control Systems Network Penetration Testing

Capacity Building for Control System Security Collaborative Project


KAL
Q:
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE... BACK HERE
CYBER SECURITY

CIA Traingle (The Holy Trinity of IT)



Phases of an Attack

- In general, there are five phases that make up an attack:
  - **Reconnaissance**- attacker gathers as much information as possible about the target
    - Active and Passive
  - **Scanning**-Attacker uses the details gathered during reconnaissance to identify specific vulnerabilities
  - **Gaining Access**- Where most of the damage is usually done
  - **Maintaining Access**-Install a backdoor or a Trojan to gain repeat access
  - **Covering Tracks**-Attempt to erase all evidence of their actions

Security Concerns

- Theft
  - Including theft of data, theft of physical property, and identity theft
- Fraud/Forgery
  - Deception made for personal gain, often monetary
- Unauthorized Information Access
  - Intercepting and changing computer resources, storing and retrieving data, or trespassing without permission
- Interception or Modification of Data
  - Can cause malicious threats, loss of important data, and network failures

Preventative Steps

- **Authentication**
  - Process of verifying the identity of an individual
- **Authorization**
  - Process that permits a person, program, or device to have access to data, functionality, or a service
- **Confidentiality**
  - Requirement that particular information be restricted to the appropriate personnel
- **Data integrity**
  - Guarantees that data is complete, correct, and not modified
- **Availability**
  - Legitimate users can access their data at any given time
- **Nonrepudiation**
  - Ensures that the appropriate party receives a transferred message

Needs Assessment Questions

- Consider the following questions:
  - How easy would it be for someone to steal corporate information?
  - How easy would it be for someone to crash the network?
  - What vulnerabilities exist in regard to the Internet connection?
  - What is the likelihood that the system will be hacked?
  - What damage could result from an attack?
  - What could an employee do with unauthorized access privileges?

Needs Assessment Questions (cont'd.)

- Consider the following questions (cont'd.):
  - How easy is it to circumvent the network's access controls?
  - How easy would it be for an insider to compromise the system?
  - How much should be spent on the IT security program?
  - Who is responsible for protecting IT and informational resources?

Penetration Testing Execution

1. **Pre-engagement Interactions**- Define the scope of the test, which includes network, Web, wireless, physical, and social engineering
2. **Information Gathering**- Obtaining both automated and manual information on the systems being tested
3. **Threat Modeling**- Identify and categorize primary and secondary assets and Identify and categorize threats and threat communities
4. **Vulnerability Testing**- Discovering flaws in systems and applications which can be leveraged by an attacker
5. **Exploitation**- Focuses solely on establishing access to a system or resource by bypassing security restrictions
6. **Post Exploitation**- Determine the value of the machine compromised and to maintain control of the machine for later use- The value of the machine is determined by the sensitivity of the data stored on it
7. **Reporting**- This section will communicate to the reader the specific goals of the Penetration Test and the high level findings of the testing exercise

For more information, consult http://www.pentest-standard.org/index.php/Main_Page

Tools Used in Penetration Testing

Questions???