CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA

Copyright © 2022 CompTIA, Inc. All Rights Reserved. | CompTIA.org

CompTIA PenTest+ Exam PT0-002

Lesson 2

Defining the Rules of Engagement

CompTIA

Copyright © 2022 CompTIA, Inc. All Rights Reserved. | CompTIA.org

Objectives

- Compare and contrast governance, risk, and compliance reports
- Explain the importance of scoping and organizational/customer requirements
- Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.

Lesson 2

Topic 2A

Assess Environmental Considerations

CompTIA

Copyright © 2022 CompTIA, Inc. All Rights Reserved. | CompTIA.org

Defining the Project Scope

- All stakeholders will define specifically what is to be *included or excluded* during the testing process.
  - This is a more cost-effective approach, as the team will have a clear idea as to when the testing is complete.
- Determine what specific environments are to be considered.
  - Once the targets are identified, this will determine the scope and type of attacks the team will attempt.
  - Can include on-site networks, specific applications, or resources in the cloud.

Gather the Requirements

- Assess the LAN and the WLAN
- Evaluate web and/or mobile applications.
  - Define guidelines, such as number of pages that require user interaction.
  - The team should obtain a variety of roles and permissions to be tested
- Test cloud resources (SaaS, IaaS and PaaS)
  - Prior to testing, obtain the proper authorization from the provider
  - Determine what type of testing will be allowed.

Define the In-Scope Assets

- The stakeholders will need to be specific as to what assets will be included in the scope. Some example include:
  - Internet Protocol (IP) addresses
  - Domain and/or subdomains
  - Application programming interfaces (APIs)
  - Users – for social engineering attacks
  - Service Set Identifiers (SSID)

Determine Locations and Hosting Methods

- Identify the physical locations that are in-scope, and whether the target is on-site or off-site.
- Other considerations:
  - Whether the team will test external or internal assets
  - Define how assets are hosted: First-Party and/or Third-Party

Restrictions that will influence testing

- Country, state, and local laws can impact testing.
  - Can restrict the technology, tools and methods used during PenTesting
- In the US, export controls regulate the shipment or transfer of certain items outside of the country.
  - Other nations might have restrictions as well
- There may also be specific language prohibiting, creating, or distributing computer security software

Review Activity: Assess Environmental Considerations

- Outline the importance of defining the Project Scope
- Discuss activities related to gathering the requirements
- Stress the importance of determining physical locations, and whether testing is on-site or off-site.
- Explain how certain restrictions can influence PenTesting

Lesson 2

Topic 2B

Outline the Rules of Engagement

CompTIA

Copyright © 2022 CompTIA, Inc. All Rights Reserved. | CompTIA.org

Providing the Details

- Stakeholders should spell out all requirements and agree on the terms before testing begins.
  - Keep the lines of communication open and clarify any issues.
- The team will need to a establish a timeline
  - Outline specific parameters along with an estimation of time needed to complete all testing that is included in the contract.
- Use good time management skills
  - Avoid distractions
  - Adhere to the timeline

Define the Restrictions

- Once the main objectives are outlined, the team will want to review other variables as they relate to testing.
- Outline any restrictions that can impact testing, that include:
  - Determine what tests are allowed
  - Adhere to the scope
  - Recognize other restrictions
  - Limit invasiveness based on scope
  - Limit the use of tools to a particular engagement

Choose the Type and Strategy

- Gather information from the stakeholders to learn more about their needs and the objectives of the PenTest.
- Common types of assessments include:
  - Compliance based
  - Red team/blue team-based
  - Goals-based/objectives-based
- Select a strategy: i.e., unknown, partially known, or known environment

Validate the Scope of the Engagement

- Reconfirm details such as whether they have appropriate system backups and recovery procedures in case recovery is needed.
- Question the client on any vague areas, so there is no confusion.
- Some elements to review can include:
  - Scope and in-scope assets
  - Any restrictions or applicable laws
  - Third-party providers, services, or off-site locations
  - Communication and updates

Review Activity: Outline the Rules of Engagement

- Outline topics to cover when defining the restrictions
- Review options when deciding on the type of assessment and selecting the strategy
- Describe ways to validate the scope of the engagement

Lesson 2

Topic 2C

Prepare Legal Documents

CompTIA

Copyright © 2022 CompTIA, Inc. All Rights Reserved. | CompTIA.org

Ensuring Confidentiality

- Avoid creating a liability, by ensuring everyone takes the necessary precautions to protect the confidentiality of the data
- Specific laws may apply while testing. Examples include:
  - **Gramm-Leach-Bliley Act (GLBA)**
  - **Driver's Privacy Protection Act**
  - **Health Insurance Portability and Accountability Act (HIPAA)**
- Because of confidentiality requirements, each team member will most likely have to sign a Nondisclosure Agreement.

Giving Permission to Attack

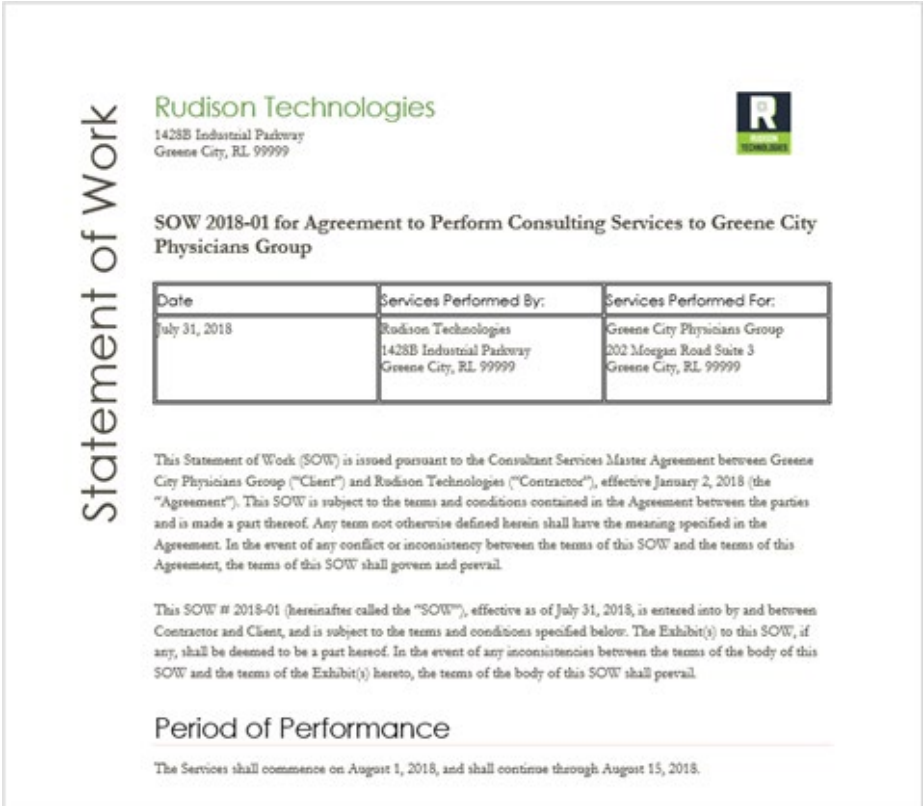
- PenTesting simulates the approach of an unauthorized hacker attacking a system in order to assess the security of an organization.
- After scoping the project, and gathering all requirements, the team will need to obtain formal permission to attack.
- Most legal documents include the following :
  - Names of the entity or Individuals that are authorized to perform the PenTest
  - What specific networks, hosts, and applications are to be included
  - The validity period of the authorization and proper data handling techniques

Master Service Agreement (MSA)

- A contract that governs all future transactions or future agreements between the PenTesting team and the client
- Can be used to cover recurring costs and any unforeseen additional charges without the need for an additional contract.
- Some of the elements should include details on the following:
  - Project scope and a definition of the work to be completed
  - Requirements for any permits, licensing, or certifications
  - Insurances such as general and liability.

Outline the Statement of Work

- Defines the expectations for a specific business arrangement.
- It typically includes:
  - List of deliverables
  - Responsibilities of both parties
  - Payment milestones
  - Schedules, and other terms.



Statement of Work

Rudison Technologies
1428B Industrial Parkway
Greene City, RL 99999

SOW 2018-01 for Agreement to Perform Consulting Services to Greene City Physicians Group

Date	Services Performed By:	Services Performed For:
July 31, 2018	Rudison Technologies 1428B Industrial Parkway Greene City, RL 99999	Greene City Physicians Group 202 Morgan Road Suite 3 Greene City, RL 99999

This Statement of Work (SOW) is issued pursuant to the Consultant Services Master Agreement between Greene City Physicians Group ("Client") and Rudison Technologies ("Contractor"), effective January 2, 2018 (the "Agreement"). This SOW is subject to the terms and conditions contained in the Agreement between the parties and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the Agreement. In the event of any conflict or inconsistency between the terms of this SOW and the terms of this Agreement, the terms of this SOW shall govern and prevail.

This SOW # 2018-01 (hereinafter called the "SOW"), effective as of July 31, 2018, is entered into by and between Contractor and Client, and is subject to the terms and conditions specified below. The Exhibit(s) to this SOW, if any, shall be deemed to be a part hereof. In the event of any inconsistencies between the terms of the body of this SOW and the terms of the Exhibit(s) hereto, the terms of the body of this SOW shall prevail.

Period of Performance

The Services shall commence on August 1, 2018, and shall continue through August 15, 2018.

Prepare the Service-Level Agreement

- Outlines the level of service expected
  - Defines the metrics which that service is measured, and any remedies or penalties should the agreed-on service levels not be achieved.
  - May include terms for security access controls and risk assessments, along with processing requirements for confidential and private data.
- Make sure to identify the proper signing authority
- All parties should arrange for legal review of the document.
- Once done, it’s time to begin the PenTest.

Review Activity: Prepare Legal Documents

- Review laws that require the confidentiality of data while testing
- List some of the information included in the documentation that gives permission to attack
- Discuss the importance of the Master Service Agreement
- Describe what's included in a Statement of Work
- Outline the components of a Service-Level Agreement

Lesson 2

Summary

Copyright © 2022 CompTIA, Inc. All Rights Reserved. | CompTIA.org