CompTIA

The Official CompTIA

PenTest+ Study Guide

Exam PT0-001

Official CompTIA Content Series for CompTIA Performance Certifications

The Official CompTIA® PenTest+® Study Guide (Exam PT0-001)

The Official CompTIA® PenTest+® Study Guide (Exam PT0-001)

Part Number: 093051
Course Edition: 1.0

Acknowledgements

Chrys Thorsen, Author	Thomas Reilly, Vice President Learning
Jason Nufryk, Author	Katie Hoenicke, Director of Product Management
Pamela J. Taylor, Author	James Chesterfield, Manager, Learning Content and Design
Brian Sullivan, Media Designer	Becky Mann, Senior Manager, Product Development
Peter Bauer, Content Editor	James Pengelly, Courseware Manager
	Rob Winchester, Senior Manager, Technical Operations

Notices

DISCLAIMER

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

TRADEMARK NOTICES

CompTIA®, PenTest+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

COPYRIGHT NOTICE

The Official CompTIA® PenTest+® Study Guide (Exam PT0-001)

About This Guide

Security remains one of the hottest topics in IT and other industries. It seems that each week brings news of some new breach of privacy or security. As organizations scramble to protect themselves and their customers, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organizations seeking protection, and ever more lucrative for those who possess these skills. In this guide, you will be introduced to some general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

This guide can also assist you if you are pursuing the CompTIA PenTest+ certification, as tested in exam PT0-001. The guide is designed to provide content and activities that correlate to the exam objectives, and therefore can be a resource as you prepare for the examination.

Guide Description

Target Student

This guide is designed for IT professionals who want to develop penetration testing skills to enable them to identify information-system vulnerabilities and effective remediation techniques for those vulnerabilities. Target students who also need to offer practical recommendations for action to properly protect information systems and their contents will derive those skills from this guide.

This guide is also designed for individuals who are preparing to take the CompTIA PenTest + certification exam PT0-001, or who plan to use PenTest+ as the foundation for more advanced security certifications or career roles. Individuals seeking this certification should have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management.

Guide Prerequisites

To be fit for this advanced guide, you should have:

- Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.
- Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.

You can obtain this level of skills and knowledge by training for *CompTIA® Security+® (Exam SY0-501)* or by demonstrating this level of knowledge by passing the exam.

Guide Objectives

After you complete this guide, you will be able to plan, conduct, analyze, and report on penetration tests.

You will:

- Plan and scope penetration tests.
- Conduct passive reconnaissance.
- Perform non-technical tests to gather information.
- Conduct active reconnaissance.
- Analyze vulnerabilities.
- Penetrate networks.
- Exploit host-based vulnerabilities.
- Test applications.
- Complete post-exploit tasks.
- Analyze and report pen test results.

How to Use This Book

As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of information designed to enable you to solidify your understanding of the informational material presented in the guide. Information is also provided for reference and reflection to facilitate understanding and practice.

At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the guide. You will also find an index to assist in locating information within the instructional components of the book.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Guide Icons

Watch throughout the material for the following visual cues.

Icon	*Description*
	A **Note** provides additional information, guidance, or hints about a topic or task.
	A **Caution** note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

1 Planning and Scoping Penetration Tests

Lesson Time: 3 hours

Lesson Introduction

In today's computing environment, security exploits and issues are more prevalent than ever. Most organizations have developed strong security postures to protect their assets. In many cases, these security postures include the practice of testing the organization's information systems to determine how resistant they are to unauthorized access and usage. Providing a clear plan and specifying the scope of these tests is essential for both the organization and the individuals performing the testing, as these actions ensure that the testing process is clearly bounded and understood by all stakeholders.

Lesson Objectives

In this lesson, you will:

- Explain common concepts related to penetration testing.
- Plan a pen test engagement.
- Scope and negotiate a pen test engagement.
- Prepare for a pen test engagement.

TOPIC A

Introduction to Penetration Testing Concepts

Before you begin to plan and scope a penetration test, it is essential that you have a grasp of certain basic concepts surrounding the practice of penetration testing. This topic introduces those concepts, along with generally accepted processes and toolsets, to provide a core base of information upon which you can build your penetration testing skills and experience.

Penetration Testing

Often, the terms "vulnerability assessment" and "penetration testing" are used interchangeably, although they are not the same. The key difference between the two is validation. ***Vulnerability assessment*** is the practice of evaluating a computer system, a network, or an application to identify potential weaknesses. It is typically performed using an automated tool, which produces a list of vulnerabilities based on known signatures. Many of these can be false positives or not actually exploitable. ***Penetration testing***, or ***pen testing***, goes beyond simple vulnerability testing. It seeks to exploit vulnerabilities and produce evidence of success as part of its report. It often includes social engineering and testing of physical controls, as well as testing technical weaknesses.

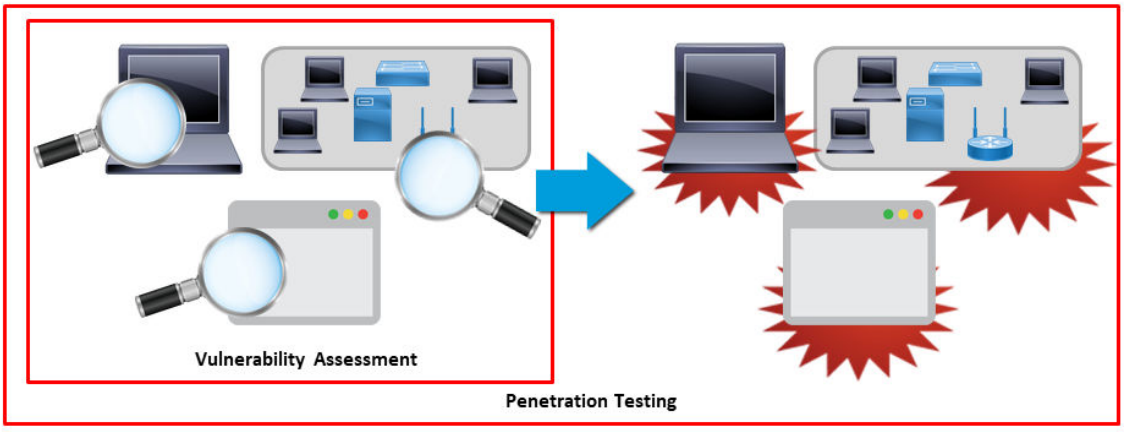


Figure 1-1: Penetration testing encompasses vulnerability assessment.

Benefits of Pen Testing

The benefits of conducting pen testing are numerous, and they include:

- Testing cyber-defense capabilities.
- Revealing vulnerabilities in computers, applications, and networks.
- Finding security holes and plugging them before an attacker can take advantage of them.
- Supporting effective risk management by showing the real risk involved with the vulnerabilities encountered.
- Enhancing QA while ensuring business continuity.
- Protecting clients, partners, and others, in addition to the organization's reputation.
- Ensuring compliance with applicable regulations and certifications.
- Maintaining trust.
- Identifying return on investment (ROI) for existing security measures and validating the need for additional controls.

Pen Testing Standards and Frameworks

Several sets of standards and frameworks have been developed to provide a common base of understanding and expectation for pen tests. Some of these are described in the following table.

Standard or Framework	*Description*
CHECK framework	Developed by the Communications-Electronic Security Group (now the National Cyber Security Centre), which is part of the UK Government Communications Headquarters. This scheme ensures that government agencies and public entities can contract with certified companies to identify vulnerabilities in their confidentiality, integrity, and availability (CIA) by testing their networks and other systems. For more information, refer to **www.ncsc.gov.uk/articles/check-fundamental-principles**.
The Open Web Application Security Project (OWASP) Testing Framework	Developed by a multinational organization that collects and shares security practices with software developers, this framework provides pen testing and other testing techniques for each part of the software development life cycle. For more information, refer to **www.owasp.org**.
Open Source Security Testing Methodology Manual (OSSTMM)	Developed by the Institute for Security and Open Methodologies (ISECOM), this document is a peer-reviewed guide to security testing and analysis that enables you to tighten up operational security. For more information, refer to **http://www.isecom.org/research/osstmm.html**.
Penetration Testing Execution Standard (PTES)	Developed by security service practitioners to provide business professionals and security service providers a basic lexicon and guidelines for performing pen tests. The PTES is the general standard, while detailed information is provided in the PTES Technical Guide. For more information, refer to **www.pentest-standard.org**.
NIST SP 800-115	Developed by the US National Institute of Standards and Technology (NIST), the **Technical Guide to Information Security Testing and Assessment** provides practical recommendations for designing, implementing, and maintaining pen test processes and procedures.

Processes Commonly Used for Pen Testing

Along with standards and frameworks, there are several processes that can be used for pen testing. These processes are similar in structure, for the most part, and often reflect the processes that are acknowledged to produce a successful cyber attack. In this example, the stages of the cyber attack process are also the middle stages of the pen test process.

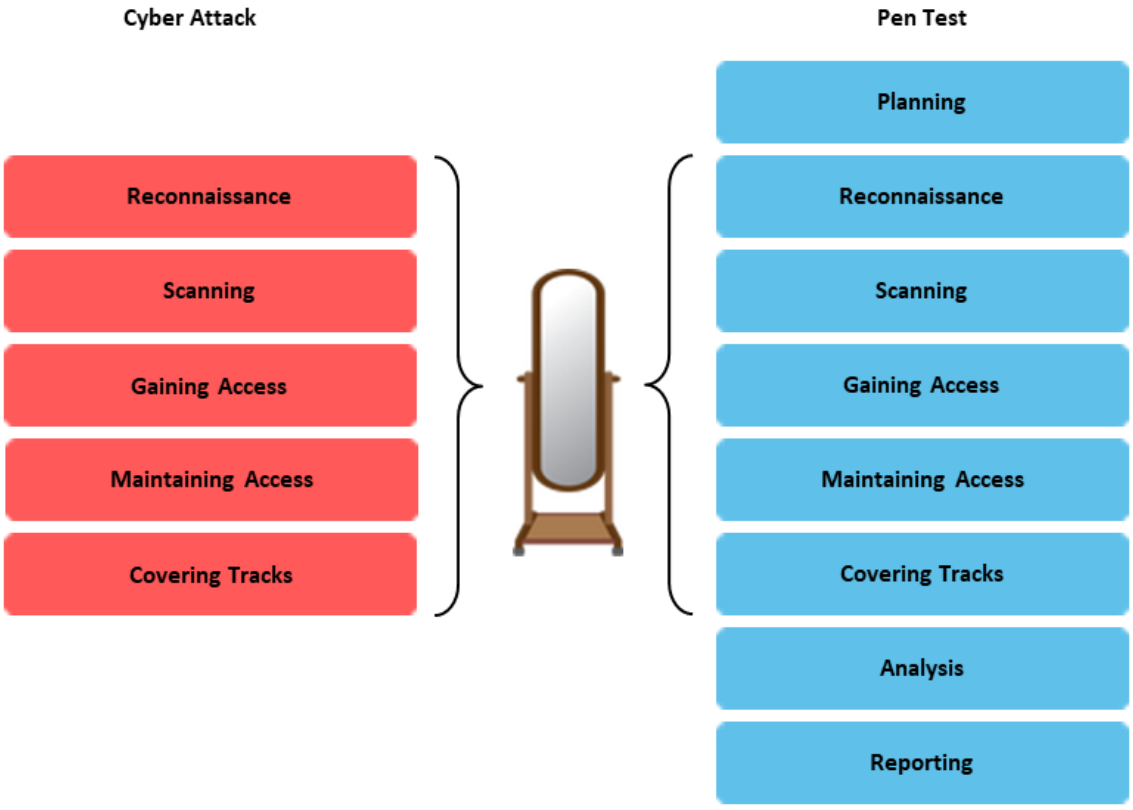


Figure 1-2: Comparing a cyber attack process with a pen test process.

The additional stages in this pen test provide the scaffolding that ensures that the intended tests are conducted and that the results are communicated to decision-makers for review and further action. In some instances where automated pen testing is used, the analysis and reporting phases might be replaced with a phase to implement configuration settings.

The phases of the pen test process are described in the following table.

Process Phase	*Description*
Planning	Most recognized pen test processes include a planning phase. Depending on the authority that promulgates the process, this phase might also include identifying the scope of the engagement, documenting logistical details, and other preliminary activities that need to occur before the commencement of the pen test.
Reconnaissance	In the reconnaissance phase, the tester gathers information about the target organization and systems prior to the start of the pen test. This can include both passive information gathering, such as collecting publicly available information about the organization, and deliberate acts, such as scanning ports to detect possible vulnerabilities.
Scanning	The scanning phase is generally a bit more in depth than the reconnaissance phase. This is where vulnerability assessment begins. Static and dynamic scanning tools evaluate how a target responds to intrusions.
Gaining access	This phase is when the actual exploit begins, by applying the information gained by reconnaissance and scanning to begin to attack target systems.

Process Phase	*Description*
Maintaining access	In this phase, the pen testers install mechanisms allowing them to continue to access the system. This phase is also where pen testers reach deeper into the network by accessing other network systems.
Covering tracks	This phase concentrates on obliterating evidence that proves an exploit occurred. It generally consists of two facets: avoiding real-time incident response efforts and avoiding post-exploit forensic liability.
Analysis	In this phase, the pen tester gathers all the information collected, identifies root causes for any vulnerabilities detected, and develops recommendations for mitigation.
Reporting	The reporting phase is where the information from testing and analysis are officially communicated to the stakeholders. Although reporting requirements can vary due to customer needs or statutory regulations, most pen test reports list: • Vulnerabilities detected. • Vulnerabilities exploited. • Sensitive data accessed. • How long the pen tester had access. • Suggestions and techniques to counteract vulnerabilities.

Variations on the Process

As with practically everything else in your IT infrastructure, the specific needs of an organization should guide the need for additional or different process stages for pen testing. For instance, here are several pen test processes from different entities.

Organization or Publication	*Pen Test Process*
CompTIA (derived from PenTest+ exam objectives)	**1.** Planning and scoping. **2.** Information gathering and vulnerability identification. **3.** Exploit vulnerabilities. **4.** Perform post-exploit techniques. **5.** Analyze tool output, data, etc. **6.** Reporting.
PTES (derived from the main sections of the PTES standard)	**1.** Pre-engagement interactions. **2.** Intelligence gathering. **3.** Threat modeling. **4.** Vulnerability analysis. **5.** Exploitation. **6.** Post exploitation. **7.** Reporting.
NIST (derived from NIST SP800-115)	**1.** Planning. **2.** Execution. **3.** Post-Execution.

Organization or Publication	Pen Test Process
SANS Institute (from the paper "Conducting a Penetration Test on an Organization")	1. Planning and preparation. 2. Information gathering and analysis. 3. Vulnerability detection. 4. Penetration attempt. 5. Analysis and reporting. 6. Cleaning up.

Tools Commonly Used in Pen Testing

Thousands of tools exist that can help you conduct pen tests. Some tools are more comprehensive, while others are specialized to assist in particular use cases. The following tables briefly describe some of the tools that you might find effective while conducting pen tests.

Scanning Tool	Description
Nmap	An open source network scanner used for network discovery and auditing. It can discover hosts, scan ports, enumerate services, fingerprint operating systems, and run script-based vulnerability tests.
Nikto	An open source web server scanner that searches for potentially harmful files, checks for outdated web server software, and looks for problems that occur with some web server software versions. It is included with Kali Linux.
OpenVAS	(Open Vulnerability Assessment System) An open source software framework for vulnerability scanning and management.
SQLmap	An open source database scanner that searches for and exploits SQL injection flaws. It is included with Kali Linux.
Nessus	A proprietary vulnerability scanner developed by Tenable Network Security. Initially open source, it scans for vulnerabilities, misconfigurations, default passwords, and susceptibility to denial of service (DoS) attacks. It can also be used for preparation for PCI DSS audits.

Credential Testing Tool	Description
Hashcat	A free password recovery tool that is included with Kali Linux and is available for Linux, OS X, and Windows. It includes a very wide range of hashing algorithms and password cracking methods. Hashcat purports itself to be the fastest recovery tool available.
Medusa	A command-line-based free password cracking tool that is often used in brute force password attacks on remote authentication servers. It purports itself to specialize in parallel attacks, with the ability to locally test 2,000 passwords per minute.
THC-Hydra	A free network login password cracking tool that is included with Kali Linux. It supports a number of authentication protocols.
CeWL	A Ruby app that crawls websites to generate word lists that can be used with password crackers such as John the Ripper. It is included with Kali Linux.

Credential Testing Tool	*Description*
John the Ripper	A free password recovery tool available for Linux, 11 versions of Unix, DOS, Win32, BeOS, and OpenVMS. It is included with Kali Linux.
Cain and Abel	A free password recovery tool available for Windows that is sometimes classified as malware by some antivirus software.
Mimikatz	An open source tool that enables you to view credential information stored on Microsoft Windows computers. It is also included with Kali Linux.
Patator	A brute force password cracking tool included with Kali Linux.
Dirbuster	A brute force tool included with Kali Linux that exposes directories and file names on web and application servers.
W3AF	(Web Application Attack and Audit Framework) A Python tool included in Kali Linux that tries to identify and exploit any web app vulnerabilities.

Debugging Tool	*Description*
OLLYDBG	A reverse-engineering tool included with Kali Linux that analyzes binary code found in 32-bit Windows applications.
Immunity debugger	A reverse-engineering tool that includes both command-line and graphical user interfaces and that can load and modify Python scripts during runtime.
GDB	(GNU Project Debugger) An open source reverse-engineering tool that works on most Unix and Windows versions, along with macOS.
WinDBG	(Windows Debugger) A free debugging tool created and distributed by Microsoft for Windows operating systems.
IDA	(Interactive Disassembler) A reverse-engineering tool that generates source code from machine code for Windows, Mac OS X, and Linux applications.

Software Assurance Tool	*Description*
Findbugs and findsecbugs	FindBugs is an open source static code analyzer or ***static application security testing (SAST)*** tool that detects possible bugs in Java programs. FindSecurityBugs is an open source plugin that detects security issues in Java web applications.
Peach	Peach Tech offers several ***dynamic application security testing (DAST)*** products for pen testing, including Peach API Security, which helps secure web APIs against the OWASP Top 10, and Peach Fuzzer, an automated security testing platform for prevention of zero-day attacks. Within Peach Fuzzer, modular test definitions called Peach Pits enable you to fully customize exploits against test targets.
AFL	(american fuzzy lop) An open source DAST tool that feeds input to a program to test for bugs and possible security vulnerabilities.
SonarQube	An open source SAST platform that continuously inspects code quality to help discover bugs and security vulnerabilities.

Software Assurance Tool	Description
YASCA	(yet another source code analyzer) An open source SAST program that inspects source code for security vulnerabilities, code quality, and performance.

OSINT Tool	Description
Whois	A protocol that queries databases that store registered users or assignees of an Internet resource, such as a domain name.
Nslookup	A Windows command-line utility that queries DNS and displays domain names or IP address mappings, depending on the options used.
FOCA	(Fingerprinting and Organization with Collected Archives) A network infrastructure mapping tool that analyzes metadata from many file types to enumerate users, folders, software and OS information, and other information.
theHarvester	A tool included with Kali Linux that gathers information such as email addresses, subdomains, host names, open ports, and banners from publicly available sources.
Shodan	A search engine that returns information about the types of devices connected to the Internet by inspecting the metadata included in service banners.
Maltego	A proprietary software tool that assists with gathering open source intelligence (OSINT) and with forensics by analyzing relationships between people, groups, websites, domains, networks, and applications. A community version named Maltego Teeth is included with Kali Linux.
Recon-ng	A web reconnaissance tool that is written in Python and is included with Kali Linux. It uses over 80 "modules" to automate OSINT. Some of its features include: search for files, discover hosts/contacts/email addresses, snoop DNS caches, look for VPNs, look up password hashes, and perform geolocation.
Censys	A search engine that returns information about the types of devices connected to the Internet.

Wireless Tool	Description
Aircrack-ng	A suite of wireless tools, including airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng. Included with Kali Linux, the suite can sniff and attack wireless connections, and crack WEP and WPA/WPA2-PSK keys.
Kismet	An 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system that is included with Kali Linux. It can be used to monitor wireless activity, identify device types, and capture raw packets for later password cracking.
WiFite	A wireless auditing tool included with Kali Linux that can attack multiple WEP, WPA, and WPS encrypted networks in a row.
WiFi-Pumpkin	A rogue wireless access point and man-in-the-middle tool used to snoop traffic and harvest credentials.

Web Proxy Tool	Description
OWASP ZAP	(Open Web Application Security Project Zed Attack Proxy) An open source web application security scanner.
Burp Suite	An integrated platform included with Kali Linux for testing the security of web applications. Acting as a local proxy, it allows the attacker to capture, analyze, and manipulate HTTP traffic.

Social Engineering Tool	Description
SET	(Social Engineer Toolkit) An open source pen testing framework included with Kali Linux that supports the use of social engineering to penetrate a network or system.
BeEF	(Browser Exploitation Framework) A pen testing tool included with Kali Linux that focuses on web browsers and that can be used for XSS and injection attacks against a website.

Remote Access Tool	Description
SSH	(Secure Shell) A program that enables a user or an application to log on to another device over an encrypted network connection, run commands in a remote machine, and transfer files from one machine to the other.
Ncat	An open source command-line tool for reading, writing, redirecting, and encrypting data across a network. Ncat was developed as an improved version of Netcat.
Netcat	An open source networking utility for debugging and investigating the network, and that can be used for creating TCP/UDP connections and investigating them.
Proxychains	Included with Kali Linux, as well as any other version of Linux, a command-line tool that enables pen testers to mask their identity and/or source IP address by sending messages through intermediary or proxy servers.

Networking Tool	Description
Wireshark	An open source network protocol analyzer that is included with Kali Linux. Can be used to sniff many traffic types, re-create entire TCP sessions, and capture copies of files transmitted on the network.
hping	A free packet generator and analyzer for TCP/IP networks. Often used for firewall testing and advanced network testing, hping3 is included with Kali Linux.

Mobile Tools	Description
Drozer	A security testing framework for Android apps and devices.
APKX	(Android Package Kit) A Python wrapper for dex converters and Java decompilers that is included in the OWASP Mobile Testing Guide.
APK Studio	A cross-platform IDE for reverse engineering Android applications.

Miscellaneous Tool	Description
Searchsploit	A tool included in the exploitdb package on Kali Linux that enables you to search the Exploit Database archive.
Powersploit	A series of Microsoft PowerShell scripts that pen testers can use in post-exploit scenarios. This tool is included in Kali Linux.
Responder	A fake server and relay tool that is included with Kali Linux. It responds to LLMNR, NBT-NS, POP, IMAP, SMTP, and SQL queries in order to possibly recover sensitive information such as user names and passwords.
Impacket	A collection of Python classes that provide low-level program access to packets, as well as to protocols and their implementation.
Empire	(PowerShell Empire) A post-exploitation framework for Windows devices. It allows the attacker to run PowerShell agents without needing powershell.exe. It is commonly used to escalate privileges, launch other modules to capture data and extract passwords, and install persistent backdoors.
Metasploit Framework	A command-line-based pen testing framework developed by Rapid 7 that is included with Kali Linux and that enables you to find, exploit, and validate vulnerabilities. Metasploit also has GUI-based commercial and community versions.

Communication and the Pen Testing Process

As with any type of review, whether internal or for hire, communication between the testing team and the stakeholders is of paramount importance. All facets of communication need to be evaluated and decided upon prior to the pen testing engagement, such as:

- **The communication path, or chain of command.** In a pen testing situation, it's equally as important to ensure that the right people are informed as to what information should be shared. For instance, the organization might not want all staff to know when a pen test is occurring, particularly if they want to check on the effectiveness of using social engineering tactics to penetrate a network. The client IT manager and CIO/CISO should be aware of the engagement. Additionally, some key department managers should also be aware in case unforeseen incidents might affect their departments.
- **Communication with client counterparts.** The designated lead of the pen testing team should have close communication with their client counterpart (typically the IT manager). To reduce possible confusion, all communication between the pen testing team and the client should go through this point of contact. The two lead roles must both be hands-on. This allows for immediate response in case of incidents, unexpected discoveries, additional client requests, or anything else that might lead to extended time or scope creep.
- **Communication within the pen testing team.** The pen testing team should have internal communication protocols as well. For example, sub-teams working on specific tasks should apprise the lead of their progress. They should inform the lead immediately of unexpected findings, such as evidence of prior security breaches or if they discover current hacking activity. The lead will then contact their client counterpart to discuss what should be done.
- **What information to communicate, and when.** What should trigger official communications? Describe any standard process stages, such as the planning and reporting stages, that require meetings to be held. Also describe the actual deliverables, such as status and interim reports, as well as the final report to be provided. What about "show stoppers" or other critical findings? The pen test team must be able to prioritize findings as they occur and identify findings that are urgent enough to trigger special communications. When a pen tester encounters evidence of a compromised system, should the Incident Response Team be notified to ensure that the organization is aware of the attack? If the evidence appears to be "fresh," the pen test might need

to be suspended until the security breach is handled. If it is historical, the pen test team should log the discovery and continue with the task at hand.

- **Regular progress briefings within the team.** If different members of the pen test team are conducting simultaneous attacks, there should be internal coordination to ensure team members are not accidentally interfering with each other. The lead might opt to have daily "scrum" type meetings, in which each member describes what they did yesterday, what they will do today, and identify anything blocking their efforts. The lead or project manager can then allocate resources or request conflicting activities to be temporarily suspended.
- **Regular progress briefings with the client.** If the pen test will take more than a few days, the client might want regular progress updates. This can be done weekly or as deemed necessary. Keep in mind that "the client" is probably not just one person but could be several managers who need to remain in the communications loop. The client may request that these managers each directly receive a copy of status updates, or they may request that reports are given to only one representative, who will internally distribute copies. Typically, the final report is given to a single party as part of a formal handoff. In some cases, certain findings may be too sensitive to share with all on the approved recipients list. However, this is more likely to be the exception rather than the rule. Having a clear communication path will ensure that all relevant parties receive reports in a timely manner. Emergencies would be handled separately, though ongoing issues such as client interference, delays, or other problems should be raised at status meetings.
- **Clear identification of the reasoning behind communication activities.** Consider how a situation might need to be addressed if the pen test attempt is detected. It is possible that several testers might focus their efforts on a key system at the same time, thus making the breach debilitating or quite obvious. In such a case, the testing team might need to work together to scale back on their efforts to de-escalate the effects of the test. Providing situational awareness to key client personnel can also help ***deconflict*** the breach, enabling the pen test to continue so that additional issues can be found, exploited, and analyzed.
- **Possible adjustments to the engagement.** The nature of a pen test is that it is a fluid process. Information that is discovered during the reconnaissance phase drives the decisions on what exploits to try and, ultimately, what solutions to propose. Awareness of the need for contingency planning for the pen test engagement itself enables you to incorporate it into your plans and to re-prioritize the goals of one activity or large sections of the pen test.
- **Disclosure of findings.** It is incumbent upon a company to fully disclose vulnerabilities and breaches to their customers, suppliers, regulators, or members of the public who may be harmed by the breach. If you, the pen tester, were paid to help discover those vulnerabilities and breaches, any findings should be strictly confidential for both legal and ethical reasons. An exception to this could be if you uncovered criminal conduct, in which case you might be obligated to notify law enforcement. If a question arises regarding disclosure of findings, even if disclosure would be for the general public good, it is not the pen tester's job to make that decision. You should consult with your team's legal counsel in such cases.

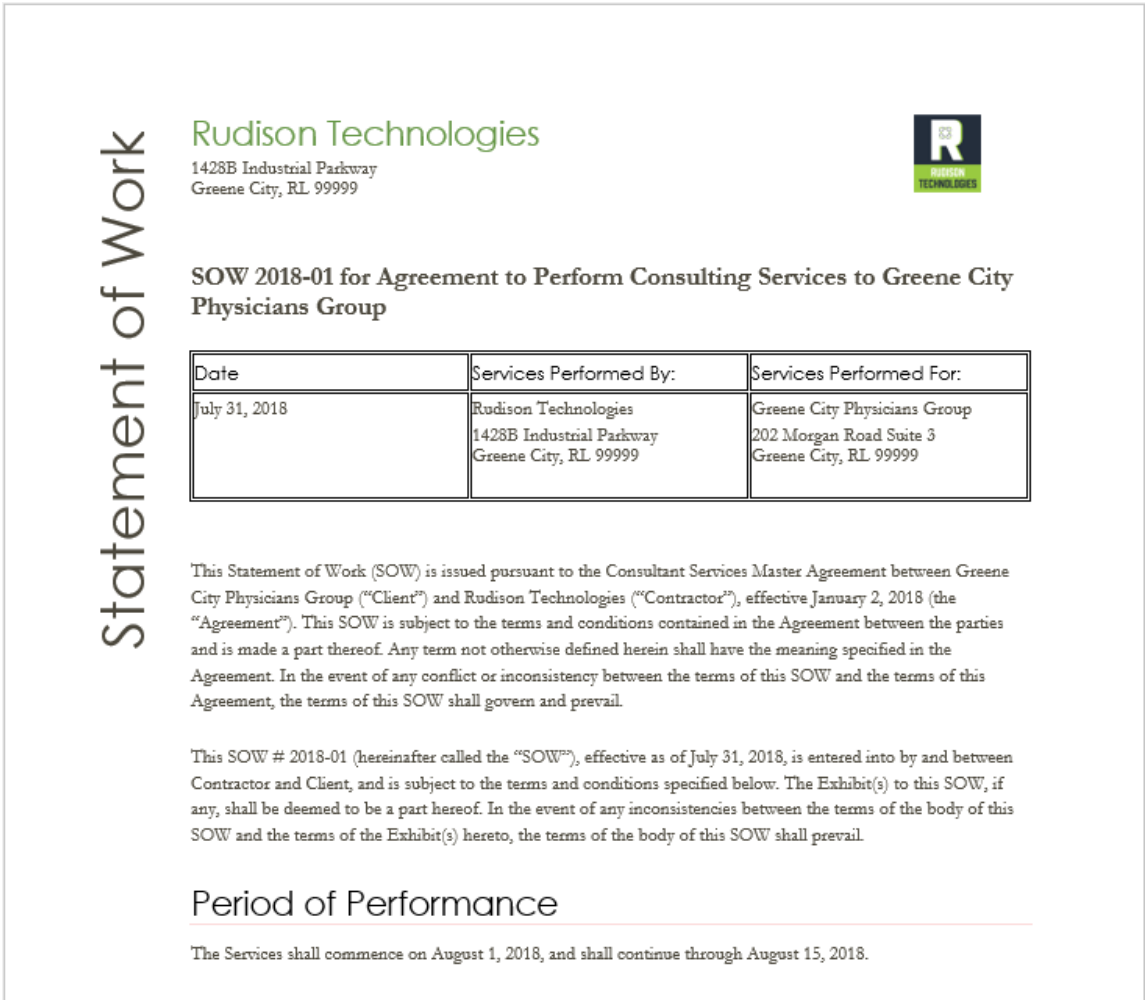
Note: For more information on vulnerability disclosure, see **https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy**.

Contract Types

As part of the legal issues relevant to the pen testing process, you will encounter several types of contractual agreements. Some of these are described in the following table.

Type of Contract	*Description*
Master service agreement (MSA)	An agreement that establishes precedence and guidelines for any business documents that are executed between two parties. It can be used to cover recurring costs and foreseen additional charges during a project without the need for an additional contract.

Type of Contract	Description
Non-disclosure agreement (NDA)	A business document that stipulates the parties will not share confidential information, knowledge, or materials with unauthorized third parties.
Statement of work (SOW)	A business document that defines the highest level of expectations for a contractual arrangement. It typically includes a list of deliverables, responsibilities of both parties, payment milestones and schedules, and other terms. Because this document details what the client is paying for, it has a direct impact on team activities. It also can be used by the pen test team to charge for out-of-scope requests and additional client-incurred costs.



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.

Figure 1-3: A sample SOW.

Authorizations

Another facet of establishing and conducting a pen testing engagement involves the process of collecting written authorizations to conduct the testing activities. In some situations, authorization documents (which can be completed and signed forms, letters, or other types of documents) exist as addenda to the SOW.

Written authorization documents help control the amount of liability incurred by the pen tester. In situations where a third-party service provider, such as a cloud service provider, might be affected,

you might need to ensure that you have proper authorization from the service provider in addition to the client.

Most written authorization documents include the following information:

- Who the proper signing authority is, or who can authorize that the pen testing can take place. This includes a statement that the undersigned is a signing authority for the organization.
- Who is authorized to perform the pen test.
- What specific networks, hosts, and applications can be tested.
- The time period that the authorization is active.

Finally, it is strongly recommended that all parties arrange for legal review of the authorization document.

SOW Addendum: Authorization for Pen Testing

Scope

To properly secure the organization's information technology assets, the InfoSec team is responsible for periodic assessment and testing of the organization's security stance. When this testing includes penetration testing, in accordance with the Statement of Work (SOW) signed on *<sow-date>*, the following activities are considered to be necessary to complete the pen testing:

- Use social engineering and other techniques to gather information about the organization and its resources.
- Scanning desktop and laptop computers, servers, network devices, and any other computing devices owned by the organization.
- Using scan results to make further inroads to the network and its resources.

Purpose

The purpose of this document is to grant authorization to the undersigned members of the InfoSec team so that they can perform penetration tests against the organization's assets in accordance with the SOW signed on *<sow-date>*.

Attestation

The following individual has the authority to grant permission for penetration tests to be conducted:

- *<name-of-signing-authority>*

The following people are granted permission to scan the organization's computer equipment to conduct penetration tests against organizational assets:

- *<name-of-tester-1>*
- *<name-of-tester-2>*

The time frame for conducting penetration tests is from *<start-date>* to *<end-date>*.

_____
<name-of-signing-authority>
<title-of-signing-authority>

<signing-date>

_____
<name-of-tester-1>
<title-of-tester-1>

_____
<name-of-tester-2>
<title-of-tester-2>

Figure 1-4: A sample authorization template.

Legal Restrictions

In addition to specific contractual requirements, other legal differences that depend on your organization's environment can affect the pen testing process. Some of these environmental restrictions include:

- Export restrictions: In the United States, ***export controls*** regulate the shipment or transfer of certain items outside of the US. These items can include software, technology, services, and other controlled items. Other nations might have similar restrictions to the sharing of certain items outside their borders.
- Local and national governmental restrictions: It is highly probable that governmental restrictions control the use of technology and tools used during the pen testing process. This includes not only the technology and tools, but also the information gathered by the testers and even the actual process of exploiting computer systems, such as port scanning.
- Corporate or organizational policies: Many companies and organizations now have specific policies that regulate pen testing activities, so you will need to be aware of any particular restrictions adopted by the company or organization that is undergoing pen testing.

TOPIC B

Plan a Pen Test Engagement

Before embarking on the pen test process, it is imperative that you plan for the engagement. Evaluating the various considerations should help you build a clear project plan that all stakeholders can use as a guide throughout the entire process.

Target Audience Types

One of the initial considerations when you are creating a pen test plan is to determine the target audience for the main deliverable, which is the pen test report. Different sorts of pen test engagements will have different sets of stakeholders from the organization whose information systems are being tested.

For the purposes of this section, let's consider that organization to be the client.

- The types of information systems being tested definitely affect the composition of the target audience. For instance, if a pen test engagement is limited to penetrating networks and hosts, but does not focus on testing web or other applications, the client might decide there is no need to include web developers in the target audience.
- The stakeholders most likely to be part of the target audience might be a combination of upper-level managers, IT management and personnel, and other individuals who will be directly affected by the pen test engagement. Several representatives of the client's security or IT team might be part of the target audience. Again, the type of information system being tested will have an effect on who belongs in the target audience. If a web server and app are being tested, the web server admin and app developer could be included.
- Whether the pen test team is an internal entity or an external consultant is another factor to consider. For internal teams, their representatives from upper management are likely to overlap with the client's management representatives, while external consultants' management teams will be different individuals.

Resources and Requirements

The goal of a pen test plan is to clearly define the parameters of the pen test engagement. Establishing what resources will be made available to the testing team and what requirements are expected from the testing team is integral in defining these parameters.

A wide variety of support resources might be made available, including those listed in the following table.

Support Resource	*Description*
WSDL and/or ***WADL***	Web Services Description Language and Web Application Description Language files are XML documents that describe SOAP-based or ***RESTful*** web services.
SOAP project file	A file that enables you to test SOAP-based web services. These files often are created from the information in a WSDL file or service.
SDK documentation	Documentation for a collection of development tools that support the creation of applications for a certain platform.
Swagger document	The ***REST*** API equivalent of a WSDL document.
XSD file	A document that defines the structure and data types for an XML schema.

Support Resource	Description
Sample application requests	Like test code or code snippets, sample app requests can assist pen testers in gaining access to resources.
Architectural diagrams	Visual representation of an application's architecture can reveal points of weakness in the app's construction, while network maps can help identify those hosts that might be good potential access points.

Some things to consider when developing and interpreting requirements include:

- **Confidentiality of findings**: During the course of any pen test, it is assumed that there is a great possibility of sensitive information being discovered by the testing team. To further reinforce the SOW and any other legal documentation in effect, the client is very likely to include confidentiality provisions within the engagement plan. This helps to ensure that the information discovered during the pen test is shared only with the appropriate entities. For example, if a pen tester finds a major code injection vulnerability in the company's public-facing website, the organization may require them to keep this information confidential to minimize risk. Or the requirements might set restrictions for which privileged personnel should be informed of the issue (e.g., the IT managers only, and not standard employees).
- **Knowns vs. unknowns**: It is difficult for any plan to totally address every possible contingency. Although most resources and requirements will be known at the onset of the engagement, others might arise during the actual performance of the pen test. A comprehensive pen test plan will recognize this and include language that allows for some adjustment during the process. For example, if a pen tester discovers evidence of a prior breach, the organization might need to alter its requirements so that the pen tester doesn't compromise evidence of the breach, and that the evidence is preserved for an upcoming forensic analysis.

Budget

Any agreement between two parties is likely to have budgetary considerations and constraints, including pen test engagements. Each party must consider the services provided worth the time and money spent. Budget often drives the scope of the penetration test:

- The service provider, or pen tester, wants to minimize the expenses associated with pen testing and maximize revenue/compensation while providing an acceptable level of quality of service to the service consumer, or client organization.
- The service consumer wants to minimize its expenses while maximizing the volume/depth of testing and overall quality of service. In addition, the service consumer considers the cost of pen testing to be an investment in the security posture of the organization.

Note: There may be cases, such as in compliance testing, where budget is less of a consideration.

Technical Constraints

A comprehensive pen test plan should not only include what should be tested, but it should also describe anything that is specifically excluded from the test engagement. In addition, there might be technical barriers in place that could prevent the pen testing team from fully testing some organizational resources. Some technical constraints, including choice of tools, will be driven by budget. All constraints should be described in detail in the pen test plan. Common technical constraint scenarios include:

- A legacy server is considered too fragile to withstand denial-of-service or buffer overflow attacks.
- Attacking a website hosted by a third party might be too disruptive to the provider's other customers.

- An offshore data center is too expensive to physically visit, so attack choices must be remote in nature.

Rules of Engagement

In pen testing, the ***rules of engagement*** is a document or section of a document that outlines how the pen testing is to be conducted. They describe the expectations of the client and the rights and limitations of the test team.

Some facets of the rules of engagement are described in this table.

Component	*Description*
Timeline	The timeline of a pen test engagement is a clear enumeration of the tasks that are to be performed as part of the engagement, and the individuals or teams responsible for performing those tasks. As the engagement progresses, stakeholders can use the timeline as a progress indicator, and adjust it as needed during the engagement to account for any unexpected events. The timeline is often shared with stakeholders in a Gantt chart format.
Location of test team	The location of the test team in relation to the client organization needs to be agreed upon. Depending on factors such as how many locations an organization occupies, whether or not remote installations are in different nations, and what sort of remote technology is available to access multiple locations, the parties should agree and record the amount of travel required, if any, to conduct the pen test.
Temporal restrictions for testing	When the actual test begins, are there constraints on the days and times that the testing can be performed?
Transparency of testing	At the client organization, who will know about the pen testing? For the test team, what information will be provided prior to the start of the engagement?
Test boundaries	What's being tested, and what is not? Define the acceptable actions, such as social engineering and physical security tasks If invasive attacks, such as DoS attacks, are part of the testing, are there any restrictions on their use?

Impact Analysis

Planning a pen test engagement involves estimating what effect testing will have on normal business operations. When planning a test, the pen test team will advise the client on potential impacts to different types of systems. This will be informed by target type, criticality to the business, and testing approach. The analysis should also allow for unforeseen impacts. Both sides must work together to manage the risk ahead of time, as well as have clear communication protocols and remediation plans in place to minimize any impact that may actually occur. There should be clear triggers, escalation procedures, and timelines for alerting the other side in case of an incident. Depending on the client's risk appetite, some systems may get more attention and faster response than others.

Remediation Timeline

Remediation is the implementation of a solution for a given vulnerability. When taken into consideration with impact analysis, organizations can choose to address the highest-risk issues first, or they might decide to address issues that can be quickly or inexpensively resolved. There might

also be issues that an organization could decide not to address, and thus accept the risk associated with those vulnerabilities.

Disclaimers

A comprehensive pen test plan should also include some disclaimer clauses to further protect the parties involved in the engagement.

To protect the pen testing team, a ***point-in-time assessment*** clause might be included in the plan. This clause should state that the pen test results have a limited life cycle and are not to be interpreted as a security guarantee. In fact, even one configuration change could cause the pen test report to be outdated. When an organization schedules periodic pen tests with the same or even different testing teams, any repercussions from configuration changes can be identified and remedied.

As you saw during the discussion of budgets, clients want the broadest scope at the lowest price, and usually expect results within the shortest possible time frame. A comprehensiveness clause can detail the boundaries with regard to scope, price, and time frame. It can also acknowledge that not every vulnerability might be found during an engagement.

Guidelines for Planning Pen Test Engagements

Consider the following guidelines as you plan your pen test engagements:

- Be sure that you understand the target audience.
- Identify the resources and requirements that will govern and facilitate the pen test engagement.
- Determine any budget restrictions that might affect the engagement.
- Document any technical constraints that will affect the engagement.
- Clearly define the rules of engagement.
- Develop impact analysis and remediation timelines.
- Identify any disclaimers that will affect the engagement.

TOPIC C

Scope and Negotiate a Pen Test Engagement

It is essential that each pen test engagement have clear boundaries that are understood and agreed to by both parties. Although often conducted in conjunction with the initial planning, you still need to make sure that scoping considerations are as accurate as possible to provide direction and level-settting to the client organization as well as the test team, particularly in the case of large or complex engagements that might need to be implemented in stages.

Scoping

Defining the ***scope*** of your engagement is one of the most crucial things you can do when negotiating a contract. The scope is the basis for the SOW. When the scope is clear, all stakeholders understand what is considered an appropriate target, and the limits of what the pen test team can do to that target. Pen test team members must know what protocol to follow when they encounter something that is out of scope.

For example, it is very common for someone from the client's IT department to ask consultants for small favors or to "check this one item" in the course of their duties. The pen tester must know if the request is within scope, and if it is not, how to respond and escalate the request. Usually, the response should be a polite, "let me check with my supervisor on how we can assist you with this."

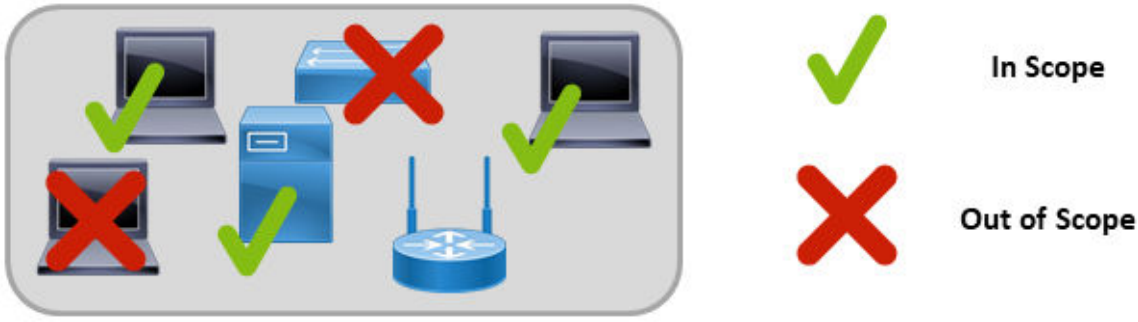


Figure 1-5: Scoping defines appropriate targets and limitations.

End Goals and Deliverables

Before an organization can begin to scope a pen test engagement, it needs to clearly identify why the pen test is being performed. Are they fulfilling a compliance or other legal requirement? Or is there a definite need and desire to improve organizational security?

There is a possibility that as the planning and scoping continue, the end goals might need to be adjusted or amended.

In virtually every pen test engagement, the major deliverable is an actionable report that describes the tests performed, vulnerabilities identified, the analysis conducted, and the mitigation solutions suggested. If more or different documentation is required by the organization, that need should be communicated to the testing entity prior to the finalization of the plan.

The testing team needs to translate technical findings into the potential risk to the organization. The final report should include a section that ranks threats by probability x impact. In some cases, this will translate directly into monetary losses, while in others, it will translate into legal issues or loss of reputation, which then correlate to monetary losses. This ranking will help the client prioritize remediation efforts and timelines.

Types of Assessments

There are several general categories of assessment that an organization can use to help define the scope of a pen test engagement.

- **Goal-based or objective-based assessments** provide focus points for the pen test. They begin by the client listing the items or information that needs to be protected. Then, the pen test team will develop plans to obtain the goal or objective through any attack techniques available. This approach closely mimics the attacks that might be launched by a malicious party, so they can provide significant ROI for the client organization.
- **Compliance-based assessments** are government- or industry-required tests based on an established compliance framework. Common US compliance frameworks include PCI DSS, DISA STIG, FEDRAMP, and FISMA.
- **Red team assessments** test an organization's detection and response capabilities by emulating a malicious actor who targets attacks and avoids detection. The red team accesses sensitive information any way it can without being caught in the act. Red teams usually have longer time frames in which to work. Because stealth and avoidance is of great importance to the red team, they function more like an advanced persistent threat (APT), keeping a low profile while infiltrating the network. By contrast, pen test teams are usually time constrained and often cannot afford to be as patient. As such, they may be "noisy," while red teams are "quieter."

Color Teams

The idea of color teams evolved from military readiness exercises. In general, red teams attack, while blue teams defend. In some instances, purple teams help coordinate interactions between red and blue teams, and in other cases, white teams establish rules and monitor the testing.

Compliance-Based Assessments

Compliance is a broader discipline in which pen testing can, but does not necessarily have to, play a part. Compliance is usually assessed through a comprehensive audit of administrative, technical, and physical controls, and their design, implementation, maintenance, and effectiveness. Penetration testing can be used to validate the effectiveness of many of these controls. Because compliance is either government- or industry-mandated, it would take precedence over any company policy. The key aspects of compliance-based assessments include:

- Clearly defined objectives based on regulations or compliance frameworks (what to look for).
- Possible mandated rules for completing the assessment (how to look).
- Focus on password policies, data isolation, and key management.
- Limitations on network or storage access.

Types of Strategies

The following table describes the types of strategies used in most pen test engagements. Which strategy you use will have an effect on the scope of the project.

Pen Test Strategy	Description
Black box test	• The pen tester is provided virtually no information about the systems or networks being tested, thus simulating an outside attacker who knows little about the target other than what can be determined through basic reconnaissance techniques. • Also referred to as a zero knowledge test, the pen tester must gather information about the target and verify that information with the client before the actual testing can begin. • The client verification confirms that the test is being conducted within the established scope. • Tests are often conducted with very few people at the target organization being aware that the testing is taking place, thus providing a test of how personnel monitor, detect, and respond to security incidents.
Gray box test	• The pen tester is provided with some knowledge and insight of internal architectures and systems, along with other preliminary information about the target and its assets, to simulate an internal attacker who knows some but not all information about the target systems and networks. • Also referred to as a partial knowledge test, the pen tester tries to gather additional information about the target through basic and advanced reconnaissance techniques.
White box test	• The pen tester is provided with knowledge about all aspects of the target systems and networks, to simulate an internal attacker who has extensive knowledge of the systems and networks that are being targeted. • Considered to be the opposite of a black box test, a white box test is often conducted as a follow-up to a black box test. • Because the tester already has information about the function and design of the targets, the reconnaissance phase can be skipped.

Types of Threat Actors

As with the black/gray/white box strategy, effectively scoping an engagement involves determining what different types of attackers will be emulated. Some organizations are primarily concerned with external threats, while others require a more comprehensive approach.

A ***threat actor*** is an entity that is partially or wholly responsible for an incident that affects or has the potential to affect an organization's security. Threat actors are also referred to as malicious actors. A common way to categorize threat actors is descriptive in nature:

- ***Script kiddies*** are novice or inexperienced hackers with limited technical knowledge who rely on automated tools to hack into targets.
- ***Hacktivists*** gain unauthorized access to and cause disruption in computer systems in an attempt to achieve political or social change.
- Organized crime perpetrators engage in criminal activity, including cyber crimes, most commonly for monetary profit.
- Nation states and advanced persistent threats (APTs) use cyber crimes to achieve political and military goals. APTs commonly use several attack vectors to ensure their success in gaining unauthorized access to information.
- ***Insider threats*** involve someone from within or related to the target organization. Insiders include present and past employees, contractors, partners, and any entity that has access to proprietary or confidential information.

- Competitor organizations might try to gain unauthorized access to a business rival's sensitive information.

Some governmental agencies categorize cyber adversaries into one of six tiers, as outlined in the following table.

Tier	Description
I	Those who invest a relatively small amount of money to use off-the-shelf tools to exploit known vulnerabilities.
II	Those who invest a relatively small amount of money to develop their own tools to exploit known vulnerabilities.
III	Those who invest millions of dollars to discover unknown vulnerabilities that enable them to steal personal and corporate data that they can sell to other criminal elements.
IV	Organized, highly technical, proficient, well-funded professionals who work in teams to discover new vulnerabilities and develop new exploits.
V	Nation states that invest billions to create vulnerabilities by influencing commercial products and services.
VI	Nation states that invest billions to carry out a combination of cyber, military, and intelligence operations to achieve a political, military, or economic goal.

Be aware that higher-tier threat actors can use lower-level methods and techniques to accomplish their objectives. Or they might use lower-level threat actors as proxies, in which case the lower-tier proxies get access to higher-tier capabilities.

Capabilities and Intent of Threat Actors

As you can see from the tier descriptions in the previous section, different types of threat actors can have varying levels of capability. Lower-tier actors are less likely to have application-development capabilities than the mid-tier and higher-tier actors. Each threat actor also has one or more overarching reasons for conducting attacks. Some threat actors might be more likely to be motivated by monetary gain, while others strive for power or even revenge. These varying motivations are directly tied to the intent of the threat actor. If greed is the motivator, then the intent is to steal information.

Identifying the capabilities and intent of the threat actors you want to emulate during a pen test engagement helps you to identify the scope of the engagement.

Threat Models

Threat models identify and classify potential attack methods, or attack vectors, which are the paths that attacks can take. They can encompass the overall security of an organization, or they can apply to specific computers or other assets that are targeted in an attack. Threat models can be activity-focused or asset-focused, and they can assist the security-conscious organization to evaluate risk and potential mitigation strategies to counter the potential attacks. When creating a threat model, the security team starts from an undesirable end result (such as data stolen from a particular database hosted on a particular server) and then reverse engineers the steps required for an attacker to finally reach that end result. Whenever possible, controls are then identified and implemented at the various attack steps. The goal of threat modeling is to disrupt the attack vector so the end goal cannot be achieved.

Types of Targets

Scoping a pen test engagement also entails determining what types of items to target. The type of target helps determine the scope and type of attack. The following table summarizes common targets and strategies for targeting them.

Target Type	*Description*	*Attack Considerations*
Internal	Assets can be accessed from within the organization. Internal attacks might be caused by malicious insiders or by external hackers who have gained credentials through a phishing attack.	An excellent candidate for all attack types IF direct access to the internal network can be established.
On-site	Asset is physically located where an attack is being carried out.	Accessibility depends on controls at the site. A physical attack might go undetected at a large facility with many people. Centralized resource locations will probably have more points of entry and attack vectors to choose from.
Off-site	Asset provides a service for an organization but is not necessarily located at the same place.	An organization's remote offices and satellite locations are less likely to have as many security controls as headquarters. As such, an attacker would lose the "cover" of anonymity. However, lax security might still make it possible to carry out physical, Wi-Fi, or possibly remote access/VPN attacks. You would have to assess if the remote location is worth the effort. If the remote location does not itself house interesting assets, it might provide a back door (such as an unguarded WAN or VPN link) to the main facility.
External	Asset is visible on the Internet, such as a website, web application, email, or DNS server.	Not a good candidate for attacks (such as sniffing or ARP poisoning) that require direct access to the network segment.
First-party hosted	Hosted by the client organization.	Might be easier to attack than third-party hosted services, as most companies do not have the same resources, expertise, or security focus as a provider.
Third-party hosted	Hosted by a vendor or partner of the client organization.	Not impossible targets, but established providers are more likely to have good controls in place. Smaller, newer hosting companies may have fewer resources and less security expertise. These might be easier to attack than larger, more mature providers. All third parties can be vulnerable to zero-day attacks.

Target Type	Description	Attack Considerations
Physical	Can include the client organization's premises or any physical device belonging to the client organization.	Physical attacks are an excellent way to plant sniffers, remote-controlled devices, keyloggers, and other attack tools in the private network.
Users	They generally have access to resources that might be restricted to outside parties.	Users are usually the easiest attack vector because they are so susceptible to social engineering.
SSIDs	Can be targets when an attacker is attempting to access a wireless network.	Evil twins and other Wi-Fi attacks require close physical proximity to the premises.
Applications	Can be targets, as they are often linked to sensitive data such as credit card numbers.	You'll have to determine which applications are in use. If it runs in user context, you'll want to escalate privilege once it is compromised.

Fragile Systems

Another type of potential target includes systems that are inherently unstable and have a tendency to crash, and systems that need to run older, unpatched versions of operating systems to support legacy applications. These are often referred to as ***fragile systems***. Part of your scoping efforts should be to identify any fragile systems that might be tested, and to what extent they can be exploited.

Specialized Systems

As you scope a pen test engagement, you will also want to identify any specialized systems that you want included in the tests. Common specialized systems are described in the following table.

Type of Specialized System	Description
Industrial control systems (***ICSs***)	Networked systems that control critical infrastructure such as water, electrical, transportation, and telecommunication services.
Embedded systems	Computer hardware and software that have a specific function within a larger system such as a home appliance or an industrial machine.
Supervisory control and data acquisition (***SCADA***) systems	ICSs that send and receive remote-control signals to and from embedded systems.
IoT devices	Any objects (electronic or not) that are connected to the Internet by using embedded electronic components.
Mobile systems	Smartphones, tablets, wearable devices, and other mobile computing devices.
Point-of-sale (PoS) systems	Stations that typically consist of a cash register, barcode scanner, and a debit and credit card scanner.
Biometric devices	Devices that identify individuals by their physical characteristics, such as thumbprint scanners, retinal scanners, voice-recognition software, and facial-recognition software.
Application containers	Virtualized environments that are designed to package and run a single computing application or service and that can share the same host kernel.

Type of Specialized System	Description
Real-time operating systems (*RTOSs*)	Specialized operating systems that feature a predictable and consistent processor scheduler.

Risk Responses

How an organization deals with identified risk depends on the thresholds established for various forms of risk, and those thresholds are normally set according to the risk appetite of the organization. The following table describes four basic risk response approaches.

Risk Response	Description
Avoidance	In *risk avoidance*, an organization takes steps to ensure that risk has been completely eliminated, or reduced to zero, by terminating the process, activity, or application that is the source of the risk.
Transference	In *risk transference*, the organization moves the responsibility for managing risk to another organization, such as an insurance company, cloud service provider, or other outsourcing provider.
Mitigation	In *risk mitigation*, the organization implements controls and countermeasures to reduce the likelihood and impact of risk, with the goal of reducing the potential effects so that they are below the organization's risk threshold.
Acceptance	In *risk acceptance*, after the organization identifies and analyzes a risk, it determines that the risk is within acceptable limits, so no additional action is required.

Not all risks can be avoided, transferred, or completely mitigated. It might take a combination of response techniques for risks to be within acceptable levels.

Tolerance to Impact

It's highly likely that pen testing will have an effect on the performance of the networks, hosts, and applications being tested. For instance, attempting to invoke a DoS attack on a public-facing website will probably prevent customers from reaching the website during the test. The client organization must balance the need for testing with the need for continuous business operations. As you are scoping a pen test engagement, the client organization needs to identify which business operations and assets can be tested without exceeding its risk tolerance levels.

In Scope	Out of Scope
• Network storage • Intranet • Product databases • Employee email accounts • Time-tracking app	• E-commerce servers • Customer-facing websites • Email servers • R&D network

Figure 1-6: Defining organizational tolerance to impact.

Scheduling

Determining a timeline for pen testing events is also an integral part of defining the scope of the engagement. For potentially disruptive actions such as launching a DoS attack, the client organization might allow the attack but specify that it take place on weekends to minimize the effect on customers. Both start and end dates should be specified in the plan, along with notification to the client stakeholders to verify the beginning and ending of each test.

Note: By nature, pen testing is time constrained. Very seldom will you find an engagement that lasts longer than 2 to 4 weeks.

Scope Creep

Scope creep is the condition that occurs when a client requests additional services after a SOW has been signed and the project scope has been documented. This is not a condition that is limited to pen testing; in fact, practically every project manager or building contractor can provide examples of scope creep that happened with various projects.

The big problem with scope creep is that it takes resources away from those items that are documented in the SOW. It can also become a source of contention when it comes time to bill the client. If you initially discussed pen testing a dozen systems in three weeks and the client asks you to test another eight systems with the same end date, several things can happen:

- The time you expected to be able to spend on each system is reduced, unless you add more testers.
- Testing of the original dozen systems might be less thorough to account for the need to test the extra systems.
- If the testing organization provided a low quote to get the client's testing business, there might be little profit built into the price, so adding more systems to be tested might force the testing organization to take a loss on the engagement.
- Any legal protection spelled out in the SOW for the original systems might not carry over to the additional systems.

While it is easy to understand the desire to keep the client organization satisfied, testing organizations should carefully explain the ramifications of performing additional work without another agreement. The testing organization can try to negotiate extra money and time, possibly at a reduced rate.

General Considerations

The following table describes some general considerations to take into account while scoping pen test engagements.

Consideration	*Description*
Organizational policies	• Organizational policies are formalized statements defining how the organization intends to meet its long-term goals. • They can cover numerous topics, including security, privacy, compliance, and acceptable use of resources. • Pen test engagements should be designed so as to be in concert with existing organizational policies.
Security exceptions	• Some organizations provide ways to apply for policy exceptions, where certain organizational policies are not enforced for identified technologies or resources. • Existing security exceptions should be identified as being either within or outside of the engagement's scope.

Consideration	Description
NAC	• Network Access Control encompasses the collected protocols, policies, and hardware that govern if and how devices can connect to a network. • If a device can pass a health check, it can connect to the network. • Devices are agent-based or agentless.
Whitelisting and blacklisting (IPS/WAF whitelisting)	• Whitelisting blocks all users or IP addresses except those included on the whitelist, while blacklisting allows all users or IP addresses except those included on the blacklist. • These practices are commonly used with intrusion protection systems (IPSs) and web application firewalls (WAFs). • It is generally recognized that implementing whitelists is more restrictive and thus more secure than implementing blacklists.
Certificate and public key pinning	• Certificate and public key pinning is the process of associating a host with its expected X.509 certificate or public key. • Pinning bypasses the certificate authority (CA) hierarchy and chain of trust to lessen the impact of man-in-the-middle attacks. • Used in securing wireless channels, the act of pinning a certificate or public key helps guard against vulnerabilities in well-known protocols such as VPN, SSL, and TLS.

Special Considerations for Scoping Engagements

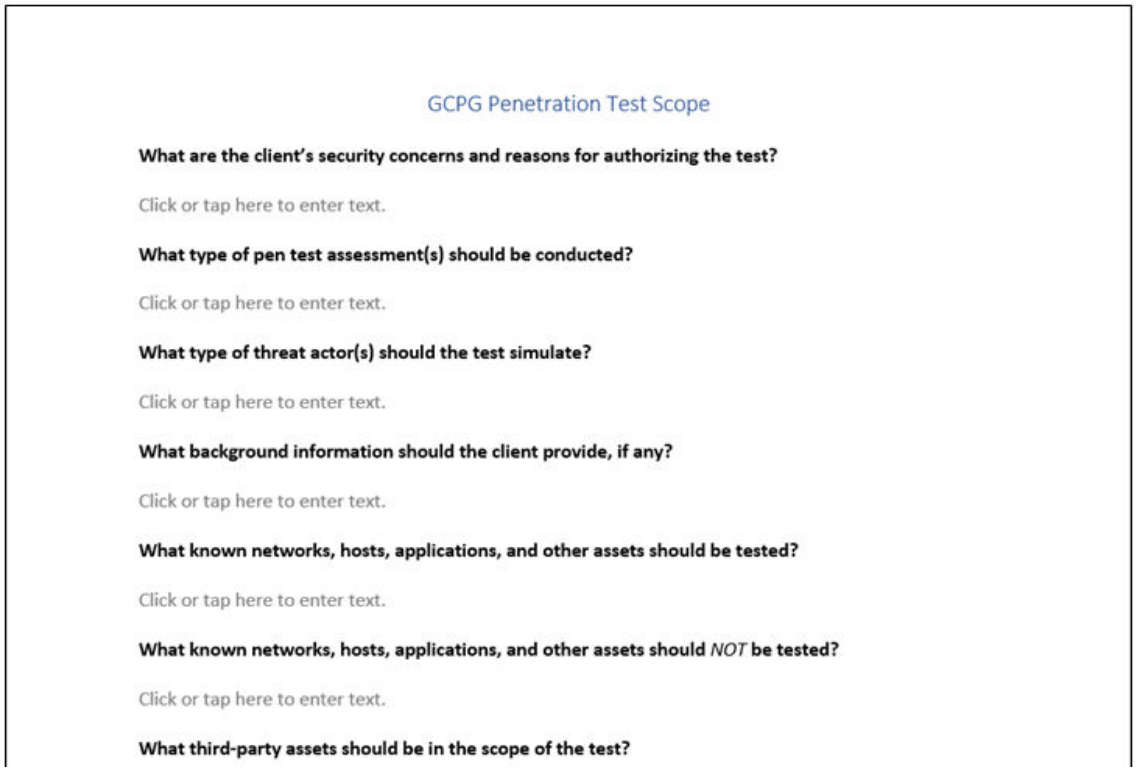
In addition to the general considerations, be aware of these special considerations when you are scoping pen test engagements.

Premerger security testing is a special type of security testing that takes place prior to an organizational merger. Premerger testing should be considered to be part of the due diligence that occurs prior to the merger. The results of these tests should be carefully analyzed to identify potential breaches that could happen at or after the merger, and to identify the countermeasures that will help prevent those breaches.

Supply chain security is the practice of analyzing and implementing controls to ensure the protection of data that moves through an organization's production processes. These processes can include vendors, partners, and service providers.

Scoping Checklists

Some organizations or testing entities employ a pen test scope document or checklist to record the information shared and decisions made during the scoping and negotiating of each engagement. There are many sample templates and checklists available on the web, so you might be able to find one that meets your needs without a lot of revision.



GCPG Penetration Test Scope

What are the client's security concerns and reasons for authorizing the test?

Click or tap here to enter text.

What type of pen test assessment(s) should be conducted?

Click or tap here to enter text.

What type of threat actor(s) should the test simulate?

Click or tap here to enter text.

What background information should the client provide, if any?

Click or tap here to enter text.

What known networks, hosts, applications, and other assets should be tested?

Click or tap here to enter text.

What known networks, hosts, applications, and other assets should *NOT* be tested?

Click or tap here to enter text.

What third-party assets should be in the scope of the test?

Figure 1-7: A sample scoping checklist.

Guidelines for Scoping and Negotiating Pen Test Engagements

Here are some guidelines for scoping and negotiating pen test engagements:

- Determine the types of assessments you want to conduct:
  - Goal-based or objective-based
  - Compliance-based
  - Red team
- Clearly define the end goals of the engagement.
- Determine what testing strategy you need to use:
  - Black box
  - Gray box
  - White box
- Determine what types of threat actors you want to emulate, and what their capabilities and intent might encompass.
- Consider recommending that the client organization engage in some threat modeling so that their objectives and expectations can be clearly defined.
- Identify all targets, whether conventional or specialized systems, and the risk tolerance associated with each.
- Be sure to account for existing controls and scenarios.
  - Existing organizational policies and security exceptions
  - Existing whitelists and/or blacklists
  - The use of certificate and public key pinning
  - The use of NAC devices and controls
  - The need for premerger or supply chain security testing
- Create, maintain, and adhere to a comprehensive schedule.

- Find ways to avoid scope creep; consider including disclaimer language to protect the test team from any adverse events resulting from allowing or denying scope creep.
- Consider using a scoping checklist to gather information that will help shape the boundaries of the engagement.
- Identify each deliverable, including all documents and meetings.

TOPIC D

Prepare for a Pen Test Engagement

After a pen test engagement is planned and properly scoped out, there are a few things the client organization and testing entity need to accomplish before the actual pen test starts. These activities will help streamline the overall process and ensure that the pen test engagement is fully documented and understood by all relevant parties.

Team Preparation

Getting ready for a penetration test involves preparing the client as much as preparing the pen test team itself. Penetration testing is, by its very nature, more intrusive than a simple vulnerability scan. Although the pen test team will take every precaution to minimize the impact of a test on the production network, issues can and do arise. For that reason, precautions and contingency plans must be in place for when an emergency arises.

Here are some best practices when preparing the client:

- Ensure that the client provides you with technical points of contact that you can reach before, during, and after the test.
- Ensure that key IT personnel have been informed about the upcoming test.
- Ensure that the client has up-to-date, verified backups of critical systems and is ready to work with you to address any unexpected consequences or availability issues.
- Ensure that all relevant client personnel are aware of the potential risks of the penetration test and are prepared to work with the pen test team to restore crashed or adversely affected systems.
- Ensure that the client understands that stepping up security just before a penetration test is not a sustainable approach:
    - You want to produce a report on the true state of the environment, not one that has been quickly spruced up a few days prior to the test.
    - Company staff, especially the IT department, should behave normally during the test, and not be in any state of heightened alertness, as this will incorrectly represent their security posture. It is usually best to only let managers know about the impending test.
    - Unless it's your intent to test a target's incident response capabilities, ensure that the IT department contacts you first when they detect a breach, rather than launching incident response procedures or calling law enforcement.

Here are some best practices when preparing the pen test team:

- Ensure that all team members are clear on the scope and limitations of the test.
- Ensure that all testers are mindful of the final objective of assessing the client's security risks and producing an actionable report.
- Ensure that all testers have contact information and clear escalation procedures in case anything goes wrong during a test.
- Ensure that all testers document their actions and outcomes in a central repository.
- Ensure that all testers have a "get out of jail free" card with them that clearly establishes authorization for their pen testing activities, including 24-hour contact information for their immediate supervisor(s).
- Ensure that the project lead is aware at all times of individual team member movements and activities, and that team members inform their supervisor(s) in real time when they begin and end each test.
- Ensure that all team members understand that missteps and accidents can and do happen, to report them immediately, and to be prepared to assist in restoring affected systems.

Data Collection and Documentation

In order to facilitate creating a final report for the client, every step of the penetration test should be well documented and have resulting data collected. Team members can and should record subjective impressions, and all test data should be uploaded in its raw form to a central repository. In this way, objective analysis can be conducted later on the data. Train your team to use the following best practices when documenting their tests and collecting data:

- Follow a plan that maps tests to objectives.
- Make sure that all tests ultimately lead to fulfilling the client's requirements.
- Ensure that all steps in a test, including missteps and accidents, are documented.
- Make sure that documentation is clear, concise, and objective.
- Use a central repository that all team members can upload results and data to.
- Collect as much test data as possible.
- Upload test results and data in the original raw form.
- Document the exact steps that were taken to collect the data, so that the results can be reproduced or at least analyzed objectively.
- Ensure that there is sufficient data for independent analysis to reach objective conclusions.
- Preserve original copies of the collected data in case they are needed for any future analysis.
- If your test or investigation uncovers evidence of previous or current hacking activity, note this in your findings and continue with your test. If the activity is ongoing, escalate findings.
- If findings uncover serious problems that are out of scope of the pen test, document the findings and pass these to your supervisor, but do not pursue them unless instructed to.

Activity Assignment and Sequencing

As with other types of projects, a penetration test should be carefully managed. This includes sequencing tasks and assigning resources to meet the schedule and objectives as outlined in the statement of work. Penetration testing, however, can be more fluid and dynamic than other types of projects. The direction of the investigation will evolve depending on findings. Teams need to be flexible and respond to changing conditions. Follow these best practices when assigning and sequencing activities in a penetration test:

- Start with initial task sequencing based on these common pen test stages:
  1. Passive reconnaissance
  2. Active reconnaissance
  3. Vulnerability assessment
  4. Penetration
  5. Exploitation
  6. Post exploitation
- Fit in non-technical tests such as social engineering and physical attacks at the earliest opportune moments.
- Whenever possible, "front load" the test with as many early assignments as possible to leave extra time at the end for the unforeseen.
- Give extra time to activities that are opportunity dependent (such as social engineering and physical attacks) or evasion-oriented (such as slow vulnerability scans).
- Be prepared for findings to spawn new investigations.
- Ensure that all investigations are driven by the requirements.
- If you are training new pen testers, pair less experienced team members with more experienced testers unless that pairing might endanger the mission of a particular activity.
- If a team member uncovers a serious problem that is outside the scope of the pen test, present the findings to the client and ask the client what they would like to do. Do not expand the scope of the investigation unless permitted by the SOW.

- When you have your initial assignments and sequencing ready, call a tactical meeting to outline the plan to the team. In some cases, an experienced team might self-organize, and collaboratively determine sequencing and task allocation.

Contingency Planning

By necessity, penetration testers use the same tools as malicious attackers. For this reason, you must expect problems to arise during the test. The SOW should list all targeted systems, but collateral damage can also occur. Testing can exacerbate existing problems, or take down an already fragile system. Before the test starts, you must make sure that the client has up-to-date, verified backups of all important systems, and contingency plans to quickly restore any system or service that has crashed. Often this can be as simple as rebooting a system or reverting a virtual machine to a previous snapshot. However, restoration activities, including reboots, can take some time. If department managers are aware of upcoming tests, they can also make provisions for downtime of any system or service that their staff depends on.

Escalation Path for Communications

Good communication is essential for the success of the penetration test. Not only must the pen test team be able to communicate amongst themselves and with their lead, but the team lead must also be able to communicate with the designated client contact. Having an escalation path for communications protects individual pen testers from having to make risky or potentially damaging decisions on their own. You also want to make sure that communications follow a chain of command, and that team members report and escalate issues only to authorized individuals. Use these best practices when establishing an escalation path for communications:

- Establish a clear chain of command in the pen test team. Make sure that communications follow that path.
- Make sure that the pen test team project supervisor has a counterpart on the client side that they can immediately bring issues to.
- Ensure that there is always a supervisor on duty, including a fail-safe operator, for team members to contact.
- Agree upon thresholds and protocols for contacting the other side during a problem, including:
  - When/how the client will notify the pen test team that a test is unacceptably interfering with operations/system performance.
  - When/how the pen test team will involve the client IT department if an accident occurs or a system becomes destabilized or unresponsive.
- Train all team members to:
  - Check in regularly with their lead, especially when starting and finishing a task.
  - Check in with their lead if they encounter anything unusual or outside the scope of their task.
  - Not make any decisions outside the scope of their task without authorization from their lead.
  - Alert their lead immediately if a problem arises.

Go Live

When the planning is done, and the team has received their starting assignments, it's time to "Go Live" and actually start the test. Although select client managers and IT personnel may know, the Go Live date and time should generally be secret and (hopefully) unexpected. In some cases, you might want to have passive reconnaissance and OSINT gathering completed even before the Go Live date.

Guidelines for Preparing for a Pen Test Engagement

Here are some guidelines you can follow when preparing for a pen test engagement.

- Ensure that your team is well trained in the tasks they will undertake.
- Make sure there is a clear chain of command with a clear communications path.
- Train the team to consult their supervisor when confronted with an unexpected situation or decision.
- Pair less experienced testers with more experienced ones unless it puts the activity at risk.
- Ensure that the client's IT department (at least the managers) is aware of the test, and that they have good backups and contingency plans to restore affected systems.
- Train your team to stay within the scope of the engagement unless authorized to expand their investigation.
- Train your team to log evidence of previous or existing malicious activity, to continue with what they are doing, and to escalate findings for further instruction.
- Ensure that the team fully documents their steps, collects as much data as possible, and uploads this information to a central repository for analysis.

ACTIVITY 1-1

Planning and Scoping Penetration Tests Review

Scenario

Answer the following review questions.

1. Do you have pen testing experience? How do the standards, frameworks, and processes discussed in this lesson map to your experiences?

2. Have you ever experienced scope creep? What were the circumstances and outcomes?

Summary

In this lesson, you planned and scoped pen tests. By clearly defining the plan and scope, you ensure that both parties in the agreement can easily determine what actions and assets are part of the pen test engagement, and what actions and assets are not.