




> **SAD_**
SEGURIDAD
Y ALTA
DISPONIBILIDAD

1.2. Exploring Penetration Testing Methodologies



I.E.S.
Doctor Balmis

Apuntes de PSP (<https://sad2asir.github.io/apuntes/es/>) creados por Vicente Martínez bajo licencia
CC BY-NC-SA 4.0  (<http://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

1.2. Exploring Penetration Testing Methodologies

1.2.1. Overview

There is more to penetration testing than hacking away at a customer's network. A haphazard approach will result in haphazard results. It is important to follow well-known methods and standards in order to approach pentesting engagements in an organized, systematic way.

You should understand the major documented methodologies and standards so that you can create strategies that draw on their strengths. Documenting your approach with the methodologies and standards that you used also provides accountability for our company and helps make our results defensible in case issues arise with our customers.

The process of completing a penetration test varies based on many factors. The tools and techniques used to assess the security posture of a network or system also vary. The networks and systems being evaluated are often highly complex. Because of this, it is very easy when performing a penetration test to go off scope. This is where testing methodologies come in. They provide a framework for the penetration tester to follow to ensure that the test is completed in a consistent manner. They also provide a way to ensure that the test is completed in a way that is repeatable and defensible.

1.2.2 Why Do We Need to Follow a Methodology for Penetration Testing?

As just mentioned, scope creep is one reason for utilizing a specific methodology; however, there are many other reasons. For instance, when performing a penetration test for a customer, you must show that the methods you plan to use for testing are tried and true. By utilizing a known methodology, you are able to provide documentation of a specialized procedure that has been used by many people.

1.2.3. Environmental Considerations

There are, of course, a number of different types of penetration tests. Often they are combined in the overall scope of a penetration test; however, they can also be performed as individual tests as well.

The following is a list of some of the most common environmental considerations for the types of penetration tests today:

Network Infrastructure Tests

Testing of the network infrastructure can mean a few things. For the purposes of this course, we say it is focused on evaluating the security posture of the actual network infrastructure and how it is able to help defend against attacks. This often includes the switches, routers, firewalls, and supporting resources, such as authentication, authorization, and accounting (AAA) servers and IPs. A penetration test on wireless infrastructure may sometimes be included in the scope of a network infrastructure test. However, additional types of tests beyond a wired network assessment would be performed. For instance, a wireless security tester would attempt to break into a network via the wireless network either by bypassing security mechanisms or breaking the cryptographic methods used to secure the traffic. Testing the wireless infrastructure helps an organization to determine weaknesses in the wireless deployment as well as the exposure. It often includes a detailed heat map of the signal disbursement.

Application-Based Tests

This type of pen testing focuses on testing for security weaknesses in enterprise applications. These weaknesses can include but are not limited to misconfigurations, input validation issues, injection issues, and logic flaws. Because a web application is typically built on a web server with a back-end database, the testing scope normally includes the

database as well. However, it focuses on gaining access to that supporting database through the web application compromise. A great resource that we mention a number of times in this book is the Open Web Application Security Project (OWASP).

md

Penetration Testing in the Cloud

Cloud service providers (CSPs) such as Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) have no choice but to take their security and compliance responsibilities very seriously. For instance, Amazon created the [\[Shared Responsibility Model\]](https://aws.amazon.com/compliance/shared-responsibility-model) (<https://aws.amazon.com/compliance/shared-responsibility-model>) to describe the AWS customers' responsibilities and Amazon's responsibilities in detail.

The responsibility for cloud security depends on the type of cloud model (software as a service [\[SaaS\]](#), platform as a service [\[PaaS\]](#), or infrastructure as a service [\[IaaS\]](#)). For example, with IaaS, the customer (cloud consumer) is responsible for data, applications, runtime, middleware, virtual machines (VMs), containers, and operating systems in VMs. Regardless of the model used, cloud security is the responsibility of both the client and the cloud provider. These details need to be worked out before a cloud computing contract is signed. These contracts vary depending on the security requirements of the client. Considerations include disaster recovery, service-level agreements (SLAs), data integrity, and encryption. For example, is encryption provided end to end or just at the cloud provider? Also, who manages the encryption keys—the CSP or the client?

Overall, you want to ensure that the CSP has the same layers of security (logical, physical, and administrative) in place that you would have for services you control. When performing penetration testing in the cloud, you must understand what you can do and what you cannot do. Most CSPs have detailed guidelines on how to perform security assessments and penetration testing in the cloud. Regardless, there are many potential threats when organizations move to a cloud model. For example, although your data is in the cloud, it must reside in a physical location somewhere. Your cloud provider should agree in writing to provide the level of security required for your customers. As an example, [\[the AWS Customer Support Policy for Penetration Testing\]](https://aws.amazon.com/security/penetration-testing) (<https://aws.amazon.com/security/penetration-testing>).

... note physical attacks vs. social engineering Many penetration testers find the **physical aspect of testing** to be the most fun because they are essentially being paid to break into the facility of a target. This type of test can help expose any weaknesses in the physical perimeter as well as any security mechanisms that are in place, such as guards, gates, and fencing. The result should be an assessment of the external physical security controls. The majority of compromises today start with some kind of **social engineering attack**. This could be a phone call, an email, a website, an SMS message, and so on. It is important to test how your employees handle these types of situations. This type of test is often omitted from the scope of a penetration testing engagement mainly because it primarily involves testing people instead of the technology. In most cases, management does not agree with this type of approach. However, it is important to get a real-world view of the latest attack methods. The result of a social engineering test should be to assess the security awareness program so that you can enhance it. It should not be to identify individuals who fail the test. One of the tools that we talk about more in a later module is the Social-Engineer Toolkit (SET), created by Dave Kennedy. This is a great tool for performing social engineering testing campaigns. ...



Bug bounty programs

Bug bounty programs enable security researchers and penetration testers to get recognition (and often monetary compensation) for finding vulnerabilities in websites, applications, or any other types of systems. Companies like Microsoft, Apple, and Cisco and even government institutions such as the U.S. Department of Defense (DoD) use bug bounty programs to reward security professionals when they find vulnerabilities in their systems. Many security companies, such as HackerOne, Bugcrowd, Intigriti, and SynAck, provide platforms for businesses and security professionals to participate in bug bounty programs. These programs are different from traditional penetration testing engagements but have a similar goal: finding security vulnerabilities to allow the organization to fix them before malicious attackers are able to exploit such vulnerabilities. You can find different bug bounty tips and resources in this [GitHub repository](https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties) (<https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties>).

When talking about penetration testing methods, you are likely to hear the terms unknown-environment (previously known as black-box), known-environment (previously known as white-box), and partially known environment (previously known as gray-box) testing. These terms are used to describe the perspective from which the testing is performed, as well as the amount of information that is provided to the tester:

md

Unknown-Environment Test

In an unknown-environment penetration test, the tester is typically provided only a very limited amount of information. For instance, the tester may be provided only the domain names and IP addresses that are in scope for a particular target. The idea of this type of limitation is to have the tester start out with the perspective that an external attacker might have. Typically, an attacker would first determine a target and then begin to gather information about the target, using public information, and gain more and more information to use in attacks. The tester would not have prior knowledge of the target's organization and infrastructure. Another aspect of unknown-environment testing is that sometimes the network support personnel of the target may not be given information about exactly when the test is taking place. This allows for a defense exercise to take place as well, and it eliminates the issue of a target preparing for the test and not giving a real-world view of how the security posture really looks.

This type of testing is often the most difficult for the tester because of the lack of information. However, it is also the most realistic because it is the closest to how an attacker would approach the target.

md

Known-Environment Test

In a known-environment penetration test, the tester starts out with a significant amount of information about the organization and its infrastructure. The tester would normally be provided things like network diagrams, IP addresses, configurations, and a set of user credentials. If the scope includes an application assessment, the tester might also be provided the source code of the target application. The idea of this type of test is to identify as many security holes as possible. In an unknown-environment test, the scope may be only to identify a path into the organization and stop there. With known-environment testing, the scope is typically much broader and includes internal network configuration auditing and scanning of desktop computers for defects. Time and money are typically deciding factors in the determination of which type of penetration test to complete. If a company has specific concerns about an application, a server, or a segment of the infrastructure, it can provide information about that specific target to decrease the scope and the amount of time spent on the test but still uncover the desired results. With the sophistication and capabilities of adversaries today, it is likely that most networks will be compromised at some point, and a white-box approach is not a bad option.

md

Partially Known Environment Test

A partially known environment penetration test is somewhat of a hybrid approach between unknown- and known-environment tests. With partially known environment testing, the testers may be provided credentials but not full documentation of the network infrastructure. This would allow the testers to still provide results of their testing from the perspective of an external attacker's point of view. Considering the fact that most compromises start at the client and work their way throughout the network, a good approach would be a scope where the testers start on the inside of the network and have access to a client machine. Then they could pivot throughout the network to determine what the impact of a compromise would be.

1.2. Explorando metodologías de pruebas de penetración

1.2.1. Descripción general

Las pruebas de penetración son mucho más que hackear la red de un cliente. Un enfoque descuidado dará como resultado resultados descuidados. Es importante seguir métodos y estándares bien conocidos para abordar las pruebas de penetración de manera organizada y sistemática.

Debe comprender las principales metodologías y estándares documentados para poder crear estrategias que aprovechen sus fortalezas. Documentar su enfoque con las metodologías y estándares que utilizó también proporciona responsabilidad para nuestra empresa y ayuda a que nuestros resultados sean defendibles en caso de que surjan problemas con nuestros clientes.

El proceso de completar una prueba de penetración varía según muchos factores. Las herramientas y técnicas utilizadas para evaluar la postura de seguridad de una red o sistema también varían. Las redes y sistemas que se evalúan a menudo son muy complejos. Debido a esto, es muy fácil cuando se realiza una prueba de penetración para salir del alcance. Aquí es donde entran las metodologías de prueba. Proporcionan un marco para que el probador de penetración siga para asegurarse de que la prueba se complete de manera consistente. También proporcionan una forma de asegurarse de que la prueba se complete de una manera que sea repetible y defendible.

1.2.2 ¿Por qué necesitamos seguir una metodología para las pruebas de penetración?

Como se mencionó anteriormente, el alcance es una razón para utilizar una metodología específica; sin embargo, hay muchas otras razones. Por ejemplo, cuando realiza una prueba de penetración para un cliente, debe mostrar que los métodos que planea utilizar para las pruebas son probados y verdaderos. Al utilizar una metodología conocida, puede proporcionar documentación de un procedimiento especializado que ha sido utilizado por muchas personas.

1.2.3. Consideraciones sobre el entorno

Existen, por supuesto, una serie de tipos diferentes de pruebas de penetración. A menudo se combinan en el alcance general de una prueba de penetración; sin embargo, también se pueden realizar como pruebas individuales.

La siguiente es una lista de algunas de las consideraciones sobre el entorno más comunes para los tipos de pruebas de penetración de hoy:

md

Pruebas de infraestructura de red

La prueba de la infraestructura de red puede significar algunas cosas. Para los fines de este curso, decimos que se centra en evaluar la postura de seguridad de la infraestructura de red real y en cómo puede ayudar a defenderse contra ataques. Esto a menudo incluye los conmutadores, enrutadores, firewalls y recursos de soporte, como la autenticación, la autorización y los servidores de contabilidad (AAA) y los IPS. Una prueba de penetración en la infraestructura inalámbrica a veces puede incluirse en el alcance de una prueba de infraestructura de red. Sin embargo, se realizarían tipos adicionales de pruebas más allá de una evaluación de red cableada. Por ejemplo, un probador de seguridad inalámbrica intentaría ingresar a una red a través de la red inalámbrica, ya sea mediante eludir los mecanismos de seguridad o romper los métodos criptográficos utilizados para asegurar el tráfico. Probar la infraestructura inalámbrica ayuda a una organización a determinar las debilidades en la implementación inalámbrica, así como la exposición. A menudo incluye un mapa de calor detallado de la distribución de la señal.

md

Pruebas basadas en aplicaciones

Este tipo de prueba de penetración se centra en probar las debilidades de seguridad en las aplicaciones empresariales. Estas debilidades pueden incluir, entre otras, configuraciones incorrectas, problemas de validación de entrada, problemas de inyección y fallas de lógica. Debido a que una aplicación web generalmente se construye en un servidor web con una base de datos de respaldo, el alcance de las pruebas normalmente incluye la base de datos también. Sin embargo, se centra

en obtener acceso a esa base de datos de soporte a través de la compromiso de la aplicación web. Un gran recurso que mencionamos varias veces en este libro es el Proyecto de seguridad de aplicaciones web abiertas (OWASP).

md

Pruebas de penetración en la nube

Los proveedores de servicios en la nube (CSP), como Azure, Amazon Web Services (AWS) y Google Cloud Platform (GCP), no tienen más remedio que tomarse muy en serio sus responsabilidades de seguridad y cumplimiento. Por ejemplo, Amazon creó el [Modelo de responsabilidad compartida](<https://aws.amazon.com/compliance/shared-responsibility-model>) para describir las responsabilidades de los clientes de AWS y las responsabilidades de Amazon en detalle.

La responsabilidad de la seguridad en la nube depende del tipo de modelo de nube (software como servicio [SaaS], plataforma como servicio [PaaS] o infraestructura como servicio [IaaS]). Por ejemplo, con IaaS, el cliente (consumidor de la nube) es responsable de los datos, las aplicaciones, el tiempo de ejecución, el middleware, las máquinas virtuales (VM), los contenedores y los sistemas operativos en las VM. Independientemente del modelo utilizado, la seguridad en la nube es responsabilidad tanto del cliente como del proveedor de la nube. Estos detalles deben resolverse antes de firmar un contrato de computación en la nube. Estos contratos varían según los requisitos de seguridad del cliente. Las consideraciones incluyen la recuperación ante desastres, los acuerdos de nivel de servicio (SLA), la integridad de los datos y el cifrado. Por ejemplo, ¿se proporciona el cifrado de extremo a extremo o solo en el proveedor de la nube? Además, ¿quién administra las claves de cifrado, el CSP o el cliente?

En general, desea asegurarse de que el CSP tenga las mismas capas de seguridad (lógica, física y administrativa) en su lugar que tendría para los servicios que controla. Al realizar pruebas de penetración en la nube, debe comprender lo que puede hacer y lo que no puede hacer. La mayoría de los CSP tienen pautas detalladas sobre cómo realizar evaluaciones de seguridad y pruebas de penetración en la nube. Independientemente, existen muchas amenazas potenciales cuando las organizaciones se mudan a un modelo de nube. Por ejemplo, aunque sus datos están en la nube, deben residir en una ubicación física en algún lugar. Su proveedor de la nube debe aceptar por escrito proporcionar el nivel de seguridad requerido para sus clientes. Como ejemplo [la Política de soporte al cliente de AWS para pruebas de penetración](<https://aws.amazon.com/security/penetration-testing>).

∴ note ataques físicos vs. ingeniería social Muchos pentesters encuentran la parte física de las pruebas como la más divertida porque esencialmente se les paga por irrumpir en la instalación de un objetivo. Este tipo de prueba puede ayudar a exponer cualquier debilidad en el perímetro físico, así como cualquier mecanismo de seguridad que esté en su lugar, como guardias, puertas y cercas. El resultado debe ser una evaluación de los controles de seguridad física externos. La mayoría de las compromisos de hoy en día comienzan con algún tipo de ataque de ingeniería social. Esto podría ser una llamada telefónica, un correo electrónico, un sitio web, un mensaje SMS, y así sucesivamente. Es importante probar cómo sus empleados manejan este tipo de situaciones. Este tipo de prueba a menudo se omite del alcance de una prueba de penetración principalmente porque implica principalmente probar a las personas en lugar de la tecnología. En la mayoría de los casos, la gerencia no está de acuerdo con este tipo de enfoque. Sin embargo, es importante obtener una visión del mundo real de los últimos métodos de ataque. El resultado de una prueba de ingeniería social debe ser evaluar el programa de concienciación de seguridad para que pueda mejorarlo. No debería ser identificar a las personas que no aprueban la prueba. Una de las herramientas de las que hablamos más adelante en un módulo posterior es el Social-Engineer Toolkit (SET), creado por Dave Kennedy. Esta es una gran herramienta para realizar campañas de prueba de ingeniería social. ∴



Programas de recompensas por errores

Los programas de recompensas por errores permiten a los investigadores de seguridad y a los probadores de penetración obtener reconocimiento (y a menudo compensación monetaria) por encontrar vulnerabilidades en sitios web, aplicaciones o cualquier otro tipo de sistemas. Empresas como Microsoft, Apple y Cisco e incluso instituciones gubernamentales como el Departamento de Defensa de EE. UU. (DoD) utilizan programas de recompensas por errores para recompensar a los profesionales de la seguridad cuando encuentran vulnerabilidades en sus sistemas. Muchas empresas de seguridad, como HackerOne, Bugcrowd, Intigriti y SynAck, proporcionan plataformas para que las empresas y los profesionales de la seguridad participen en programas de recompensas por errores. Estos programas son diferentes

de las pruebas de penetración tradicionales pero tienen un objetivo similar: encontrar vulnerabilidades de seguridad para permitir que la organización las solucione antes de que los atacantes maliciosos puedan explotar dichas vulnerabilidades. Hay diferentes consejos y recursos acerca de recompensas por errores en este [repositorio GitHub](https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties) (<https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties>)

Cuando se habla de métodos de prueba de penetración, es probable que escuche los términos entorno desconocido (anteriormente conocido como caja negra), entorno conocido (anteriormente conocido como caja blanca) y entorno parcialmente conocido (anteriormente conocido como caja gris) prueba. Estos términos se utilizan para describir la perspectiva desde la cual se realiza la prueba, así como la cantidad de información que se proporciona al probador:

md

Prueba de entorno desconocido

En una prueba de penetración de entorno desconocido, el probador generalmente solo recibe una cantidad muy limitada de información. Por ejemplo, el probador puede recibir solo los nombres de dominio y las direcciones IP que están dentro del alcance de un objetivo en particular. La idea de este tipo de limitación es que el probador comience con la perspectiva que un atacante externo podría tener. Típicamente, un atacante primero determinaría un objetivo y luego comenzaría a recopilar información sobre el objetivo, utilizando información pública y obteniendo más y más información para usar en ataques. El probador no tendría conocimiento previo de la organización y la infraestructura del objetivo. Otro aspecto de las pruebas de entorno desconocido es que a veces al personal de soporte de red del objetivo no se le da información sobre cuándo exactamente se está llevando a cabo la prueba. Esto permite que también se lleve a cabo un ejercicio de defensa y elimina el problema de que un objetivo se prepare para la prueba y no dé una visión del mundo real de cómo se ve realmente la postura de seguridad.

Este tipo de prueba suele ser la más difícil para el probador debido a la falta de información. Sin embargo, también es el más realista porque es el más cercano a cómo un atacante se acercaría al objetivo.

md

Prueba de entorno conocido

En una prueba de penetración de entorno conocido, el probador comienza con una cantidad significativa de información sobre la organización y su infraestructura. Normalmente, al probador se le proporcionarían cosas como diagramas de red, direcciones IP, configuraciones y un conjunto de credenciales de usuario. Si el alcance incluye una evaluación de la aplicación, el probador también podría recibir el código fuente de la aplicación objetivo. La idea de este tipo de prueba es identificar la mayor cantidad de agujeros de seguridad posible. En una prueba de entorno desconocido, el alcance puede ser solo identificar un camino hacia la organización y detenerse allí. Con las pruebas de entorno conocido, el alcance suele ser mucho más amplio e incluye auditorías de configuración de red interna y escaneo de computadoras de escritorio en busca de defectos. El tiempo y el dinero son factores decisivos típicos en la determinación de qué tipo de prueba de penetración completar. Si una empresa tiene preocupaciones específicas sobre una aplicación, un servidor o un segmento de la infraestructura, puede proporcionar información sobre ese objetivo específico para disminuir el alcance y la cantidad de tiempo dedicado a la prueba, pero aún así descubrir los resultados deseados. Con la sofisticación y las capacidades de los adversarios de hoy, es probable que la mayoría de las redes se vean comprometidas en algún momento, y un enfoque de caja blanca no es una mala opción.

md

Prueba de entorno parcialmente conocido

Una prueba de penetración de entorno parcialmente conocido es algo así como un enfoque híbrido entre pruebas de entorno desconocido y conocido. Con las pruebas de entorno parcialmente conocido, los probadores pueden recibir credenciales pero no documentación completa de la infraestructura de red. Esto permitiría a los probadores seguir proporcionando resultados de sus pruebas desde la perspectiva del punto de vista de un atacante externo. Teniendo en cuenta el hecho de que la mayoría de las infracciones comienzan en el cliente y se abren camino en toda la red, un buen enfoque sería un alcance donde los probadores comiencen en el interior de la red y tengan acceso a una máquina cliente. Luego podrían pivotar en toda la red para determinar cuál sería el impacto de una violación.

1.2. Explorant metodologies de proves de penetració

1.2.1. Descripció general

Les proves de penetració son molt més que hackejar la xarxa d'un client. Un enfocament descuidat donarà com a resultat resultats descuidats. És important seguir mètodes i estàndards ben coneguts per abordar les proves de penetració de manera organitzada i sistemàtica.

Ha de comprendre les principals metodologies i estàndards documentats per poder crear estratègies que aprofitin les seves fortaleses. Documentar el seu enfocament amb les metodologies i estàndards que va utilitzar també proporciona responsabilitat per a la nostra empresa i ajuda a que els nostres resultats siguin defensables en cas que sorgeixin problemes amb els nostres clients.

El procés de completar una prova de penetració varia segons molts factors. Les eines i tècniques utilitzades per avaluar la postura de seguretat d'una xarxa o sistema també varien. Les xarxes i sistemes que s'avaluen sovint són molt complexos. A causa d'això, és molt fàcil quan es realitza una prova de penetració per sortir de l'abast. Aquí és on entren les metodologies de prova. Proporcionen un marc perquè el provador de penetració segueixi per assegurar-se que la prova es completi de manera consistent. També proporcionen una manera de assegurar-se que la prova es completi d'una manera que sigui repetible i defensable.

1.2.2 Per què necessitem seguir una metodologia per a les proves de penetració?

Com s'ha esmentat anteriorment, l'abast és una raó per utilitzar una metodologia específica; no obstant això, hi ha moltes altres raons. Per exemple, quan realitza una prova de penetració per a un client, ha de mostrar que els mètodes que planeja utilitzar per a les proves són provats i veritables. En utilitzar una metodologia coneguda, pot proporcionar documentació d'un procediment especialitzat que ha estat utilitzat per moltes persones.

1.2.3. Consideracions de l'entorn de proves

Hi ha, per descomptat, una sèrie de tipus diferents de proves de penetració. Sovint es combinen en l'abast general d'una prova de penetració; no obstant això, també es poden realitzar com a proves individuals.

La següent és una llista d'algunes de les consideracions de l'entorn de proves més comunes per als tipus de proves de penetració d'avui:

Proves d'infraestructura de xarxa

La prova de la infraestructura de xarxa pot significar algunes coses. Per als fins d'aquest curs, diem que es centra en avaluar la postura de seguretat de la infraestructura de xarxa real i en com pot ajudar a defensar-se contra atacs. Això sovint inclou els commutadors, encaminadors, firewalls i recursos de suport, com l'autenticació, l'autorització i els servidors de comptabilitat (AAA) i els IPS. Una prova de penetració en la infraestructura sense fil a vegades pot incloure's en l'abast d'una prova d'infraestructura de xarxa. No obstant això, es realitzarien tipus addicionals de proves més enllà d'una avaluació de xarxa cablejada. Per exemple, un provador de seguretat sense fil intentaria ingressar a una xarxa a través de la xarxa sense fil, ja sigui mitjançant l'elusió dels mecanismes de seguretat o trencant els mètodes criptogràfics utilitzats per assegurar el trànsit. Provar la infraestructura sense fil ajuda una organització a determinar les debilitats en la implementació sense fil, així com l'exposició. Sovint inclou un mapa de calor detallat de la distribució de la senyal.

md

md

Proves basades en aplicacions

Aquest tipus de prova de penetració es centra en provar les debilitats de seguretat en les aplicacions empresarials. Aquestes debilitats poden incloure, entre altres, configuracions incorrectes, problemes de validació d'entrada, problemes d'injecció i fallades de lògica. Degut a que una aplicació web generalment es construeix en un servidor web amb una base de dades de suport, l'abast de les proves normalment inclou la base de dades també. No obstant això, es centra en obtenir accés a aquesta base de dades de suport a través de la compromís de l'aplicació web. Un gran recurs que mencionem diverses vegades en aquest llibre és el Projecte de seguretat d'aplicacions web obertes (OWASP).

md

Proves de penetració al núvol

Els proveïdors de serveis al núvol (CSP), com Azure, Amazon Web Services (AWS) i Google Cloud Platform (GCP), no tenen més remei que prendre's molt seriosament les seves responsabilitats de seguretat i compliment. Per exemple, Amazon va crear el [Model de responsabilitat compartida](<https://aws.amazon.com/compliance/shared-responsibility-model>) per descriure les responsabilitats dels clients d'AWS i les responsabilitats d'Amazon en detall.

La responsabilitat de la seguretat al núvol depèn del tipus de model de núvol (programari com a servei [SaaS], plataforma com a servei [PaaS] o infraestructura com a servei [IaaS]). Per exemple, amb IaaS, el client (consumidor de la núvol) és responsable de les dades, les aplicacions, el temps d'execució, el middleware, les màquines virtuals (VM), els contenidors i els sistemes operatius en les VM. Independentment del model utilitzat, la seguretat al núvol és responsabilitat tant del client com del proveïdor de la núvol. Aquests detalls s'han de resoldre abans de signar un contracte de computació al núvol. Aquests contractes varien segons els requisits de seguretat del client. Les consideracions inclouen la recuperació davant de desastres, els acords de nivell de servei (SLA), la integritat de les dades i el xifrat. Per exemple, es proporciona el xifrat d'extrem a extrem o només en el proveïdor de la núvol? A més, qui administra les claus de xifrat, el CSP o el client?

En general, desitja assegurar-se que el CSP tingui les mateixes capes de seguretat (lògica, física i administrativa) en el seu lloc que tindria per als serveis que controla. En realitzar proves de penetració al núvol, ha de comprendre què pot fer i què no pot fer. La majoria dels CSP tenen pautes detallades sobre com realitzar avaluacions de seguretat i proves de penetració al núvol. Independentment, hi ha moltes amenaces potencials quan les organitzacions es traslladen a un model de núvol. Per exemple, tot i que les seves dades estan al núvol, han de residir en una ubicació física en algun lloc. El seu proveïdor de la núvol ha d'acceptar per escrit proporcionar el nivell de seguretat requerit pels seus clients. Com a exemple, [la Política de suport al client d'AWS per a proves de penetració](<https://aws.amazon.com/security/penetration-testing>).

::: note atacs físics vs. enginyeria social Molts pentesters troben l'aspecte físic de les proves com allò més divertit perquè essencialment se'ls paga per irrompre en la instal·lació d'un objectiu. Aquest tipus de prova pot ajudar a exposar qualsevol debilitat en el perímetre físic, així com qualsevol mecanisme de seguretat que estigui en el seu lloc, com a guàrdies, portes i tanques. El resultat ha de ser una avaluació dels controls de seguretat física externs. La majoria de les compromisos d'avui en dia comencen amb algun tipus d'atac d'enginyeria social. Això podria ser una trucada telefònica, un correu electrònic, un lloc web, un missatge SMS, i així successivament. És important provar com els seus empleats manegen aquest tipus de situacions. Aquest tipus de prova sovint s'omet dels abast d'una prova de penetració principalment perquè implica principalment provar a les persones en lloc de la tecnologia. En la majoria dels casos, la gerència no està d'acord amb aquest tipus d'enfocament. No obstant això, és important obtenir una visió del món real dels últims mètodes d'atac. El resultat d'una prova d'enginyeria social ha d'ésser avaluar el programa de conscienciació de seguretat perquè pugui millorar-lo. No hauria de ser identificar a les persones que no aproven la prova. Una de les eines de les quals parlem més endavant en un mòdul posterior és el Social-Engineer Toolkit (SET), creat per Dave Kennedy. Aquesta és una gran eina per realitzar campanyes de prova d'enginyeria social. :::



Programes de recompenses per errors

Els programes de recompenses per errors permeten als investigadors de seguretat i als provadors de penetració obtenir reconeixement (i sovint compensació monetària) per trobar vulnerabilitats en llocs web, aplicacions o qualsevol altre tipus de sistemes. Empreses com Microsoft, Apple i Cisco i fins i tot institucions governamentals com el Departament de Defensa dels EUA (DoD) utilitzen programes de recompenses per errors per recompensar els professionals de la seguretat quan troben vulnerabilitats en els seus sistemes. Moltes empreses de seguretat, com HackerOne, Bugcrowd, Intigriti i SynAck, proporcionen plataformes perquè les empreses i els professionals de la seguretat participin en programes de recompenses per errors. Aquests programes són diferents de les proves de penetració tradicionals però tenen un objectiu similar: trobar vulnerabilitats de seguretat per permetre que l'organització les solucioni abans que els atacants maliciosos puguin explotar aquestes vulnerabilitats. Hi ha diferents consells i recursos sobre recompenses per errors en aquest [repositori GitHub \(https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties\)](https://github.com/The-Art-of-Hacking/h4cker/tree/master/bug-bounties).

Quan es parla de mètodes de prova de penetració, és probable que escolti els termes entorn desconegut (anteriorment conegut com a caixa negra), entorn conegut (anteriorment conegut com a caixa blanca) i entorn parcialment conegut (anteriorment conegut com a caixa gris) prova. Aquests termes s'utilitzen per descriure la perspectiva des de la qual es realitza la prova, així com la quantitat d'informació que es proporciona al provador:

md

Prova d'entorn desconegut

En una prova de penetració d'entorn desconegut, el provador generalment només rep una quantitat molt limitada d'informació. Per exemple, el provador pot rebre només els noms de domini i les adreces IP que estan dins de l'abast d'un objectiu en particular. La idea d'aquest tipus de limitació és que el provador comenci amb la perspectiva que un atacant extern podria tenir. Típicament, un atacant primer determinaria un objectiu i després començaria a recopilar informació sobre l'objectiu, utilitzant informació pública i obtenint més i més informació per utilitzar en atacs. El provador no tindria coneixement previ de l'organització i la infraestructura de l'objectiu. Un altre aspecte de les proves d'entorn desconegut és que a vegades al personal de suport de xarxa de l'objectiu no se li dona informació sobre quan exactament s'està duent a terme la prova. Això permet que també es dugui a terme un exercici de defensa i elimina el problema que un objectiu es prepari per a la prova i no doni una visió del món real de com es veu realment la postura de seguretat.

Aquest tipus de prova sol ser la més difícil per al provador a causa de la manca d'informació. No obstant això, també és el més realista perquè és el més proper a com un atacant s'acostaria a l'objectiu.

md

Prova d'entorn conegut

En una prova de penetració d'entorn conegut, el provador comença amb una quantitat significativa d'informació sobre l'organització i la seva infraestructura. Normalment, al provador se li proporcionarien coses com diagrames de xarxa, adreces IP, configuracions i un conjunt de credencials d'usuari. Si l'abast inclou una avaluació de l'aplicació, el provador també podria rebre el codi font de l'aplicació objectiu. La idea d'aquest tipus de prova és identificar la major quantitat de forats de seguretat possible. En una prova d'entorn desconegut, l'abast pot ser només identificar un camí cap a l'organització i aturar-se allà. Amb les proves d'entorn conegut, l'abast sol ser molt més ampli i inclou auditories de configuració de xarxa interna i escaneig d'ordinadors d'escriptori per defectes. El temps i els diners són factors decisius típics en la determinació de quin tipus de prova de penetració completar. Si una empresa té preocupacions específiques sobre una aplicació, un servidor o un segment de la infraestructura, pot proporcionar informació sobre aquest objectiu específic per disminuir l'abast i la quantitat de temps dedicat a la prova, però encara descobrir els resultats desitjats. Amb la sofisticació i les capacitats dels adversaris d'avui, és probable que la majoria de les xarxes es vegin compromeses en algun moment, i un enfocament de caixa blanca no és una mala opció.

md

Prova d'entorn parcialment conegut

Una prova de penetració d'entorn parcialment conegut és quelcom així com un enfocament híbrid entre proves d'entorn desconegut i conegut. Amb les proves d'entorn parcialment conegut, els provadors poden rebre credencials però no documentació completa de la infraestructura de xarxa. Això permetria als provadors seguir proporcionant resultats de les

seves proves des de la perspectiva del punt de vista d'un atacant extern. Tenint en compte el fet que la majoria de les infraccions comencen al client i s'obren camí a tota la xarxa, un bon enfocament seria un abast on els provadors comencin a l'interior de la xarxa i tinguin accés a una màquina client. Llavors podrien pivotar a tota la xarxa per determinar quin seria l'impacte d'una violació.

1.2.4. Practice - Types of Penetration Tests

1.2.5 Surveying Different Standards and Methodologies

There are a number of penetration testing methodologies that have been around for a while and continue to be updated as new threats emerge.

The following is a list of some of the most common penetration testing methodologies and other standards: