




> **SAD_**
SEGURIDAD
Y ALTA
DISPONIBILIDAD

1.1. Understanding Ethical Hacking & Penetration Testing



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>)

1.1. Understanding Ethical Hacking & Penetration Testing

1.1. Comprendiendo el hacking ético y las pruebas de penetración

1.1. Comprendre el hacking ètic i les proves de penetració

1.1.1. Overview

1.1.1. Descripción general

1.1.1. Descripció general

As a refresher, the term ethical hacker describes a person who acts as an attacker and evaluates the security posture of a computer network for the purpose of minimizing risk. The NIST Computer Security Resource Center (CSRC) defines a hacker as an "unauthorized user who attempts to or gains access to an information system." Now, we all know that the term hacker has been used in many different ways and has many different definitions. Most people in a computer technology field would consider themselves hackers based on the simple fact that they like to tinker. This is obviously not a malicious thing. So, the key factor here in defining ethical versus malicious hacking is that the latter involves malicious intent. The permission to attack or permission to test is crucial and what will keep you out of trouble! This permission to attack is often referred to as "the scope" of the test (what you are allowed and not allowed to test). More on this later in this module.

A modo de recordatorio, el término hacker ético describe a una persona que actúa como atacante y evalúa la postura de seguridad de una red informática con el propósito de minimizar el riesgo. El Centro de Recursos de Seguridad Informática (CSRC) del Instituto Nacional de Estándares y Tecnología (NIST) define a un hacker como un "usuario no autorizado que intenta o accede a un sistema de información". Ahora, todos sabemos que el término hacker se ha utilizado de muchas maneras diferentes y tiene muchas definiciones diferentes. La mayoría de las personas en un campo de tecnología informática se considerarían hackers en base al simple hecho de que les gusta trastear. Obviamente, esto no es algo malicioso. Por lo tanto, el factor clave aquí para definir el hacking ético frente al no ético es que este último implica una intención maliciosa. ¡La autorización para atacar o la autorización para probar es crucial y lo que te mantendrá fuera de problemas! Esta autorización para atacar a menudo se denomina "el alcance" de la prueba (lo que se le permite y no se le permite probar). Más sobre esto más adelante en este módulo.

Com a recordatori, el terme hacker ètic descriu una persona que actua com a atacant i avalua la postura de seguretat d'una xarxa informàtica amb la finalitat de minimitzar el risc. El Centre de Recursos de Seguretat Informàtica (CSRC) de l'Institut Nacional d'Estàndards i Tecnologia (NIST) defineix a un hacker com un "usuari no autoritzat que intenta o accedeix a un sistema d'informació". Ara, tots sabem que el terme hacker s'ha utilitzat de moltes maneres diferents i té moltes definicions diferents. La majoria de les persones en un camp de tecnologia informàtica es considerarien hackers en base al simple fet que els agrada trastear. Òbviament, això no és quelcom maliciós. Per tant, el factor clau aquí per definir el hacking ètic front al no ètic és que aquest últim implica una intenció maliciosa. L'autorització per atacar o l'autorització per provar és crucial i el que et mantindrà fora de problemes! Aquesta autorització per atacar sovint es denomina "l'abast" de la prova (el que se li permet i no se li permet provar). Més sobre això més endavant en aquest mòdul.

A security researcher looking for vulnerabilities in products, applications, or web services is considered an ethical hacker if he or she responsibly discloses those vulnerabilities to the vendors or owners of the targeted research. However, the same type of "research" performed by someone who then uses the same vulnerability to gain unauthorized access to a target network/system would be considered a malicious hacker. We could even go so far as to say that someone who finds a vulnerability and discloses it publicly without working with a vendor is considered a malicious hacker – because this could lead to the compromise of networks/systems by others who use this information in a malicious way.

Un investigador de seguridad que busca vulnerabilidades en productos, aplicaciones o servicios web se considera un hacker ético si divulga responsablemente esas vulnerabilidades a los proveedores o propietarios de la investigación objetivo. Sin embargo, el mismo tipo de "investigación" realizada por alguien que luego usa la misma vulnerabilidad para obtener acceso no autorizado a una red / sistema objetivo se consideraría un hacker no ético. Incluso podríamos ir tan lejos como para decir que alguien que encuentra una vulnerabilidad y la divulga públicamente sin trabajar con un proveedor se considera un hacker no ético, porque esto podría conducir a la compromiso de redes / sistemas por otros que usan esta información de manera maliciosa.

Un investigador de seguretat que busca vulnerabilitats en productes, aplicacions o serveis web es considera un hacker ètic si divulga responsablement aquestes vulnerabilitats als proveïdors o propietaris de la investigació objectiu. No obstant això, el mateix tipus d "investigació" realitzada per algú que després utilitza la mateixa vulnerabilitat per obtenir accés no autoritzat a una xarxa / sistema objectiu es consideraria un hacker no ètic. Fins i tot podríem anar tan lluny com per dir que algú que troba una vulnerabilitat i la divulga públicament sense treballar amb un proveïdor es considera un hacker no ètic, perquè això podria conduir a la compromís de xarxes / sistemes per altres que utilitzen aquesta informació de manera maliciosa.

The truth is that as an ethical hacker, you use the same tools to find vulnerabilities and exploit targets as do md:no-line-numberstical hackers. However, as an ethical hacker, you would typically report your findings to the vendor or customer you are helping to make the network more secure. You would also try to avoid performing any tests or exploits that might be destructive in nature.

La realidad es que como hacker ético, utilizas las mismas herramientas para encontrar vulnerabilidades y explotar objetivos que los hackers no éticos. Sin embargo, como hacker ético, normalmente informarías tus hallazgos al proveedor o cliente al que estás ayudando a hacer que la red sea más segura. También intentarías evitar realizar pruebas o exploits que puedan ser destructivos por naturaleza.

La realitat es que com a hacker ètic, utilitzeu les mateixes eines per trobar vulnerabilitats i explotar objectius que els hackers no ètics. No obstant això, com a hacker ètic, normalment informàrieu els vostres descobriments al proveïdor o client al qual esteu ajudant a fer que la xarxa sigui més segura. També intentaríeu evitar realitzar proves o exploits que puguin ser destructius per naturalesa.

An ethical hacker's goal is to analyze the security posture of a network's or system's infrastructure in an effort to identify and possibly exploit any security weaknesses found and then determine if a compromise is possible. This process is called security penetration testing or ethical hacking.

Un hacker ético tiene como objetivo analizar la postura de seguridad de la infraestructura de una red o sistema en un esfuerzo por identificar y posiblemente explotar cualquier debilidad de seguridad encontrada y luego determinar si es posible un compromiso. Este proceso se llama prueba de penetración de seguridad o hacking ético.

Un hacker ètic te com objectiu analitzar la postura de seguretat de la infraestructura d'una xarxa o sistema en un esforç per identificar i possiblement explotar qualsevol debilitat de seguretat trobada i després determinar si és possible un compromís. Aquest procés es diu prova de penetració de seguretat o hacking ètic.

**TIP**

Hacking is NOT a Crime ([hackingisnotacrime.org](https://www.hackingisnotacrime.org/) (<https://www.hackingisnotacrime.org/>)) is a nonprofit organization that attempts to raise awareness about the pejorative use of the term hacker. Historically, hackers have been portrayed as evil or illegal. Luckily, a lot of people already know that hackers are curious individuals who want to understand how things work and how to make them more secure. The organization's goal is to educate the public about the positive aspects of hacking and to dispel the negative connotations associated with the term.

Hackear NO es un crimen ([hackingisnotacrime.org](https://www.hackingisnotacrime.org/) (<https://www.hackingisnotacrime.org/>)) es una organización sin fines de lucro que intenta crear conciencia sobre el uso peyorativo del término hacker. Históricamente, los hackers han sido retratados como malvados o ilegales. Afortunadamente, mucha gente ya sabe que los hackers son personas curiosas

que quieren entender cómo funcionan las cosas y cómo hacerlas más seguras. El objetivo de la organización es educar al público sobre los aspectos positivos del hacking y disipar las connotaciones negativas asociadas con el término.

Hackear NO es un crimen ([hackingisnotacrime.org](https://www.hackingisnotacrime.org/) (<https://www.hackingisnotacrime.org/>)) es una organización sin ánimo de lucro que intenta crear conciencia sobre el uso peyorativo del término hacker. Históricamente, los hackers han estado retratados como malvados o ilegales. Afortunadamente, mucha gente ya sabe que los hackers son personas curiosas que quieren entender cómo funcionan las cosas y cómo hacerlas más seguras. El objetivo de la organización es educar al público sobre los aspectos positivos del hacking y disipar las connotaciones negativas asociadas con el término.

1.1.2. Why Do We Need to Do Penetration Testing?

1.1.2. ¿Por qué necesitamos hacer pruebas de penetración?

1.1.2. Per què necessitem fer proves de penetració?

So, why do we need penetration testing? Well, first of all, as someone who is responsible for securing and defending a network/system, you want to find any possible paths of compromise before the bad guys do. For years we have developed and implemented many different defensive techniques (for instance, antivirus, firewalls, intrusion prevention systems [IPSs], anti-malware). We have deployed defense-in-depth as a method to secure and defend our networks. But how do we know if those defenses really work and whether they are enough to keep out the bad guys? How valuable is the data that we are protecting, and are we protecting the right things? These are some of the questions that should be answered by a penetration test. If you build a fence around your yard with the intent of keeping your dog from getting out, maybe it only needs to be 4 feet tall. However, if your concern is not the dog getting out but an intruder getting in, then you need a different fence – one that would need to be much taller than 4 feet. Depending on what you are protecting, you might also want razor wire on the top of the fence to deter the bad guys even more. When it comes to information security, we need to do the same type of assessments on our networks and systems. We need to determine what it is we are protecting and whether our defenses can hold up to the threats that are imposed on them. This is where penetration testing comes in. Simply implementing a firewall, an IPS, anti-malware, a VPN, a web application firewall (WAF), and other modern security defenses isn't enough. You also need to test their validity. And you need to do this on a regular basis. As you know, networks and systems change constantly. This means the attack surface can change as well, and when it does, you need to consider reevaluating the security posture by way of a penetration test.

Entonces, ¿por qué necesitamos pruebas de penetración? Bueno, en primer lugar, como alguien que es responsable de asegurar y defender una red / sistema, desea encontrar cualquier posible camino de compromiso antes de que lo hagan los tipos malos. Durante años hemos desarrollado e implementado muchas técnicas defensivas diferentes (por ejemplo, antivirus, firewalls, sistemas de prevención de intrusiones [IPS], anti-malware). Hemos implementado la defensa en profundidad como un método para asegurar y defender nuestras redes. Pero, ¿cómo sabemos si esas defensas realmente funcionan y si son suficientes para mantener alejados a los tipos malos? ¿Qué tan valiosos son los datos que estamos protegiendo y estamos protegiendo las cosas correctas? Estas son algunas de las preguntas que debería responder una prueba de penetración. Si construye una cerca alrededor de su patio con la intención de evitar que su perro salga, tal vez solo necesite tener 4 pies de altura. Sin embargo, si su preocupación no es que el perro salga sino que un intruso entre, entonces necesita una cerca diferente, una que necesitaría ser mucho más alta que 4 pies. Dependiendo de lo que esté protegiendo, es posible que también desee alambre de púas en la parte superior de la cerca para disuadir aún más a los tipos malos. Cuando se trata de seguridad de la información, necesitamos hacer el mismo tipo de evaluaciones en nuestras redes y sistemas. Necesitamos determinar qué es lo que estamos protegiendo y si nuestras defensas pueden resistir las amenazas que se les imponen. Aquí es donde entran las pruebas de penetración. Simplemente implementar un firewall, un IPS, anti-malware, una VPN, un firewall de aplicaciones web (WAF) y otras defensas de seguridad modernas no es suficiente. También debe probar su validez. Y necesitas hacer esto de forma regular. Como saben, las

redes y los sistemas cambian constantemente. Esto significa que la superficie de ataque también puede cambiar, y cuando lo hace, debe considerar reevaluar la postura de seguridad mediante una prueba de penetración.

Llavors, per què necessitem proves de penetració? Bé, en primer lloc, com a algú que és responsable d'assegurar i defensar una xarxa / sistema, desitja trobar qualsevol possible camí de compromís abans que ho facin els tipus dolents. Durant anys hem desenvolupat i implementat moltes tècniques defensives diferents (per exemple, antivirus, firewalls, sistemes de prevenció d'intrusions [IPS], anti-malware). Hem implementat la defensa en profunditat com un mètode per assegurar i defensar les nostres xarxes. Però, com sabem si aquestes defenses realment funcionen i si són suficients per mantenir allunyats els tipus dolents? Quan valuosos són les dades que estem protegint i estem protegint les coses correctes? Aquestes són algunes de les preguntes que hauria de respondre una prova de penetració. Si construeix una tanca al voltant del seu pati amb la intenció d'evitar que el seu gos surti, potser només necessita tenir 4 peus d'altura. No obstant això, si la seva preocupació no és que el gos surti sinó que un intrús entri, llavors necessita una tanca diferent, una que necessitaria ser molt més alta que 4 peus. Depenent del que estigui protegint, és possible que també vulgueu filferro a la part superior de la tanca per dissuadir encara més als tipus dolents. Quan es tracta de seguretat de la informació, necessitem fer el mateix tipus d'avaluacions a les nostres xarxes i sistemes. Necessitem determinar què és el que estem protegint i si les nostres defenses poden resistir les amenaces que se'ls imposen. Aquí és on entren les proves de penetració. Simplement implementar un firewall, un IPS, anti-malware, una VPN, un firewall d'ap

1.1.3 Lab - Researching PenTesting Careers 1.1.3 Laboratorio - Investigación de carreras de PenTesting 1.1.3 Laboratori - Investigació de carreres de PenTesting

It is important for you to understand the employment landscape and the different roles and responsibilities that cybersecurity professions include. A good general reference to explore for descriptions of different job roles is The National Initiative for Cybersecurity Careers and Studies (NICCS) [Cyber Career Pathways Tool \(https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool\)](https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool) . It offers a visual way to discover and compare different job roles in our profession.

Es importante que comprendas el panorama laboral y las diferentes funciones y responsabilidades que incluyen las profesiones de ciberseguridad. Una buena referencia general para explorar las descripciones de los diferentes roles de trabajo es la The National Initiative for Cybersecurity Careers and Studies (NICCS) [Cyber Career Pathways Tool \(https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool\)](https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool) . Ofrece una forma visual de descubrir y comparar diferentes roles de trabajo en nuestra profesión.

És important que entengueu el panorama laboral i les diferents funcions i responsabilitats que inclouen les professions de ciberseguretat. Una bona referència general per explorar les descripcions dels diferents rols de treball és la The National Initiative for Cybersecurity Careers and Studies (NICCS) [Cyber Career Pathways Tool \(https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool\)](https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool) . Ofereix una forma visual de descobrir i comparar diferents rols de treball en la nostra professió.

1.1.3. Activity Lab - Researching PenTesting Careers

1.1.3. Actividad Laboratorio - Investigación de carreras de PenTesting

1.1.3. Activitat Laboratori - Investigació de carreres de PenTesting

1.1.4. Threat Actors

1.1.4. Atacantes

1.1.4. Atacants

Before you can understand how an ethical hacker or penetration tester can mimic a threat actor (or malicious attacker), you need to understand the different types of threat actors. The following are the most common types of malicious attackers we see today. Select each for more information.

Abans de poder comprendre cómo un hacker étic o un probador de penetració puede imitar a un actor de amenazas (o atacante malicioso), debe comprender los diferentes tipos de actores de amenazas. Los siguientes son los tipos más comunes de atacantes maliciosos que vemos hoy en día. Seleccione cada uno para obtener más información.

Abans de poder comprendre com un hacker ètic o un provador de penetració pot imitar un actor de amenaces (o atacant maliciós), heu de comprendre els diferents tipus d'actors de amenaces. Els següents són els tipus més comuns d'atacants maliciosos que veiem avui en dia. Seleccioneu cadascun per obtenir més informació.

md

****Organized Crime****

Several years ago, the cybercrime industry took over the number-one spot, previously held by the drug trade, for the most profitable illegal industry. As you can imagine, it has attracted a new type of cybercriminal. Just as it did back in the days of Prohibition, organized crime goes where the money is. Organized crime consists of very well-funded and motivated groups that will typically use any and all of the latest attack techniques. Whether that is ransomware or data theft, if it can be monetized, organized crime will use it.

****Crimen organizado****

Hace varios años, la industria del cibercrimen se apoderó del primer lugar, anteriormente ocupado por el narcotráfico, por la industria ilegal más rentable. Como puedes imaginar, ha atraído a un nuevo tipo de ciberdelincuente. Tal como lo hizo en los días de la Prohibición, el crimen organizado va donde está el dinero. El crimen organizado consiste en grupos muy bien financiados y motivados que típicamente usarán todas y cada una de las últimas técnicas de ataque. Ya sea ransomware o robo de datos, si se puede monetizar, el crimen organizado lo usará.

****Crim organitzat****

Fa diversos anys, la indústria del cibercrimen es va apoderar del primer lloc, anteriorment ocupat pel narcotràfic, per la indústria il·legal més rendible. Com podeu imaginar, ha atret a un nou tipus de ciberdelinqüent. Tal com ho va fer en els dies de la Prohibició, el crim organitzat va on està el diner. El crim organitzat consisteix en grups molt ben finançats i motivats que típicament utilitzaran totes i cadascuna de les últimes tècniques d'atac. Ja sigui ransomware o robatori de dades, si es pot monetitzar, el crim organitzat ho utilitzarà.

md

****Hacktivists****

This type of threat actor is not motivated by money. Hacktivists are looking to make a point or to further their beliefs, using cybercrime as their method of attack. These types of attacks are often carried out by stealing sensitive data and then revealing it to the public for the purpose of embarrassing or financially affecting a target.

****Hacktivistas****

Este tipo de actor de amenazas no está motivado por el dinero. Los hacktivistas buscan hacer un punto o promover sus creencias, utilizando el cibercrimen como su método de ataque. Estos tipos de ataques se llevan a cabo a menudo robando datos sensibles y luego revelándolos al público con el propósito de avergonzar o afectar financieramente a un objetivo.

****Hacktivistes****

Aquest tipus d'actor de amenaces no està motivat pel diner. Els hacktivistes busquen fer un punt o promoure les seves creences, utilitzant el cibercrim com el seu mètode d'atac. Aquests tipus d'atacs es duen a terme sovint robant dades sensibles i després revelant-les al públic amb la finalitat d'avergonyir o afectar financerament a un objectiu.

md

****State-Sponsored Attackers****

Cyber war and cyber espionage are two terms that fit into this category. Many governments around the world today use

cyber attacks to steal information from their opponents and cause disruption. Many believe that the next Pearl Harbor will occur in cyberspace. That's one of the reasons the United States declared cyberspace to be one of the operational domains that U.S. forces would be trained to defend.

****Atacantes patrocinados por los estados****

La guerra cibernética y el espionaje cibernético son dos términos que se ajustan a esta categoría. Muchos gobiernos de todo el mundo utilizan hoy ataques cibernéticos para robar información de sus oponentes y causar interrupciones. Muchos creen que el próximo Pearl Harbor ocurrirá en el ciberespacio. Esa es una de las razones por las que Estados Unidos declaró que el ciberespacio sería uno de los dominios operativos para los que las fuerzas estadounidenses estarían capacitadas para defenderse.

****Atacants patrocinats pels estats****

La guerra cibernètica i l'espionatge cibernètic són dos termes que s'ajusten a aquesta categoria. Molts governs d'arreu del món utilitzen avui atacs cibernètics per robar informació dels seus oponents i causar interrupcions. Molts creuen que el proper Pearl Harbor ocorrerà en el ciberespai. Aquesta és una de les raons per les quals els Estats Units van declarar que el ciberespai seria un dels dominis operatius per als quals les forces estatunidenques estarien capacitades per defensar-se.

md

****Insider Threats****

An insider threat is a threat that comes from inside an organization. The motivations of these types of actors are normally different from those of many of the other common threat actors. Insider threats are often normal employees who are tricked into divulging sensitive information or mistakenly clicking on links that allow attackers to gain access to their computers. However, they could also be malicious insiders who are possibly motivated by revenge or money.

****Amenazas internas****

Una amenaza interna es una amenaza que proviene de dentro de una organización. Las motivaciones de estos tipos de actores normalmente son diferentes de las de muchos de los otros actores de amenazas comunes. Las amenazas internas a menudo son empleados normales que son engañados para divulgar información confidencial o hacer clic por error en enlaces que permiten a los atacantes acceder a sus computadoras. Sin embargo, también podrían ser insiders maliciosos que posiblemente estén motivados por la venganza o el dinero.

****Amenaces internes****

Una amenaça interna és una amenaça que prové de dins d'una organització. Les motivacions d'aquests tipus d'actors normalment són diferents de les de molts dels altres actors de amenaces comuns. Les amenaces internes sovint són empleats normals que són enganyats per divulgar informació confidencial o fer clic per error en enllaços que permeten als atacants accedir als seus ordinadors. No obstant això, també podrien ser insiders maliciosos que possiblement estiguin motivats per la venjança o el diner.