Selezione pubblica per esami a una (1) unità di personale a tempo determinato, area dei funzionari, con contratto di 12 mesi, eventualmente prorogabile, a tempo pieno (36 ore settimanali), presso il Dipartimento di Matematica del Politecnico di Milano; 2025_PTA_TD_D_DMAT_1

Prova scritta 1

Traccia 1

Un Dipartimento universitario gestisce una rete complessa che include ambienti eterogenei (es. laboratori studenti, sale riunioni, uffici riservati ai docenti) e server su cui sono memorizzati dati sensibili (ricerca, didattica, amministrazione). Parte della rete dipartimentale utilizza tecnologia Wi-Fi e il Dipartimento consente l'uso di dispositivi personali (BYOD). Alcuni dati sono scambiati tra la sede del Dipartimento e utenti tramite internet.

Il Candidato illustri gli elementi di un'architettura di sicurezza di rete che protegga in modo efficace le risorse del Dipartimento. Nella risposta:

- Descriva una strategia di segmentazione e controllo degli accessi informatici
- Illustri come implementare sistemi di rilevamento e risposta alle intrusioni
- Spieghi come e dove utilizzerebbe la crittografia (es. per protezione dati in transito, VPN, storage, Wi-Fi, Email)
- Analizzi i rischi legati al BYOD e come possano essere mitigati in questo contesto

Traccia 2

Il Candidato illustri il modello OSI e il protocollo TCP/IP descrivendone i livelli e le principali funzioni. Spieghi come questi si applichino nella gestione di una rete LAN Dipartimentale, includendo:

- i dispositivi principali (switch, router, firewall) e le loro funzioni nei vari livelli
- la segmentazione di rete e l'uso delle VLAN
- l'integrazione di Microsoft Remote Desktop Services (RDS) in un'infrastruttura di rete
- il funzionamento di RDS, i ruoli principali (RD Session Host, RD Gateway, RD Licensing) e le best practice per garantire sicurezza e scalabilità in ambienti multi-utente

Traccia 3

Il Candidato descriva nel dettaglio le attività relative alla manutenzione evolutiva di un sito web sviluppato con un CMS (es. WordPress). Illustri il processo di aggiornamento del core del CMS, dei temi e dei plugin, evidenziando i rischi associati (compatibilità, sicurezza, malfunzionamenti) e le buone pratiche per la gestione in ambienti di produzione. Porti esempi concreti di strumenti o workflow adottabili per automatizzare parte del processo.

Selezione pubblica per esami a una (1) unità di personale a tempo determinato, area dei funzionari, con contratto di 12 mesi, eventualmente prorogabile, a tempo pieno (36 ore settimanali), presso il Dipartimento di Matematica del Politecnico di Milano; 2025_PTA_TD_D_DMAT_1.

Prova scritta 2 (Estratta)

Traccia 1

Un Dipartimento universitario ha sviluppato un'applicazione web che gestisce iscrizione ad eventi e scambio di documenti tra studenti e docenti. L'applicazione non è mai stata sottoposta a un security assessment. Alcune funzioni prevedono l'invio di email contenenti link di accesso a documenti personali e lo scambio di file PDF firmati digitalmente.

Il Candidato analizzi i rischi principali legati alla sicurezza dell'applicazione web. Nella risposta:

- Identifichi e descriva almeno due vulnerabilità critiche comuni nelle web application (esempi concreti e impatto)
- Spieghi il ruolo della crittografia nella protezione dei dati sensibili (in transito, a riposo e nei file PDF firmati)
- Illustri le caratteristiche salienti di un sistema sicuro di gestione delle sessioni e delle identità (es. gestione identità in SSO)
- Illustri le procedure da implementare per garantire il continuo aggiornamento del framework applicativo (front-end, back-end) e/o CMS utilizzato

Traccia 2

Il Candidato descriva le principali caratteristiche architetturali e funzionali di Microsoft Windows 11 Professional, Linux (es. Ubuntu Server) e macOSX. In particolare ci si riferisca ai seguenti punti nell'ottica di fornire supporto ad un'utenza dipartimentale eterogenea:

- la gestione dei processi e dei servizi
- il file system e i permessi di accesso
- il supporto alle reti TCP/IP
- l'integrazione in una rete dipartimentale basata su reti federate

Traccia 3

Il Candidato analizzi le principali problematiche tecniche e normative legate all'utilizzo dei cookie nei siti web, con particolare riferimento al GDPR. Spieghi le differenze tra cookie tecnici, analitici e di profilazione, e descriva una strategia tecnica per il corretto blocco preventivo e la gestione del consenso, citando eventuali librerie o soluzioni di implementazione.

Selezione pubblica per esami a una (1) unità di personale a tempo determinato, area dei funzionari, con contratto di 12 mesi, eventualmente prorogabile, a tempo pieno (36 ore settimanali), presso il Dipartimento di Matematica del Politecnico di Milano; 2025_PTA_TD_D_DMAT_1.

Prova scritta 3

Traccia 1

Un Dipartimento universitario ha parzialmente migrato i propri sistemi in cloud (es. Office 365, AWS, Azure), mantenendo altri servizi su infrastruttura on-premise (es. server LDAP, NAS, archivi documentali). Gli studenti accedono da remoto tramite VPN, e alcuni dati sono altamente sensibili (es. dati di ricerca, testi di esame).

Il Candidato illustri gli elementi di una strategia di governance della sicurezza informatica per questa architettura ibrida. Nella risposta:

- Descriva un modello di gestione delle identità e degli accessi (IAM, SSO, MFA)
- Illustri le principali differenze nella protezione dei dati tra ambienti cloud e on-premise.
- Analizzi il ruolo della crittografia end-to-end per garantire riservatezza e compliance (es. GDPR)
- Illustri elementi di garanzia della conservazione dei dati (es. Data retention policy)

Traccia 2

Il Candidato illustri il funzionamento di Active Directory Domain Services (AD DS) e Active Directory Federation Services (AD FS) in un ambiente complesso. Nella risposta si illustrino:

- la struttura gerarchica di AD (foresta, domini, unità organizzative)
- la gestione delle identità, dei criteri di gruppo (GPO) e della delega di controllo
- il ruolo di AD FS nella federazione dell'identità e nell'autenticazione Single Sign-On (SSO), anche in ambienti ibridi (on-premise e cloud)
- vantaggi e rischi nell'utilizzo di AD FS rispetto a metodi di autenticazione tradizionali

Traccia 3

Il Candidato valuti criticamente l'utilizzo di strumenti basati su intelligenza artificiale per la generazione automatica di contenuti web (testi, immagini, video). Illustri i vantaggi in termini di produttività, ma anche i limiti tecnici e i potenziali problemi etici o di qualità (es. plagio, accuratezza, bias). Descriva come si può integrare l'IA in un flusso di lavoro editoriale mantenendo un controllo umano sui contenuti pubblicati.

PROVA ORALE 1

Il/la candidato/a risponda alle seguenti domande

1. In un sistema basato su Ubuntu Linux, quale comando si utilizza per installare un pacchetto software e quale comando per aggiornarlo?

2. Cos'è il GDPR e come influisce sulla gestione dei dati personali in un'università?

3. Quali sono le differenze nella programmazione web Server Side e Client Side?

4. Il/la candidato/a legga e traduca il seguente brano

Prova di conoscenza lingua inglese

Traccia 1

Il Candidato legga e traduca il testo seguente:

What is Two-Step Authentication

Passwords are the de-facto standard for logging in on the web, but they're relatively easy to break. Even if you make good passwords and change them regularly, they need to be stored wherever you're logging in, and a server breach can leak them. There are three ways to identify a person, things they are, things they have, and things they know.

Something You Are

There are a lot of properties that are unique to each user and can be used to identify them. The most popular is fingerprints, but retinas, voice, DNA, or anything else specific to an individual will work. This is called biometric information because these pieces of information all belong to a person's biology.

Biometric factors are interesting because they are not easily forged and the user can never lose or forget them. However, biometric authentication is tricky because a lost fingerprint can never be replaced. If hackers were to gain access to a database of fingerprints, there is no way that users could reset them or get a new set.

Something You Have

Also known as the possession factor, users can be identified by the devices which they carry. Traditionally, a company that wanted to enable two-step authentication would distribute secure keychain fobs to users. The keychain fobs would display a new number every 30 seconds, and that number would be needed to be typed along with the password every time a user logged in.

Modern two-step authentication more frequently relies on a user's smartphone than on a new piece of hardware. One common model of this uses SMS in order to provide an easy second factor. When the user enters their password, they are sent a text message with a unique code. By entering that code, after the password, they supposedly prove that they also have their phone. Unfortunately, SMS is not a secure communication channel, so smartphone apps and plugins have been developed to create that secure channel.

Something You Know

The most familiar form of authentication is the knowledge factor, or password. As old as Open Sesame, passwords have long been a standard for anonymous authentication. In order for a knowledge factor to work, both parties need to know the password, but other parties must not be able to find or guess it.

The first challenge is in exchanging the password with the trusted party safely. On the web, when you register for a new site, your password needs to be sent to that site's servers and might be intercepted in the process (which is why you should always check for SSL when registering or logging in — HTTPS).

Once the password has been received, it must be kept secret. The user shouldn't write it down or use it anywhere else, and the site needs to carefully guard its database to ensure that hackers can't access the passwords.

Finally, the password needs to be verified. When a user visits the site, they need to be able to provide the password and have it verified against the stored copy. This exchange can also be intercepted (and so should always be done over SSL — HTTPS) and exposes the user to another risk.

PROVA ORALE 2

Il/la candidato/a risponda alle seguenti domande

1. In Linux, quale comando si utilizza per cambiare i permessi di un file e cosa rappresentano i numeri utilizzati con il comando chmod?

2. Nel GDPR cosa si intende per Data Breach e quali sono le linee guida di gestione dello stesso?

3. Qual è la differenza tra i protocolli HTTP e HTTPS?

4. Il/la candidato/a legga e traduca il seguente brano

Prova di conoscenza lingua inglese

Traccia 2

Il Candidato legga e traduca il testo seguente:

Hardening WordPress

Security in WordPress is taken very seriously, but as with any other system there are potential security issues that may arise if some basic security precautions aren't taken. This article will go through some common forms of vulnerabilities, and the things you can do to help keep your WordPress installation secure.

What is Security?
Fundamentally, security is not about perfectly secure systems. Such a thing might well be impractical, or impossible to find and/or maintain. What security is though is risk reduction, not risk elimination. It's about employing all the appropriate controls available to you, within reason, that allow you to improve your overall posture reducing the odds of making yourself a target, subsequently getting hacked.

Website Hosts
Often, a good place to start when it comes to website security is your hosting environment. Today, there are a number of options available to you, and while hosts offer security to a certain level, it's important to understand where their responsibility ends and yours begins. Here is a good article explaining the complicated dynamic between web hosts and the security of your website. A secure server protects the privacy, integrity, and availability of the resources under the server administrator's control.

Qualities of a trusted web host might include:
Readily discusses your security concerns and which security features and processes they offer with their hosting.
Provides the most recent stable versions of all server software.
Provides reliable methods for backup and recovery.
Decide which security you need on your server by determining the software and data that needs to be secured. The rest of this guide will help you with this.

Website Applications
It's easy to look at web hosts and pass the responsibility of security to them, but there is a tremendous amount of security that lies on the website owner as well. Web hosts are often responsible for the infrastructure on which your website sits, they are not responsible for the application you choose to install.

To understand where and why this is important you must understand how websites get hacked, Rarely is it attributed to the infrastructure, and most often attributed to the application itself (i.e., the environment you are responsible for).

Security Themes
Keep in mind some general ideas while considering security for each aspect of your system:

Limiting access
Making smart choices that reduce possible entry points available to a malicious person.
Containment
Your system should be configured to minimize the amount of damage that can be done in the event that it is compromised.
Preparation and knowledge
Keeping backups and knowing the state of your WordPress installation at regular intervals. Having a plan to backup and recover your installation in the case of catastrophe can help you get back online faster in the case of a problem.
Trusted Sources

PROVA ORALE 3

Il/la candidato/a risponda alle seguenti domande

1. In Windows, come si configura un indirizzo IP statico in una rete locale (LAN)?

2. Con riferimento al GDPR, qual è la differenza fra dato e informazione?

3. Cos'è una sessione e come viene gestita in ambito web?

4. Il/la candidato/a legga e traduca il seguente brano

Prova di conoscenza lingua inglese

Traccia 3

Il Candidato legga e traduca il testo seguente:

Cache

WordPress caching is the fastest way to improve performance. If your site is getting hit right now install W3 Total Cache, WP Super Cache or Cache Enabler.

Caching Plugins
Plugins like W3 Total Cache, WP Super Cache and Cache Enabler can be easily installed and will cache your WordPress posts and pages as static files. These static files are then served to users, reducing the processing load on the server. This can improve performance several hundred times over for fairly static pages.

When combined with a system level page cache such as Varnish, this can be quite powerful.

If your posts/pages have a lot of dynamic content configuring caching can be more complex. Search for "WordPress cache plugin" for more info.

Browser Caching
Browser caching can help to reduce server load by reducing the number of requests per page. For example, by setting the correct file headers on files that don't change (static files like images, CSS, JavaScript etc) browsers will then cache these files on your visitor's computer. This technique allows the browser to check to see if files have changed, instead of simply requesting them. The result is your web server can answer many more 304 responses, confirming that a file is unchanged, instead of 200 responses, which require the file to be sent.
Look into HTTP Cache-Control (specifically max-age) and Expires headers, as well as Entity Tags for more information.

Object Caching
Object caching in WordPress is the act of moving data from a place of expensive and slow retrieval to a place of cheap and fast retrieval. An object cache is also typically persistent, meaning that data cached during one request is available during subsequent requests.
In addition to making data access much easier, cached data should always be replaceable and regenerable. If an application experiences database corruption (e.g., MySQL, Postgres, Couchbase), there will and should be severe consequences for this database (and let us hope that there is a good backup plan in place). In contrast with the main data store for the application, if a cache is corrupted, the application should continue to function as the cached data should regenerate itself. No data will be lost, although there will likely be some performance problems as the cache regenerates.
The storage engine for an object cache can be a number of technologies. Popular object caching engines include Redis, Memcached, APC, and the file system. The caching engine used should be dictated by the needs of the application. Each has its advantages and disadvantages. At a bare minimum the engine used should make accessing the data more performant than regenerating the data.

Server Caching
Web server caching is more complex but is used in very high traffic sites. A wide range of options are available, beyond the scope of this article. The simplest solutions start with the server caching locally while more complex and involved systems may use multiple caching servers (also known as reverse proxy servers) "in front" of web servers where the WordPress application is actually running.
Adding an opcode cache like Opcache, or WinCache on IIS, to your server will improve PHP's performance by many times.
Varnish cache is very powerful when used with a WordPress caching plugin such as W3TC.