BUSTA 1

1)

Descriva l'approccio metodologico che adotta per risolvere un problema tecnico segnalato da un utente

2)

In cosa consiste un attacco DDoS e quali contromisure possono essere adottate?

3)

Che cos'è la latenza e perché è critica nelle comunicazioni audio/video?

Testo inglese

Arch User Repository continues to be under a DDoS attack that has been going on for more than two weeks.

If you use Arch Linux, you know about Arch User Repository (AUR), which houses a large number of user-submitted applications. As well, if you've been paying attention to Linux news, you know that the AUR has been under a distributed denial-of-service (DDoS) attack for two weeks now.

In addition to the attack on AUR, Arch's main web page and forums have also been under attack. The good news is that both the web page and forum are now available (at least for some -- I was able to reach both).

At the moment, it seems someone has released a botnet to bring down the repository. Regarding recent service outages, the Arch developers have said, "We are aware of the problems that this creates for our end users and will continue to actively work with our hosting provider to mitigate the attack." They continue with, "We are also evaluating DDoS protection providers while carefully considering factors including cost, security, and ethical standards."

(Linux Magazine)

BUSTA 2

1)

Un utente segnala che una stampante di rete non stampa. Quali verifiche effettua?

2)

Che cos'è una SQL Injection e come può essere prevenuta?

3)

Che differenza c'è tra macchine virtuali e container?

Testo inglese

Russian hackers use Hyper-V to hide malware within Linux virtual machines.

Curly COMrade – a Russian hacking group that's been active since 2024 and is aligned with Russian political movements – has been abusing the Microsoft Hyper-V within Windows to bypass detection by creating a virtual machine (VM) based on Alpine Linux to deploy malware.

The VM only uses 120MB of disk space and 256MB of memory, making it less detectable. Once the VM has been deployed, the malware uses the CurlyShell reverse shell and the CurlCat reverse proxy for stealth and communication.

According to Bitdefender, "By isolating the malware and its execution environment within a VM, the attackers effectively bypassed many traditional host-based EDR [endpoint detection and response] detections. EDR needs to be complemented by host-based network inspection to detect C2 traffic escaping the VM, and proactive hardening tools to restrict the initial abuse of native system binaries."

(Linux Magazine)

BUSTA 3

1)

Come individua se un malfunzionamento è causato da un problema hardware o software?

2)

Perché è importante mantenere i sistemi aggiornati dal punto di vista della sicurezza, e come comportarsi in caso di vecchi software non più compatibili con tali aggiornamenti

3)

Quali sono le principali differenze tra segnali audio/video analogici e digitali?

Testo inglese

What is a Command and Control Server?

In cybersecurity, a Command and Control (C2) server - also called a C&C server - is a computer system controlled by an attacker, acting as a central hub for communicating with and managing compromised devices within a network. Once malware infects a device, it “phones home” to the C2 server, opening a covert channel through which attackers can issue remote commands, deliver additional payloads, or exfiltrate sensitive data.

The terms C2, C&C, and command and control are often used interchangeably to describe this essential element of modern cyberattacks. Without a C2 infrastructure, most sophisticated cyberattacks would have great difficulty in expanding their initial breach, being unable to adjust strategies or escalate privileges effectively.

Historically, the use of C2 servers can be traced back to the early days of malware, when attackers relied on basic methods like IRC channels to issue remote commands. Over time, attackers evolved from basic communication channels to sophisticated peer-to-peer botnets, domain generation algorithms, and encrypted traffic that seamlessly blends with legitimate communications.

(bitdefender.com)

BUSTA 4

1)

Come gestisce una situazione in cui l'utente segnala un problema poco chiaro o descritto in modo impreciso?

2)

Che cos'è il phishing e come può essere riconosciuto e prevenuto?

3)

Cos'è l'effetto Larsen (o Feedback) e come prevenirlo?

Testo inglese

If you're a developer wanting to create a new Gnome extension, you'd best set aside that AI code generator, because the extension team will have none of that.

Shell extensions are a crucial part of the Gnome desktop. Without shell extensions, Gnome would not be nearly as customizable, which would very likely send users packing.

Recently, Gnome extension reviewer Javad Rahmatzadeh, who spends nearly six hours a day reviewing extension code, has noticed a rise in submissions that contain AI-generated code.

The Gnome extension team is not amused. According to Rahmatzadeh, the team has noticed "unnecessary lines and bad practices. And once a bad practice is introduced in one package, it can create a domino effect, appearing on other extensions. That alone has increased the waiting time for all packages to be reviewed."

In other words, poorly written AI code is causing trouble for legitimate extensions.

The team isn't saying that extension developers are not allowed to use AI for things like learning or fixing issues. However, if you write an extension using AI, your code will be rejected.

(Linux Magazine)

BUSTA 5

1)

Un computer risulta molto lento all'avvio e durante l'uso. Quali controlli effettua?

2)

Spieghi il concetto di SSO e i vantaggi in termini di sicurezza.

3)

In un ambiente virtualizzato, che differenza c'è tra risorsa fisica e risorsa virtuale?
Perché la virtualizzazione permette un utilizzo più efficiente dell'hardware?

Testo inglese

With a new CEO in control, Mozilla is doubling down on a strategy of trust, all the while leaning into AI.

Mozilla has a new CEO, Anthony Enzor-DeMeo, who's determined to revive trust in the organization. Oddly enough, Enzor-DeMeo plans on doing that by evolving Firefox into an AI browser.

Enzor-DeMeo says very clearly, "Every product we build must give people agency in how it works." That's great, but what does it mean? He continues with, "Privacy, data use, and AI must be clear and understandable. Controls must be simple. AI should always be a choice — something people can easily turn off. People should know why a feature works the way it does and what value they get from it."

The ability to disable AI in Firefox is a smart move, because there's a large chunk of the Linux community that does not want AI sullying the open source operating system.

(Linux Magazine)