**SAD Lab**

**ASSIGNMENT NO. 1**

# **Q1. Among Windows and Linux which one provides security and list them down.**

Every system administrator has their own favorite kind of box, and while most enterprises these days tend to have a mix of operating systems in their fleet, organizational needs will typically favor deployment of one platform over another. This leads to the inevitable comparison of operating systems in terms of security, with some admins believing one platform is intrinsically more secure than another. If one administrator insists Security-Enhanced Linux is more secure than Microsoft Windows, and another chimes in that Microsoft Windows is more secure, who are you to believe?

Although security often comes down to end-user training regardless of OS, there are some things that make Linux systems more secure than Windows. This is especially true when it comes to malicious software.

1. Hackers don't typically target Linux: The most cited reason for Linux's safety relates to its low usage numbers. Linux has less than three percent of the market, compared to Windows, which operates on more than 80 percent of all devices. For those creating malicious software, it makes more sense to target Windows, because one piece of code will reach the largest segment of the population. This keeps Linux users safer, as even Mac has a larger segment of the market.
2. Difficult to execute a dangerous attachment in Linux: If you've never worked with Linux, you may not realize that it doesn't operate quite the same as Windows or Mac. In those environments, opening a dangerous attachment is simply a matter of double-clicking. On Linux, users need to save the attachment before executing it, and if set up correctly, they would need permissions granted before they could open it. These extra steps can help safeguard a business from the internal user Kill that is so often the cause of security breaches.
3. No users admin access by default in Linux: In a Windows environment, users are often given a high level of access automatically. This lets them click on links and download files indiscriminately, easily leading to the issues mentioned above. Many users don't have access to the root directories on their computers, which means that even if they do manage to infect their systems, they'll be limited in the damage they can do.
4. Linux has more people looking out for security issues: With so many people monitoring for issues, it's likely someone will catch a vulnerability long before hackers can target it. Once spotted, Linux users don't have to wait months for Microsoft to finally investigate the issue and fix it. They can repair it themselves, from wherever they are. This not only improves security for the platform, but it also keeps things stable to prevent downtime.

Although Linux may be safer, there are things administrators can do to keep systems safe. If a hacker does target your network, these small measures will either prevent it or minimize any damage it might do. A firewall can also help keep your systems safe, and best of all, you have plenty of options available for free. Lastly, make sure you keep all your software up-to-date, just as you would do with any operating system.

# **Q2. Explain the critical components of cyber security governance.**

Clearly defined cyber security governance allows organizations to maximize the benefits of operating in a digital economy. Effective cyber security governance supports the success and sustainability of digital business transformation. Without good cyber security governance, organizations will find it increasingly difficult to ensure basic business continuity or maintain the confidence of external stakeholders.

Cyber security governance lists the following key activities, or components that constitute effective security governances:

1. Building a Culture of Cyber Security: A positive cyber security culture of awareness and accountability is driven by the board. The existing culture should be recognised, but influenced by a demonstrated commitment to achieving cyber resilience. The development of a cyber security strategy can promote cultural change, showing the relationship between the organization’s vision and cyber security.
2. Establishing Roles and Responsibilities: Achieving effective cyber security governance requires defining and establishing the organization’s cyber security roles and responsibilities. After they are created, consider at what level in the organization they need to be performed.
3. Holistic Risk Management: Effective risk management is a core component of governance and must be embedded within the organization. A framework is needed to effectively identify, analyze, evaluate, and manage cyber security risks. The framework supports consistent decision-making and prioritization within an organization, maximizing the benefit of investment in cyber security.
4. Cyber Security Collaboration: Translating a cyber security strategy and vision into action requires the buy-in and support of the wider organization. This can be achieved by establishing a committee containing key stakeholders from across the business. The main objective of the steering committee is to achieve consensus and align cyber security priorities with the organization’s objectives.
5. Create a Cyber Security Programme: Organizations should establish a measurable cyber security programme. The programme translates the strategy into action, driving initiatives and continuous improvements in cyber resilience. The steering committee oversees the cyber security programme.
6. Measuring Resilience: The effectiveness of cyber security activities should be accurately measured, assessed and reported. These actions indicate the current cyber resilience of an organization and progress made through the cyber security programme. Measurement and reporting are vital to good governance, enabling informed decision-making and sustainable investment in cyber security.

# **Q3. Explain the role of CERT, the emergency response team for data security mechanisms.**

Computer emergency response teams (CERT) are groups of subject matter experts which handle computer security incidents. The CERT typically researches vulnerabilities and develops security solutions, information and training to relevant network, computer, and internet security problems.

The roles of CERT can be classified under two branches:

1. Reactive Roles: CERT-In acts as a single point of contact for reporting a local problem. It provides consultation to organizations that are prone to threats to/from computers. The information that CERT/CC (Coordination Center) and its subsidiaries accumulate is further shared with other organizations in the computing field. It also performs tracing and analysis of threats, incident response, 24×7 security service, and recommends recovery methods to affected organizations.
2. Proactive Roles: In order to prevent incidents and generate awareness about cybersecurity, the CERT issues security guidelines and advisories. It analyses and responds to system vulnerabilities and risks for providing timely advice against potential anticipated threats. It carries out profiling of threats to identify certain trends in attacker activity. CERT further collaborates with its customers and organizes training programmes, simulation exercises etc. to improve efficacy.

The CERT deploys its functions in the following manner:

1. Reporting: Functions as a nodal point for reporting incidents that occur in the territory of India. It also stores and records all the history of incidents.
2. Identification: Verifies the existence, determines the nature of the incident, and ensures the protection of evidence.
3. Containment: Controls the scope of the incident and tries to minimize the damage made to computer systems.
4. Eradication: Removes or neutralizes the cause of the incident.
5. Recovery: Takes steps and provides assistance in order to restore normal operations

.

1. Prevention: Analyses the patterns of incidents and takes progressive measures to prevent future attacks.

Roles of individuals and organizations that must mandatorily report the following cyber security incident to CERT-In as early as possible. They are:

* Targeted scanning, probing of critical networks and systems
* Compromise of critical systems and information
* Unauthorized access of IT systems and data
* Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code and links to external websites
* Malicious code attacks such as spreading of Virus, Worm, Trojan, Botnets and Spyware
* Attacks on servers such as Database, Mail and DNS and network devices such as Routers
* Identity Theft, spoofing and phishing attacks
* Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
* Attacks on Critical infrastructure, SCADA Systems and Wireless networks
* Attacks on Applications such as E-Governance and E-Commerce

# **Q4. What approach can you take to defend the phishing attempts?**

Phishing scams are one of the most common methods of attack you’re likely to come across. They are a hugely profitable attack method for cybercriminals, as thousands fall victim to them every year. Fortunately, due to their commonplace nature, phishing scams are avoidable if you know how to correctly identify and prevent them. Here are 10 simple tips for identifying and preventing phishing scams.

1. Know what a phishing scam looks like: New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers.
2. Don’t click on that link: It’s generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information.
3. Get free anti-phishing add-ons: Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.
4. Don’t give your information to an unsecured site: If the URL of the website doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it’s better to be safe than sorry.
5. Rotate passwords regularly: If you’ve got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.
6. Don’t ignore those updates: Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If you don’t update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.
7. Install firewalls: Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.
8. Don’t be tempted by those pop-ups: Pop-ups aren’t just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups.
9. Don’t give out important information: As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.
10. Data Security Platform to spot signs of an attack: If you are unfortunate enough to be the victim of a successful phishing attack, then it’s important you are able to detect and react in a timely manner. Having a data security platform in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files.

# **Q5. Mention the OWASP risk rating methodology?**

There are many different approaches to risk analysis. The OWASP approach presented here is based on these standard methodologies and is customized for application security. Let’s start with the standard risk model of Risk = Likelihood \* Impact. Below, the factors that make up “likelihood” and “impact” for application security are broken down.

Step 1: Identifying a Risk

The first step is to identify a security risk that needs to be rated. The tester needs to gather information about the threat agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the business. There may be multiple possible groups of attackers, or even multiple possible business impacts.

Step 2: Factors for Estimating Likelihood

Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the “likelihood”. At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient.

There are a number of factors that can help determine the likelihood. The first set of factors are related to the threat agent involved which are Skill Level, Motive, Opportunity and Size. The next set of factors are related to the vulnerability involved which are Ease of Discovery, Ease of Exploit, Awareness and Intrusion Detection.

Step 3: Factors for Estimating Impact

When considering the impact of a successful attack, it’s important to realize that there are two kinds of impacts. The first is the “technical impact” on the application, the data it uses, and the functions it provides. The other is the “business impact” on the business and company operating the application.

There are a number of factors that can help determine the impact. Technical impact can be broken down into factors aligned with the traditional security areas of concern: Confidentiality, Integrity, Availability, and Accountability. Next Business impact can be broken down into factors aligned with the business areas of concern: Financial damage, Reputation damage, Non-compliance, and Privacy violation.

Step 4: Determining the Severity of the Risk

In this step, the likelihood estimate and the impact estimate are put together to calculate an overall severity for this risk. This is done by figuring out whether the likelihood is low, medium, or high and then do the same for impact. The 0 to 9 scale is split into three parts which are Informal Method, Repeatable Method and Determining Severity.

Step 5: Deciding What to Fix

After the risks to the application have been classified, there will be a prioritized list of what to fix. As a general rule, the most severe risks should be fixed first. It simply doesn’t help the overall risk profile to fix less important risks, even if they’re easy or cheap to fix. Remember that not all risks are worth fixing, and some loss is not only expected, but justifiable based upon the cost of fixing the issue.

Step 6: Customizing the Risk Rating Model

Having a risk ranking framework that is customizable for a business is critical for adoption. A tailored model is much more likely to produce results that match people’s perceptions about what is a serious risk. A lot of time can be wasted arguing about the risk ratings if they are not supported by a model like this. There are several ways to tailor this model for the organization by Adding factors, Customizing options or Weighting factors

# **Q6. Mention the list of challenges for the successful deployment and monitoring of web intrusion detection?**

Network and host-based intrusion detection systems play an important role in cyber security by alerting organizations to potential malicious activity across networks and devices. To realize the full power of this technology however, organizations must first overcome a variety of challenges.

1. Ensuring an effective deployment: To attain a high level of threat visibility, organizations must ensure that intrusion detection technology is correctly installed and optimized. Due to budgetary and monitoring constraints it may not be practical to place NIDS and HIDS sensors throughout an IT environment. With many organizations lacking a complete overview of their IT network however, deploying IDS effectively can be tricky and if not done well may leave critical assets exposed.
2. Managing the high volume of alerts: The vast quantity of alerts generated by intrusion detection can be a significant burden for internal teams. Many system alerts are false positives but rarely do organizations have the time and resources to screen every alert, meaning that suspicious activity can often slip under the radar.

Most intrusion detection systems come loaded with a set of predefined alert signatures but for most organizations these are insufficient, with additional work needed to baseline behaviors specific to each environment.

1. Understanding and investigating alerts: IDS alerts consist of base-level security information which, when viewed in isolation, may mean very little. Upon being presented with an alert, it is often not immediately obvious what caused it, or what actions are required to establish whether or not it poses a genuine threat.

Investigating IDS alerts can be very time and resource-intensive, requiring supplementary information from other systems to help determine whether an alarm is serious. Specialist skills are essential to interpret system outputs and many organizations lack the dedicated security experts capable of performing this crucial function.

1. Knowing how to respond to threats: A common problem for organizations that implement IDS is that they lack an appropriate incident response capability. Identifying a problem is half the battle, knowing how to respond appropriately and having the resources in place to do so is equally important.

Effective incident response requires skilled security personnel with the knowledge of how to swiftly remediate threats, as well as robust procedures to address issues without impacting day-to-day operations. In many organizations there is a big disconnect between the people charged with monitoring alerts and those managing infrastructure, meaning that swift remediation can be difficult to achieve.