Cyber Security Fundamentals

Assignment-3

N Ravinder Reddy

Roll No:

Q. 1. Describe the key differences between intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Ans: An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action. An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident.

In the end, the intrusion prevention system vs intrusion detection system comparison comes down to what action they take if such an intrusion is detected. An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action. An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident.

While their responses may differ, they serve similar purposes, potentially making them seem redundant. Despite this, both of them have benefits and deployment scenarios to which one is better suited than the other:

- **Intrusion Detection System:** An IDS is designed to detect a potential incident, generate an alert, and do nothing to prevent the incident from occurring. While this may seem inferior to an IPS, it may be a good solution for systems with high availability requirements, such as industrial control systems (ICS) and other critical infrastructure. For these systems, the most important thing is that the systems continue running, and blocking suspicious (and potentially malicious) traffic may impact their operations. Notifying a human operator of the issue enables them to evaluate the situation and make an informed decision on how to respond.
- **Intrusion Prevention System:** An IPS, on the other hand, is designed to take action to block anything that it believes to be a threat to the protected system. As malware attacks become faster and more sophisticated, this is a useful capability because it limits the potential

damage than an attack can cause. An IPS is ideal for environments where any intrusion could cause significant damage, such as databases containing sensitive d

IDSs and IPSs both have their advantages and disadvantages. When selecting a system for a potential use case, it is important to consider the tradeoffs between system availability and usability and the need for protection. An IDS leaves a window for an attacker to cause damage to a target system, while a false positive detection by an IPS can negatively impact system usability.

The choice between IDS software and IPS software for a particular use case is an important one. However, an even more vital factor to consider is the effectiveness of a given IDS/IPS solution. An IDS or IPS can suffer from false positive or false negative detections, either blocking legitimate traffic or allowing through real threats. While there is often a tradeoff between these two, the more sophisticated the system, the lower the total error rate an organization will experience.

Check Point has years of experience in developing IDS/IPS software, and Check Point next-generation firewalls (NGFWs) contain the latest in threat detection technology. To learn more about how Check Point can help to improve your network security, contact us for more information. Then, schedule a demonstration to see the power of Check Point's advanced network threat prevention solutions in action.

Q. 2. Design a hypothetical network architecture for a medium-sized enterprise and outline how you would integrate both intrusion detection and prevention mechanisms. Consider factors such as placement of sensors, types of detection techniques (e.g., signature-based, anomaly-based), and strategies for blocking or mitigating identified threats.

Ans:

1. Step 1: Identify Your Network. The first step in building an IDS is identifying the devices and networks you want to monitor. ...
2. Step 2: Determine Your IDS Needs. ...
3. Step 3: Choose Your IDS Tools. ...
4. Step 4: Install and Configure Your IDS. ...
5. Step 5: Monitor and Analyze Your IDS Alerts.

Intrusion detection systems (IDS) play an important role in helping managed services providers (MSPs) establish robust and comprehensive security. There are several different types of IDS, which can often lead to confusion when deciding which type is best suited to the needs of your business, as well as those of your customers.

To help you understand the types of intrusion detection systems available—such as host-based, network-based, signature-based, and anomaly-based—this guide will explain the key differences and use cases for each.

An intrusion detection system is typically either a software application or a hardware device that monitors incoming and outgoing network traffic for signs of malicious activity or violations of security policies. Intrusion detection systems and IDS products are often likened to intruder alarms, notifying you of any activity that might compromise your data or network.

IDS products search for suspicious behavior or signs of a potential compromise by analyzing the packets that move across your network and the network traffic patterns to identify any anomalies. Intrusion detection systems are generally passive by nature, although some intrusion detection systems can act when they detect malicious behavior. On the whole, however, they're largely used to achieve real-time visibility into instances of potential network compromises.

Depending on the type of intrusion detection system that has been deployed, various IDS products will behave differently. For example, a network-based intrusion detection system (NIDS) will strategically place sensors in several locations across the network itself. These sensors will then monitor network traffic without creating performance issues or bottlenecks. Host-based intrusion detection systems (HIDS), on the other hand, are run on certain devices and hosts, and are only capable of monitoring the traffic for those specific devices and hosts.

When it comes to the detection method used, both HIDS and NIDS can take either a signature-based or anomaly-based approach. Some IDS products are even able to combine both detection methods for a more comprehensive approach.

Signature vs. anomaly-based intrusion detection systems

Signature-based and anomaly-based are the two main methods of detecting threats that intrusion detection systems use to alert network administrators of signs of a threat.

Signature-based detection is typically best used for identifying known threats. It operates by using a pre-programmed list of known threats and their indicators of compromise (IOCs). An IOC might be a specific behavior that generally precedes a malicious network attack, file hashes, malicious domains, known byte sequences, or even the content of email subject headings. As a signature-based IDS monitors the packets traversing the network, it compares these packets to the database of known IOCs or attack signatures to flag any suspicious behavior.

On the other hand, anomaly-based intrusion detection systems can alert you to suspicious behavior that is unknown. Instead of searching for known threats, an anomaly-based detection system utilizes machine learning to train the detection system to recognize a normalized baseline. The baseline represents how the system normally behaves, and then all network activity is compared to that baseline. Rather than searching for known IOCs, anomaly-based IDS simply identifies any out-of-the-ordinary behavior to trigger alerts.

With an anomaly-based IDS, anything that does not align with the existing normalized baseline—such as a user trying to log in outside of standard business hours, new devices being added to a network without authorization, or a flood of new IP addresses trying to establish a connection with a network—will raise a potential flag for concern. The disadvantage here is that many non-malicious behaviors will get flagged simply for being atypical. The increased likelihood for false positives with anomaly-based intrusion detection can require additional time and resources to investigate all the alerts to potential threats.

At the same time, this potential disadvantage is also what makes anomaly-based intrusion detection able to detect zero-day exploits signature-based detection cannot. Signature-based detection is limited to a list of known, existing threats. On the other hand, it also has a high processing speed and greater accuracy for known attacks. These two detection methods have advantages and disadvantages that generally complement each other well, and are often used best in tandem.

Q. 3. Analyze the impact of social engineering attacks on individuals and organizations, considering factors such as financial losses, reputational damage, and compromised data security.

Ans: Essentially, this **allows an attacker to act as a malicious insider to infiltrate multiple organization systems and exfiltrate sensitive data**. Ultimately, social engineering could lead to complete organization compromise, meaning all organization data (emails, credentials, source code, client data, etc.)

Successful social engineering attacks could lead to **identity theft, malware attacks, ransomware attacks, reputational damage, data theft, service disruption and unauthorized access**, among others

Social engineering attacks can lead to data breaches, where hackers steal sensitive information such as passwords, credit card numbers, or personal data. It can cause financial losses, damage to the business's reputation, and legal liabilities.

The Cost of Social Engineering Attacks

Social engineering attacks can have a significant impact on the financial and reputational well-being of organizations. Here are some of the costs that organizations may incur as a result of a successful social engineering attack:

1. Financial Losses: Social engineering attacks can result in direct financial losses, such as stolen funds or the cost of repairing systems and data that have been compromised. Additionally, there may be indirect costs, such as lost productivity or revenue, as a result of the disruption caused by the attack.

2. Legal and Regulatory Penalties: Organizations may face legal and regulatory penalties if they are found to have been non-compliant with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States.

3. Reputational Damage: Social engineering attacks can also damage an organization's reputation, which can have long-term consequences. Customers may lose trust in the organization and choose to take their business elsewhere. Additionally, media coverage of the attack can damage the organization's brand and public image.

4. Loss of Competitive Advantage: Organizations that have been successfully targeted by social engineering attacks may lose their competitive advantage, as their confidential information and trade secrets may be stolen and used by their competitors.

5. Cost of Remediation: The cost of remediation following a social engineering attack can be significant, as organizations may need to invest in new security measures, hire additional staff, or engage the services of third-party experts to assist with the recovery process.

Overall, the costs of social engineering attacks can be significant and long-lasting. To minimize these costs, organizations should invest in robust cybersecurity measures, including employee education and training, technical controls, and incident response planning. Additionally, organizations should have a plan in place to address the aftermath of a successful social engineering attack, including how to communicate with stakeholders and rebuild their reputation.

Q. 4. Compare and contrast the characteristics of malware and ransomware attacks, including their methods of propagation, objectives, and potential consequences for victims. Evaluate the effectiveness of proactive measures such as regular software updates, antivirus software, and user awareness training in preventing and mitigating the impact of these types of cyber threats.

Ans: Malware is any software used to gain unauthorized access to IT systems in order to steal data, disrupt system services or damage IT networks in any way. Ransomware is a type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided.

Malware is one of the greatest security threats enterprises face. Security departments must actively monitor networks to catch and contain malware before it can cause extensive damage. With malware, however, prevention is key. But to prevent an attack, it is critical to first understand what malware is, along with the most common types of malware.

Ransomware can be disseminated through many approaches, the most familiar approach that known by people is phishing attack (Richardson & North, 2017). The attacker will create a crafted email to the victim and trick them to click on the attachment or links that contain malicious code. Those malicious content can be send together, in many form with the link or attachment, for example, PDF, ZIP, Word Doc or JavaScript (*.exe, *.pdf, *.doc, *.cmd, *.scr, *.jar file). After the victim has a click on the links or attachments, they will redirect to the malicious site. The harmful file will spread into the device before the victim realize they are clicking on a weird malicious site and started the trigger action such as locked device, encrypt file and program, stealing information and so on.

In case the user is an employee from an organization, they suggest to visit and access the safety site based on the "whitelist" which allow the specific program to run on the device and block others disallowed program to avoid

the malicious attack (Sittig & Singh, 2016) Attackers use malware, short for malicious software, to intentionally harm and infect devices and networks. The umbrella term encompasses many subcategories, including the following:

1. Viruses.
2. Worms.
3. Ransomware.
4. Bots.
5. Trojan horses.
6. Keyloggers.
7. Rootkits.
8. Spyware.
9. Fileless malware.
10. Cryptojacking.
11. Wiper malware.
12. Adware.

Identify Ransomware with Different Approach

Currently, many approaches take place to avoid the attack of ransomware on the device. The first approach that is used in avoiding ransomware is the Signature-based approach. This approach is the most common technique for detecting malware include ransomware. The process will be going on by detecting the unique characteristic of it such as a series of bytes in ransomware script, functions, and message of required demand (Ashwin et al., 2019). The antivirus is involved in this approach to detect a footprint of known malicious software in a device. The mistake ratio is quite low and an alarm will trigger if a well-known pattern appears. However, the antivirus is not able to solve completely the problem of malware, it can only detect the ransomware but the action can't be stopped once it is taking over (Mohammad, 2020). Next, the behavior-based approach also the popular approach used by people nowadays due to the efficient tools to protect the attack from threats. It will estimate the object depends on the expected actions before the actual behavior observation. The actions that will be triggering by a behavior- based approach are file access and file system activity and network behavior (Alshaikh et al., 2020). The others approach that might use to identify the occurrence of ransomware is heuristic detection techniques. The heuristic detection technique is a process of analyzing malicious code. It will evaluate the command in the software or system that are not often occurring in the application. The engine of the heuristic technique can search for the function of the malicious file. There are three sub-analysis under the heuristic detection technique that are file-based analysis, weight-based heuristic analysis, and rule-based heuristic analysis (Ashwin et al., 2019). The file-based analysis will investigate the file path and understand it. The file will be categories as malicious if the command in it includes a delete or harmful file. The weight-based analysis will be analyzing all functionality on weight with the rate of danger that may cause. The file considers as malicious if the total weight same or over. Last, rule-based analysis focused on analyzing the malicious file where getting rule from the file, then measure up the previous rule with the initial rule. If both of the rules are the same, then it will send a warning to the user.

Solutions after Ransomware Attack

Attacking from ransomware to the vulnerability of a program or device is an unexpected incident even the prevention is made and detection technique always used to avoid it. The victim for sure desires to reduce the losses to the minimum, get back the information data, and trying to recover. Based on the advice from the FBI, the first thing to do is make sure you never pay the demand for an attacker after you confirm that you are infected and attack by ransomware on your device. This is because ransomware attacks are considered cybercriminal that spread quickly globally. The case of ransomware attack might be gain due to attackers will gain money through the way, they know that the victim or their company are willing to pay the demand to get back all the important information (Lee et al., 2021). However, the data and information that encrypt might not completely get back from the attacker. This section will review commonly used solutions in others research after ransomware.

Back Up and Unplug the Infected Device

The value of data and the appearance of crypto-currencies is the reason that makes ransomware effective nowadays. This situation creates a road for the attacker to receive the demand payment anonymously. The user must back up all the significant ad useful data in an offline approach. During the process of backup, the user must ensure that the backup set is not connected to the computer, this will save the data from stealing or destroying if the device is hit by the attacking again (Sittig & Singh, 2016). For an example in organization or healthcare center, once you have realized your device are infect by the ransomware, please immediately unplug the device to reduce smash up of file and program. Besides, inform the IT professional to immediately secure the important data, copy an offline backup, and store it in another safety device. The administrator needs to take responsibility to turn off the network that connects to the infected device to minimize the spreading of ransomware (Zetter, 2016).

Prevention

The advancement of science and technology has brought people a lot of conveniences and improved the quality of life, especially the internet. The huge rate of internet usage during the pandemic within 2020 to 2021 proved

the statement above, in which people used the internet and technology to overcome the impact that causes by Covid-19. The employee continues their work with the use of the internet on a work-from-home basis, the student continues their studies with online class are the great example for it. Although the advancement of science and technology has brought a lot of conveniences, it has also brought a lot of harm to the community, such as cybercrime and cyber-attacks. The cyber attacker will try to steal, encrypt the file of the user to gain money from demand by using malicious software. Users can re-access their device or file after paying the demand via crypto- currency such as bitcoin (Aurangzeb et al., 2017). The worst cyber-attack that happen within the year was "WannaCrypto" or known as WannaCry, it was happening in May 2017. WannaCry Ransomware is one of the malware that encrypts and locks the file, program or data hostage of the user in a device, the user is only allowed to access the encrypted file after they pay the ransom demand (Mohurle, & Patil, 2017). This attack has attack around 230,000 devices all over the world. However, the infection of ransomware can be carry on with the entire prevention. This section will discuss the prevention method proposed by the authors.

Update Operating System and Security Software

There is an entire user that not aware of the damage of out date operating system and software. These operating systems and software will no longer to against the attack due to the weak defense system and protection. The operating system that out of date is not allowed to support the latest update that released by the vendor. The attacker would like to hit the victim if they found that the security vulnerability occurred. Operating system, explorer, and defender application must always keep it in the latest version, the third-party plug-ins application are strongly recommended installing in the device to increase the safety of device if the device is allowed to support it (Richardson & North, 2017). The example of the third-party plugins is Java and Flash Player. This is one of the ways to protect the device from attack but not to escape from unharmed

Q. 5. How has the IT Act of 2000, along with its subsequent amendments, shaped the legal landscape for addressing cyber-crime and offenses in India? Discuss the key provisions of the Act related to cyber-security and examine their effectiveness in prosecuting cyber-criminals and protecting individuals and organizations from cyber threats.

Ans: This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 94 sections. The last four sections that starts from ‘section 91 – section 94’, deals with the revisions to the Indian Penal Code 1860.

The IT Act, of 2000 has two schedules:

First Schedule –

Deals with documents to which the Act shall not apply.

- **Second Schedule –**
  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :
The offences and the punishments that falls under the IT Act, 2000 are as follows :-

1. Tampering with the computer source documents.

2. Directions of Controller to a subscriber to extend facilities to decrypt information.

3. Publishing of information which is obscene in electronic form.

4. Penalty for breach of confidentiality and privacy.

5. Hacking for malicious purposes.

6. Penalty for publishing Digital Signature Certificate false in certain particulars.

7. Penalty for misrepresentation.

8. Confiscation.

9. Power to investigate offences.

10. Protected System.

11. Penalties for confiscation not to interfere with other punishments.

12. Act to apply for offence or contravention committed outside India.

13. Publication for fraud purposes.

Power of Controller to give directions.

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with

	sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image of private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

Importance of Cyber Law:

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. **Fraud:**
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. **Copyright:**
   The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.

3. **Defamation:**
   Several personnel uses the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

4. **Harassment and Stalking:** Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

5. **Freedom of Speech:** Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allows people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. **Trade Secrets:** Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade secrets.

7. **Contracts and Employment Law:** Every time you click a button that says you agree to the terms and conditions of using a website, you have

used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notifications on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
- Cyber Law provides both hardware and software security.