D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Information Security
Module: 5

- Faculty: Mrs. Bhavana Alte
- Mr. Prathmesh Gunjgur

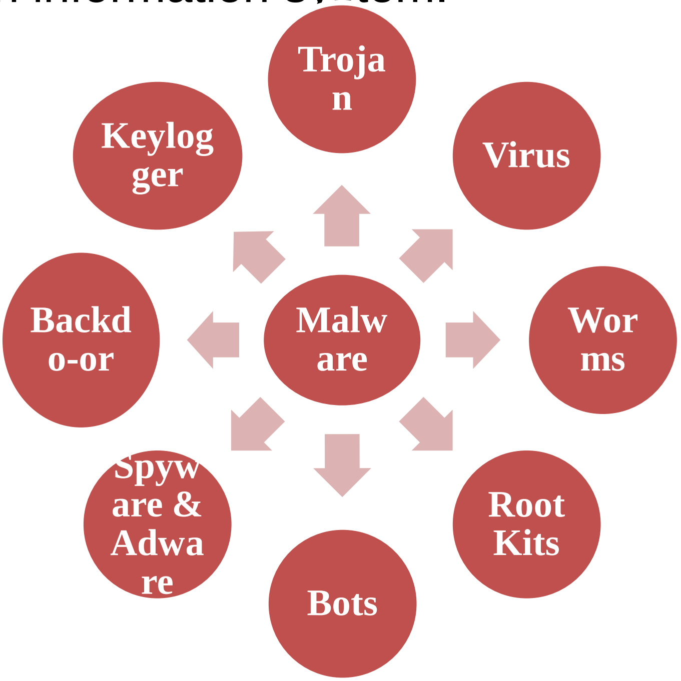
Contents

Module 5:

Lecture 25: Malicious Logic

Malicious Logic

- Malicious Logic is hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.



Malicious Logic

Viruses:

- A computer virus is a program that inserts itself into one or more files and then performs so action.
- When the Trojan horse can propagate freely and insert a copy of itself into another file, it becomes a computer virus.
- A computer virus is a piece of software that can “infect” other programs by modifying them; the modification includes injecting the original program with a routine to make copies of the virus
- program, which can then go on to infect other programs.
- The typical virus becomes embedded in a program on a computer.
- Then, whenever the infected computer comes into contact with an uninfected piece of software,
- a fresh copy of the virus passes into the new program.
- Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network.

Malicious Logic

Worms:

- A worm is a program that can replicate itself and send copies from computer to computer across network connections.
- A computer virus infects other programs. A variant of the virus is a program that spreads from computer to computer, spawning copies of itself on each one.
- Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.
- An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.
- However, we can still classify it as a virus because it uses a document modified to contain viral macro content and requires human action.
- A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for attacks on other machines.
- Network worm programs use network connections to spread from system to system.

Malicious Logic

- A Trojan (or Trojan Horse) disguises itself as legitimate software to trick you into executing malicious software on your computer. Because it looks trustworthy, users download it, inadvertently allowing malware onto their device. Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once a Trojan is installed on a device, hackers can use it to delete, modify or capture data, harvest your device as part of a botnet, spy on your device, or gain access to your network.
- Spyware is a form of malware that hides on your device, monitors activity, and steals sensitive information like financial data, account information, logins, and more. Spyware can spread by exploiting software vulnerabilities or else be bundled with legitimate software or in Trojans.
- Adware, a contraction of ‘advertising-supported software’, displays unwanted and sometimes malicious advertising on a computer screen or mobile device, redirects search results to advertising websites, and captures user data that can be sold to advertisers without the user's consent. Not all adware is malware, some is legitimate and safe to use. Users can often affect the frequency of adware or what kinds of downloads they allow by managing the pop-up controls and preferences within their internet browsers or using an ad blocker.

Malicious Logic

- A Trojan (or Trojan Horse) disguises itself as legitimate software to trick you into executing malicious software on your computer. Because it looks trustworthy, users download it, inadvertently allowing malware onto their device. Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once a Trojan is installed on a device, hackers can use it to delete, modify or capture data, harvest your device as part of a botnet, spy on your device, or gain access to your network.
- Spyware is a form of malware that hides on your device, monitors activity, and steals sensitive information like financial data, account information, logins, and more. Spyware can spread by exploiting software vulnerabilities or else be bundled with legitimate software or in Trojans.
- Adware, a contraction of ‘advertising-supported software’, displays unwanted and sometimes malicious advertising on a computer screen or mobile device, redirects search results to advertising websites, and captures user data that can be sold to advertisers without the user's consent. Not all adware is malware, some is legitimate and safe to use. Users can often affect the frequency of adware or what kinds of downloads they allow by managing the pop-up controls and preferences within their internet browsers or using an ad blocker.

Malicious Logic

- A bot is a computer that has been infected with malware so it can be controlled remotely by a hacker. The bot – sometimes called a zombie computer – can then be used to launch more attacks or become part of a collection of bots called a botnet. Botnets can include millions of devices as they spread undetected. Botnets help hackers with numerous malicious activities, including DDoS attacks, sending spam and phishing messages, and spreading other types of malware.
- Ransomware is malware designed to lock users out of their system or deny access to data until a ransom is paid. Crypto-malware is a type of ransomware that encrypts user files and requires payment by a specific deadline and often through a digital currency such as Bitcoin. Ransomware has been a persistent threat for organizations across industries for many years now. As more businesses embrace digital transformation, the likelihood of being targeted in a ransomware attack has grown considerably.

Module 5:

Lecture 26: Vulnerability Analysis

Vulnerability Analysis

- A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage. Using a risk-based approach, vulnerability assessments may target different layers of technology, the most common being host-, network-, and application-layer assessments.

- A vulnerability can be defined in two ways:
  - A bug in code or a flaw in software design that can be exploited to cause harm. Exploitation may occur via an authenticated or unauthenticated attacker.
  - A gap in security procedures or a weakness in internal controls that when exploited results in a security breach.

Vulnerability Analysis

There are three primary objectives of a vulnerability assessment.

- Identify vulnerabilities ranging from critical design flaws to simple misconfigurations.
- Document the vulnerabilities so that developers can easily identify and reproduce the findings.
- Create guidance to assist developers with remediating the identified vulnerabilities.

Vulnerability Analysis

vulnerability analysis tools include:

- OpenVAS for All Systems: OpenVAS is one of the most far-reaching scanning tools as it covers not only web apps and web servers but also your network, operating systems, virtual machines, and databases. When vulnerabilities are discovered, the risk assessments and recommendations will help you decide what to do next.
- SolarWinds for Network Errors: SolarWinds offers a network configuration manager that allows vulnerability testing in areas many other tools don’t cover. By revealing misconfigured equipment on your network, SolarWinds can help you discover missing information about your system and the risks it is exposed to.
- Intruder for Cloud Storage: While Intruder is not free, it is a powerful tool for scanning cloud-based storage systems, and the best part is that it monitors constantly and scans automatically, ensuring vulnerabilities are detected as quickly as possible. It also offers recommendations and quality reports to guide your strategy.

Vulnerability Analysis

vulnerability analysis tools include:

- Nikto2 for Web Apps: If you’re looking for an open-source tool to help you scan web applications, Nikto2 is capable software that can alert you to web server vulnerabilities. The downside is that it does not offer any risk assessment features or recommendations, so you’ll have to decide what to do with the vulnerabilities that are found.
- Nexpose for New Vulnerabilities: Nexpose is another open-source tool that’s completely free to use to scan your web apps, devices, and networks. Plus, since it’s updated with the newest vulnerabilities every day via its active community, you can trust Nexpose to provide a reliable scanning solution. The tool also categorizes vulnerabilities based on risk, allowing you to focus on the most pressing issues.

Auditing

- An information security audit is an audit on the level of information security in an organization. It is an independent review and examination of system records, activities, and related documents. These audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes.
- Benefits of auditing
  - weighs your current security structure and protocols and helps you define a standard for your organization with the audit results.
  - Mitigates hacker-risks by discovering potential hacker entry points and security flaws well in advance.
  - Verifies how compliant your IT infrastructure is with top regulatory bodies and helps you conform in accordance.
  - Finds lag in your organization’s security training and awareness and helps you make informed decisions towards its betterment.

Auditing Types

- Approach Based
  - Black Box Audit: Here, the auditor only knows about the info that is publicly available regarding the organization that is to be audited.
  - White Box Audit: In this type of security audit, the auditor is provided with detailed info (i.e. source code, employee access, etc) regarding the organization that is to be audited.
  - Grey Box Audit: Here, the auditor is provided with some info, to begin with, the auditing process. This info can also be gathered by the auditors themselves but is provided to save time.
- Methodology Based
  - Penetration Tests: The auditor tries to break into the organization's infrastructure.
  - Compliance Audits: Only certain parameters are checked to see if the organization is complying with security standards.
  - Risk Assessments: An analysis of critical resources that may be threatened in case of a security breach.
  - Vulnerability Tests: Necessary scans are performed to find possible security risks. Many false positives may be present.
  - Due Diligence Questionnaires: Used for an analysis of existing security standards in the organization.

Auditing Types

Importance of an IT security audit

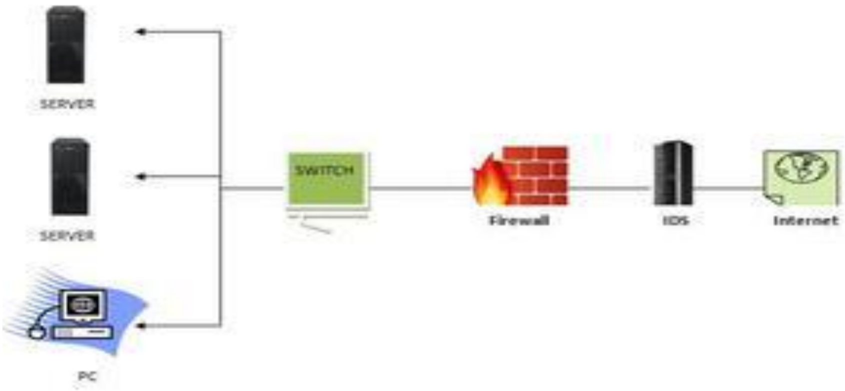
- Protects the critical data resources of an organization.
- Keeps the organization compliant to various security certifications.
- Identifies security loopholes before the hackers.
- Keeps the organization updated with security measures.
- Identifies physical security vulnerabilities.
- Helps in formulating new security policies for the organization.
- Prepares the organization for emergency response in case of a cybersecurity breach.

Module 4:

Lecture 27: Intrusion Detection

Intrusion Detection

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.



Intrusion Detection

How does an IDS work?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.

- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.

- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.

- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.

- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Intrusion Detection

IDS are classified into 5 types:

- Network Intrusion Detection System (NIDS): Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.
- Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

Intrusion Detection

IDS are classified into 5 types:

- Protocol-based Intrusion Detection System (PIDS): Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- Application Protocol-based Intrusion Detection System (APIDS): An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

Intrusion Detection

IDS are classified into 5 types:

- Hybrid Intrusion Detection System: Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Intrusion Detection

Benefits of IDS

- Detects malicious activity: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.

- Improves network performance: IDS can identify any performance issues on the network, which can be addressed to improve network performance.

- Compliance requirements: IDS can help in meeting compliance requirements by monitoring network activity and generating reports.

- Provides insights: IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Intrusion Detection

Detection Method of IDS

- Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.

- Anomaly-based Method: Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

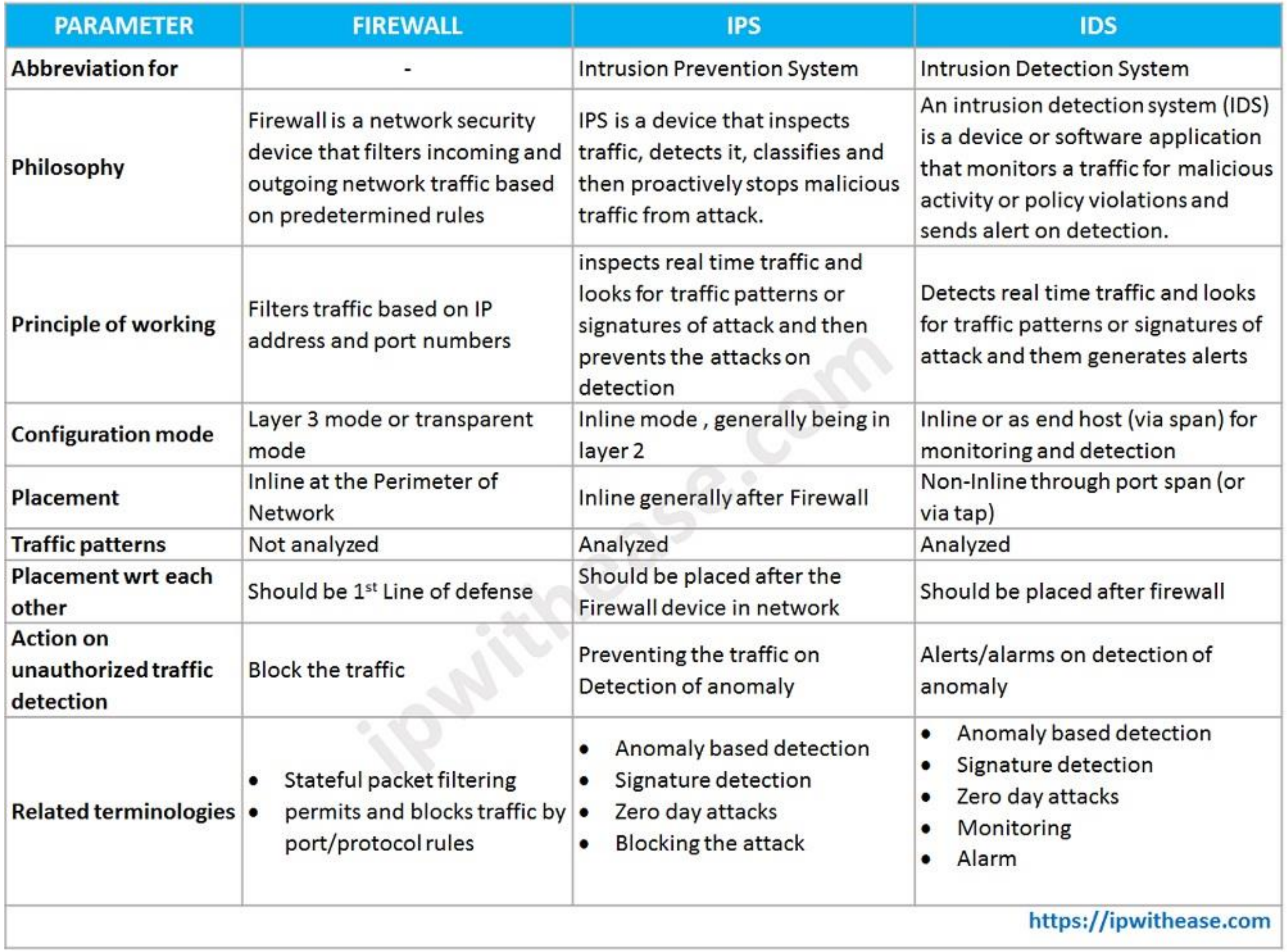
Intrusion Detection

Detection Method of IDS

- Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.

- Anomaly-based Method: Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Intrusion Detection



PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	• Stateful packet filtering • permits and blocks traffic by port/protocol rules	• Anomaly based detection • Signature detection • Zero day attacks • Blocking the attack	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm

https://ipwithease.com

D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You