BSIT – 7th Semester (M) – (2020 – 2024)

Course – CC-312-3 – Information Security

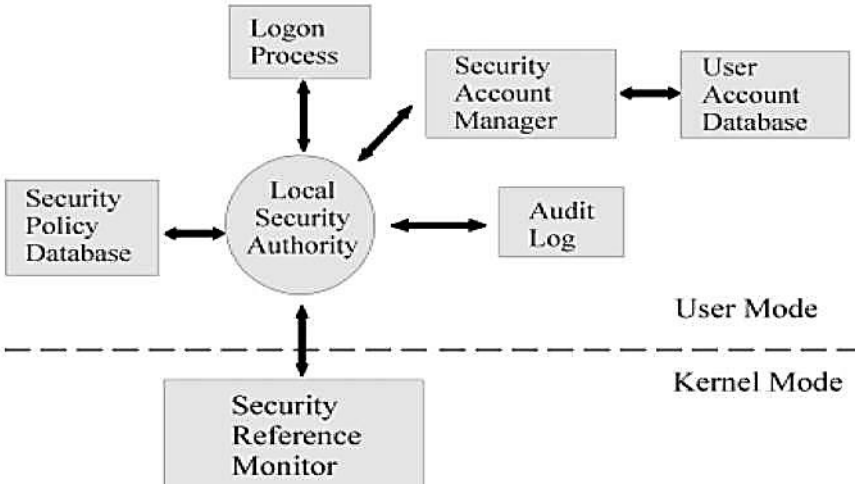
Subject Teacher: Mr. Rizwan Abbas

Lecture 10: Windows Security Architecture

Security Architecture refers to the underlying framework and components that Microsoft has designed to protect the system and the data and applications that run on it from various security threats. Security architecture determines the mechanisms and algorithms to define security policies, access controls, auditing process and so on.

Windows Security architecture has evolved over the years and encompasses a wide range of features and technologies aimed at safeguarding Windows systems.

The following diagram shows the security architecture of Windows NT and Windows 2000.



Main Components of Windows Security Architecture:

- SAM (Security Account Manager)
- LSA (Local Security Authority)
- SRM (Security Reference Monitor)

Security Account Manager

The Security Account Manager (SAM) is responsible for managing user account information, including usernames and password hashes on a local system. This service is responsible for making the connection to the **User Account Database**.

Local Security Authority

LSA is the core of security architecture that is responsible for authentication/validating users for both local and remote logons. The LSA also maintains the local security policy.

- **Logon Process**: During the local logon to a machine, a person enters his name and password to the logon dialog. This information is passed to the LSA. The password is sent in a nonreversible secret key format using a one-way hash function. The LSA then queries the SAM for the User's account information. If the key provided matches the one in the SAM, the SAM returns the users SID and the SIDs of any groups the user belongs to. The LSA then uses these SIDs to generate the **security access token**.

- **Security Policies:** LSA enforces security policies that control various aspects of system security, including password complexity requirements, account lockout policies, and user rights assignments. Security policies are like rules and guidelines that help keep things safe and protected. They are a set of instructions that tell people and computers what they can and cannot do to make sure information and systems stay secure.

- **Audit log**: An audit log also known as security log, is a chronological record of events and activities that occur within a computer system, network, or application. The primary purpose of an audit log is to provide a detailed history of actions and transactions for the purpose of monitoring, security, compliance, and troubleshooting.

Security Reference Monitor

The Security Reference Monitor is a security architecture component that is used to control user requests to access objects in the system by implementing access control models at kernel level. The SRM enforces the access validation and audit generation. Windows NT forbids the direct access to objects. Any access to an object must first be validated by the SRM. For example, if a user wants to access a specific file the SRM will be used to validate the request.

Windows Vulnerabilities

Vulnerabilities in an operating system refer to weaknesses or flaws in the OS's design, code, or configuration that can be exploited by malicious individuals or software to compromise the security, stability, or functionality of the system. These vulnerabilities may manifest as software

bugs, coding errors, or misconfigurations that could lead to unauthorized access, data breaches, system crashes, or other adverse consequences if exploited by attackers.

Why is Windows 10 vulnerable to attacks?

- **Popularity:** Windows 10 is the most widely used operating system, making it a prime target for attackers due to its large user base.
- **Diverse User Base:** While some Windows 10 users have an IT background, a significant majority lacks in-depth knowledge in IT and cybersecurity. This means that the majority of users are less aware of cyber threats and security measures.
- **Outdated Systems:** Many users do not keep their Windows systems up to date, which can expose them to vulnerabilities.

5 Common Types of Vulnerabilities in Windows 10:

1. **Elevation of Privilege (EOP):** Elevation of Privilege vulnerabilities allow an attacker to gain higher levels of access or privileges on a system. This means they can elevate their permissions to a level where they have complete control over the targeted machine, enabling them to execute malicious actions with greater control.

2. **Remote Code Execution:** Remote Code Execution vulnerabilities enable an attacker to execute arbitrary code on a remote system, often without requiring authentication. This can lead to a complete compromise of the system.

3. **Denial of Service (DoS):** Denial of Service vulnerabilities can be exploited to overwhelm a system with excessive traffic or resource requests, rendering it unavailable to legitimate users.

4. **Information Disclosure:** Information Disclosure vulnerabilities may expose sensitive information, such as passwords, user tokens, or encryption keys, to unauthorized users. This compromises the confidentiality of user data.

5. **Cross-Site Scripting (XSS):** Cross-Site Scripting vulnerabilities typically affect web applications on Windows servers. Attackers can inject malicious scripts into web pages viewed by other users, potentially stealing their data or session information.

Common Practices to Mitigate Vulnerabilities:

- Keeping your Windows updated, as, Microsoft continuously releases patches for security fixes. By keeping up to date you might be able to mitigate some of these vulnerabilities.

- Make your employees acknowledge the importance of cybersecurity and how to protect themselves from cyber-attacks.
- Hardening all the end-points in your infrastructure, so that you always have control over the configuration of your system.

Windows Security Defenses

Windows offers a variety of security defenses and mechanisms to protect against a wide range of threats. These defenses have evolved over the years to address the changing landscape of cyber threats. Here are some of the key Windows security defenses

Security Defenses of Windows 10:

1. **Windows Updates:** Regularly updating Windows is essential for staying protected against security vulnerabilities. Windows Update delivers security patches, bug fixes, and feature updates to the OS. This is the most important security setting for any Windows 10 device.

2. **Windows Defender Antivirus:** Windows Defender is the built-in antivirus and anti-malware solution, provides real-time protection against viruses and other malicious software. Unlike other antivirus software's, Windows Defender does not require any manual configuration or any support whatsoever (other than the windows updates).

3. **Microsoft SmartScreen:** SmartScreen is a built-in feature that scans and blocks execution of known malicious programs. In addition, it can notify Windows 10 users when they are about to visit suspicious websites and emails because it compares their reliability against a Microsoft's blacklist.

4. **Windows Sandbox:** Windows Sandbox enables new apps to operate in isolated virtual environment to test whether the app is safe to use or not. This feature is quite handy in order to prevent full threat exposure.

5. **Windows hello:** Windows Hello is a multi-factor authentication platform that can work with biometric data (e.g., fingerprints or facial recognition), as well as be paired with "companion devices" (smart phones, smart watches, etc.) to ensure only authorized users can have access to the computer on which Windows 10 is installed.

6. **BitLocker:** BitLocker encrypts your entire drive with an encryption code, whose default encryption strength is 128-bit. This makes it impossible for malicious actors to steal your information. Probably the best part is how unobtrusive and easy to use this feature is — you will usually not notice any difference in system performance and you will not need anything other than a Windows user account password to start it.

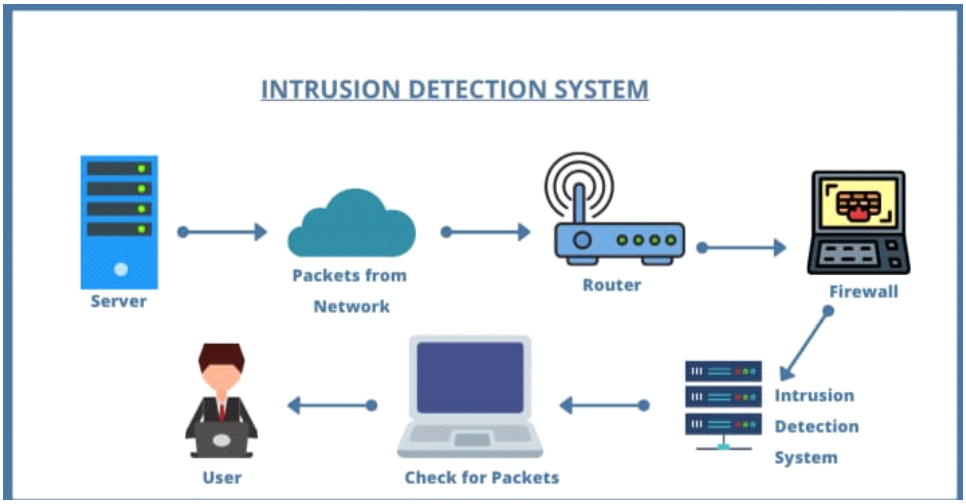
7. **Credential Guard:** Credential Guard isolates and protects sensitive credentials, such as password hashes, fingerprint scans etc. from attackers. It allows you to save your credentials in your device without any worry of confidentiality attack.

8. **User account control:** User Account is an important security tool of Windows 10 to keep unauthorized changes at bay. This is because it is always asking for an administration-level permission in the event of important changes such as removing an application or installing a program.

Lecture 11: Intruder Detection

What is 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. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users.



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.

Detection Methods of IDS:

1. 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 Os in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used KB/73% 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.

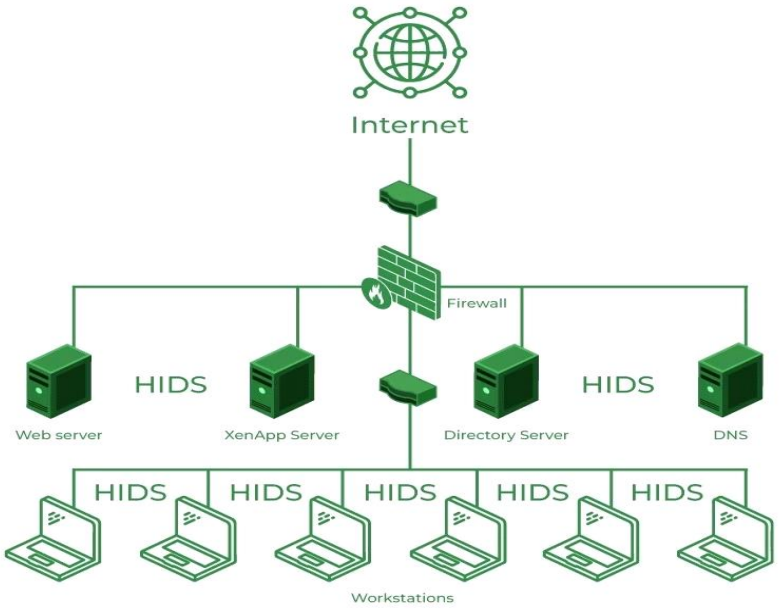
2. Anomaly-based Method:

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.

3. Behavior-based Method:

A Behavior-Based Intrusion Detection System (IDS) is a type of security system that focuses on monitoring and analyzing the behavior of entities within a computer system. or network to identify potential security threats or anomalies. Unlike traditional signature-based IDS, which relies on a database of known attack patterns, behavior- based IDS looks for deviations from normal behavior.

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.

Advantages:

- Monitor in term of who accessed what
- Can map problem activities to a specific user id
- System can track behavior changes associated with misused
- Can operate in encrypted environment
- Operates in switched networks
- Monitoring load distributed against multiple hosts and not on a single host, reporting only relevant data to central console

Disadvantages:

- Cannot see all network activities.
- Running audit mechanisms adds overload to system, performance may be an issue.
- Audit trails can take lots of storage.
- Escalation of false positive.
- Greater deployment and maintenance cost.

What is distributed intrusion detection system?

A Distributed Intrusion Detection System (DIDS) is an approach to intrusion detection that involves the use of multiple sensors or detectors that are distributed across a network. The goal is to enhance the overall detection capability and provide a more comprehensive view of potential security threats. Here are key points about Distributed Intrusion Detection Systems:

- **Multiple Sensors**:

Uses many detectors placed across a network.

- **Coordinated Analysis:**

Analyzes data collaboratively for a comprehensive view.

- **Collaborative Decision-Making:**

Encourages sensors to share information for better threat identification.

- **Redundancy and Reliability:**

Adds backup sensors for reliability if one fails.

- **Scalability:**

Easily expands to cover larger or more complex networks.

Techniques for intruder detection:

1. Network Node Intrusion Detection System:

A Network Node Intrusion Detection System (NNIDS) is technically a variation of a NIDS, but since it works differently, we'll consider it a different type of IDS.

A NNIDS also analyzes the packets that pass through it. However, instead of relying on a central device to monitor all network traffic, the system watches over each node connected to your network.

2. Protocol-Based Intrusion Detection System (PIDS):

PIDS, a Protocol-based Intrusion Detection System, is a system or agent that resides consistently at the front end of the server to control and interpret the protocol between the user and the server.

PIDS is for securing the web server by monitoring the HTTPS protocol stream. A typical use of PIDS is at the front end of the web server, keeping a check on the HTTP or HTTPS stream.

3. Application Protocol-Based Intrusion Detection System (APIDS):

An application-based intrusion detection system is a system that stays within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.

APIDS uses machine language to establish the baseline of the expected system behavior in terms of bandwidth, parts, protocol, and device usage.

Lecture 12: Network Based Intruder Detection

Definition and Purpose:

NIDS monitors network traffic for suspicious activities or patterns that may indicate unauthorized access or attacks.

Importance in Cybersecurity:

Crucial for detecting and preventing various cyber threats, such as malware, DoS attacks, and unauthorized access attempts.

Types of Network-Based Intrusion Detection Systems

Signature-Based NIDS:

Matches known attack patterns or signatures in network traffic.

Efficient for detecting known threats but may miss new or zero-day attacks.

Anomaly-Based NIDS:

Learns normal network behavior and alerts on deviations from the baseline.

Effective in detecting novel attacks but may generate false positives.

Components and working of NIDS

Sensors:

Collect and analyze network traffic data.

Analyzers:

Interpret data collected by sensors to detect anomalies or known attack patterns.

User Interface:

Provides a graphical or command-line interface for managing and monitoring the system.

Challenges and Limitations:

False Positives:

Anomaly-based systems may trigger alarms for normal activities, leading to unnecessary alerts.

Encrypted Traffic:

Difficulty in inspecting encrypted data, which can bypass detection systems.

Scalability:

Handling large volumes of network traffic while maintaining accuracy is a significant challenge.

Best Practices for Deploying NIDS

Continuous Monitoring:

Regularly update signatures and baseline models to adapt to new threats.

Network Segmentation:

Implementing segments can contain potential breaches and limit the scope of attacks.

Collaboration and Information Sharing:

Sharing threat intelligence among organizations can enhance the effectiveness of NIDS.

Future Trends in Network-Based Intrusion Detection

Machine Learning and AI:

Advancements in AI algorithms improve the accuracy of anomaly detection.

Integration with Threat Intelligence:

Leveraging external threat intelligence sources to enhance detection capabilities.

IoT Security:

NIDS adapting to secure the increasingly interconnected Internet of Things devices.

Conclusion

Network-Based Intrusion Detection Systems are vital components of cybersecurity infrastructure.

Continuous advancements and proactive measures are essential to counter evolving cyber threats effectively.

Lecture 13: Malicious Software

Malicious Software:

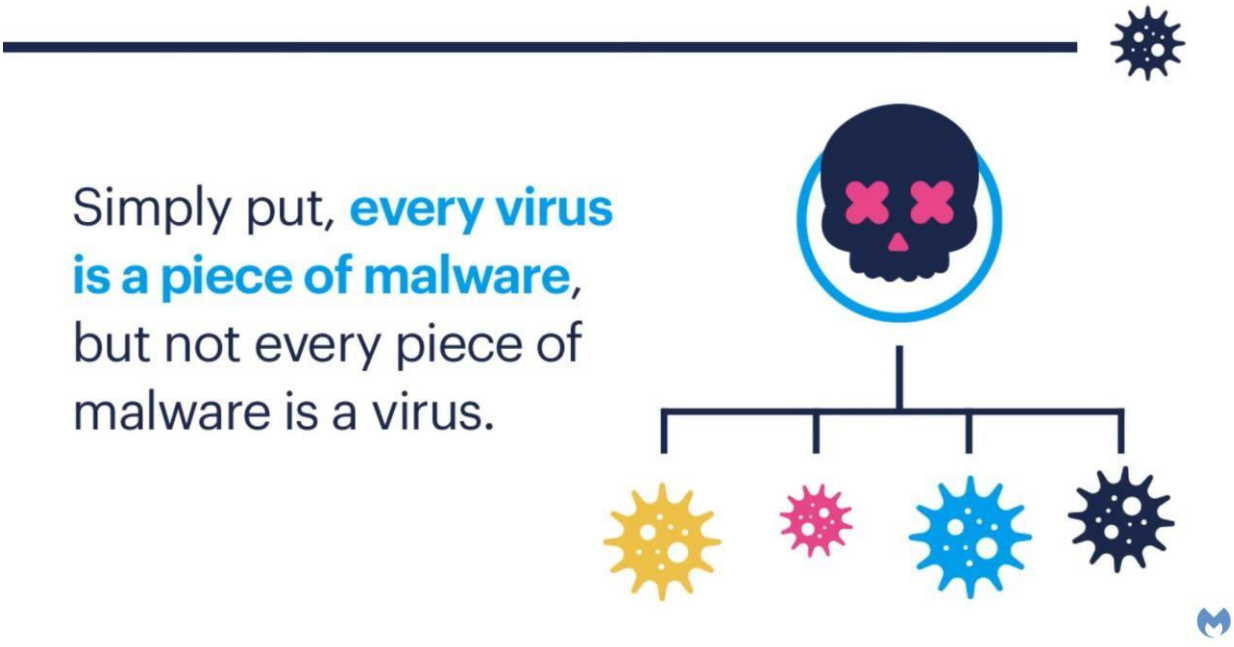
The word **malicious** is derived from a Latin word **militia** which means **bad or evil**.

Malicious software, or malware, refers to software specifically designed to harm, exploit, or compromise computer systems, networks, or user devices for malicious purposes, such as stealing information, disrupting operations, or gaining unauthorized access.

Malware, Viruses, Attacks?

All these words, sounds too familiar, and almost seem to be the same but they aren't.

- **Malware** is the umbrella term encompassing all malicious software designed to harm a computer system or network.
- **Viruses** are a specific type of malware that self-replicates and spreads through a system by attaching itself to other programs or files.
- **Attacks** are the actions taken by malicious actors to exploit vulnerabilities in computer systems or networks and cause harm.



Types of Malicious Software:

(i) Trojan Horse:

A Trojan horse is a type of malware that disguises itself as legitimate software to deceive users into installing it. Unlike viruses, Trojans do not self-replicate but often create a backdoor on the user's system for unauthorized access or other malicious activities.

E.G: Poison Ivy is a remote access Trojan (RAT) that provides attackers with backdoor access.

(ii) Adware:

Adware is a type of software that displays unwanted advertisements on a user's device. These advertisements can manifest as pop-ups, banners, or other forms, often disrupting the user's online experience.

E.G: Fireball: This relatively new adware, from 2017, infected millions of devices worldwide. It hijacked browsers, changed search engines, downloaded unwanted files.

(iii) Ransomware:

Ransomware is malicious software that encrypts a user's files, rendering them inaccessible. Attackers demand a ransom for the decryption key.

E.G: RobinHood ransomware, in **2018** halted all government activities in the city of **Baltimore**.

(iv) Spyware:

Spyware is software designed to secretly monitor a user's activities, capturing sensitive information such as keystrokes, login credentials, and browsing habits.

E.G: FinFisher is a spyware tool used for espionage. It can infiltrate systems, capture screenshots, record keystrokes, and access files on infected devices.

Virus:

A virus is a specific type of malware characterized by its ability to replicate by attaching itself to other files or programs. Unlike the broader term "malware," which encompasses various types of harmful software, a virus specifically relies on host files to propagate. When an infected file is executed, the virus activates, attaches to other files, and spreads.

Types of Viruses:

(i) Boot Sector Virus:

A boot sector virus infects the master boot record (MBR) or boot sector of storage devices. It can manipulate essential startup information, potentially causing damage.

E.G: Form is a boot sector that infects the boot sector of floppy disks and hard drives.

(ii) Logic Bomb:

A logic bomb is dormant code in a system set to execute malicious actions based on specific conditions. It remains inactive until said event occurs.

E.G: Michelangelo destroys data on the hard disk on the specific date it is said to be triggered.

(iii) Resident Virus:

A resident virus embeds itself in a computer's memory (RAM) after infecting a host file.

E.G: CMJ (CME-24) can actively infect other executable files that are loaded into memory, it can compromise the integrity of various files, potentially causing data corruption.

(iv) Browser Hi-jacker:

This virus type infects your browser and redirects you to malicious websites.

E.G: CoolWebSearch is a notorious browser hijacker that, redirects users to unwanted and potentially harmful websites. It can modify browser settings, alter search results.

Malware/Virus Counter-Measures:

(i) Anti-Virus Software:

Install reputable antivirus software on your computer. Keep the antivirus program updated to ensure it is always active.

(ii) Avoid Pirated Software:

Refrain from downloading or using pirated software. Unauthorized software often contains hidden malware, increasing the risk of infection. Stick to official paid versions.

(iii) Safe Online Practices:

Develop safe online habits by avoiding suspicious links, refraining from downloading files from unknown sources, and being cautious with email attachments. Think before you click to minimize the risk of encountering malware.

(iv) Secure Removable Storage Media:

Be cautious when using removable storage devices. Scan external drives for malware before accessing files, and avoid using unknown USB devices. This reduces the risk of spreading infections through removable media.

Lecture 14: Bots & Rootkits

Bots

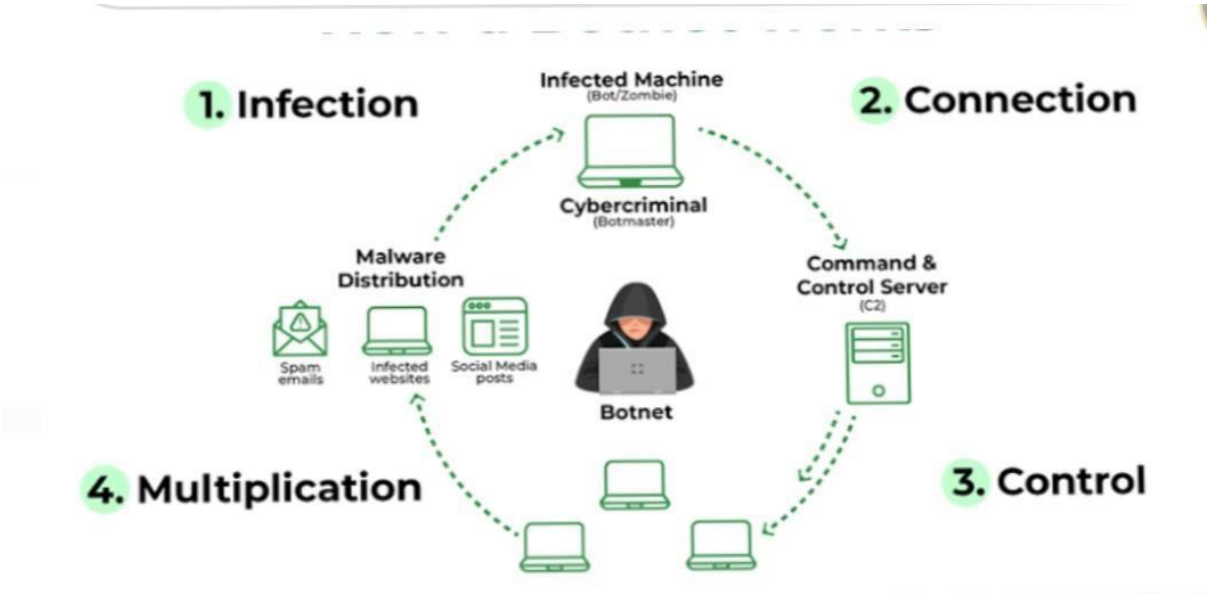
Bots, short for robots, are software applications that execute automated tasks, These bots can be created using programming languages, trojans, and worms.

What is a Botnet?

A botnet is a group/network of bots controlled by a central server or a command-and-control (C&C) panel. Once a system is infected with a bot, it can be remotely controlled by an attacker who can then use it to perform malicious tasks such as launching DDoS attacks, stealing personal data, and spreading malware.

Bot is also called a **zombie**, and a botnet is referred to as a **zombie army.**
This software is mostly written in C++ & C, which introduced a new kind of Crime called **Cybercrime**

The Spread of Bots and Botnets:



Types of Bots and Botnets:

1. ChatBots:

Catbots simulate human conversation with artificial intelligence and machine learning (AI/ML) technologies. They can respond to queries on behalf of the customer support team. Highly intelligent Chabot's like Amazon Alexa.

2**. DDoS BOTS**

"Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

3. Spam Bots

A spambot is an Internet application designed to gather email addresses for spam mailing lists.

4. Social Media Bots

Bots are operated on social media networks, and used to automatically generate messages, advocate ideas, act as a follower of users, and as fake accounts to gain followers themselves.

Preventing Botnet Attacks:

Keep Your Software Up to Date

Make sure your operating system, antivirus software, and firewalls are all up to date. This can help protect you from known vulnerabilities and attacks.

Enable Two-Factor Authentication

Adding an extra layer of security to your accounts can help prevent unauthorized access and keep your data safe.

Avoid Suspicious Links

Clicking on suspicious links or downloading unverified files can potentially infect your system with malware, leading to a botnet attack.

Rootkits:

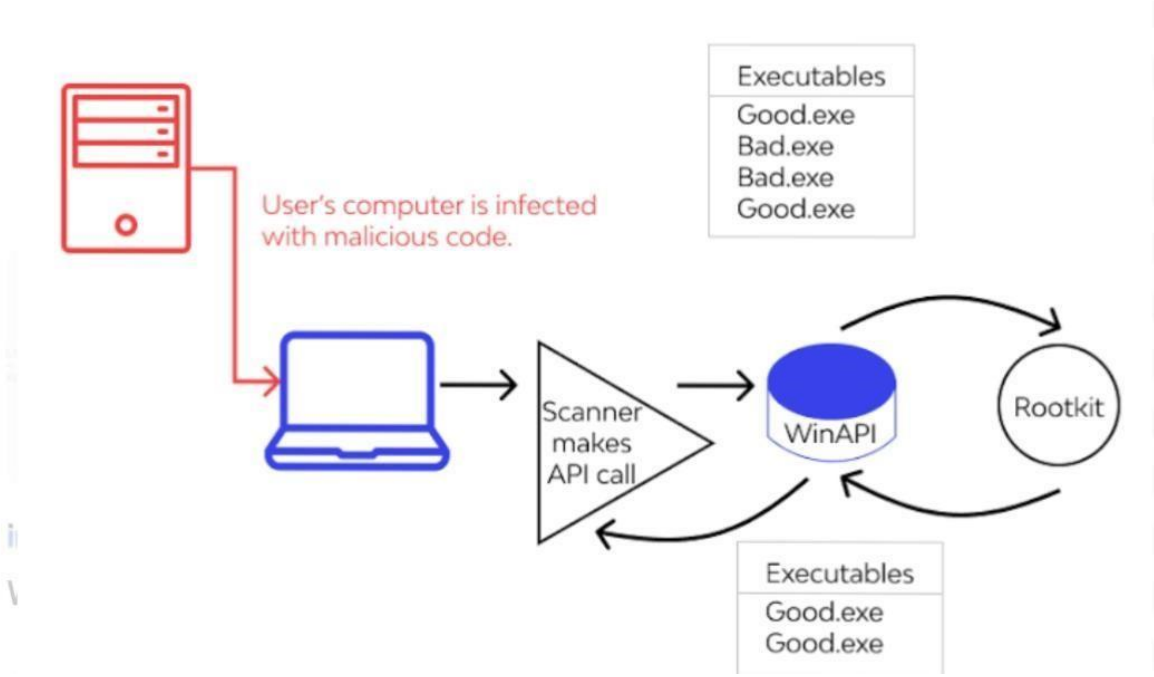
The term rootkit is a combination of the word “root” and “kit.” “Root,” with the admin status of an operating system. Meanwhile, “kit” means a package of software tools.

So, a rootkit is a set of tools that gives someone the highest privileges in a system.

“A rootkit is a type of malware that allows an attacker to gain unauthorized root access and control over a computer and remain undetected.”

rootkits usually come together with various types of malware and grant the hacker access to your computer with administrative rights.

Rootkits are the sneakiest, toughest-to-find kind of malicious software.



Usage:

rootkits can be used to do things like deactivate your antivirus software, steal sensitive data, or execute other malware on the device.

Types of Rootkits:

Kernel Mode Rootkits

These rootkits operate at the kernel level of an operating system, enabling them to control system functions and intercept low-level commands.

Hardware or firmware rootkit

Hardware or firmware rootkits can affect your hard drive, your router, or your system's BIOS, which is the software installed on a small memory chip in your computer's motherboard.

Application rootkit

Application rootkits replace standard files in your computer with rootkit files and may even change the way standard applications work. These rootkits infect programs like Microsoft Office

Bootloader Rootkits

These rootkits target the bootloader, the first code executed when a computer starts up, allowing them to control the system from the very beginning of the boot process.

Preventions against Rootkits:

Protecting against rootkits requires a multi-layered approach:

Keep Software Updated

Regularly update your operating system, applications, and security software to patch vulnerabilities that could be exploited by rootkits.

Use Strong Authentication

Implement complex passwords and multi-factor authentication to reduce the risk of unauthorized access

Practice Safe Browsing

Avoid clicking on suspicious links, downloading files from untrusted sources, or visiting potentially harmful websites.

Lecture 17

Denial of Services Attacks + Flooding Attacks

Denial of Service:

It is an **interruption** in an authorized user's access to a network, typically caused with **malicious intent** in order to damage personal data.

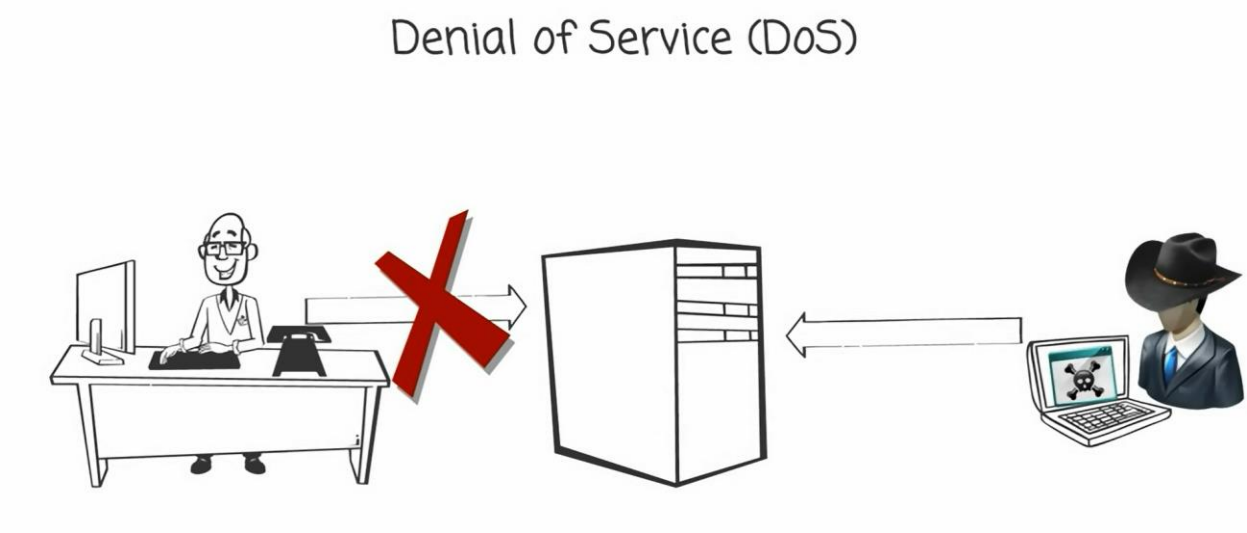
Attack:

As discussed in earlier lectures, an **attack** is an activity in which an **attempt** is made to gain **unauthorized access** to a person's data.

Denial of Service Attack:

A **denial-of-service (DoS)** attack is a malicious attempt to disrupt the normal functioning of a target system, service, or network.

The goal of a DoS attack is to disrupt the availability of the targeted system rather than to compromise its data or steal information. However, in more sophisticated cases, attackers may use a DoS attack as a smokescreen to distract security personnel while other malicious activities, such as data breaches, take place.



The objective is to render the targeted system or network non-functional, denying legitimate users access.

Types of DOS Attacks:

1. **Resource Depletion Attacks:**

Exhausting critical system resources, such as CPU, memory, or disk space, to impede the normal functioning of a system or service.

Example: Continuously running processes that consume all available CPU resources, making the system unresponsive to legitimate user requests.

2. **Application Layer Attacks:**

Targeting vulnerabilities in specific applications or services to disrupt their normal operation, leading to service unavailability.

Example: Exploiting a known vulnerability in a web application to crash it.

3. **Browser Redirection:**

This happens when you are trying to reach a webpage, however, another page with a different URL opens. You can view only the directed page and are unable to view the contents of the original page. This is because the hacker has redirected the original page to a different page.

Example: Visiting one site and immediately being redirected to another.

4. **Closing Connections:**

After closing the connection, there can be no communication between the sender(server) and the receiver(client). The hacker closes the open connection and prevents the user from accessing resources.

Example: Disabling the route between the sender and the receiver.

5. **Data Destruction:**

This is when the hacker destroys the resource so that it becomes unavailable. He might delete the resources, erase, wipe, overwrite or drop tables for data destruction.

Example: Removing the source at its root.

Flooding Attacks:

They are a **type** of **DOS Attack,** but their main concept is based to disrupt the server, by **overwhelming** it with **internet traffic.**

Types of Flooding Attacks:

1. **UDP Flood:**

   Overwhelming a target with a high volume of User Datagram Protocol (UDP) packets, saturating network bandwidth and potentially causing service disruption.

   Example: An attacker may use a botnet to flood a gaming server with UDP packets, causing the server to become unresponsive to legitimate players.

2. **HTTP Flood:**

   Overloading a web server by sending an exceptionally large number of HTTP requests, exceeding its capacity to handle incoming connections and process requests.

   Example: A device may be used to launch an HTTP flood against an e-commerce website during a high-traffic period, causing the site to slow down or become temporarily unavailable.

3. **TCP ACK Flood:**

   Overwhelming a target by sending a high volume of TCP acknowledgment (ACK) packets, exhausting its resources and disrupting normal communication.

   Example: An attacker may use a botnet to initiate a TCP ACK flood against an online service, preventing legitimate users from establishing successful connections.

4. **SMTP Flooding (Mail Bombing):**

   Overloading an email server by sending a massive volume of email messages, causing the server to become congested and potentially leading to service disruption.

   Example: An individual may flood a targeted email address with an excessive number of emails in a short period, causing the email server to be overwhelmed and slowing down email delivery.

5. **DNS Water Torture Attack:**

   Exploiting a target's DNS server by sending a steady and low-rate stream of DNS queries over an extended period, aiming to exhaust the server's resources over time.

   Example: An attacker may continuously send a small number of DNS queries to a specific domain, aiming to gradually consume the target's DNS server resources without triggering immediate alarms.

Impacts of DOS Attacks:

1. **Loss of Revenue:**

An e-commerce website experiences an HTTP flood attack during a major sale event, rendering the website inaccessible to customers. As a result, the company loses substantial revenue as users are unable to complete purchases.

2. **Damage to Reputation:**

A popular social media platform becomes the target of a sustained DoS attack, causing prolonged outages. Users, frustrated by the service disruptions, start expressing dissatisfaction on various online platforms, leading to negative media coverage and damaging the platform's reputation.

3. **Financial Losses:**

A financial institution faces a sophisticated DoS attack that targets its online banking services. In addition to the direct financial losses from disrupted services, the institution incurs substantial costs for deploying advanced mitigation measures, legal expenses, and compensating affected customers for any financial losses incurred during the attack.

4. **Disruption of Critical Services:**

A hospital's online patient management system is targeted by a DoS attack, disrupting access to critical patient information for healthcare professionals. The attack causes delays in treatment, and emergency services are affected, potentially putting patients' lives at risk.

Lecture # 18

Outlines:

- DDOS Attack and its working
- Types of DDOS Attacks
- Defenses against DDOS Attacks

DDoS Attack

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker overwhelms a server with internet traffic to prevent users from accessing online services and sites.

Denial of Service Attacks are carried out by one machine but Distributed Denial-of-Service (DDoS) Attacks are carried out with network of Internet-connected machines.

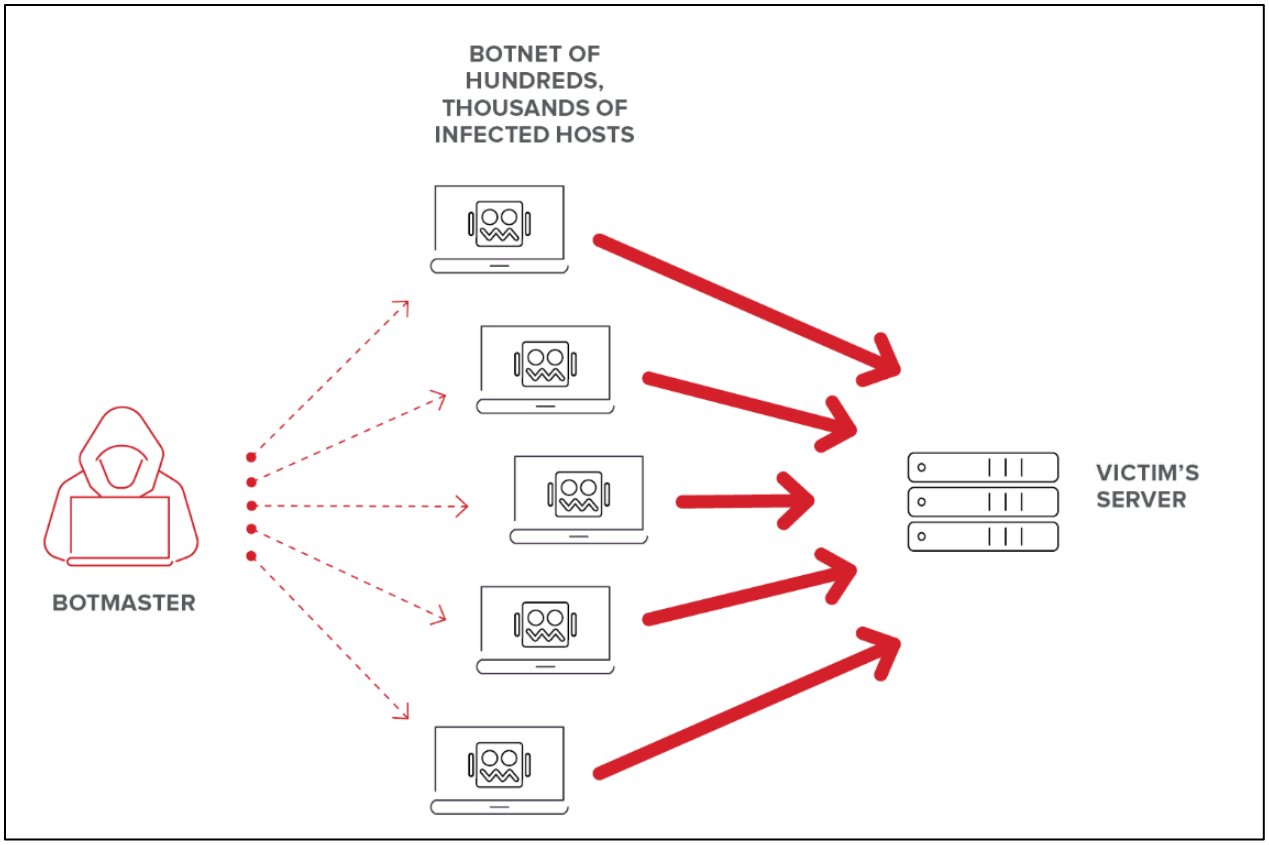
Working

It consist of devices which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots and a group of bots is called a **botnet**.

Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, causing the server or network to become overwhelmed, resulting in a denial-of-service to legitimate traffic.

Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.



Types of DDOS Attacks

- Application Layer Attacks
- Protocol Attacks
- Volumetric Attacks

Application Layer Attacks

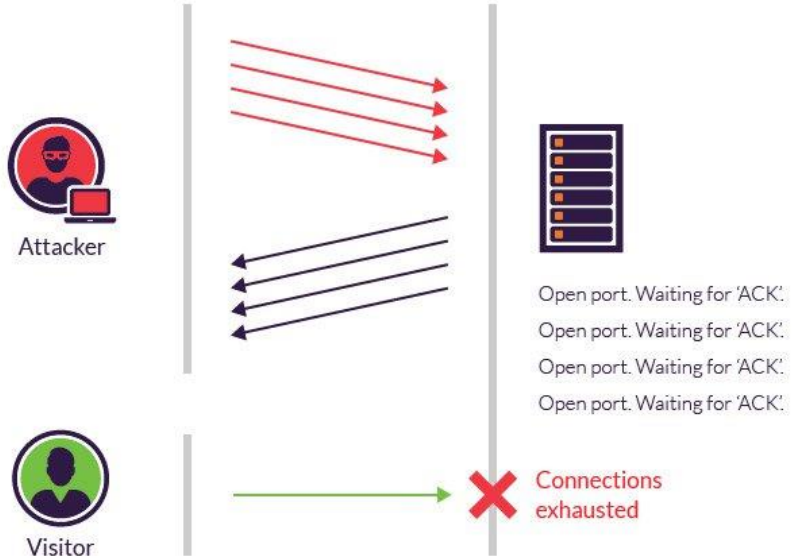
Sometimes referred to as a layer 7 DDoS attack, the goal of these attacks is to exhaust the target's resources to create a denial-of-service.

This attack is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial-of-service. (also called HTTP Flood)

These attacks are difficult to defend against, since it can be hard to differentiate malicious traffic from legitimate traffic.

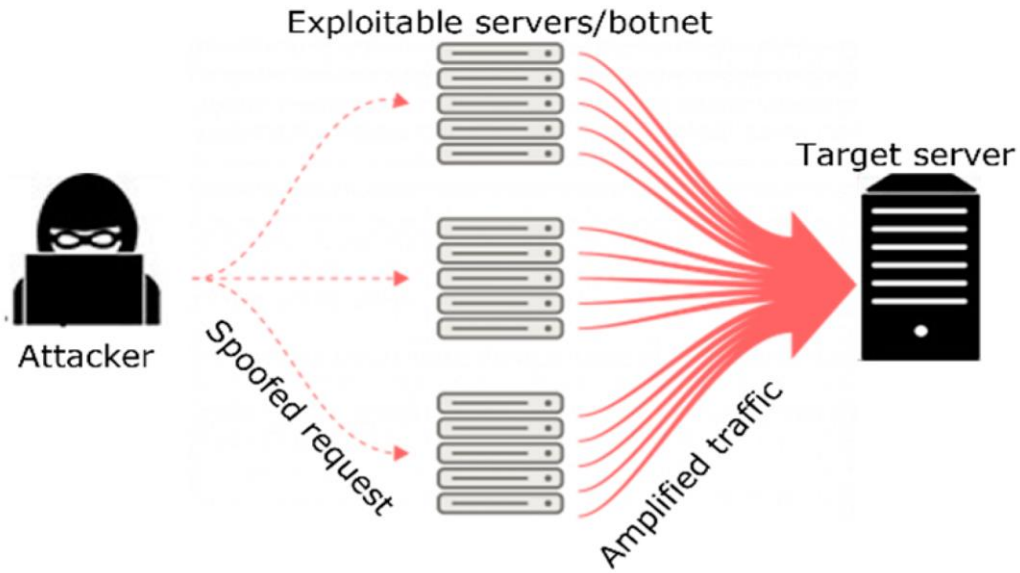
Protocol Attacks

Protocol attacks consume all available capacity of web servers or other resources, such as firewalls. They expose weaknesses in Layers 3 and 4 of the OSI protocol stack to render the target inaccessible. SYN flood is an example of it. It sends massive numbers of SYN requests to a server without replying with ACK packet to overwhelm it with open connections.



Volumetric Attack

This type of attack aims to control all available bandwidth between the victim and the larger internet. DNS amplification is an example of a volume-based attack. It uses DNS servers to amplify requests and targets the victim server by spoofing server's IP address.



Defenses against DDOS Attacks

Risk Assessments

Organizations should regularly conduct **risk assessments** and audits on their devices, servers, and network. While it is impossible to completely avoid a DDoS, a thorough awareness of both the strengths and vulnerabilities of the organization's hardware and software assets and network is key to understanding which strategy to implement to lessen the damage of DDoS attack.

Anycast Network Service

As a mitigation strategy, use an Anycast routing network to scatter the attack traffic across a network of distributed servers. Anycast distributes the remaining attack traffic across multiple servers, preventing any one location from becoming overwhelmed with requests. This is performed so that the traffic is absorbed by the network and becomes more manageable.

Cloudflare is a common Anycast Network Service provider.

Black hole routing

Another form of defense is black hole routing, in which a network administrator creates a black hole route and pushes traffic into that black hole. With this strategy, all traffic, both good and bad, is routed to a null route and essentially dropped from the network. This can be rather extreme, as legitimate traffic is also stopped and can lead to business loss.

Rate Limiting

Limiting the number of requests a server will accept over a certain time window is also a way of mitigating denial-of-service attacks.

While rate limiting is useful in mitigating brute force login attempts, it alone will likely be insufficient to handle a complex DDoS attack effectively.

Web Application Firewall (WAF)

To lessen the impact of an application-layer or Layer 7 attack, some organizations opt for a Web Application Firewall (WAF).

A WAF is a tool that sits between the internet and a company's servers. As with all firewalls, an organization can create a set of rules that filter requests. They can start with one set of rules and then modify them based on what they observe as patterns of suspicious activity carried out by the DDoS Attacks.