Vulnerabilities and Access Control

UNIT 2

What are Cyber Security Vulnerabilities?

Cybersecurity vulnerability applies to any form of exploitable weak spot that is damaging your organization's cybersecurity. E.g., if your company does not have a lock on the front door because you can easily walk in and grab things like a printer, this presents a security vulnerability. Similarly, a hacker will quickly find his way into your networks and capture sensitive data if your company does not have adequate firewalls. Since the compromised commodity is a digital one, not having sufficient firewalls poses a risk to cyber defense.

Vulnerabilities in Cyber security:

In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data.

Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications

Many vulnerabilities impact popular software, placing the many customers using the software at a heightened risk of a data breach, or supply chain attack.

Vulnerability definition:

There are a many definitions of vulnerability. Here is a list of definitions from various cybersecurity authorities.

National Institute of Standards and Technology (NIST): Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

ISO 27005: A weakness of an asset or group of assets that can be exploited by one or more cyber threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.

IETF RFC 4949: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

ENISA: The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

The Open Group: The probability that threat capability exceeds the ability to resist the threat.

Factor Analysis of Information Risk: The probability that an asset will be unable to resist the actions of a threat agent.

What is the difference between vulnerability and risk?

Cyber security risks are commonly classified as vulnerabilities. However, vulnerability and risk are not the same thing, which can lead to confusion.

Think of risk as the probability and impact of a vulnerability being exploited.

If the impact and probability of a vulnerability being exploit is low, then there is low risk. Inversely, if the impact and probability of a vulnerability being exploit is high, then there is a high risk.

Generally, the impact of a cyber attack can be tied to the CIA triad or the confidentiality, integrity or availability of the resource. Following this train of reasoning, there are cases where common vulnerabilities pose no risk. For example, when the information system with the vulnerability has no value to your organization.

Types of Cyber Security Vulnerabilities

What are the fundamental forms of cybersecurity flaws that might lead to active attacks and data breaches, and how can we minimize them ideally? Here is everything you need to know.

Weak Authentication and Credential Management

A lack of sound credential protection is one of the most frequent sources of compromise and violations of this cybersecurity weakness. People use the same password repeatedly, and many programs and utilities enable poor security practices. This is one of the leading causes mentioned in the Verizon DBIR list of associated attack vectors.

Causes: In several cases, the lack of governance and regulation of the credential lifecycle and legislation triggers poor authentication and credential management. This requires user rights, password rules, interfaces and controls for authentication, and privilege escalation for applications and utilities that, in many situations, may not be usable or open.

Measures: Implementing tight password controls is the key to most organizations. This consists of long and complicated passwords, or more regular password changes, or even a mixture. Longer passwords that are not always rotated are, in general, better than shorter passwords. Users should also be allowed to use multifactor authentication to enter sensitive data or pages with any discreet access, often with multi factor authentication tools.

Types of Cyber Security Vulnerabilities

Poor Security Awareness

A big challenge that plagues organizations is the vulnerability of end consumers to social engineering. The 2019 Verizon DBIR reports that the top hazard action in violations is an end-user mistake. Many organizations find that by targeted social engineering, most often phishing, the initial point of attack is.

Causes: A lack of sound protection awareness training and end-user confirmation is the most prevalent source of active phishing, pretexting, and other social engineering attacks. Organizations are also grappling with how to teach users to search through and report attempts at social engineering.

Measures: More institutions need to perform daily training activities, including phishing drills, pretexting, and additional psychological innovation. The teaching has to be contextual and related to the work functions of workers.

Types of Cyber Security Vulnerabilities

Poor Network Segmentation and Monitoring

Many attackers rely on poor network segmentation and monitoring to gain complete access to a network subnet. This has contributed to the considerable persistence of attackers breaching modern technologies and retaining more extended access.

Causes: A lack of subnet surveillance is a substantial root cause of this flaw, as is a lack of outbound operation monitoring that may suggest command and traffic control. This can be a problematic initiative, particularly in large organizations, when hundreds or thousands of systems can communicate inside the network simultaneously and send outbound traffic.

Measures: Organizations should closely monitor network connectivity to subnet networks and develop better identification and warning techniques for lateral movement. They should concentrate on unusual DNS lookups and odd network traffic behavioral patterns. Proxies, firewalls, and software for micro-segmentation will help build more stringent

Types of Cyber Security Vulnerabilities

Poor Endpoint Security Defenses

Zero-day attacks are becoming more widespread. Many of the security endpoint protections have proven ineffective in tackling sophisticated ransomware and intrusions targeting end-users and server platforms.

Causes: Traditional antivirus signature-based solutions are no longer considered sufficient since many savvy attackers can quickly bypass the signatures. Finally, many endpoint security protections, particularly on a broad scale, have not allowed security teams to respond to or investigate endpoints dynamically.

Measures: More companies need to invest in new endpoint detection and response tools that combine next-generation antivirus, behavioral intelligence, and real response capability. Consider an update to add more behavioral inspection and real-time reaction capability if you are presently using standard antivirus software.

Types of Cyber Security Vulnerabilities

Poor Data Backup and Recovery

Organizations have a pressing need to backup and restore data with the latest threat of malware looms high, along with conventional disasters and other failures. Unfortunately, many companies don’t succeed in this region due to a lack of proper backup and recovery options.

Causes: Many entities, including duplication of databases, storage synchronization or archival and preservation of end-user storage, ignore one or more aspects of backup and recovery.

Measures: Most organizations require a multi-pronged strategy of backup and recovery. This may provide snapshots and synchronization of data center storage, network storage, tape or file copies, and often cloud-based) end-user storage. Look for enterprise-class software that can handle measurements and report for granular backup and recovery.

What causes vulnerabilities?

Complexity
Complex systems increase the probability of a flaw, misconfiguration or unintended access

Familiarity
Common code, software, operating systems and hardware increase the probability that an attacker can find or has information about known vulnerabilities

Connectivity
The more connected a device is the higher the chance of a vulnerability.

Poor password management
Weak passwords can be broken with brute force and reusing passwords can result in one data breach becoming many.

What causes vulnerabilities?

Operating system flaws
Like any software, operating systems can have flaws. Operating systems that are insecure by default and give all users full access can allow viruses and malware to execute commands.

Internet usage
The Internet is full of spyware and adware that can be installed automatically on computers.

Software bugs
Programmers can accidentally or deliberately leave an exploitable bug in software.

Unchecked user input
If your website or software assume all input is safe it may execute unintended SQL commands.

People
The biggest vulnerability in any organization is the human at the end of the system. Social engineering is the biggest threat to the majority of organizations.

Examples of vulnerabilities

Vulnerabilities can be classified into six broad categories:

1. Hardware

Susceptibility to humidity, dust, soiling, natural disaster, poor encryption or firmware vulnerability.

2. Software

Insufficient testing, lack of audit trail, design flaws, memory safety violations (buffer overflows, over-reads, dangling pointers), input validation errors (code injection, cross-site scripting (XSS), directory traversal, email injection, format string attacks, HTTP header injection, HTTP response splitting, SQL injection), privilege-confusion bugs (clickjacking, cross-site request forgery, FTP bounce attack), race conditions (symlink races, time-of-check-to-time-of-use bugs), side channel attacks, timing attacks and user interface failures (blaming the victim, race conditions, warning fatigue).

3. Network

Unprotected communication lines, man-in-the-middle attacks, insecure network architecture, lack of authentication or default authentication.

Examples of vulnerabilities:

4. Personnel

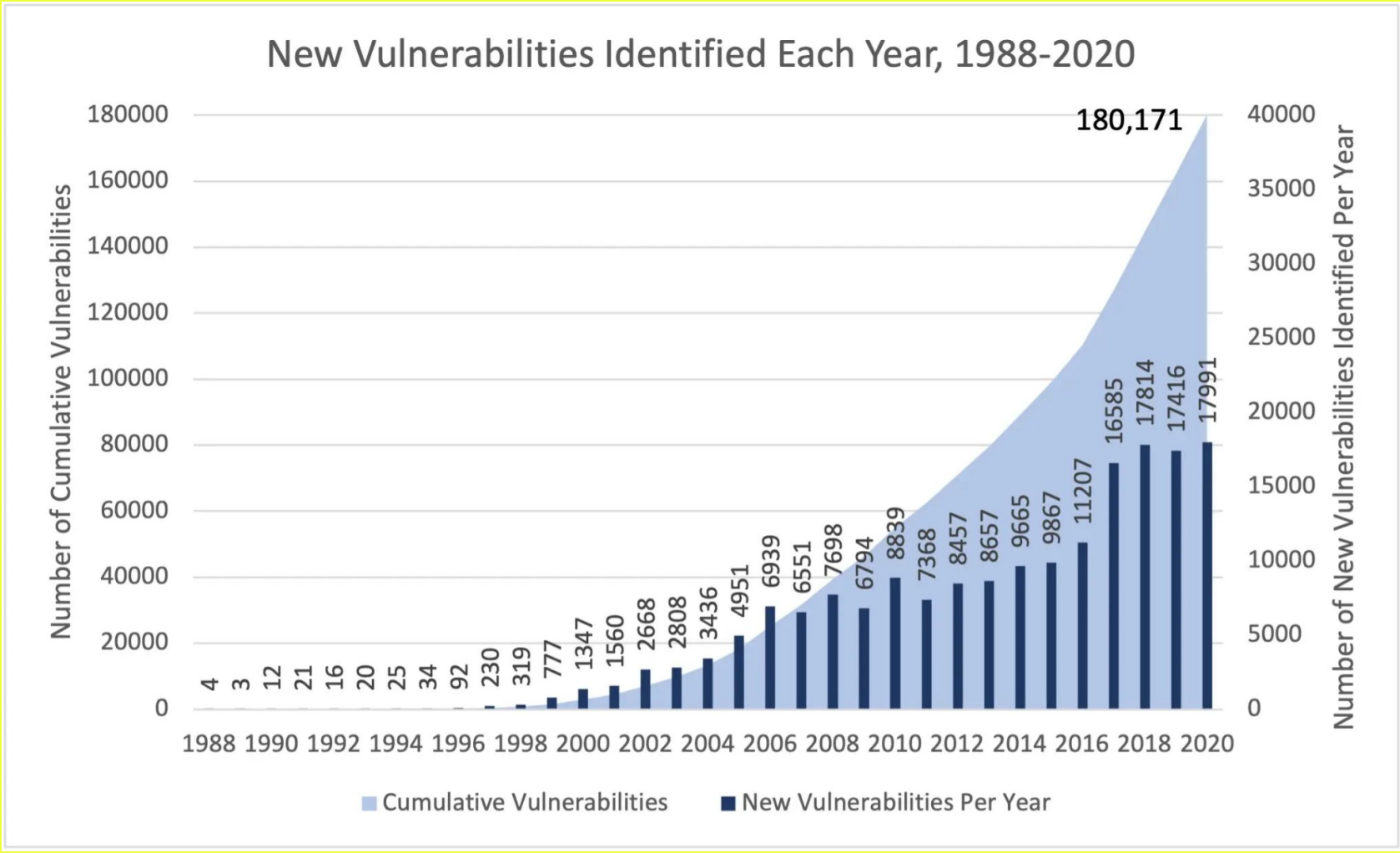
Poor recruiting policy, lack of security awareness and training, poor adherence to security training, poor password management or downloading malware via email attachments.

5. Physical site

Area subject to natural disaster, unreliable power source or no keycard access.

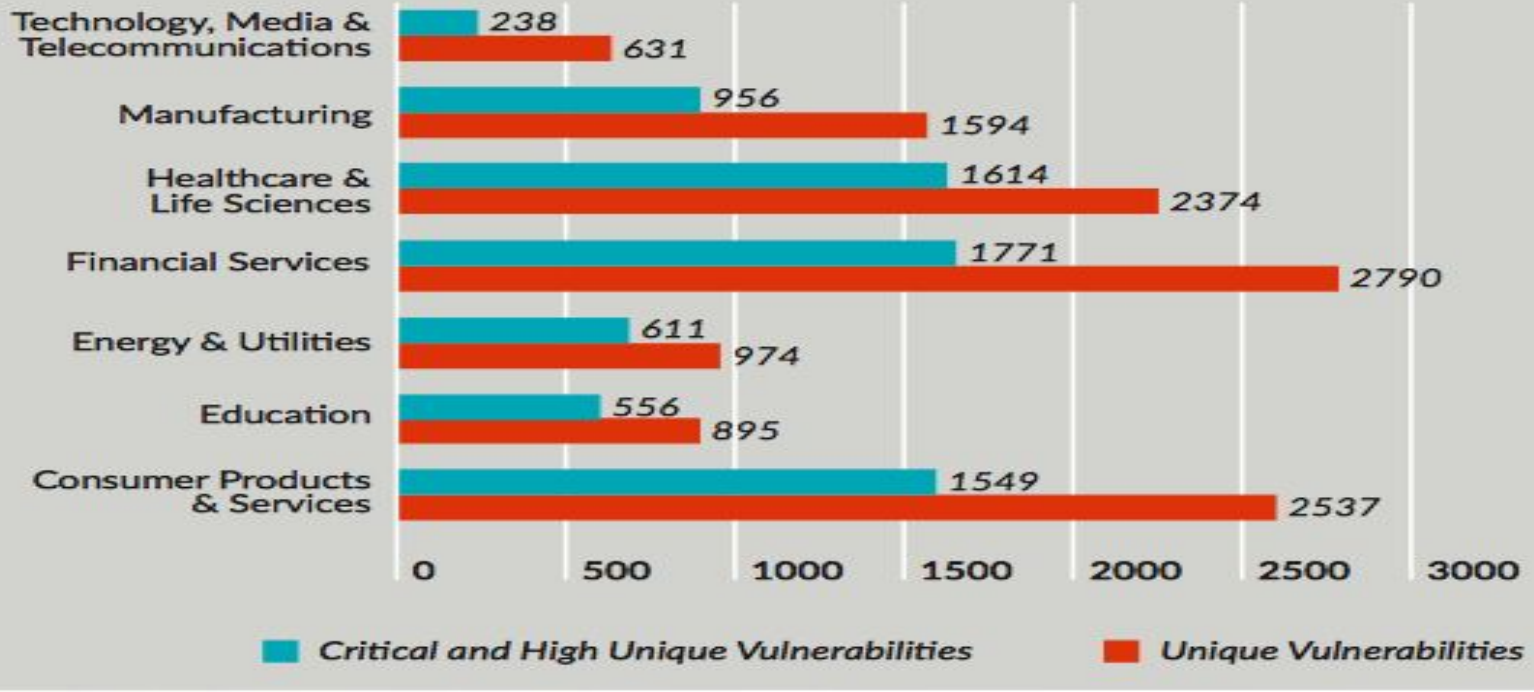
6. Organizational

Lack of audit, continuity plan, security or incident response plan.


New Vulnerabilities Identified Each Year, 1988-2020
Number of Cumulative Vulnerabilities
Number of New Vulnerabilities Identified Per Year
180,171
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
40000
35000
30000
25000
20000
15000
10000
5000
0
4
3
12
21
16
20
25
34
92
230
319
777
1347
1560
2668
2808
3436
4951
6939
6551
7698
6794
8839
7368
8457
8657
9665
9867
11207
16585
17814
17416
17991
1988 1990 1992 1994 1996 1998 2000 2002 2004 2006 2008 2010 2012 2014 2016 2018 2020
Cumulative Vulnerabilities
New Vulnerabilities Per Year

Technology, Media and Telecommunications organizations had the lowest percentage of vulnerabilities that were "critical" or "high" in severity.

Vulnerability Severity by Industry



vulnerabilities in software

Software Vulnerabilities Definition

Software vulnerabilities are weaknesses or flaws present in your code.

A software vulnerability is an instance of a fault in the specification, development, or configuration of software such that its execution can violate the (implicit or explicit) security policy.Reverse Engineering (Software Security)

Unfortunately, testing and manual code reviews cannot always find every vulnerability. Left alone, vulnerabilities can impact the performance and security of your software. They could even allow untrustworthy agents to exploit or gain access to your products and data.

Software Vulnerabilities

As we know a vulnerable software system can be exploited by attackers and the system could be compromised, the attacker might take control of the system to damage it, to launch new attacks or obtain some privileged information that he can use for his own benefit.

Considering this, it is important to know the different types of vulnerabilities, their prevention and detection in order to try to avoid their presence in the final software version of the system and then reduce the possibility of attacks and costly damages.

Types of Software Vulnerabilities

- Buffer overflows
  - Smash the stack
  - Overflows in setuid regions
- Heap overflows
- Format string vulnerabilities
- Reverse Engineering (Software Security)

Examples of vulnerabilities

Most of the known vulnerabilities are associated to an incorrect manner of dealing with the inputs supplied by an user of the system, if these inputs are not correctly processed before using them inside the program they can generate unexpected behavior of the system. For instance, some known and frequent vulnerabilities are

Buffer overflow: it occurs usually with fixed length buffers when some data is going to be written beyond the boundaries of the current defined capacity.This could lead to mal functioning of the system since the new data can corrupt the data of other buffers or processes. The buffer overflow can be used also to inject malicious code, and then the execution sequence of the program could be altered in order to execute the injected code and take control of the system.

XSS or cross site scripting: usually associated to web applications, consists in the injection of code in the pages accessed by other users. If exploited an attacker can bypass access controls, perform phishing, identity theft or expose connections.

SQL injection: it consists in the injection of code with the intension of exploiting the content of a database. Usually happens because the inputs are not handled correctly, the attacker can get sensitive information from the database.

When Attackers Target Vulnerabilities

Attacker creates exploits to target software vulnerability

OR

1. Exploits may arrive via:
- Attachment to email messages
- Comproised websites
- Social networking sites

2. Attacker may directly target vulnerable servers

Users are lured into executing the exploit via social engineering techniques

OR

Exploits may drop malware onto the vulnerable system or allow attackers remote control

REDUCING SOFTWARE VULNERABILITY

NIST National Institute of Standards and Technology U.S. Department of Commerce

New NIST interagency report (NISTIR) 8151 has five main sets of approaches for reducing vulnerabilities in software. In simple terms, according to NIST's Paul E. Black, these approaches are:

FORMAL METHODS

Math-based verification tools coders can easily apply.

"I drive a car. But even though I know nothing about hi-temperature steel or tire rubber, it just works."

SYSTEM LEVEL SECURITY

Modularizing a computer's programs so if one piece breaks the whole thing doesn't collapse.

"If my toaster breaks it shouldn't fry my house's circuit. But computers don't always have these 'circuit breaker' type structures."

ADDITIVE SOFTWARE ANALYSIS

Connecting analysis tools that currently operate in isolation.

"You get a better suit if the guy who measures your chest and the guy measuring your inseam communicate with each other."

DOMAIN SPECIFIC FRAMEWORKS

Use a more appropriate programming language for the task.

"Why not use a language that has words and concepts and data structures that are specific to that app? In fact they exist and are mature."

MOVING TARGET DEFENSE AND AUTOMATIC SOFTWARE DIVERSITY

"If someone's attacking you, instead of building walls while they find out where you are and drop bombs, it would be nice to be able to pick up and move rather than wait for the airstrike."

What is an exploit?

Exploits are automated scripts or sequences of commands that attackers use to manipulate vulnerabilities to their advantage. Exploit takes advantage of the vulnerability to break into the system and delivers the payload, which could be malware with instructions to disrupt system functions, steal sensitive data, or establish a connection with the remote hacker's systems.

System Administration

What is vulnerability management?

Vulnerability management is a cyclical process of identifying IT assets and correlating them with a continually updated vulnerability database to identify threats, misconfigurations, and vulnerabilities. Another aspect of vulnerability management includings validating the urgency and impact of each vulnerability based on various risk factors and responding to the critical threats swiftly.

Vulnerability assessment

Leverage risk-based assessment to prioritize imminent and impactful vulnerabilities

Security configuration management

Identify configuration drifts and misconfigurations and bring them back to compliance.

High-risk software audit

Audit and eliminate unauthorized, unsupported software in your network with the click of a button.

Web server hardening

Safeguard your internet-facing servers from many attack variants, like XSS and clickjacking.

patch management

Automate the entire cycle of patching to Windows, Mac, Linux and over 350 third-party applications.

Active port audit

Identify active ports and instances where a port has been activated by malicious executables.

Why do you need vulnerability management?

According to a recent Forrester Global Security Survey, '49 percent of organizations have suffered one or more breaches in the past year, and software vulnerabilities were the largest factor in those breaches'. On top of that, a whopping 22,316 new security holes were disclosed in 2019, and over one-third of them had an exploit available, highlighting the importance of organizations including vulnerability management in their security strategies.

Because, all it takes is a single vulnerability for the bad guys to stealthily slipin and steal data. It's not without reason there's such an emphasis on vulnerability management in the top 10 security controls published by Center for Internet Security (CIS).

But before you implement vulnerability management software in your organization, you should familiarize yourself with the barriers that stand in the way of effective vulnerability management and how you can break through them with Vulnerability Manager Plus.

Complex Network Architectures

COMPLEX NETWORK SYSTEM

Complex network systems cover most aspects of our daily life and are concerned with a wide range of communities, such as transportation, communication and information, energy systems, disaster and risk reduction and mitigation, finance, social networks and perception, and biological and medical systems, as well as academic researchers on theories of reliability, safety, risk, complexity, and networks .

Despite their enormous benefits to daily life, complex network systems also exhibit disadvantages, and one of the most challenging issues is the risk and safety of complex network systems. In a network system, the impact of a local hazard/fault/disturbance can easily spread out to the whole system due to domino effect, cascading effect, and/or ripple effect and eventually evolves into a large-scale disaster .

The finding of “six degrees of separation” may partially illustrate how efficiently the impact of a local event can spread in a network . The speedup of globalization process nowadays just makes the situation even worse .

WEAK AUTHENTICATION

Weak Authentication

Weak authentication refers to the vulnerabilities or weaknesses inherent in an online platform or application that allows hackers to bypass the login security and gain access to all the privileges owned by the hacked user.

Authentication ensures that only a verified user can access the information and privileges on the web application.

It gets ‘broken’ when an attacker bypasses the process and impersonates the user on the application.

These inherent weaknesses mentioned earlier can broadly be classified into two categories -namely, poor session management and poor credential management.

What is Weak Authentication ?

The more difficult an authentication mechanism is to defeat the stronger it is. Clearly the authentication strength of a system should correlate to the value of the assets it is protecting. Two-Factor and Multi-Factor Authentication solutions are appropriate for systems that deal with highly valued assets.

Weak Authentication describes any scenario in which the strength of the authentication mechanism is relatively weak compared to the value of the assets being protected. It also describes scenarios in which the authentication mechanism is flawed or vulnerable.

How do authentication vulnerabilities arise?

Broadly speaking, most vulnerabilities in authentication mechanisms arise in one of two ways:

- The authentication mechanisms are weak because they fail to adequately protect against brute-force attacks.
- Logic flaws or poor coding in the implementation allow the authentication mechanisms to be bypassed entirely by an attacker. This is sometimes referred to as "broken authentication".

In many areas of web development, logic flaws will simply cause the website to behave unexpectedly, which may or may not be a security issue. However, as authentication is so critical to security, the likelihood that flawed authentication logic exposes the website to security issues is clearly elevated.

What is the impact of vulnerable authentication?

The impact of authentication vulnerabilities can be very severe. Once an attacker has either bypassed authentication or has brute-forced their way into another user's account, they have access to all the data and functionality that the compromised account has. If they are able to compromise a high-privileged account, such as a system administrator, they could take full control over the entire application and potentially gain access to internal infrastructure.

Even compromising a low-privileged account might still grant an attacker access to data that they otherwise shouldn't have, such as commercially sensitive business information. Even if the account does not have access to any sensitive data, it might still allow the attacker to access additional pages, which provide a further attack surface. Often, certain high-severity attacks will not be possible from publicly accessible pages, but they may be possible from an internal page.

Vulnerabilities in authentication mechanisms

A website's authentication system usually consists of several distinct mechanisms where vulnerabilities may occur. Some vulnerabilities are broadly applicable across all of these contexts, whereas others are more specific to the functionality provided.

We will look more closely at some of the most common vulnerabilities in the following areas:

- Vulnerabilities in password-based login
- Vulnerabilities in multi-factor authentication
- Vulnerabilities in other authentication mechanisms

Example Of Weak Authentication

Session Hijacking: As explained above, verified Session IDs may be hijacked impersonate user identities. If a user forgets to log off from a public computer, any other individual can continue that session using the same Session ID that was previously created for the original user. If the same ID is issued before and after authentication, it may lead to a type of broken authentication attack, known as Session Fixation attacks.

Session ID URL: In this example, the Session ID appears in the website URL, and any individual who accesses the URL through a wired or wireless network, can use it to impersonate the user's identity.

Credential Stuffing: Sometimes, hackers access a database containing users' user-passwords that are unencrypted, and may often employ tactics to determine if the passwords are valid and functional. This is called credential stuffing, and a secure web application must have protocols that guard against such attempts.

Password Spraying: Password spraying refers to the use of the most common and weak passwords, such as 'password' or '123456' by hackers trying to access secure accounts. Consequently, minimum password requirements have been introduced to avoid such attacks.

Phishing Attacks: Hackers o phish by sending users links to a website that resembles the original web application, to get users to divulge their login credentials. Phishing attacks can be easily prevented, however, with proper diligence and by verifying the web application in use.

Cyber Security Safeguards:Overview

A DEFINITION OF CYBER SECURITY

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

THE IMPORTANCE OF CYBER SECURITY

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it.

As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation’s top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

Cybersecurity safeguards

Cybersecurity safeguards are the fundamental part of a cybersecurity investment. They are the expected outcomes of a cybersecurity investment and must be understood sufficiently so that they can be analyzed and evaluated within a systematic decision making process. This chapter explains the basics of safeguards and shows how they can be distinguished from the perspectives of function and time. From the functional perspective, there are administrative and technical safeguards. This perspective will be taken into account when it shall be clarified if technical means are necessary to support or enable the safeguards.

Cybersecurity safeguards

The perspective of time allows a distinction between preventive, detective and corrective safeguards. This considers the time when a safeguard becomes effective, in particular before, while or after an event. Based on these perspectives, a structure of safeguards is presented, which helps to specify safeguards concurrently regarding function and time. Then, the most common safeguards are explained in detail. Every safeguard is described in order to create an understanding that is focused on the basic characteristics and the intentional use of the safeguards.

Example Of Cyber Security Safe Gaurds

These include virus scanners, firewalls, monitoring operating system logs, software logs, version control and document disposition certification. Encrypted storage and transmission is necessary for particularly sensitive personal health information.

Access control

Access control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: **physical and logical.**

Physical access control limits access to campuses, buildings, rooms and physical IT assets.

Logical access control limits connections to computer networks, system files and data.

Access control

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

Why is access control important?

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information (PII) and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on (SSO) systems to unified access management, which offers access controls for on-premises and cloud environments.

How access control works?

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or Internet Protocol (IP) address. Directory services and protocols, including Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Organizations use different access control models depending on their compliance requirements and the security levels of information technology (IT) they are trying to protect

Access control software

There are many types of access control software and technology, and often, multiple components are used together to maintain access control. The software tools may be on premises, in the cloud or a hybrid of both. They may focus primarily on a company's internal access management or may focus outwardly on access management for customers. Some of the types of access management software tools include the following:

- reporting and monitoring applications
- password management tools
- provisioning tools
- identity repositories
- security policy enforcement tools

Microsoft Active Directory (AD) is one example of software that includes most of the tools listed above in a single offering. Other vendors with popular products for identity and access management (IAM) include IBM, Idaptive and Okta.

Audit

What is a cyber security audit?

- A cyber security audit is a systematic and independent examination of an organization's cyber security. An audit ensures that the proper security controls, policies, and procedures are in place and working effectively.
- Your organization has a number of cyber security policies in place. The purpose of a cyber security audit is to provide a 'checklist' in order to validate your controls are working properly. In short, it allows you to inspect what you expect from your security policies.
- The objective of a cyber security audit is to provide an organization's management, vendors, and customers, with an assessment of an organization's security posture.
- Audits play a critical role in helping organizations avoid cyber threats. They identify and test your security in order to highlight any weaknesses or vulnerabilities that could be expolited by a potential bad actor.

What does an audit cover?

A cyber security audit focuses on cyber security standards, guidelines, and policies. Furthermore, it focuses on ensuring that all security controls are optimized, and all compliance requirements are met.

Specifically, an audit evaluates:

- Operational Security (a review of policies, procedures, and security controls)
- Data Security (a review of encryption use, network access control, data security during transmission and storage)
- System Security (a review of patching processes, hardening processes, role-based access, management of privileged accounts, etc.)
- Network Security (a review of network and security controls, anti-virus configurations, SOC, security monitoring capabilities)
- Physical Security (a review of role-based access controls, disk encryption, multifactor authentication, biometric data, etc.)

Unlike a cyber security assessment, which provides a snapshot of an organization's security posture. An audit is a 360 in-depth examination of an organization's entire security posture.

Benefits of a cyber security audit

A cyber security audit is the highest level of assurance service that an independent cyber security company offers.

It provides an organization, as well as their business partners and customers, with confidence in the effectiveness of their cyber security controls. Unfortunately, internet threats and data breaches are more prevalent than ever before. As a result, business leaders and consumers increasingly prioritize and value cyber security compliance.

Benefits of a cyber security audit

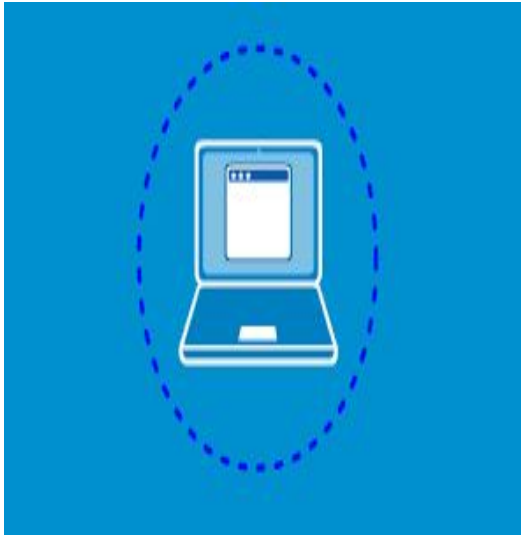
Specfically the following are some benefits of performing an audit:

- Identifying gaps in security
- Highlight weaknesses
- Compliance
- Reputational value
- Testing controls
- Improving security posture
- Staying ahead of bad actors
- Assurance to vendors, employees, and clients
- Confidence in your security controls
- Increased performance of your technology and security

AUTHENTICATION

The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization .

AUTHENTICATION



It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be.

A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process.

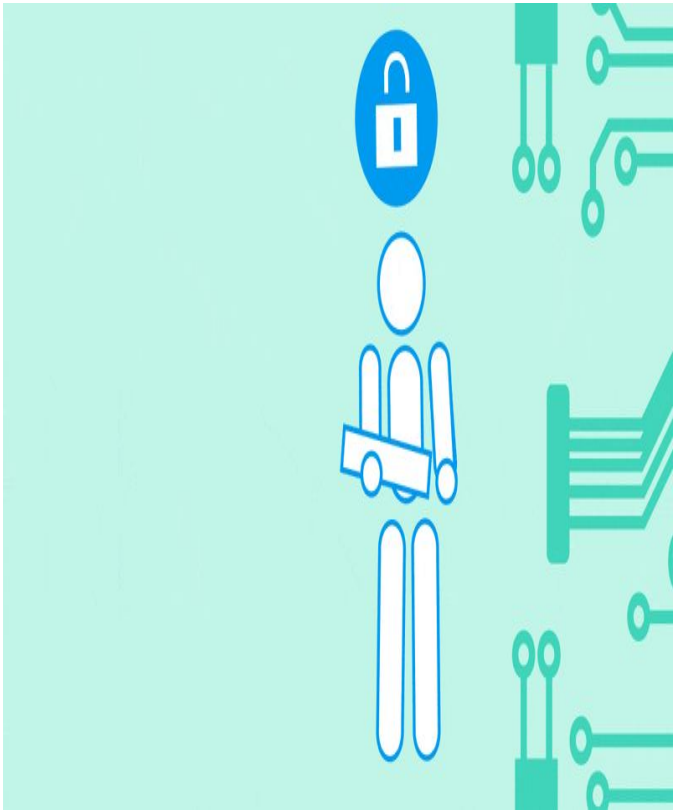
AUTHENTICATION

It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

Authentication

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network.

In some of the bigger organizations or an organization which deals in sensitive information like defence agencies, financial institutions, planning commissions, etc. a hybrid authentication system is used which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use VPN(Virtual Private Network), which is one of the method to provide secure access via hybrid security authentication to the company network over internet.




Multi-Factor Authentication
Password
Verification
Access

BIOMETRIC

Biometrics

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics.

The technology is mainly used for identification and access control or for identifying individuals who are under surveillance.

The basic premise of biometric authentication is that every person can be accurately identified by their intrinsic physical or behavioral traits.

The term biometrics is derived from the Greek words ***bio, meaning life, and metric, meaning to measure.***

How biometrics works?

Authentication by Biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale (POS) applications.

In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry.

Some biometric methods, such as measuring a person's gait, can operate with no direct contact with the person being authenticated.

How biometrics works ?

Components of biometric devices include the following:

- a reader or scanning device to record the biometric factor being authenticated;
- software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data; and
- a database to securely store biometric data for comparison.

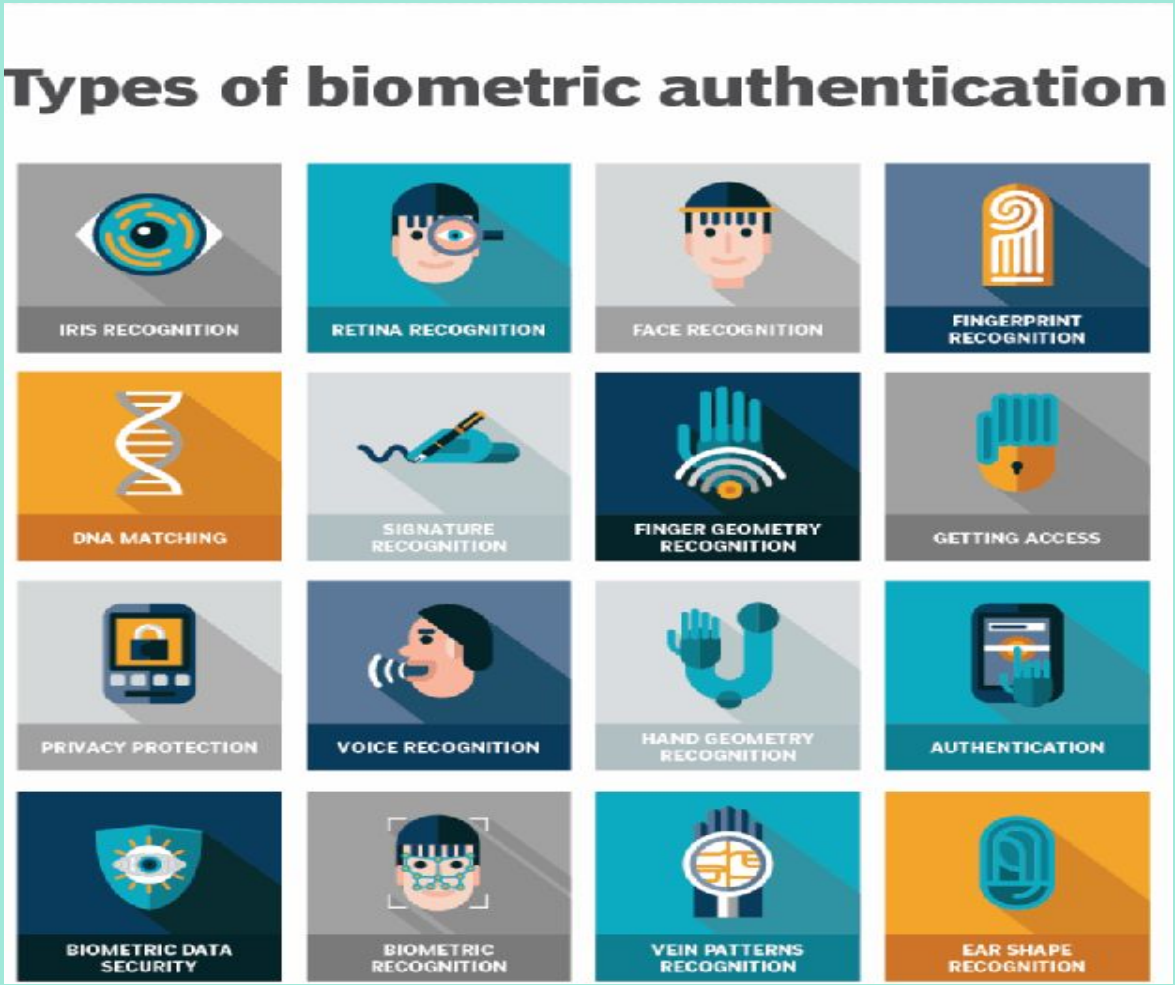
Biometric data may be held in a centralized database, although modern biometric implementations often depend instead on gathering biometric data locally and then cryptographically hashing it so that authentication or identification can be accomplished without direct access to the biometric data itself.

Types of biometrics

The two main types of biometric identifiers are either physiological characteristics or behavioral characteristics.

Physiological identifiers relate to the composition of the user being authenticated and include the following:

- Facial recognition
- Fingerprints
- Finger geometry (the size and position of fingers)
- Vein recognition
- Retina scanning
- **DNA (deoxyribonucleic acid) matching**
- digital signatures



Biometric data can be used to access information on a device like a smartphone, but there are also other ways biometrics can be used.

For example, biometric information can be held on a smart card, where a recognition system will read an individual's biometric information, while comparing that against the biometric information on the smart card.

Advantages of biometrics

The use of biometrics has plenty of advantages and disadvantages regarding its use, security and other related functions. Biometrics are beneficial because they are:

- hard to fake or steal, unlike passwords;
- easy and convenient to use;
- generally, the same over the course of a user's life;
- nontransferable; and
- efficient because templates take up less storage.

Disadvantages

- It is costly to get a biometric system up and running.
- If the system fails to capture all of the biometric data, it can lead to failure in identifying a user.
- Databases holding biometric data can still be hacked.
- Errors such as false rejects and false accepts can still happen.
- If a user gets injured, then a biometric authentication system may not work -- for example, if a user burns their hand, then a fingerprint scanner may not be able to identify them

Examples of biometrics in use

Aside from biometrics being in many smartphones in use today, biometrics are used in many different fields. As an example, biometrics are used in the following fields and organizations:

Law enforcement. It is used in systems for criminal IDs, such as fingerprint or palm print authentication systems.

The United States Department of Homeland Security. It is used in Border Patrol branches for numerous detection, vetting and credentialing processes -- for example, with systems for electronic passports, which store fingerprint data, or in facial recognition systems.

Healthcare. It is used in systems such as national identity cards for ID and health insurance programs, which may use fingerprints for identification.

Airport security. This field sometimes uses biometrics such as iris recognition.

However, not all organizations and programs will opt in to using biometrics. As an example, some justice systems will not use biometrics so they can avoid any possible error that may occur.

Biometric vulnerabilities

While high-quality cameras and other sensors help enable the use of biometrics, they can also enable attackers. Because people do not shield their faces, ears, hands, voice or gait, attacks are possible simply by capturing biometric data from people without their consent or knowledge.

An early attack on fingerprint biometric authentication was called the gummy bear hack, and it dates back to 2002 when Japanese researchers, using a gelatin-based confection, showed that an attacker could lift a latent fingerprint from a glossy surface; the capacitance of gelatin is similar to that of a human finger, so fingerprint scanners designed to detect capacitance would be fooled by the gelatin transfer.

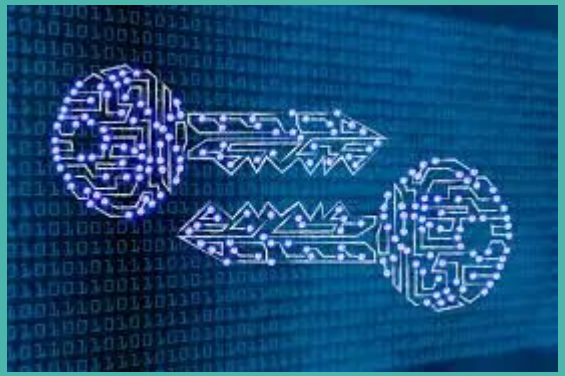
Biometric vulnerabilities

Determined attackers can also defeat other biometric factors. In 2015, Jan Krissler, also known as Starbug, a Chaos Computer Club biometrics researcher, demonstrated a method for extracting enough data from a high-resolution photograph to defeat iris scanning authentication. In 2017, Krissler reported defeating the iris scanner authentication scheme used by the Samsung Galaxy S8 smartphone. Krissler had previously recreated a user's thumbprint from a high-resolution image to demonstrate that Apple's Touch ID fingerprinting authentication scheme was also vulnerable.

After Apple released iPhone X, it took researchers just two weeks to bypass Apple's Face ID facial recognition using a 3D-printed mask; Face ID can also be defeated by individuals related to the authenticated user, including children or siblings.

https://youtu.be/i4YQRLQVixM

Cryptography



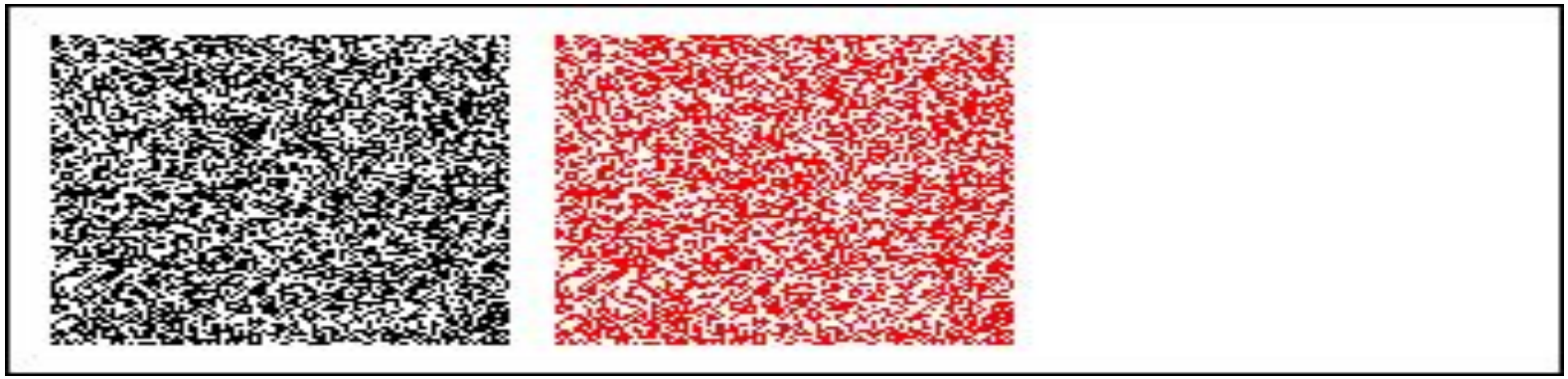
Cryptography

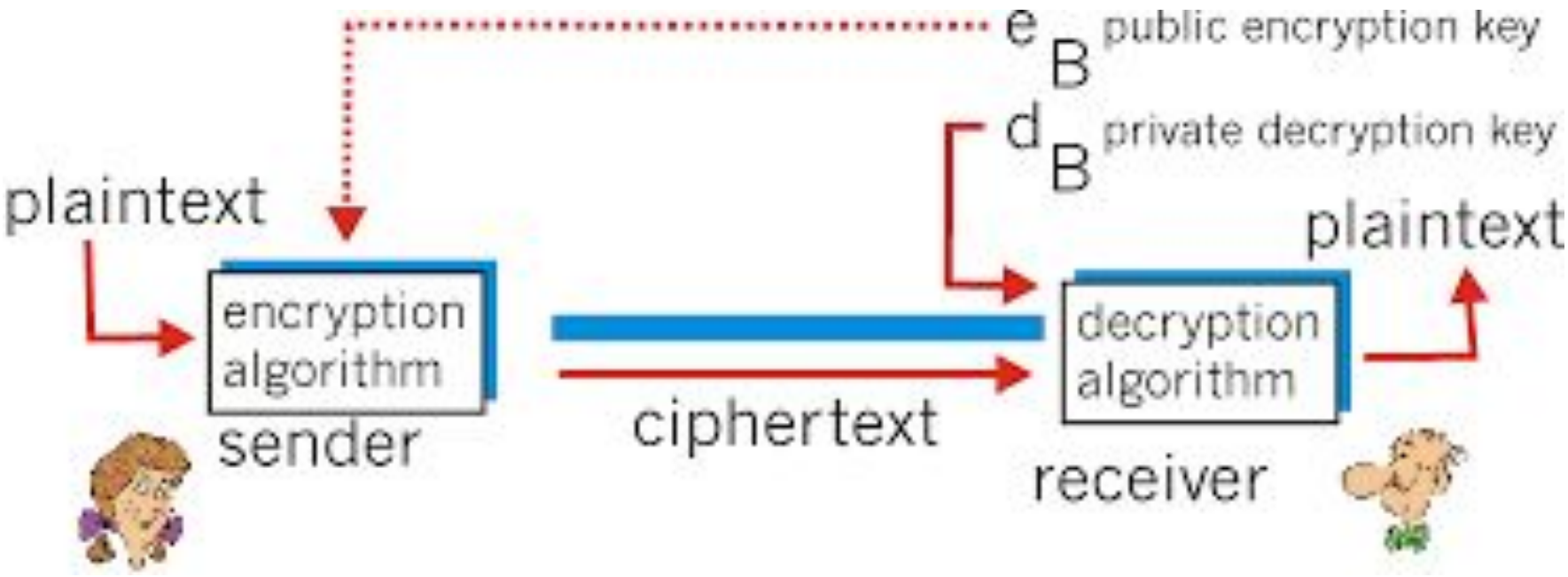
Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Definition:

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.




e
B
public encryption key
d
B
private decryption key
plaintext
encryption
algorithm
sender
ciphertext
decryption
algorithm
receiver
plaintext

Techniques used For Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Plain Text Message

Features Of Cryptography are as follows

Confidentiality:

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity:

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:

The creator/sender of information cannot deny his or her intention to send information at later stage.

Authentication:

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

2. Hash functions.

3. Public-key cryptography

Symmetric-key Cryptography:

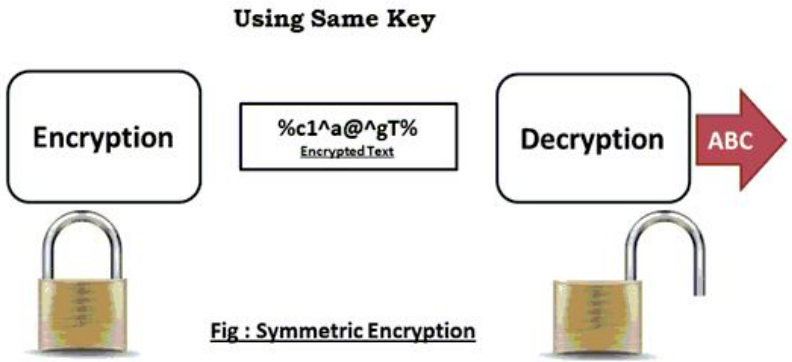


Fig : Symmetric Encryption

Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

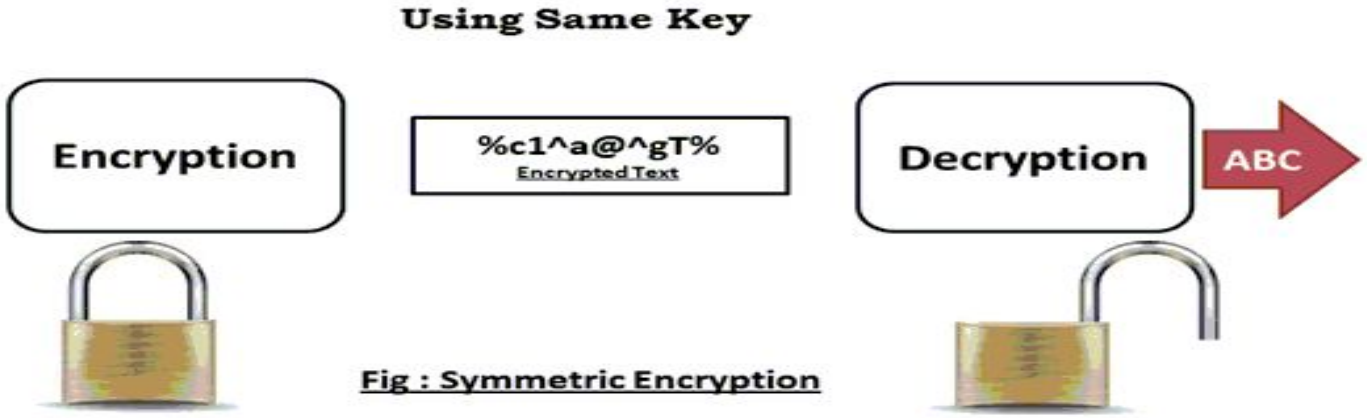


Fig : Symmetric Encryption

Public-Key Cryptography:

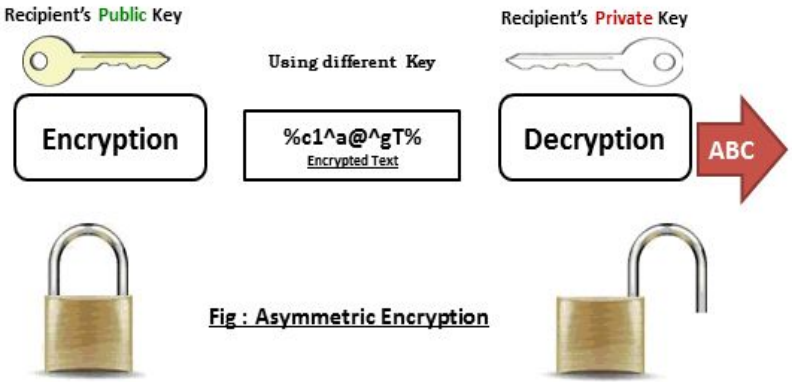


Fig : Asymmetric Encryption

This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

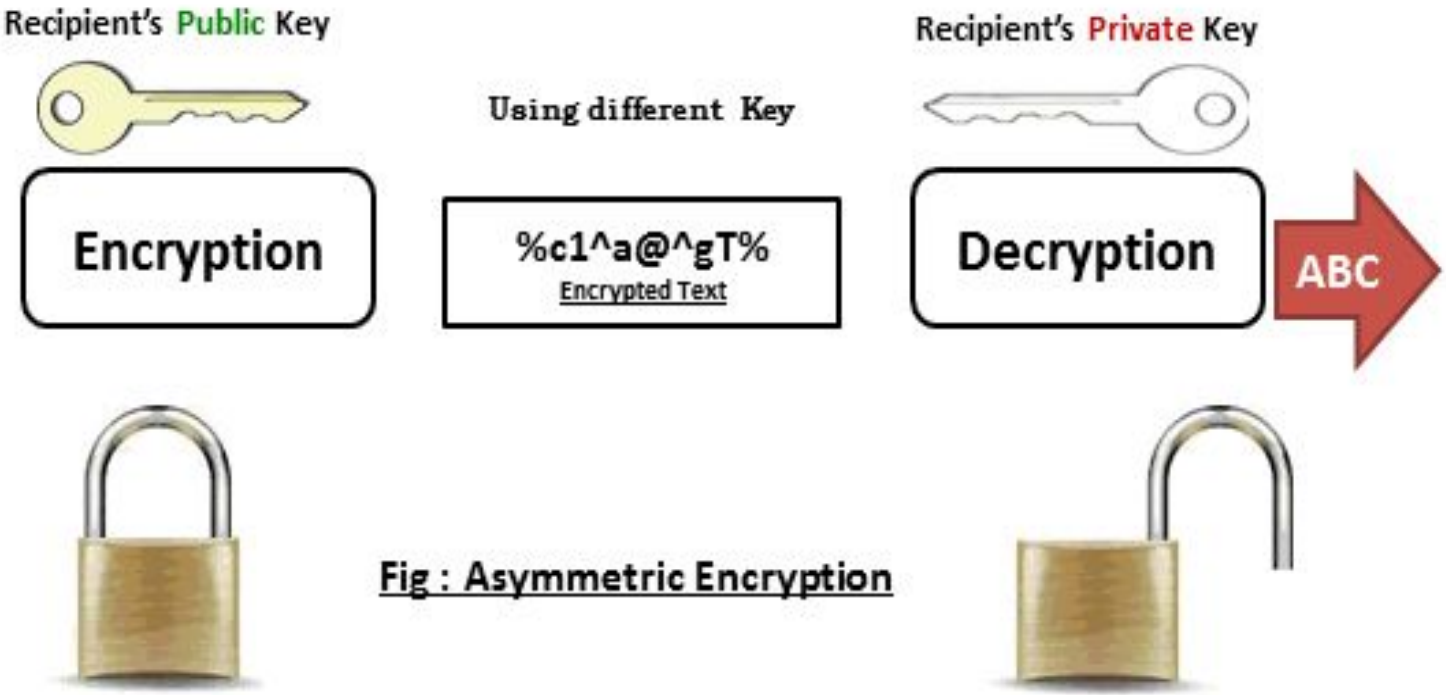
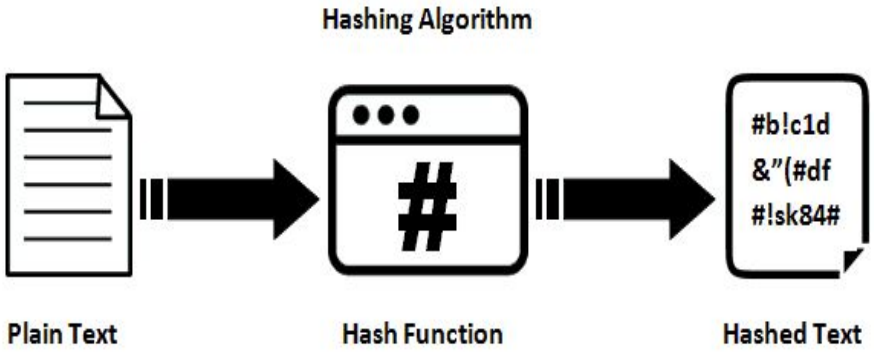


Fig : Asymmetric Encryption

Hash Functions:



No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

DECEPTION

Deception technology is an emerging category of cyber security defense. Deception technology products can detect, analyze, and defend against zero-day and advanced attacks, often in real time

Deception technology

The aim of deception technology is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage. The technology works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure. These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials. Once a trap is triggered, notifications are broadcast to a centralized deception server that records the affected decoy and the attack vectors that were used by the cybercriminal.

Deception technology

Deception technology is usually not a primary cybersecurity strategy that organizations adopt. The goal of any security posture is protection against all unauthorized access, and deception technology can be a useful technique to have in place once a suspected breach has occurred. Diverting the cyber criminal to fake data and credentials can be key to protecting the enterprise's real assets.'

Another benefit of deception technology is research. By analyzing how cyber criminals break the security perimeter and attempt to steal what they believe to be legitimate data, IT security analysts can study their behavior in depth. In fact, some organizations deploy a centralized deception server that records the movements of malicious actors—first as they gain unauthorized access and then as they interact with the decoy. The server logs and monitors any and all vectors used throughout the attack, providing valuable data that can help the IT team strengthen security and prevent similar attacks from happening in the future.

.

Deception technology

The downside or risk of deception technology is that cyber criminals have escalated the size, scope, and sophistication of their attacks, and a breach may be greater than what the deception server and its associated shadow or mock assets can handle. Further, cyber criminals may be able to quickly determine that they themselves are being tricked as the deception server and decoy assets become immediately obvious to them. As such, they can quickly abort the attack—and likely return even stronger.

To function properly, deception technology must not be obvious to an enterprise's employees, contractors, or customers.

examples of common lures and breadcrumbs are fake network drive maps, fake network connections, fake browser history, fake registry entries, fake files and many, many others.

Ethical Hacking

Ethical Hacking

Ethical Hacking tutorial provides basic and advanced concepts of Ethical Hacking. Our Ethical Hacking tutorial is developed for beginners and professionals.

Ethical hacking tutorial covers all the aspects associated with hacking. Firstly, we will learn how to install the needed software. After this, we will learn the 4 type of penetration testing section which is network hacking, gaining access, post exploitation, website hacking.

In network hacking section, we will learn how networks work, how to crack Wi-Fi keys and gain access the Wi-Fi networks. In Gaining access section, we will learn how to gain access to the servers and personal computers. In the post-exploitation section, we will learn what can we do with the access that we gained in the previous section. So we learn how to interact with the file system, how to execute a system command, how to open the webcam. In the website hacking section, we will learn how the website works, how to gather comprehensive information about website. In the end, we will learn how to secure our system from the discussed attacks.

Hacking

Gaining access to a system that you are not supposed to have access is considered as hacking. For example: login into an email account that is not supposed to have access, gaining access to a remote computer that you are not supposed to have access, reading information that you are not supposed to able to read is considered as hacking. There are a large number of ways to hack a system.

In 1960, the first known event of hacking had taken place at MIT and at the same time, the term Hacker was organized.

Ethical hacking

Ethical hacking is also known as White hat Hacking or Penetration Testing. Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system or data. Ethical hacking is used to improve the security of the systems and networks by fixing the vulnerability found while testing.

Ethical hackers improve the security posture of an organization. Ethical hackers use the same tools, tricks, and techniques that malicious hackers used, but with the permission of the authorized person. The purpose of ethical hacking is to improve the security and to defend the systems from attacks by malicious users.

Hacker and Ethical Hacker

❖ **Hacker**

- Access computer system or network without authorization
- Breaks the law

❖ **Ethical Hacker**

- Performs most of the same activities but with owner's permission
- Employed by companies to perform Penetration Tests

Importance of Ethical Hacking?

In the dawn of international conflicts, terrorist organizations funding cybercriminals to breach security systems, either to compromise national security features or to extort huge amounts by injecting malware and denying access. Resulting in the steady rise of cybercrime. Organizations face the challenge of updating hack-preventing tactics, installing several technologies to protect the system before falling victim to the hacker.

New worms, malware, viruses, and ransomware are primary benefit are multiplying every day and is creating a need for ethical hacking services to safeguard the networks of businesses, government agencies or defense.

Ethical Hackers but not Criminal Hackers

Completely trustworthy.

Strong programming and computer networking skills.

Learn about the system and trying to find its weaknesses.

Techniques of Criminal hackers-Detection- Prevention.

Types of Hacking

Network Hacking: Network hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert, etc.

Website hacking: Website hacking means taking unauthorized access over a web server, database and make a change in the information.

Computer hacking: Computer hacking means unauthorized access to the Computer and steals the information from PC like Computer ID and password by applying hacking methods.

Password hacking: Password hacking is the process of recovering secret passwords from data that has been already stored in the computer system.

Email hacking: Email hacking means unauthorized access on an Email account and using it without the owner's permission.

Advantages of Hacking

1. It is used to recover the lost of information, especially when you lost your password.
2. It is used to perform penetration testing to increase the security of the computer and network.
3. It is used to test how good security is on your network.

Disadvantages of Hacking

1. IT can harm the privacy of someone.
2. Hacking is illegal.
3. Criminal can use hacking to their advantage.
4. Hampering system operations.

Benefits of Ethical Hacking?

- The primary benefit of ethical hacking is to prevent data from being stolen and misused by malicious attackers, as well as:
- Discovering vulnerabilities from an attacker's POV so that weak points can be fixed.
- Implementing a secure network that prevents security breaches.
- Defending national security by protecting data from terrorists.
- Gaining the trust of customers and investors by ensuring the security of their products and data.
- Helping protect networks with real-world assessments.

Types of Hackers

- Hackers are of different types and are named based on their intent of the hacking system. Broadly, there are two main hackers – White-Hat hacker and Black-Hat hacker.
- The names are derived from old Spaghetti Westerns, where the good guy wears a white hat and the bad guy wears a black hat.

Black Hat Hacker

Black-hat Hackers are also known as an Unethical Hacker or a Security Cracker. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

White hat Hackers are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good guys of the hacker world.

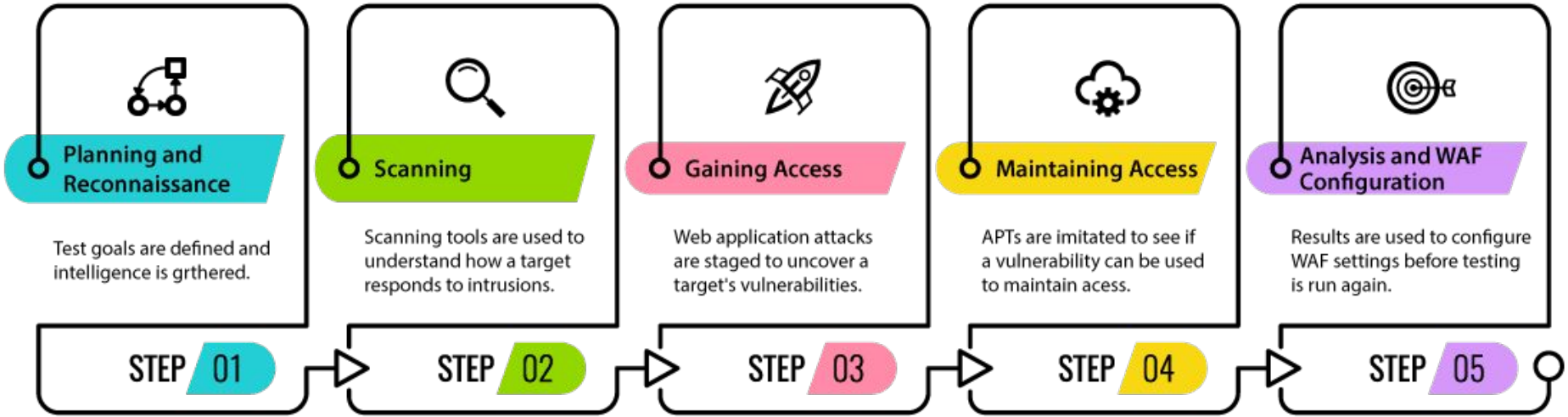
These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

Phases of Ethical Hacking



Phases of Ethical Hacking

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points. An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.

An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system. The ethical hacking process begins with looking for various ways to hack into the system, exploiting vulnerabilities, maintaining steady access to the system, and lastly, clearing one's tracks.

Required Skills of an Ethical Hacker

Microsoft: skills in operation, configuration and management. Linux: knowledge of

Linux/Unix; security setting, configuration, and services.

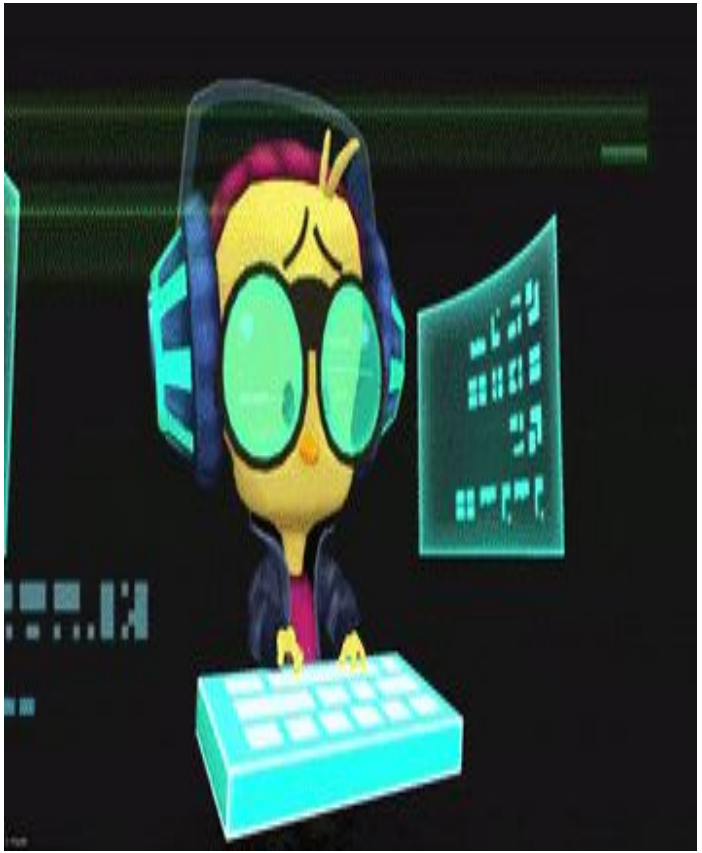
Firewalls: configurations, and operation of intrusion detection systems.

Routers: knowledge of routers, routing protocols, and access control lists

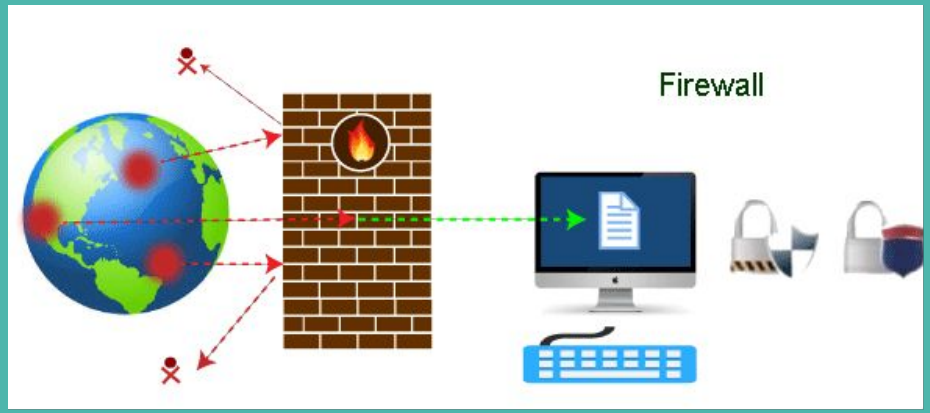
Mainframes : knowledge of mainframes

Network Protocols: TCP/IP; how they function and can be manipulated.

Project Management: leading, planning, organizing, and controlling a penetration testing team.



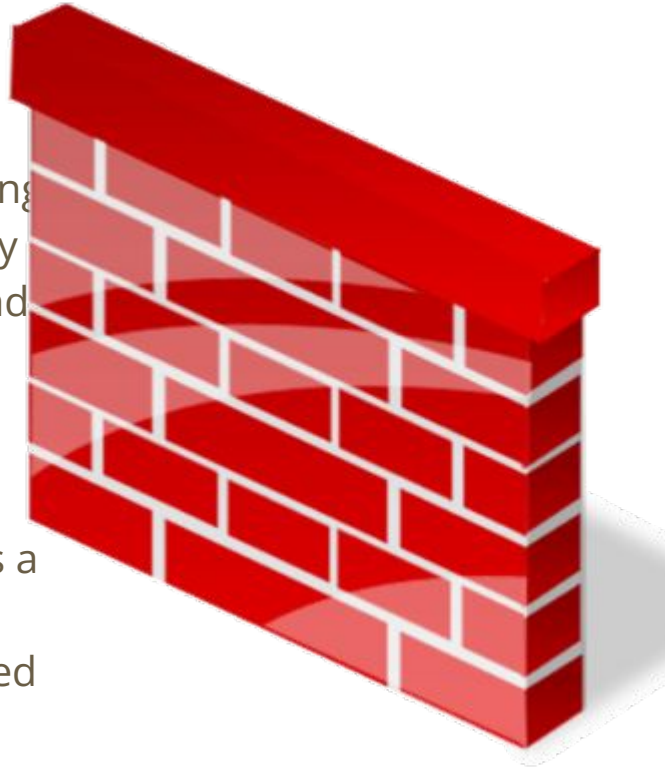
FIREWALL



What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

Firewalls

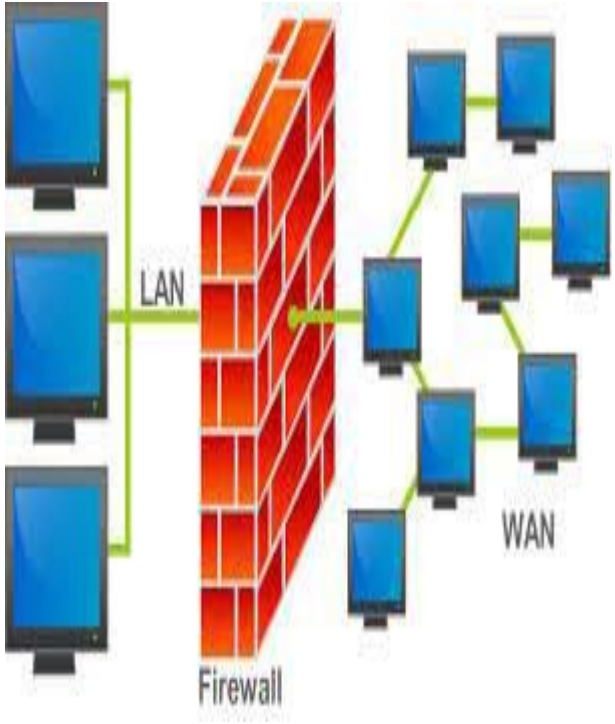
It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.

Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations‟ network.

Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.



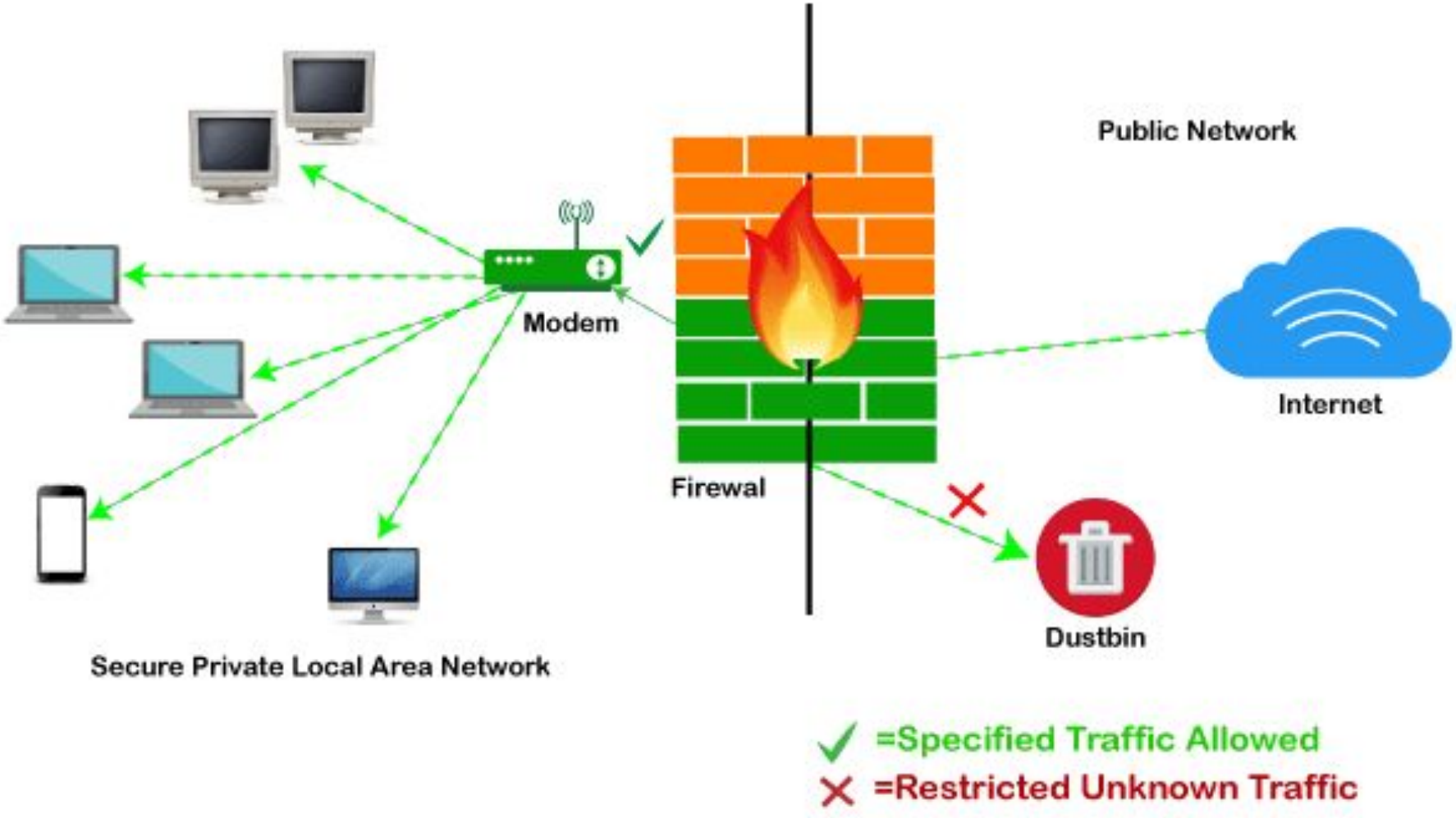
Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as traffic controller.

Some of the important risks of not having a firewall are:

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.


Public Network
Modem
Firewal
Internet
Dustbin
Secure Private Local Area Network
=Specified Traffic Allowed
=Restricted Unknown Traffic

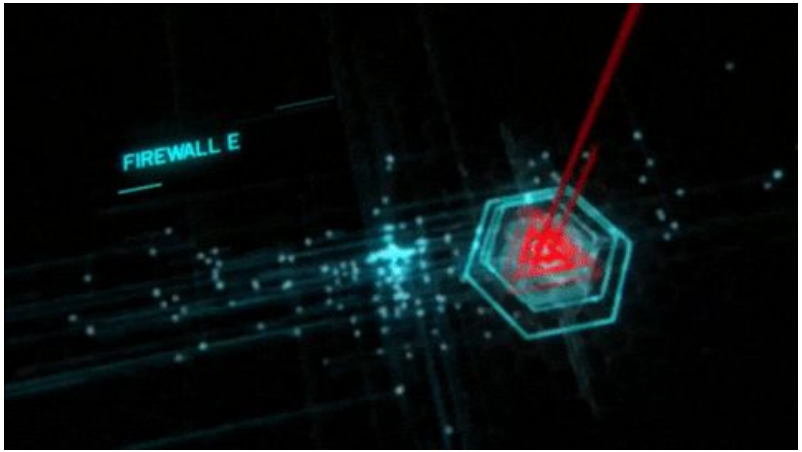
Open Access

If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

Lost or Comprised Data

Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

Network Crashes



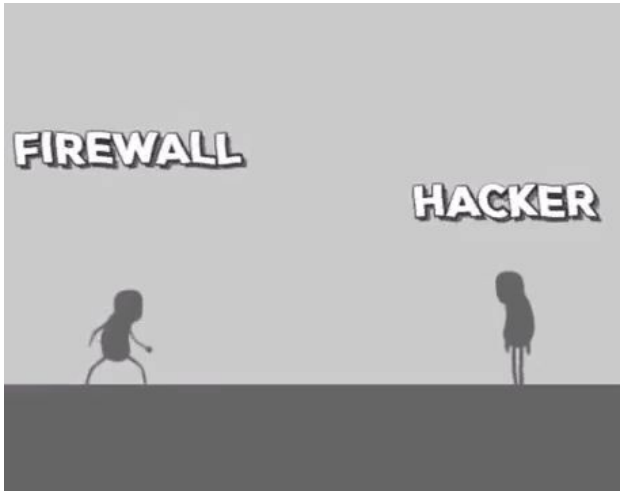
In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.

Functions of Firewall

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

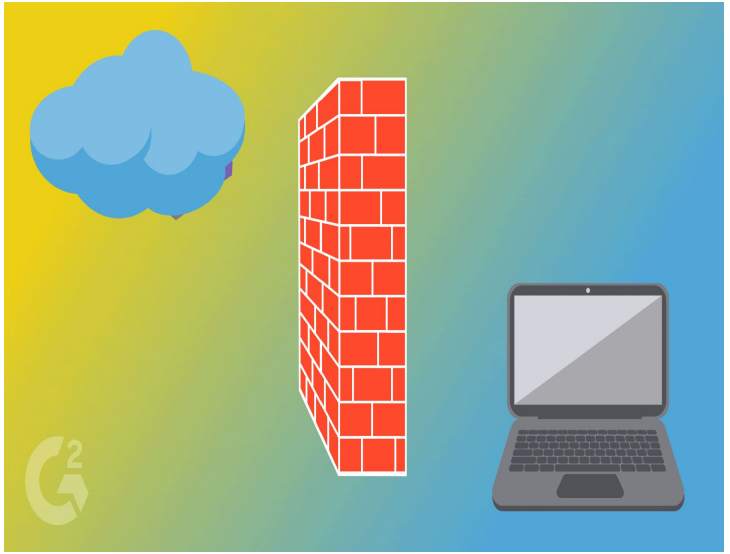
Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.



Functions of Firewall

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events



Limitations Of Firewall

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- **Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.**
- **Firewalls cannot protect against the transfer of virus-infected files or software.**
- **Firewalls cannot prevent misuse of passwords.**
- **Firewalls cannot protect if security rules are misconfigured.**
- **Firewalls cannot protect against non-technical security risks, such as social engineering.**
- **Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.**
- **Firewalls cannot secure the system which is already infected.**

Different Types of Firewalls

There are two types of firewalls: network firewalls and host-based firewalls. Network firewalls are typically used by businesses that contain a comprehensive network of multiple computers, servers, and users. The network firewall monitors the communications occurring between the company computers and outside sources. If a company wishes to restrict certain websites, IP addresses, or services like Instant Messenger, it can do so using a network firewall.

Aside from controlling employee behavior on office equipment, this type of firewall safeguards the sensitive internal data of the company, such as customer databases and employee information. Firewalls stop intruders from accessing this information and protect the business from cyber attacks.

Different Types of Firewalls

Host-based firewalls work similarly but are stored locally on a single computer. Every home computer should have some kind of host-based firewall installed on it. This functions as the first line of defense against cyber criminals and various online scams and attacks.

Host-based firewalls are also recommended for business computers that are network connected but not protected by a network firewall. They can also be useful for homes with multiple computers sharing the same network.

Most of the time, home computers are covered by a hardware firewall, like a router, which protects the network. But every home computer should also have a host-based system kind in place to guard against specific types of attacks.

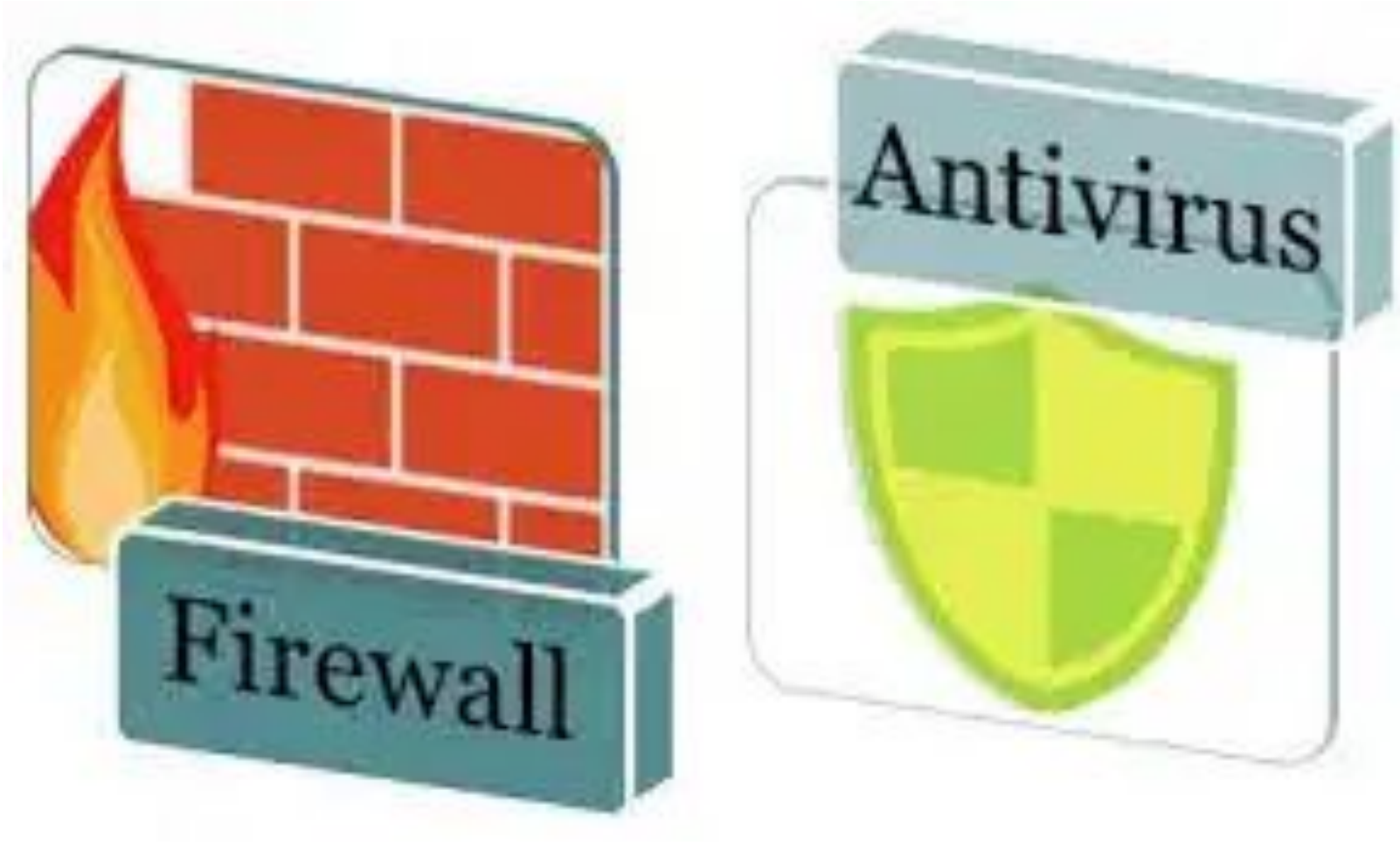
Host-based firewalls are easy to install and protect your computer from malware, cookies, email viruses, pop-up windows, and more. Along with desktop computers, mobile devices can be installed with firewalls to protect online activity on the go

Mobile Firewalls

Most smartphones include basic security settings like PIN numbers. While this may be enough to keep your best friend from using your phone, it’s not ever going to be enough to ward off sophisticated online attackers.

Mobile firewalls provide a barrier against certain kinds of attacks. For example, when certain settings like file share or networking are enabled on the device, the phone is designed to respond to outside requests automatically. First of all, these settings should be kept off whenever possible. What’s more, a firewall would stop these kinds of automatic response from happening in the first place.

Types of Firewall


Antivirus
Firewall

BASIS FOR COMPARISON	FIREWALL	ANTIVIRUS
Implemented in	Both hardware and software	Software only
Operations performed	Monitoring and Filtering (Specifically IP filtering)	Scanning of infected files and software.
Deals with	External threats	Internal as well as external threats.
Inspection of attack is based on	Incoming packets	Malicious software residing on a computer
Counter attacks	IP spoofing and routing attacks	No counter attacks are possible once a malware has removed

Difference between Firewall and Antivirus

One of the fundamental differences between antivirus and firewall is in the implementation of the roles. You can employ a firewall through both hardware and software. On the contrary, the antivirus can only be used via software.

The type of security provided by both firewall and antivirus are quite different. Packet filtering, IP blocking are some of the deposits that the firewall offers. The antivirus helps to give application like security by detecting the worms and viruses and removing them from the system.

A firewall is like a security system that acts as a wall that filters, scans, and monitors the incoming and outgoing data and files to keep the system safe from external threats. Simultaneously, the antivirus helps to scan and look for the infected files and remove them from the system.

Difference between Firewall and Antivirus

The two security systems have different functions. There are two kinds of threats to a network. One that acts as the internal threat and another as external. While antivirus deals with internal and external threats, the firewall only detects and deals with external threats. The antivirus can also scan storage devices like flash drives, which are not possible for the firewall to perform.

Once the antivirus helps remove the viruses and worms, there is no reason to wait for counterattacks. However, since the firewall works on external threats, there is a chance of spoofing and rooting attacks.

Intrusion Detection System (IDS)

What is an Intrusion Detection System (IDS)?

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

An IDS is any combination of hardware & software that monitors a system or network for malicious activity.

Examples of IDSs in real life

- Car alarms
- Fire detectors
- House alarms
- Surveillance systems
- Introduction

Classification of Intrusion Detection Systems

Intrusion detection systems are designed to be deployed in different environments. And like many cybersecurity solutions, an IDS can either be host-based or network-based.

Host-Based IDS (HIDS): A host-based IDS is deployed on a particular endpoint and designed to protect it against internal and external threats. Such an IDS may have the ability to monitor network traffic to and from the machine, observe running processes, and inspect the system's logs. A host-based IDS's visibility is limited to its host machine, decreasing the available context for decision-making, but has deep visibility into the host computer's internals.

Classification of Intrusion Detection Systems

Network-Based IDS (NIDS): A network-based IDS solution is designed to monitor an entire protected network. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata and contents. This wider viewpoint provides more context and the ability to detect widespread threats; however, these systems lack visibility into the internals of the endpoints that they protect.

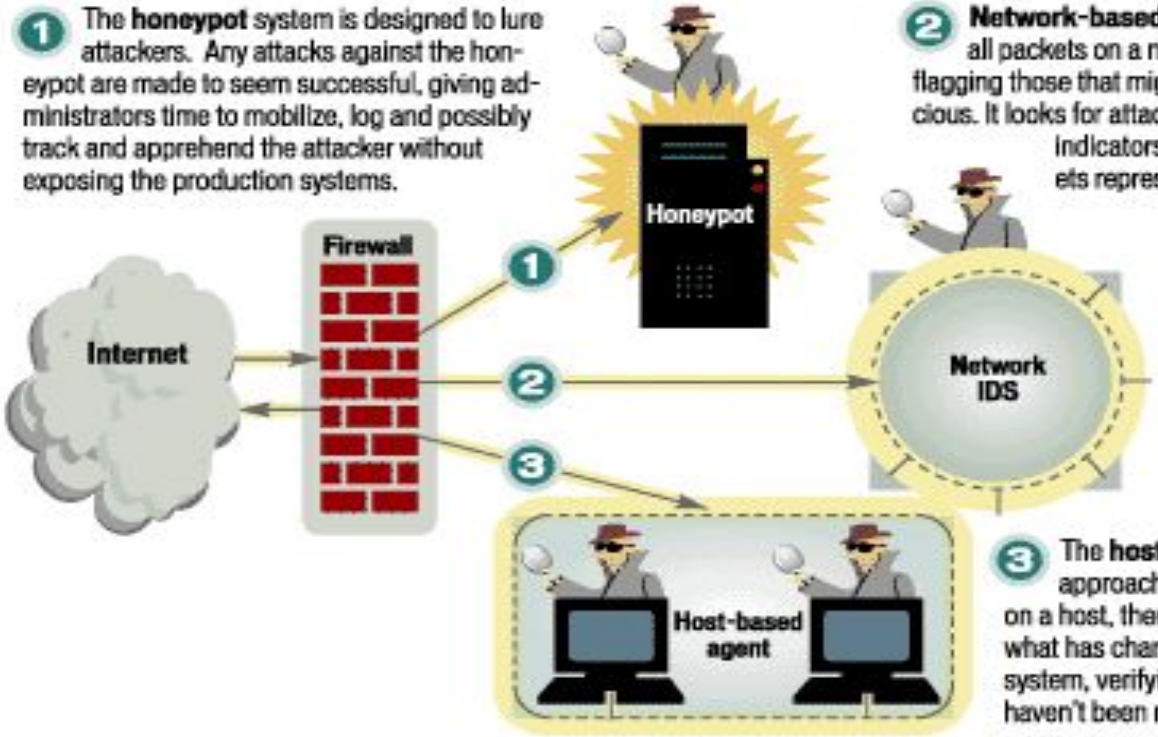
Due to the different levels of visibility, deploying a HIDS or NIDS in isolation provides incomplete protection to an organization's system. A unified threat management solution, which integrates multiple technologies in one system, can provide more comprehensive security.

Intrusion-Detection Systems

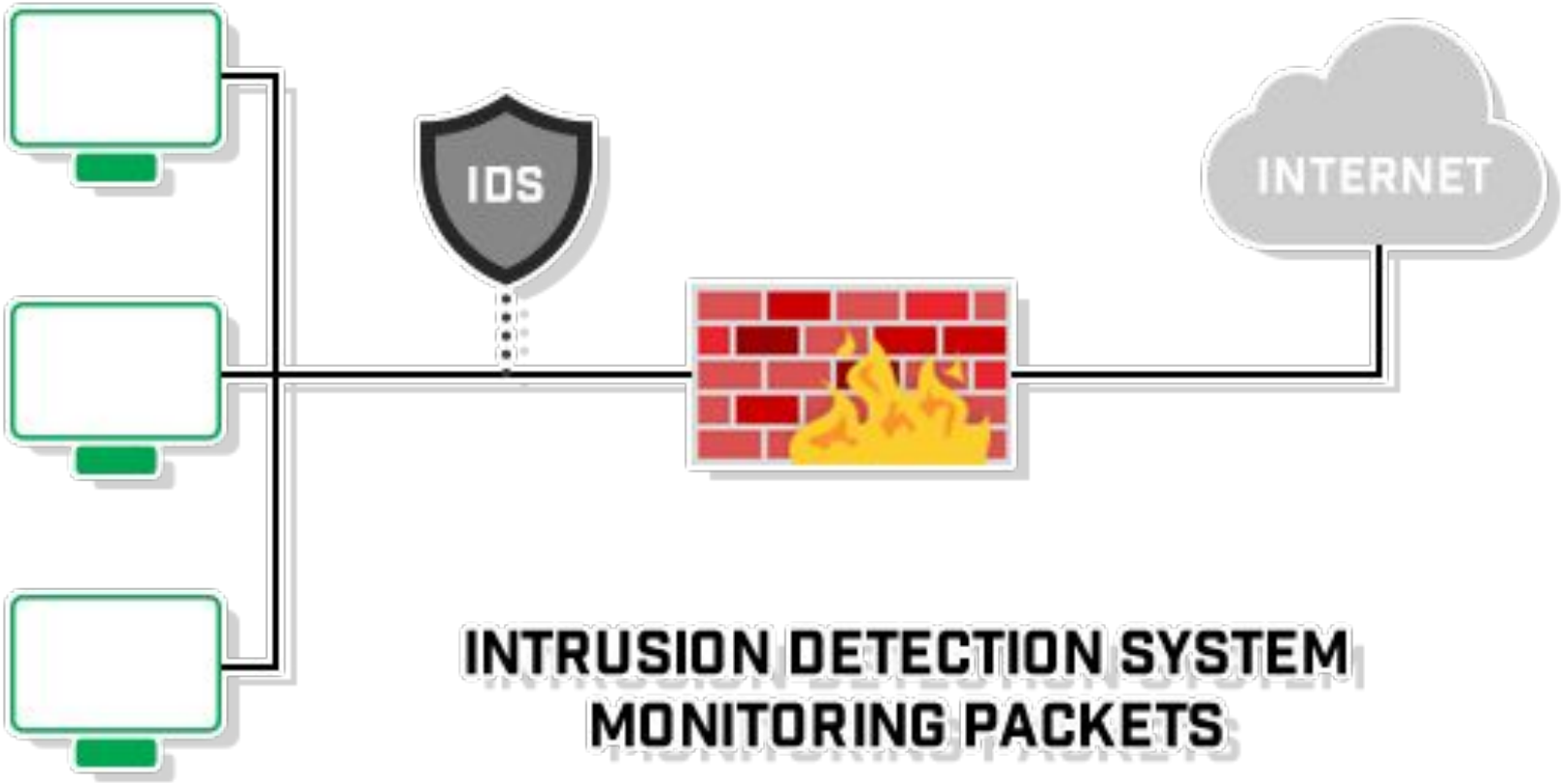
ID stands for intrusion detection, which is the art of detecting inappropriate, incorrect or anomalous activity. ID systems that operate on a host to detect malicious activity are called host-based ID systems. ID systems that operate on network data flows are called network-based ID systems. These two systems can be used in conjunction with each other.

1 The **honeypot** system is designed to lure attackers. Any attacks against the honeypot are made to seem successful, giving administrators time to mobilize, log and possibly track and apprehend the attacker without exposing the production systems.

2 **Network-based** ID scrutinizes all packets on a network segment, flagging those that might be suspicious. It looks for attack signatures – indicators that the packets represent an intrusion.



3 The **host-based agent** approach installs the ID on a host, then checks to see what has changed on the system, verifying that key files haven't been modified.


IDS
INTERNET
INTRUSION DETECTION SYSTEM
MONITORING PACKETS

Detection Method of IDS Deployment

Beyond their deployment location, IDS solutions also differ in how they identify potential intrusions:

Signature Detection: Signature-based IDS solutions use fingerprints of known threats to identify them. Once malware or other malicious content has been identified, a signature is generated and added to the list used by the IDS solution to test incoming content. This enables an IDS to achieve a high threat detection rate with no false positives because all alerts are generated based upon detection of known-malicious content. However, a signature-based IDS is limited to detecting known threats and is blind to zero-day vulnerabilities.

Detection Method of IDS Deployment

Anomaly Detection: Anomaly-based IDS solutions build a model of the “normal” behavior of the protected system. All future behavior is compared to this model, and any anomalies are labeled as potential threats and generate alerts. While this approach can detect novel or zero-day threats, the difficulty of building an accurate model of “normal” behavior means that these systems must balance false positives (incorrect alerts) with false negatives (missed detections).

Hybrid Detection: A hybrid IDS uses both signature-based and anomaly-based detection. This enables it to detect more potential attacks with a lower error rate than using either system in isolation.

IDS vs Firewalls

Intrusion Detection Systems and firewalls are both cybersecurity solutions that can be deployed to protect an endpoint or network. However, they differ significantly in their purposes.

An IDS is a passive monitoring device that detects potential threats and generates alerts, enabling security operations center (SOC) analysts or incident responders to investigate and respond to the potential incident. An IDS provides no actual protection to the endpoint or network. A firewall, on the other hand, is designed to act as a protective system. It performs analysis of the metadata of network packets and allows or blocks traffic based upon predefined rules. This creates a boundary over which certain types of traffic or protocols cannot pass.

IDS vs Firewalls

Since a firewall is an active protective device, it is more like an Intrusion Prevention System (IPS) than an IDS. An IPS is like an IDS but actively blocks identified threats instead of simply raising an alert. This complements the functionality of a firewall, and many next-generation firewalls (NGFWs) have integrated IDS/IPS functionality. This enables them to both enforce the predefined filtering rules (firewalls) and detect and respond to more sophisticated cyber threats (IDS/IPS). Learn more about the IPS vs IDS debate here.

Scanning

What is Scanning Techniques?

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker). Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks. This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms. So a pen-tester and ethical hacker list down all such vulnerabilities found in an organization's network.

Scanning Methodologies

1. Hackers and Pen-testers check for Live systems.
2. Check for open ports (The technique is called Port Scanning, which will be discussed below)
3. Scanning beyond IDS (Intrusion Detection System)
4. Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack. This information may be used by intruders/hackers to portray the lists of applicable exploits.
5. Scan for vulnerability
6. Prepare Proxies

Tools And Steps Used

If a hacker wants to perform ICMP (Internet Control Message Protocol) scanning, it can be done manually. The steps are:

Open Windows OS

Press Win+R (Run) buttons in combination

In the Run, type- cmd

Type the command:
ping IP Address
or type:
ping DomainName

Tools that can are used to scan networks and ports are:

Nmap: extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems, and OS versions.

Angry IP Scanner: scans for systems available in a given input range.

Hping2/Hping3: are command-line packet crafting and network scanning tools used for TCP/IP protocols.

Superscan: is another powerful tool developed by Mcafee, which is a TCP port scanner, also used for pinging.

ZenMap: is another very powerful Graphical user interface (GUI) tool to detect the type of OS, OS version, ping sweep, port scanning, etc

Tools that can are used to scan networks and ports are:

Net Scan Tool Suite Pack: is a collection of different types of tools that can perform a port scan, flooding, webrippers, mass emailers; and This tool is a trial version, but paid versions are also available.

Wireshark and Omnipeak are two powerful and famous tools that listen to network traffic and act as network analyzers.

Names of other famous PCs tools are Advanced Port Scanner, Net Tools, MegaPing, CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory Explorer, etc.

There are various other scanners available free and inbuilt in Kali Linux OS.

Tools and software that are used in mobiles as scanners include the names such as Umit Network Scanner, Fing, IP network Scanner, PortDroid network Analysis, Panm IP Scanner, Nessus Vulnerability Scanner, Shadow Sec Scanner, etc

Threat Management

What is threat management?

Threat management is a process used by cybersecurity professionals to prevent cyber attacks, detect cyber threats and respond to security incidents

Why is threat management important?

Most security teams face information fragmentation, which can lead to blind spots in security operations. And wherever they exist, blind spots compromise a team’s ability to identify, protect against and respond to security threats promptly.

Today's dangers now include mutating malware, advanced persistent threats (APT), insider threats, and vulnerabilities around cloud-based computing services, more than antivirus software can handle. With the ever-disappearing perimeter of a protected IT infrastructure and remote workforce, enterprises face complex risks and security threats they've never experienced before. Against the backdrop of this evolving threat landscape and shift to cloud, security professionals have adopted a new mindset—to assume that breaches have occurred and will occur.

Enhanced with automation and informed by AI, a cyber threat management system can help counter today’s advanced attacks by cybercriminals. It gives security teams the visibility they need to succeed. By unifying security data, security teams can navigate with confidence, identifying data at risk and vulnerabilities across networks on thousands of endpoints and between clouds.

How threat management works

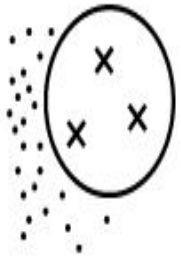
Many modern threat management systems use the cybersecurity framework established by the National Institute of Standards and Technology (NIST). NIST provides comprehensive guidance to improve information security and cybersecurity risk management for private sector organizations. One of their guides, the NIST Cybersecurity Framework (NIST CF), consists of standards and best practices. Five primary functions make up its core structure. They are to identify, protect, detect, respond and recover.

Identify

Cybersecurity teams need a thorough understanding of the organization's most important assets and resources. The identify function includes categories, such as asset management, business environment, governance, risk assessment, risk management strategy and supply chain risk management.

Protect

The protect function covers much of the technical and physical security controls for developing and implementing appropriate safeguards and protecting critical infrastructure. These categories are identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance and protective technology.



Detect

The detect function implements measures that alert an organization to cyberattacks. Detect categories include anomalies and events, continuous security monitoring and early detection processes.

Respond

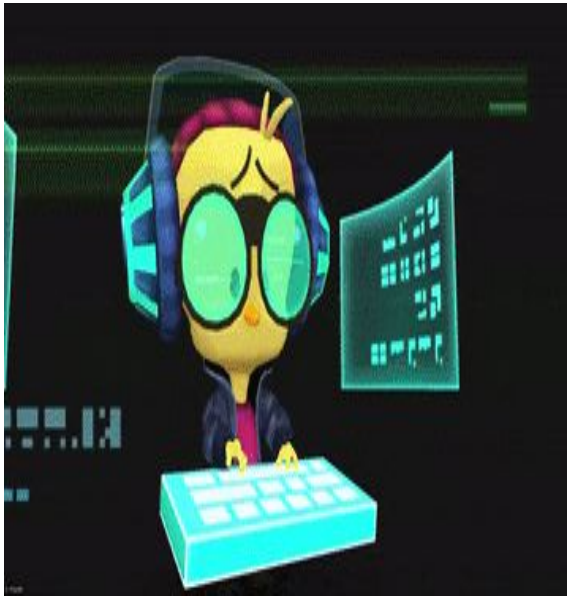
The respond function ensures an appropriate response to cyberattacks and other cybersecurity events. Categories include response planning, communications, analysis, mitigation and improvements.

Recover

Recovery activities implement plans for cyber resilience and ensure business continuity in the event of a cyberattack, security breach or another cybersecurity event. The recovery functions are recovery planning improvements and communications.

Threat management technology

Today's enterprise organizations install security operation centers (SOC) equipped with modern technology, like AI, to efficiently detect, manage, and respond to threats. By implementing AI-powered technology and an open, modular range of threat management solutions and services, organizations can spend less time and resources integrating and operating fragmented tools and data sources. The technology can establish efficient, interconnected data exchange, analytics and response processes that transform and enhance security operations capabilities. Vendors can deliver threat management solutions like software, software as a service (SaaS)or as managed services based on client requirements. Solution providers can also custom design, build, manage or provide the tools to deliver all aspects of the threat management lifecycle. They support SOC teams with the same AI-powered threat detection and investigation tools and threat management solutions and services to get the most value out of existing resources and investments.



THANK YOU!