**Principles of Cybersecurity**

An organization or an individual can develop a proper response plan only when they have good cyber security fundamentals.

* Confidentiality
* Integrity
* Availability

Confidentiality

1. Confidentiality is about preventing the disclosure of data to unauthorized parties and making accessible only to authorized parties.
2. It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.
3. Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.
4. Standard measures to establish confidentiality include:
5. Data encryption
6. Two-factor authentication
7. Biometric verification
8. Security tokens

Integrity

1. Integrity refers to protecting information from being modified by unauthorized parties.
2. Maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle.
3. Standard measures to guarantee integrity include:
4. Cryptographic checksums
5. Using file permissions
6. Uninterrupted power supplies
7. Secure Data backups

Availability

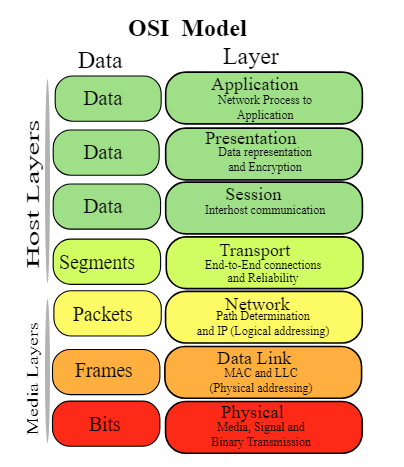
1. Availability is making sure that authorized parties are able to access the information when needed.
2. Standard measures to guarantee availability include:
3. Backing up data to external drives
4. Implementing firewalls
5. Having backup power supplies
6. Data redundancy
7. Robust backup and disaster recovery mechanisms to enable timely restoration of services.

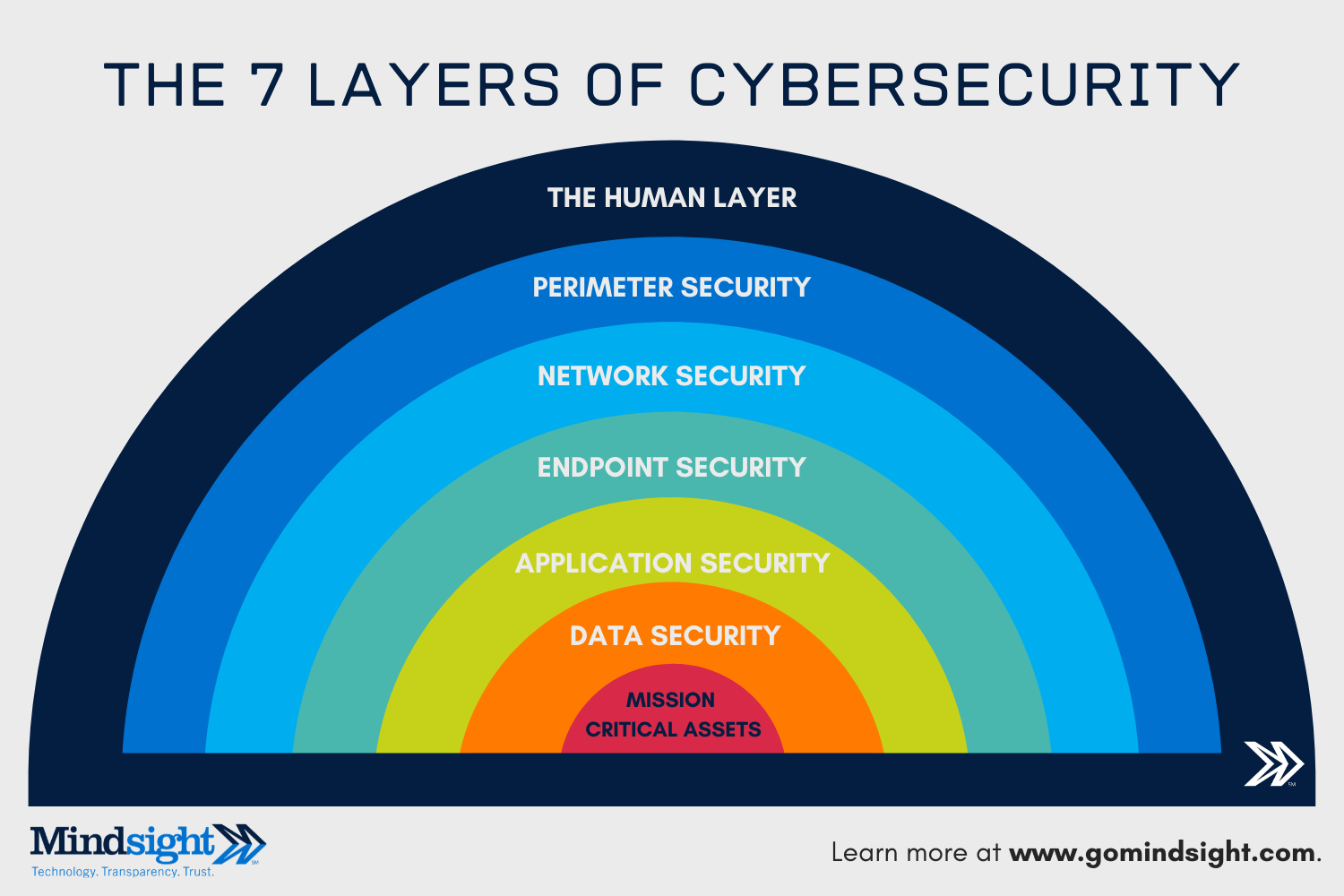
Accountability

1. Accountability is an assurance that an individual or an organization will be evaluated on their performance or behaviour related to something for which they are responsible.
2. Standard measures to guarantee accountability include:
3. User Accountability - by following security protocols, protecting their credentials, and exercising caution to prevent unauthorized access or data breaches.
4. Organizational Accountability for implementing security measures, providing training and awareness programs, and enforcing protecting policies.
5. Administrator Accountability for managing user accounts, enforcing security controls, and promptly responding to vulnerabilities.

Auditability:

1. A security audit is a systematic evaluation of the security of a company’s information system by measuring how well it conforms to a set of established criteria.
2. Standard measures to guarantee auditability include:
   1. Implementing logging and auditing mechanisms to track user activities
   2. detect security incidents
   3. facilitate forensic investigations





1. Mission Critical Assets – This is the data you need to protect
2. Data Security – Data security controls protect the storage and transfer of data.

The most care must be taken with this layer as it is the foundation of the company.

Security Strategy: At this level, keeping things secure entails file and disc encryption, frequent backups of all crucial data and procedures, two-factor authentication, enterprise rights management, and rules that make sure data is erased from devices that are no longer in use to another employee.

1. Application Security – Applications security controls protect access to an application, an application’s access to your mission critical assets, and the internal security of the application.

Security Strategy: Keeping the programs up to date. This guarantees that the application is as secure as possible and that any known security vulnerabilities are addressed.

1. Endpoint Security – Endpoint security controls protect the connection between devices and the network.

Security Strategy: Endpoint encryption is required to make sure that the devices are operating in secure environments.

1. Network Security

Network security controls protect an organization’s network and prevent unauthorized access of the network.

The key worry of the network layer is what users and devices can access once they are within your system.

Security Strategy: If no one has access to everything, then any cyberattack only results in a small portion of the network being breached. So only give employees and devices access to the parts of the network that are 100% necessary for them.

1. Perimeter Security

Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

Define the perimeter before determining the sort of data being transmitted across this layer, and then both the data and the device can be secured.

Security Strategy: This includes firewalls, data encryption, antivirus software, device management.

1. The Human Layer

Humans are the weakest link in any cyber security posture and responsible for 90% of data breaches.

Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Security Strategy: Education and training, which include instructions on how to recognize and deal with phishing attacks, strong password strategies, system hardening, and cyber security awareness, are the best ways to keep the human layer secure. Access controls are a smart notion which can reduce the amount of harm from a successful attack.

**Active attacks:**

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

**Types of Active attacks:**

1. **Masquerade:**

in this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

1. **Session replay:**

In this type of attack, a hacker steals an authorized user’s log in information by stealing the session ID. The intruder gains access and the ability to do anything what the authorized user can do on the website.

1. **Message modification:**

In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

1. In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.
2. In a distributed denial-of-service (DDoS) exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

The intention is to overwhelm the target's resources, such as bandwidth, processing power, or memory, making the system or network inaccessible to legitimate users.

DDoS attacks can disrupt online services, websites, and networks, causing financial losses and impacting the reputation of targeted organizations.

**Passive Attack**

Passive attacks are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted.

**Types of Passive attacks:**

1. Eavesdropping (tapping):

The attacker secretly listens to messages exchanged by two entities. For the attack to be made, the traffic must not be encrypted.

Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

1. Traffic analysis:

The attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.).

In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

1. Software Attacks:

Malicious code (sometimes called malware) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval.

It can be very difficult to remove and very damaging.

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:

1) Web-based attacks

2) System-based attacks

Web-based attacks

1. Injection attacks

It is the attack in which some malicious data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

1. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer.

The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

1. Session Hijacking

It is a security attack on a user session over a protected network.

Web applications create cookies to store the state and user sessions.

By stealing the cookies, an attacker can have access to all of the user data.

1. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

1. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

1. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked

site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a

packet.

Application layer attacks- Its goal is to crash the web server and is

measured in request per second.

1. Dictionary attacks

This type of attack stored the list of a commonly used password and

validated them to get original password.

1. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and

one can make a web server to deliver web pages for which he is not

authorized to browse.

1. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or

essential files which is available on the web server or to execute malicious

files on the web server by making use of the include functionality.

1. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection

between client and server and acts as a bridge between them. Due to this, an

attacker will be able to read, insert and modify the data in the intercepted

connection.

System-based attacks

1. Virus

* It is a type of malicious software program that spread throughout the computer files without the knowledge of a user.
* It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed.
* It can also execute instructions that cause harm to the system.

2. Worm

* It is a type of malware whose primary function is to replicate itself to spread

to uninfected computers. It works same as the computer virus.

* Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

* It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle.
* It misleads the user of its true intent.
* It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process.

A developer may create a backdoor so that an application or operating system can be

accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services.

Some bots program run automatically, while others only execute commands when they receive specific input.

Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Security Policies of an organisation

1. Acceptable Use Policy (AUP): Establish guidelines for the acceptable use of technology resources within the educational institution, including proper internet usage, email communication, and responsible handling of personal and sensitive data.
2. Password Policy: Enforce strong password requirements, regular password updates, and discourage the sharing of passwords. Implement multi-factor authentication (MFA) to add an extra layer of security.
3. Data Protection Policy: Define protocols for handling and safeguarding sensitive data, such as student records, financial information, and research data. Include procedures for encryption, secure storage, data backups, and data retention periods.
4. Network Security Policy: Implement firewalls, intrusion detection and prevention systems, and regular network monitoring to detect and prevent unauthorized access. Restrict access to sensitive systems and ensure secure wireless network configurations.
5. Incident Response Policy: Develop a comprehensive incident response plan that outlines the steps to be taken in case of a security breach, including incident reporting, containment, investigation, communication, and recovery procedures.
6. Patch Management Policy: Establish a process for regularly updating and patching software, operating systems, and firmware to address vulnerabilities and protect against known exploits.
7. Employee Security Awareness Training: Conduct regular training sessions to educate staff, teachers, and students about cybersecurity best practices, phishing awareness, social engineering techniques, and the importance of reporting any suspicious activities.
8. Physical Security Policy: Implement measures to secure physical access to servers, data centers, and other critical infrastructure. This may include surveillance systems, access controls, visitor management, and secure storage for portable devices.
9. Bring Your Own Device (BYOD) Policy: Establish guidelines and security requirements for allowing personal devices on the institution's network, including policies on device registration, malware protection, and data segregation.
10. Vendor Management Policy: Ensure that third-party vendors and service providers adhere to appropriate security standards and conduct regular security assessments to mitigate potential risks associated with their services.

These cybersecurity mitigation methods aim to reduce risks, protect against threats, and enhance the overall security posture of an organization's IT infrastructure and assets.

1. Security Baseline:

A security baseline is a starting point for measuring changes and improvements in system configurations.

It involves defining a set of security controls and configurations that should be implemented as a minimum standard.

2. Threat Monitoring Plans:

This involves keeping an eye on the system to detect any suspicious activities or attempts to break into it. It includes checking access logs, monitoring network traffic on external gateway, and tracking accesses to sensitive files or data.

3. Computer Virus Controls:

These are measures to prevent and control computer viruses. It includes regularly updating antivirus software, testing it before use, and distributing and updating definitions on all platforms.

Establishing communication mechanisms for reporting and handling potential viruses.

4. Microcomputer Security:

This refers to protecting individual computers or workstations.

It involves

1. monitoring software licenses,
2. keeping track of installed software,
3. following approved software usage policies,
4. preventing the use of unauthorized software,
5. ensuring the physical and digital security of important computers, and
6. having backup plans in case something goes wrong.

5. Physical and Environmental Security:

This is about securing the physical aspects of the IT infrastructure.

It includes

1. using locks, guards, and monitoring devices,
2. controlling access to the premises,
3. maintaining logs of who enters the facility, and
4. having backup power, fire protection, and disaster recovery plans in place.

6. Backup and Recovery:

This is the process of making copies of important system files and data so that they can be restored in case of loss or damage.

The backups should be stored in a safe place away from the main systems during any physical incidents. Proper labelling and tracking of backup media are also important.

7. Network Assessment:

This involves evaluating the network infrastructure to identify any vulnerabilities or weaknesses. It includes

1. reviewing network documentation,
2. talking to network administrators, and
3. assessing network management, security practices, and response capabilities in case of network issues.

8. Operating System Security Assessment:

This is about checking the security of the computer's operating system.

It includes

1. reviewing security settings,
2. user and group management,
3. strong password policies, network settings,
4. use of file and directory permissions, and
5. backup procedures.

9. Challenges in Implementing Information Security:

These are common difficulties faced in maintaining information security.

It includes

1. getting support from management,
2. understanding the risks involved,
3. allocating enough resources,
4. managing security during mergers and acquisitions,
5. dealing with different security practices, and
6. maintaining security when working with third-party vendors.

These methods help protect computer systems, networks, and data from unauthorized access, threats, and vulnerabilities. They aim to minimize risks and ensure the overall security of an organization's information technology infrastructure.

The security policy cycle typically consists of three main phases:

**Risk Management Assessment:**

Asset Identification: Identify and inventory the organization's assets, including hardware, software, data, and intellectual property.

Threat Identification: Identify potential threats and risks that could affect the organization's assets, such as cyber-attacks, natural disasters, or human error.

Vulnerability Appraisal: Assess the vulnerabilities or weaknesses in the organization's systems, processes, or controls that could be exploited by threats.

Risk Assessment: Evaluate and prioritize the identified risks based on their potential impact and likelihood of occurrence.

Risk Mitigation: Develop strategies and controls to mitigate or reduce the identified risks to an acceptable level.

**Policy Creation:**

Based on the information gathered from the risk management assessment, create a comprehensive security policy that outlines the organization's approach to managing and mitigating risks.

The policy should define the security objectives, roles and responsibilities, standards, procedures, guidelines, and best practices to be followed throughout the organization.

It should also consider relevant legal, regulatory, and compliance requirements specific to the industry or region.

**Policy Review for Compliance:**

Regularly review and update the security policy to ensure its effectiveness and alignment with changing technology, threats, and organizational requirements.

Assess the policy's compliance with applicable laws, regulations, industry standards, and internal policies.

Engage stakeholders, including management, employees, and security professionals, in the review process to gather feedback and address any concerns.

Make necessary adjustments to the policy based on the review findings and ensure it remains relevant and enforceable.

Cyber threats can arise from various sources, and they can be either inadvertent or deliberate in nature. Here are some common sources of cyber threats:

**Inadvertent Threats:**

Human Error: Unintentional actions or mistakes made by individuals, such as misconfiguration of systems, accidental data leaks, or clicking on malicious links.

Negligence: Failure to follow security best practices, lack of awareness about potential threats, or inadequate training, leading to vulnerabilities and breaches.

**Deliberate Threats:**

Political Motivation: Cyberattacks conducted by nation-states or state-sponsored groups for political purposes, such as espionage, disruption of critical infrastructure, or gaining a strategic advantage.

Economic Motivation: Cybercriminals targeting organizations or individuals to steal sensitive financial information, conduct ransomware attacks, or engage in identity theft for financial gain.

Socio-cultural Motivation: Cyberactivists or hacktivist groups targeting organizations or individuals to promote a social or ideological agenda, raise awareness about specific issues, or protest against perceived injustices.

**Insider Threats:**

Disgruntled Employees: Current or former employees with access to sensitive information who misuse their privileges to harm the organization, steal data, or disrupt operations.

Insider Sabotage: Individuals with authorized access who intentionally cause harm to the organization's systems, data, or reputation due to personal grievances or malicious intent.

1) BLACK HAT HACKER

i. Black hat hackers are the "bad guys" of the hacking scene and also called as security crackers.

ii. They are highly skilled individuals who illegally hack into the systems.

iii. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign.

iv. These individuals’ actions can inflict serious damage on both computer users and the organizations they work for.

v. They can steal sensitive personal information, compromise computer and financial systems, and alter or take down the functionality of websites and critical networks.

vi. DarkFire, a black hat group known for launching targeted ransomware attacks against critical infrastructure, demanding hefty payments for their release.

WHITE HAT HACKERS

i. White hat hackers can be seen as the “good guys” who attempt to prevent the success of black hat hackers through proactive hacking.

ii. They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking.

iii. This helps to expose vulnerabilities in systems before black hat hackers can detect and exploit them.

iv. The techniques white hat hackers use are similar to or even identical to those of black hat hackers, but these individuals are hired by organizations to test and discover potential holes in their security defences.

GRAY HAT HACKERS

i. Grey hat hackers sit somewhere between the good and the bad guys.

ii. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially.

iii. Their actions are typically carried out for the common good.

iv. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly.

1. This alerts malicious actors to the existence of the vulnerability

2) **Tools for Penetration Testing:**

Penetration testing, or pen testing, involves actively assessing the security of systems /networks by identifying vulnerabilities and potential weaknesses. Some common pen testing tools include:

1. Nmap: Nmap is a powerful network scanning tool used to discover hosts, open ports, and services running on a network. It works by sending data packets on a specific targeted and by interpreting the incoming packets to determine what ports are open or closed, whether firewalls or filters are setup and enable and finally what operating system is running.

2. Metasploit: Metasploit is a widely used framework that helps in developing, scanning and executing exploits against vulnerable systems. It provides a range of modules and tools for penetration testing.

3. Openvas (open vulnerability assessment system) is powerful and management package tool that makes the process of scanning network simple and scans end-to-end. openvas scanner tool runs the plugin NVT-Network Vulnerability Tests and feed of NVT’s is updated regularly.

A SQLite database for string, Test configuration and NVT’s results and configs.

4. Wireshark is a network protocol analyzer used for capturing and analyzing network traffic. It helps in identifying network vulnerabilities, troubleshooting network issues, and detecting suspicious activities. It allows to inspect packets, analyze protocols, and identify potential security issues.

5. Nessus: Nessus is a popular vulnerability scanner that scans systems and networks for known vulnerabilities. It provides detailed reports and recommendations for mitigating identified vulnerabilities.

**3) Phases of Penetration Testing**

* Reconnaissance and Information Gathering
* Network Enumeration and Scanning
* Vulnerability Testing and Exploitation
* Reporting

**Reconnaissance and Information Gathering**

Purpose: To discover as much information about a target (individual or organization) as possible without actually making network contact with said target.

Methods:

1. Discovering Organization info via WHOIS
2. Google search
3. Website browsing

WHOIS Results for www.netflix.com

Domain Name: netflix.com

Registry Domain ID: 1404215\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2021-10-09T09:37:28+0000

Creation Date: 1997-11-11T05:00:00+0000

Registrar Registration Expiration Date: 2023-11-10T00:00:00+0000

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: email@markmonitor.com

Registrar Abuse Contact Phone: +1.2083895770

Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)

Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)

Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)

Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)

Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)

Registry Registrant ID:

Registrant Name: Domain Administrator

Registrant Organization: Netflix, Inc.

Registrant Street: 100 Winchester Circle,

Registrant City: Los Gatos

Registrant State/Province: CA

Registrant Postal Code: 95032

Registrant Country: US

Registrant Phone: +1.4085403700

Registrant Phone Ext:

Registrant Fax: +1.4085403737

Registrant Fax Ext:

Registrant Email: email@netflix.com

**Network Enumeration and Scanning**

Purpose: To discover existing networks owned by a target as well as live hosts and services running on those hosts.

Methods:

1. Scanning programs that identify live hosts, open ports, services, and other info (Nmap, autoscan)
2. DNS Querying
3. Route analysis (traceroute)

NMap Results

*nmap -sS 127.0.0.1*

Starting Nmap 4.01 at 2006-07-06 17:23 BST

Interesting ports on chaos (127.0.0.1):

(The 1668 ports scanned but not shown below are in state: closed)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

631/tcp open ipp

6000/tcp open X11

Nmap finished: 1 IP address (1 host up) scanned in 0.207 seconds

**Vulnerability Testing and Exploitation**

Purpose: To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities.

Methods:

1. Remote vulnerability scanning (Nessus, OpenVAS)
2. Active exploitation testing
3. Login checking and bruteforcing
4. Vulnerability exploitation (Metasploit, Core Impact)
5. 0day and exploit discovery (Fuzzing, program analysis)
6. Post exploitation techniques to assess severity (permission levels, backdoors, rootkits, etc)

**Reporting**

Purpose: To organize and document information found during the reconnaissance, network scanning, and vulnerability testing phases of a pentest.

Methods:

1. Documentation tools (Dradis)
2. Organizes information by hosts, services,
3. identified hazards and risks,
4. recommendations to fix problems

Penetration Testing

It is the process of evaluating the security of an organization by exploiting the vulnerabilities in a way the attackers could exploit them and thereby defending as well as documenting the procedure of attack.

**4) Types of penetration testing methodologies:**

**Black box:**

1. The penetration tester will not be given any details related to the network, or infrastructure of the organization.
2. Have no prior knowledge or access to the target system
3. Burden is on the tester to find these details to externally attack.
4. Company staff does not know about the test.
5. Tests if security personnel are able to detect an attack.

**White Box (transparent box or clear box testing):**

1. The penetration tester will be aware of the complete details of the network topology, infrastructure to be tested
2. Have full knowledge and access to the target system
3. Makes tester’s job a little easier
4. Tester is authorized to interview IT personnel and company employees

**Grey box:**

1. The penetration tester will be provided with a limited knowledge about the systems to be tested.
2. May have access to certain credentials, system information, etc.
3. It is combination of the white and black box models

**5) Penetration Testing Methods**

**External testing**

External penetration tests target the assets of a company that are visible on the internet, e.g., The web application itself, the company website, and email and domain name servers (DNS).

The goal is to gain access and extract valuable data.

**Internal testing**

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider.

This isn’t necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

**Blind testing**

In a blind test, a tester is only given the name of the enterprise that’s being targeted.

This gives security personnel a real-time look into how an actual application assault would take place.

**Targeted testing**

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements.

This is a valuable training exercise that provides a security team with real-time feedback from a hacker’s point of view.

**6) 1. Planning and reconnaissance**

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

Gathering information (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

**2. Scanning**

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

**Static analysis** – Inspecting an application’s code to estimate the way it behaves while running. These tools can scan the entirely of the code in a single pass.

**Dynamic analysis** – Inspecting an application’s code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application’s performance.

**3. Gaining Access**

This stage uses web-based attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target’s vulnerabilities.

Testers then try and exploit these vulnerabilities, to understand the damage they can cause typically by escalating privileges, stealing data, intercepting traffic, etc.,

**4. Maintaining access**

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access.

The idea is to imitate advanced persistent threats for months, in order to steal an organization’s most sensitive data.

**5. Analysis**

The results of the penetration test are then compiled into a report detailing:

1. Specific vulnerabilities that were exploited
2. Sensitive data that was accessed
3. The amount of time, the pen tester was able to remain in the system undetected
4. This information is analysed by security personnel to help configure an enterprise’s Web Application Firewall (WAF) settings and other application security solutions to patch vulnerabilities and protect against future attacks.

**7) Legal aspects of Penetration Testing**

**Legal Issues**

The legal issues that have to be considered when conducting penetration tests can be subdivided into three types:

1. **Legal issues** that can induce or motivate a business or a public authority to conduct a penetration test.
2. **Legal regulations and principles** that the tester should observe when conducting penetration tests and which should be clarified with the client prior to testing.
3. **Legal aspects form the basis** of the contract between client and penetration tester.

**Legal Reasons for Penetration Testing**

While there are no laws that require a company/public authority to commission penetration tests, there are binding legal provisions relating to

• Security handling and the availability of data relevant to tax and commercial law,

• Treatment of personal data,

• The establishment and organization of an internal control system.

**What You Can Do Legally**

• Laws involving technology change as rapidly as technology changes itself

• Find what is legal for you locally – Laws change from place to place

• Be aware of what is allowed and what is not allowed

• Contact local law enforcement agencies before installing hacking tools

• Written words are open to interpretation

**What You Cannot Do Legally**

• Accessing a computer without permission is illegal

• Hacking Tools on your computer might be illegal to possess

• Other illegal actions

– Installing worms or viruses

– DOS attacks

– Denying users access to network resources

• Be careful your actions do not prevent customers

• Governments are getting more serious about punishment for cybercrimes

**Laws of the Land**

• Hacking Tools on your computer might be illegal to possess

• Contact local law enforcement agencies before installing hacking tools

• Written words are open to interpretation

• Governments are getting more serious about punishment for cybercrimes

**Is Port Scanning Legal?**

1. Some states deem it legal, not always the case
2. Federal Government does not see it as a violation
3. Allows each state to address it separately
4. Read your ISP’s “Acceptable Use Policy”
5. IRC “bots” may be forbidden
6. Program that sends automatic responses to users
7. Gives the appearance of a person being present

**Federal Laws**

• Federal computer crime laws are getting more specific

– Cover cybercrimes and intellectual property issues

• Computer Hacking and Intellectual Property (CHIP)

– New government branch to address cybercrimes and intellectual property issues