CYBER SECURITY

Computer security, cyber security or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field is becoming increasingly significant due to the increased reliance on computer systems, the Internal and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable vulnerability is one for which at least one working attack or "exploit" exists.[12] Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts.[13][14] To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of these categories below:

Backdoor

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for many reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Backdoors can be very hard to detect, and detection of backdoors are usually discovered by someone who has access to application source code or intimate knowledge of Operating System of the computer.

Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

TWITTER

The popular social media company was breached in July, by three individuals in an embarrassing incident that saw several high profile Twitter accounts hijacked. Through a social engineering attack, later confirmed by Twitter to be phone phishing, the attackers stole employees' credentials and gained access to the company's internal management systems; dozens of high-profile accounts including those of former President Barack Obama, Amazon CEO Jeff Bezos, and Tesla and SpaceX CEO Elon Musk, were hacked. The threat actors then used the accounts to tweet out bitcoin scams that earned them over $100,000. Two weeks after the breach, the Department of Justice (DOJ) arraigned the three suspects and charged 17-year-old Graham Ivan Clark as an adult for the attack he allegedly "masterminded," according to authorities.

Introduction to Social Engineering

➤ Social Engineering is an act of stealing data from humans. because it doesn't have any interaction with target system or network, it's considered as a non-technical attack. Social Engineering is taken into account because the art of convincing the target to reveal information. it's going to be physically one-to-one interaction with the target or convincing the target on any platform like social media may be a popular platform for social engineering. this is often the very fact that folks are careless, or unaware of the importance of the precious information they possess.

Phases in a Social Engineering Attack

Social Engineering attacks aren't the complex attack which needs strong technical knowledge. An attacke could be Non-technical personal as defined earlier; it's an act of stealing information from people

> Research: Research phase includes a set of data about target organization. it's going to be collected by dumpster diving, scanning

websites of the organization, finding information on the web, gathering information from users of the target organization, etc.

Select Target: within the selection of target phase, attacker select the target among other employees of an organization. A frustrated target is more preferred because it are going to be easy to reveal information from him. > Relationship: Relationship phase holds creating a relationship with the target within the way that he couldn't identify the intention actually target are going to be trusting the attacker. More Trust level between target and attacker are going to be easier to extract data.

> Exploit: Exploit of relationship by a set of sensitive information like Username, Passwords, networkinformation, etc.

Types of Social Engineering

Social Engineering attacks are often performed by different techniques.

Different social engineering attack techniques are classified into the subsequent types: -

Human-based Social Engineering Gathers Sensitive information by interaction

Computer-based Social Engineering Social engineering is administered with the assistance ofcomputers

Mobile-based Social Engineering It is administered with help of mobile applications

How to Defend against phishing attacks

Never Click on Hyperlinks in Email

Never Enter Sensitive data in a Pop Up Window

Verify HTTPS on Address Bar

Education on Phishing Attacks

Keep Antivirus Protection Current

Utilize Anti-Spam Software

Utilize Anti-Spy Software

Install and Maintain a Reliable Firewall

Protect Against DNS Pharming Attacks

Utilize Backup System Copies