Task6-1017-Vuppala Likitha

1.what is Wardriving?

Wireless Networks have brought a lot of convenience to our lives, allowing us to work or surf from almost anywhere- home, theaters, airports, hotels around the globe. Unfortunately, wireless networks have also brought convenience to hackers as it gives the opportunity to capture all data that we type in our computers or any connected devices through the air, and they can even gain control of them. We call this act of cruising for unsecured wireless networks “War Driving”.

2.What is Shoulder Surfing?

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information.

Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a [PIN](https://www.techtarget.com/whatis/definition/pin-or-PIN) at an ATM or pay for something using a credit card.

Shoulder surfing can also be done from a long distance with the aid of binoculars or other vision-enhancing devices.

3.What is Zero-day Vulnerability?

A **zero-day vulnerability** is a [vulnerability](https://www.trendmicro.com/vinfo/us/security/definition/vulnerability)in a system or device that has been disclosed but is not yet patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit.

Because they were discovered before security researchers and software developers became aware of them—and before they can issue a patch—zero-day vulnerabilities pose a higher risk to users for the following reasons:

* Cybercriminals race to exploit these vulnerabilities to cash in on their schemes
* Vulnerable systems are exposed until a patch is issued by the vendor.

Zero-day vulnerabilities are typically involved in targeted attacks; however, many campaigns still use old vulnerabilities.

4.What is Brute-force Attack?

A brute force attack is a hacking method that uses trial and error to crack passwords, [login credentials](https://www.fortinet.com/resources/cyberglossary/login-credentials), and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations’ systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

5.What is Ransomware?

Ransomware is a type of malware (malicious software) that locks a victim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransom to the attacker. According to the IBM Security X-Force Threat Intelligence Index 2023, ransomware attacks represented 17 percent of all cyberattacks in 2022.

6.What is DoS Attack?

Denial of service" or "DoS" describes the ultimate goal of a class of cyber attacks designed to render a service inaccessible. The DoS attacks that most people have heard about are those launched against high profile websites, since these are frequently reported by the media.

7.What is DDos Attack?

DDoS stands for Distributed Denial of Service, and it's a method where cybercriminals flood a network with so much malicious traffic that it cannot operate or communicate as it normally would. This causes the site's normal traffic, also known as legitimate packets, to come to a halt.